

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

Title of Invention	SECURE WIEGAND COMMUNICATIONS
<p>As the below named inventor(s), I/we declare that:</p> <p>This declaration is directed to:</p> <p><input type="checkbox"/> The attached application, or</p> <p><input checked="" type="checkbox"/> Application No. <u>12/539,431</u> filed on <u>August 11, 2009</u></p> <p><input type="checkbox"/> As amended on _____ (if applicable);</p> <p>I/we believe that I/we am/are the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought;</p> <p>I/we have reviewed and understand the contents of the above-identified application, including the claims, as amended by any amendment specifically referred to above;</p> <p>I/we acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me/us to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.</p> <p style="text-align: center;">WARNING:</p> <p>Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.</p> <p>All statements made herein of my/our own knowledge are true, all statements made herein on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and may jeopardize the validity of the application or any patent issuing thereon.</p> <p>FULL NAME OF INVENTOR(S)</p> <p>Inventor one: <u>Scott B. Guthery</u> Date: <u>8/14/2009</u></p> <p>Signature: <u>[Signature]</u> Citizen of: <u>U.S.</u></p> <p>Inventor two: <u>Mark Robinton</u> Date: _____</p> <p>Signature: _____ Citizen of: <u>U.S.</u></p> <p><input checked="" type="checkbox"/> Additional inventors or a legal representative are being named on <u>1</u> additional form(s) attached hereto.</p>	

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of
Invention **SECURE WIEGAND COMMUNICATIONS**

As the below named inventor(s), I/we declare that:

This declaration is directed to:

- ☐ The attached application, or
☒ Application No. 12/539,431 filed on August 11, 2009
☐ As amended on _____ (if applicable);

I/we believe that I/we am/are the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought;

I/we have reviewed and understand the contents of the above-identified application, including the claims, as amended by any amendment specifically referred to above;

I/we acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me/us to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

All statements made herein of my/our own knowledge are true, all statements made herein on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF INVENTOR(S)

Inventor one: Scott B. Guthery Date: _____

Signature: _____ Citizen of: U.S.

Inventor two: Mark Robinton Date: 9/23/09

Signature: [Signature] Citizen of: U.S.

☒ Additional inventors or a legal representative are being named on 1 additional form(s) attached hereto.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention **SECURE WIEGAND COMMUNICATIONS**

As the below named inventor(s), I/we declare that:

This declaration is directed to:

- ☐ The attached application, or
☒ Application No. 12/539,431 filed on August 11, 2009
☐ As amended on _____ (if applicable);

I/we believe that I/we am/are the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought;

I/we have reviewed and understand the contents of the above-identified application, including the claims, as amended by any amendment specifically referred to above;

I/we acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me/us to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

All statements made herein of my/our own knowledge are true, all statements made herein on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF INVENTOR(S)

Inventor one: Michael Davis Date: 8/17/2009
 Signature: Michael Davis Citizen of: U.S.

Inventor two: David Andresky Date: _____
 Signature: _____ Citizen of: U.S.

☐ Additional inventors or a legal representative are being named on _____ additional form(s) attached hereto.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)****Title of
Invention****SECURE WIEGAND COMMUNICATIONS**

As the below named inventor(s), I/we declare that:

This declaration is directed to:

☐

The attached application, or

☒Application No. 12/539,431 filed on August 11, 2009☐

As amended on _____ (if applicable);

I/we believe that I/we am/are the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought;

I/we have reviewed and understand the contents of the above-identified application, including the claims, as amended by any amendment specifically referred to above;

I/we acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me/us to be material to patentability as defined in 37 CFR 1.58, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

All statements made herein of my/our own knowledge are true, all statements made herein on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF INVENTOR(S)Inventor one: Michael Davis

Date: _____

Signature: _____

Citizen of: U.S.Inventor two: David AndreskyDate: 8/18/09Signature: [Signature]Citizen of: U.S.☐

Additional inventors or a legal representative are being named on _____ additional form(s) attached hereto.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		SECURE WIEGAND COMMUNICATIONS		
First Named Inventor/Applicant Name:		Tam Hulusi		
Filer:		Matthew Ryan Ellsworth/Leslie Roberts		
Attorney Docket Number:		2943AAAB-178-DIV		
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Utility application filing	1011	1	390	390
Utility Search Fee	1111	1	620	620
Utility Examination Fee	1311	1	250	250
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1260

Electronic Acknowledgement Receipt	
EFS ID:	14342648
Application Number:	13689088
International Application Number:	
Confirmation Number:	9927
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Tam Hulusi
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Leslie Roberts
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943AAAB-178-DIV
Receipt Date:	29-NOV-2012
Filing Date:	
Time Stamp:	16:27:09
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 1260
RAM confirmation Number	3751
Deposit Account	191970
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		PATENT_APPLICATION.pdf	255811 <div>6e2dd520c9ebc8a701c56d213ace74f7968f1bc0</div>	yes	51
	Multipart Description/PDF files in .zip description				
	Document Description		Start		End
	Specification		1		46
	Claims		47		50
	Abstract		51		51
Warnings:					
Information:					
2	Drawings-only black and white line drawings	FIGS.pdf	86037 <div>4a6ebfa107621e1412a29aa2cb1cd31f0a61f9d9</div>	no	5
Warnings:					
Information:					
3	Application Data Sheet	ADS.pdf	1067512 <div>99e4d6804c11403c0fd337fbc9c3a70a2e1fee9</div>	no	6
Warnings:					
Information:					
4	Oath or Declaration filed	DECLARATION.pdf	588297 <div>06dfc10a4b9cd89ee5416574ed1b604d4aee89e3e</div>	no	4
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	33465 <div>144c11ae83cb494b2933d566034fa82e397a7ee2</div>	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			2031122		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Acknowledgement Receipt	
EFS ID:	14342648
Application Number:	13689088
International Application Number:	
Confirmation Number:	9927
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Tam Hulusi
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Leslie Roberts
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943AAAB-178-DIV
Receipt Date:	29-NOV-2012
Filing Date:	
Time Stamp:	16:27:09
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 1260
RAM confirmation Number	3751
Deposit Account	191970
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		PATENT_APPLICATION.pdf	255811	yes	51
			6e2dd520c9ebc8a701c56d213ace74f7968f1bc0		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	46	
	Claims		47	50	
	Abstract		51	51	
Warnings:					
Information:					
2	Drawings-only black and white line drawings	FIGS.pdf	86037	no	5
			4a6ebfa107621e1412a29aa2cb1cd31f0a61f9d9		
Warnings:					
Information:					
3	Application Data Sheet	ADS.pdf	1067512	no	6
			99e4d6804c11403c0fd337fbc9c3a70a2e1fee9		
Warnings:					
Information:					
4	Oath or Declaration filed	DECLARATION.pdf	588297	no	4
			06dfc110a4b9c89ee5416574ed1b604d4aee89e3e		
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	33465	no	2
			144c11ae83cb494b2933d566034fa82e397a7ee2		
Warnings:					
Information:					
Total Files Size (in bytes):			2031122		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

SECURE WIEGAND COMMUNICATIONS

CROSS REFERENCE TO RELATED APPLICATIONS

This application is a divisional of U.S. Patent Application Serial No. 12/539,431, filed August 11, 2009, which claims the benefit of U.S. Provisional Application Number 61/087,941, filed August 11, 2008, the entire disclosures of which are hereby incorporated herein by reference.

FIELD OF THE INVENTION

The present invention is generally directed to authentication of a reader and the security, privacy and efficiency of messaging in a secure access control system. More specifically, the present invention provides extensions to unidirectional security protocols, such as the Wiegand protocol.

BACKGROUND

The Wiegand protocol is the predominant method by which physical access control card readers communicate with upstream devices such as local controllers, access control panels and host computer systems. Because of the popularity and almost universal support of the Wiegand protocol in access control panels, other devices besides access control readers are also available that support the Wiegand protocol. Such devices include biometric-based devices such as fingerprint, hand-geometry, iris, facial recognition, and vein scan. Other devices that utilize the Wiegand protocol include motion sensors, thermostats and smoke detectors.

Both the electrical and logical aspects of the Wiegand communication protocol are codified in the Security Industry Association (SIA) standard AC-01 entitled “Access Control Standard Protocol for the 26-Bit Wiegand Reader Interface”, the entire contents of which are incorporated herein by this reference in their entirety and will henceforth be referred to as the “SIA standard”.

Subsequent to the issuing of this standard, both the electrical and logical portions of the standard have been used to transmit bit stream messages, often called formats, longer than 26 bits. 35- and 37-bit formats are found widely and the US Government’s PIV standard defines some formats of up to 300 bits. The evolution of upstream devices and middleware to use these longer formats has been slow and is still taking place.

Although other methods are utilized for carrying the informational aspects of the Wiegand protocol over communication bearers such as RS-485, F/2F, and various Internet protocols such as TCP/IP and UDP, none has achieved the widespread usage that Wiegand has in the security and access control market segments. This is primarily because each manufacturer utilizes their own proprietary protocols even when using standardized communication bearers such as TCP/IP.

The widespread adoption of the Wiegand protocol is due to several advantages with the primary advantages of the Wiegand protocol being that its implementation in devices is very economical and that it allows very long cable runs which, depending on the gauge of the wire used, can be as long as 500 feet.

The electrical aspect of the Wiegand protocol uses five wires. Two of these wires are used to provide power to the reader. The remaining three wires are used for data communication and signaling and use the open collector electrical standard, which means

that the circuit acts as either an infinite resistance or a short circuit to ground. Typically the upstream device employs a pull-up resistor, which keeps the signal at a high voltage (+5) when it is in the open circuit state. When the signal is asserted, the output is forced to 0 volts. Note that the open state (+5 volts) represents a data value of zero and the asserted state (0 volts) represents the data value of one. This is generally referred to as an “active low” configuration where the active state is the low voltage.

Two of the three data communication and signaling wires are used by the reader to transmit data to an upstream device *e.g.*, control panel, intermediate device, routing device, lock control mechanism, computing platform, host, or the like. These two wires are referred to as DATA0 and DATA1. As the names suggest, the DATA0 signal transmits the "0" bits of the data stream to the upstream device, and the DATA1 signal transmits the "1" bits. Fig. 1 graphically illustrates the representation of a Wiegand data stream for the binary data of “01101”. Each dip in the line represents a change from 5V to 0V, thus communicating a single bit of data of the entire message.

The third data communication and signaling wire is used by the upstream device to signal the reader. This wire is called LEDCTL because it is often used by the upstream device to control a light-emitting diode (LED) in the reader and provides feedback to the card holder.

SUMMARY

The SIA standard defines the timing of the signals on the DATA0 and DATA1 lines as shown in Fig. 2 and Table 1 shown below:

<u>SYMBOL</u>	<u>DESCRIPTION</u>	<u>MIN</u>	<u>MAX</u>
---------------	--------------------	------------	------------

TPW	Pulse Width Time	20 μ s	100 μ s
TPI	Pulse Interval Time	200 μ s	20 mS

Table 1: Timing Characteristics of DATA0 and DATA1

The typical timing uses a pulse width of 50 μ s and a 1 ms gap between pulses. The pulse timing between gaps determines the data rate and, as longer bit streams are used, may be reduced from the 1 ms gap typically used. An effective baud rate table calculated using various values for TPW (pulse width time) and TPI (pulse interval time) is depicted in Table 1A shown below:

<u>TPI</u>	<u>TPW</u>	<u>BAUD</u>
200 μ s	50 μ s	4000.00
250 μ s	50 μ s	3333.33
1 ms	50 μ s	952.38
2 ms	50 μ s	487.80
5 ms	50 μ s	198.02
10 ms	50 μ s	99.50
20 ms	50 μ s	49.88

Table 1A: Effective Baud Rate

The baud rates depicted in Table 1A represent a TPI from 200 μ s to 20 ms, which is the range of allowable TPI values defined by the SIA standard. All of the baud rates in Table 1A were calculated using a TPW value of 50 μ s. However, as noted above, the TPW value may range between 20 μ s and 100 μ s.

Since TPW and TPI are specified as a range by the SIA standard, this fact can be exploited to provide a secondary covert communication channel over the existing communication and signaling wires. If the spacing of TPI and/or width of length TPW, for example, were to vary, this variance could be tracked by the host. As an example,

using a TPI of 1 ms to represent a binary zero bit and a TPI of 2 ms to represent a binary one bit, the reader could send at least as many bits of data as there are in the primary communications path by varying TPI between 1 and 2 ms. This data could simply be additional format data or, as described below, this data could be security and authentication data, or the presence of this data can be used by the upstream device to realize that is communicating with a reader capable of supporting all of the improvement described herein. Because these secondary signals conform to the SIA standard, utilizing this method would always be backwards compatible with existing legacy systems. Another use for this secondary communications channel would be to inform the host device that the reader supports the security improvement inventions contained herein. Any host capable of detecting this could use any of the Wiegand control signals as an acknowledgement

The SIA standard defines signal levels on the LEDCTL line but does not set forth any method of encoding data on this line as it does for the DATA0 and DATA1 lines. Thus, implementers of the SIA standard are free to use the LEDCTL line for arbitrary communication between the upstream devices and middleware and the reader. Moreover, the SIA standard does not preclude manufacturers from including additional features on either readers or upstream devices (*i.e.*, panels). The SIA standard defines the minimum set of features a reader or panel must provide to be in compliance. Manufacturers may have additional features so long as they do not conflict with the SIA standard.

Access control panels may connect to as many as eight readers. The hardware cost trade-offs intrinsic to the panel-to-reader ratio has caused most panel manufacturers to support just two readers in a single panel.

It is important to point out that, if a reader is controlling an exterior door to a premise and consequently mounted on the outside of the premises, the wiring from the reader to the upstream device may be accessed by unauthorized persons.

As popular as the Wiegand interface has become, it has shortcomings. One such shortcoming arises due to the use of open collector signaling makes it very easy to connect a “listening” device to the communication and signaling wires to monitor communications between a card reader and an upstream device and thereby harvest data streams that can be used to compromise the system. Once a rogue device has been connected to monitor communications between the reader and an upstream device, an attacker can note when the door has been unlocked and record the most recent data stream as one that will open the door. Then, whenever illicit entry is desired, the attacker can replay the recorded data stream causing the door to unlock. The attacker need not remove the rogue device from the communication wires to gain unauthorized entry because of the Wiegand communications open collector data interface allows both the monitoring of messages and generation of messages from the same connection.

Furthermore, an attacker can harvest more than one valid message to gain unauthorized entry using different cardholder data so that no suspicions are aroused. Unauthorized access to the Wiegand communications wires is aided by the fact that at least one reader is typically deployed on the unsecured side of a wall or door and, because of the nature of access control, may be at a location that is not under continuous observation or scrutiny. Making matters worse, many access control readers do not include any tamper detection mechanisms so that the removal of a reader to access the internal wiring or even to replace the reader with another compromised reader or illicit

device is undetectable. Even when tamper detection mechanisms are included in a reader, they are often not activatedutilized because the installer of the reader does not want to incur the additional costs associated with installing additional wiring from the tamper detection mechanism back to the upstream device

Certain weaknesses of the existing Wiegand protocol have been publicly exploited by hackers, such as Zac Franken. Mr. Franken has developed a device (known as the Gecko) that is capable of capturing and storing communications transmitted by a reader, , and transmitting the stored communication at a later time thereby allowing unauthorized access to assets secured by the reader. This type of attack is known as a man-in-the-middle store-and-forward attack. Details of this attack will be described in further detail below along with ways that embodiments of the present invention ameliorate and/or eliminate susceptibility to such attacks.

There have been some attempts to address the shortcomings of the Wiegand protocol. One example of an extension to the Wiegand protocol is described in U.S. Patent No. 6,988,203 to Davis et al., the contents of which are hereby incorporated herein by this reference. The '203 patent describes appending additional bits to the Wiegand format. These additional bits can provide supplementary information from the reader to the upstream device as well as error detection and/or correction bits for the transmitted data. The '203 patent further describes transmitting data back to the reader from the upstream device via an LED control line.

Additionally, in PCT Application No. WO 2005/038729 to Merkert, which is herein incorporated by this reference, an access control system that includes a signal generator located between a reader and a control panel is described. The reader utilizes a

dynamic timing element that ensures a replay attack cannot be used to gain unauthorized access to an asset. The reader stamps any signal sent therefrom with a time stamp indicating when the message was generated. Then the control panel reads the time stamp to ensure that the message is current and not the replaying of a previously recorded message. An attempt to harvest a signal and resubmit that signal again at a later time will result in the control panel determining the signal is invalid. To ensure channel security between system elements, encryption and/or digital signatures are used. Unfortunately, this solution requires additional hardware to support implementation thereby increasing the overall cost of the system.

In the current art and in US 2007/0046424, the entire contents of which are incorporated herein by this reference, encryption techniques are posited to obscure the data sent from the card reader to the access control panel. Each such encryption technique assumes a managed key infrastructure for its operation and proper functioning.

There are a number of disadvantages in using keyed encryption techniques to protect the data in transmission from the reader to the panel. First, creating, administering and managing a key infrastructure can be complex and costly. The additional implementation and administration costs of a key management system to accompany the physical access control system can be a disincentive for purchasing a physical access control system that uses keyed encryption techniques.

Second, the physical access control systems, of which the reader and the panel are a part of, are typically installed and managed by personnel that are not familiar with handling and protection of cryptographic keys. Thus, there is a high likelihood that the encryption keys used to protect the data in transmission would be compromised without

this compromise being detected. As a result, the data protection feature of using encryption in reader-to-panel communication may be rendered ineffective and yet the overhead performance and administration costs of the feature would endure.

Third, the amount of executable computer code needed to implement encryption techniques is not insignificant.. Additional memory has to be added to each reader to contain this executable code thereby increasing the cost of the reader.

Fourth, execution of the encryption computer code will take additional processing time and thereby lengthen the response time of the reader and consequently reduce the rate at which, for example, people can pass through the door protected by the reader. Furthermore, the additional processing may require the use of a more capable microprocessor in the reader thereby further increasing the costs of each reader and the overall physical access control system.

Some security issues associated with the Wiegand protocol have been addressed in U.S. Patent Application No. 11/464,912 to Davis et al., the entire contents of which are incorporated herein by this reference. For example, the '912 application helps upstream devices determine whether Wiegand data is being received from a valid device or is simply a replay attack. This security feature is accomplished through the use of rolling codes to obfuscate the Wiegand data. The implementation of the technique mixes some bits known only to the reader and the panel (*i.e.*, the rolling codes) into the existing format data.

In a first aspect of the present invention, the particular rolling code that is mixed into the format data serves to identify the reader sending the data and to time-stamp the transmission. This first aspect is henceforth referred to as *stamping*.

In a second aspect of the present invention, the manner in which the rolling code is mixed into the format data serves to obfuscate the true values of the data contained in the message and thus hide these values from prying eyes. This second aspect is henceforth referred to as *blinding*. In accordance with at least one embodiment of the present invention, the rolling code is exclusive OR'd (XOR'd) with the format data to obfuscate the format data sent in the message. This obfuscation requires significantly less processing power and processing time than traditional encryption techniques such as DES or AES

In accordance with at least some embodiments of the present invention, by using the rolling codes both for authentication (stamping) and privacy (blinding), a marked improvement may be obtained in a number of security aspects of the overall system with the addition of very little added system complexity or administration cost.

In accordance with at least one embodiment of the present invention, a security method and system are provided where the rolling code used to authenticate the reader is also used to shroud, obscure and otherwise obfuscate data sent from the reader to the upstream device. This inventive method offers a number of improvements over using keyed encryption techniques to protect the data. First, dual-purposing the rolling code avoids the cost of implementing an independent key infrastructure to secure the data. This helps reduce the overall cost of the system while increasing the security associated therewith.

Second, as the rolling code changes with every transmission, discovering the rolling code for a particular transmission will not enable the discovery of any other transmissions, either before or after the broken transmission, since the codes will be

different for each transmission.

Thirdly, data blinding and obfuscation techniques require fewer computer instructions to implement and execute faster than keyed encryption techniques. While data blinding and obfuscation techniques may, in some cases, provide a lower level of data security than keyed cryptography techniques, they are certainly an improvement over no data protection at all and, in many instances, may be deemed appropriate relative to the value of the underlying data or facility being protected.

In accordance with still further embodiments of the present invention, two devices may be enabled to use a synchronized pseudo-random number generator (PRNG) to secure the communication between them, for example. Synchronization of the PRNG between the two devices is lost, for example, when one device suffers a power cycle (*i.e.*, loss of power). In accordance with at least some embodiments of the present invention, the two devices can regain synchronization of the pseudo-random number sequence without opening the possibility of a replay attack on the pseudo-random number sequence. This may be accomplished by having the two devices share one or more different PRNGs. The PRNG used to secure the communication between them is used every time they communicate and may therefore be called the primary communication or “fast” PRNG. Another PRNG may only be used when the devices need to resynchronize the fast PRNG. This second PRNG may be called the secondary synchronization or “slow” PRNG. By implementing a fast and slow PRNG, the two devices that are connected to one another, for example through Wiegand wires, may be adapted to automatically synchronize and re-synchronize with each other dynamically and without user intervention.

Table 2 lists the features and benefits of the stamping aspect of embodiments of the present invention:

<u>FEATURE</u>	<u>BENEFIT</u>
Each message includes a time-based unique identifier by virtue of the fact that rolling codes are sequential	Access events can be reliably associated with time for accounting and forensic purposes without a secure logging facility. The system is protected against replay of previous messages
Each reader or group of readers can use a different sequence of unique identifiers	The unique identifier serves to authenticate the reader or reader group that sent the message

Table 2: Features and Benefits of Wiegand Stamping

Table 3 lists the features and benefits of the blinding aspect of embodiments of the present invention:

<u>FEATURE</u>	<u>BENEFIT</u>
Personal identification data (PID) in the message is obfuscated	The privacy of the system is improved since no PID is revealed
The blinding can carry additional information	More information can be carried from the reader to the upstream device without altering the current message size or the current message format. Authentication information is added via use of the rolling code (<i>e.g.</i> , which is XOR'd with the card data).

Table 3: Features and Benefits of Wiegand Blinding

Table 4 lists how embodiments of the present invention addresses a number of attacks on physical access control systems using the Wiegand protocol.

<u>THREAT</u>	<u>PROTECTION</u>
Rogue Reader: A rogue or non-certified reader could be substituted for the original reader.	Embodiments of the present invention are operable to detect rogue readers due to the authentication mechanisms provided by the

<p>Man-in-the-Middle (MIM) Attack: The broadcast of an exact copy of a message between a reader and an upstream device that was previously captured.</p> <ol style="list-style-type: none"> 1. A person presents their card and an unauthorized MIM device inserted between the reader and the upstream device captures this message and subsequently passes it along unmodified. 2. If the host asserts the LEDCTL signal indicating that the cardholder will be granted access, then the MIM device keeps a copy of the message otherwise it is discarded. 3. Whenever illicit entry is desired, the MIM device simply replays the saved message. 	<p>rolling code.</p> <p>Embodiments of the present invention prevent MIM attacks due to the authentication mechanism provided by the rolling code; a replay attack would contain an earlier sequenced rolling code.</p>
<p>MIM Store and Forward Attack: The broadcast of an exact copy of a Wiegand message between a reader and an upstream device that was previously captured. This type of attack is more sophisticated than the previous MIM attack scenario because it uses social engineering in an attempt to defeat the rolling code protection.</p> <ol style="list-style-type: none"> 1. A person presents their card and an unauthorized MIM device inserted between the reader and the upstream device captures this message and blocks its transmission to the upstream device 2. The user presents their card again since the door was not unlocked the first time it was presented. 3. The MIM device releases 	<p>The MIM Store and Forward attack is prevented by the periodic assertion of the LEDCTL signal which requests the next rolling code from the reader causing the retained message to be out of sequence when it is used.</p>

<p>the first Wiegand message which results in the door being unlocked yet the MIM device still retains the second message which is in proper rolling code sequence to unlock the door at a later time for a perpetrator.</p> <p>4. Whenever illicit entry is desired, the MIM device simply replays the saved message.</p>	
<p>MIM Data Substitution Attack: Another form of the man-in-the-middle attack in which the Wiegand message is altered as it transmitted from the reader to the upstream device; alteration could be, for example, altering the card number data.</p>	<p>Embodiments of the present invention mitigate this risk due to its obfuscation of the card number by blinding, making it extremely difficult to alter data without destroying the integrity of the rolling code.</p>
<p>MIM Spoof Attack: A specialized form of the man-in-the-middle attack in which the Wiegand messages from one reader are copied and replayed at another reader.</p>	<p>Embodiments of the present invention are essentially immune to this type of attacks because the rolling code will not be in sync with another reader.</p>
<p>Passive eavesdropping / Privacy leakage: Attack in which the Wiegand messages between a reader and an upstream device can be surreptitiously observed by a third-party.</p>	<p>If the Wiegand wires are cut during attachment of any in-line device, this may be detected depending upon the frequency of the periodic assertion of the LEDCTL signal. However, if a device is merely “attached” to the Wiegand data lines to passively monitor the data, attachment of the device will not be detected but the data itself will remain private due to its obfuscation by blinding with the rolling code.</p>
<p>Tracking: The capture of a Wiegand message between a reader and an upstream device and optionally extracting the card number, its association with a person, and the subsequent correlation of the person’s whereabouts using Wiegand messages obtained from other readers.</p>	<p>Embodiments of the present invention mitigate this risk due to its obfuscation of the card number by blinding since the message is essentially different even if the same person presents the same card at the same reader.</p>

<p>Targeting: The ability to perform an action based on identifying an individual from the card number obtained from the passive eavesdropping of the Wiegand messages sent from the card reader to the upstream device.</p>	<p>Embodiments of the present invention mitigate this risk due to its obfuscation of the card number by blinding since the message is essentially different even if the same person presents the same card at the same reader.</p>
<p>Denial of Service (DOS): An attack in which the reader is made unavailable. As it relates to the Wiegand protocol, DOS may be accomplished by cutting power to the reader, cutting or shorting the DATA0 and DATA1 signals, or connecting a rogue device that continuously sends Wiegand data to jam the channel possibly causing the host to become inoperable because it may be continuously responding to bogus Wiegand data.</p>	<p>Unlike the current Wiegand Protocol, the host is able to detect when the reader becomes non-responsive due to a denial of service attack in which the reader power is interrupted or the integrity of the data lines are compromised because the reader will no longer respond to the periodic assertion of the LEDCTL signal. Jamming can be detected and reported by judicious firmware in the upstream device or by converting back to a legacy Wiegand operational mode. In accordance with at least some embodiments of the present invention, all of the features of the secure Wiegand can be implemented in an intermediate device located between the reader and control panel. Thus, the intermediate device can filter against DOS attacks directed toward the host, control panel, or similar upstream devices.</p>
<p>Buffer Overflow Attack: Attack in which an unexpectedly long Wiegand message causes data to be stored beyond the boundaries of a fixed-length buffer resulting in unexpected and undesirable behavior by the upstream device.</p>	<p>Working with panel manufacturers can help ensure that firmware is not susceptible to this type of attack and tests for susceptibility to buffer overrun attacks could be included in any validation tools provided to test for compliance with the embodiments of the inventions contained herein. Also, updated firmware designed to detect and react to these kinds of attacks may be included in an intermediate device between the legacy reader and upstream device. Thus, the intermediate device can filter against buffer overrun attacks directed toward the host, control panel, or similar upstream devices.</p>

Table 4: Resistance to common threats

In accordance with at least one embodiment of the present invention, systems and methods are provided that allow existing physical access control systems using Wiegand wires for communication between readers and upstream system components such as control panels to be modified to also support data communication from the upstream components back to the readers. This may be affected by making modifications solely to the software and firmware contained in the readers and upstream devices and thus without making any changes to existing hardware. As an immediate consequence of the application of these inventive means, methods and systems, two-way, communication may be realized between card readers and upstream devices.

More specifically, in the current art, Wiegand wires are used to carry format and reader status data read from an access control credential such as a Prox or iCLASS® card by a card reader to an upstream component of an access control system which is often an access control panel. The upstream device analyzes this data and may perform operations based on this analysis such as unlocking a door located near the reader that sent the data. As described in the SIA standard and as implemented by the physical access control industry, Wiegand wires provide only a one-way channel for the communication of digital data, namely from the card reader to the upstream device.

A number of advanced features of physical access control systems can be realized if communication in the other direction, namely from the upstream device to the card reader, can be achieved. The realization of these advanced features would be particularly attractive if the communication from the upstream device to the card reader could be achieved in the following manner:

1. without modifying or changing in any way the hardware of existing components of the system including readers and upstream devices;

2. using the physical and electrical properties of any existing Wiegand wires and still operating within the electrical characteristics of the industry standard Wiegand protocol;
3. continuing compliance with the SIA standard; and
4. maintaining complete backward compatibility with all existing system functionality.

At least some embodiments of the present invention help to achieve these desirable advantages. Elements of this particular aspect include electrical and logical digital encoding techniques that enable the transmission of digital data to card readers in access control systems from upstream devices such as control panels. This is accomplished by utilizing one or more of the Wiegand wires currently defined to carry only a high-low indicator signal with pre-defined semantics to carry packets of digital data.

The existing methods of communication on Wiegand wires as described by the SIA standard only provide for the transmission of a single high- low indicator to be sent from an upstream device to the reader, in particular on the LEDCTL wire. The meaning of this high- low signal as described by the SIA standard is the on/off control of a cardholder feedback indicator such as an LED and does not include the encoding of digital data.

Consequently, there are a number of advanced features of physical access control systems that are not implemented in systems using Wiegand wires because of the lack of a digital communication path from the upstream device to the card reader other than the high-low LEDCTL signal. For example, it is impossible for the upstream device to send the reader messages to reconfigure the reader's operating characteristics. Nor is it possible for the upstream device to reconfigure the security properties of the

communication from the reader to the upstream device. And finally, without true bi-directional data communication, there is no way that a reader can receive new configuration data, keys, or firmware without human intervention such as, for example, presenting a special configuration card to the reader or removing the reader from the wall to connect to a serial communication port reserved for this purpose.

In the current art, as defined by the SIA standard, a reader need only sense a high-low level signal on the LEDCTL wire and the response of the reader to changes in this signal is defined by the SIA standard. According to the SIA standard, for readers with a single color LED, when a high signal is sensed on the LEDCTL, the reader's LED is turned off. For readers with bi-color (or tri-color) LEDs, when a high signal is sensed on the LEDCTL, the reader's LED is illuminated in red or some other color, for example. Similarly, according to this standard, when a low level is present on the LEDCTL signal, the LED in a reader with a bi-color LED will be illuminated in green and is illuminated in red for readers with a single red color LED. Although it is not defined in the standard, some manufacturers will treat oscillation of the LEDCTL signal as an indication to illuminate the reader's LED in a third color (usually yellow in readers with a tri-color LED or perceived as yellow in readers with a bi-color LED by quickly alternating the flashing of the red and green LEDs). In accordance with at least some embodiments of the present invention, additional meaning is given to both the levels and transitions of the LEDCTL signal. By programming these additional meanings into the software of the reader, packets of digital data can be sent from the upstream components including control panels back to the reader.

Additionally, the frequency with which these control signals are transmitted from

the upstream device to the reader can be altered in such a way as to communicate data from the upstream device to the reader. More specifically, PSK, and FSK may be utilized for transmitting data or other types of signals and data from the upstream device to the reader. A transition in signal frequency, duty cycle, or phase, for example, may provide a certain meaning to the signal that can be interpreted by the reader. Alternatively, predetermined frequencies or amplitudes may correspond to different signals and based on the frequency, for instance, of the signal transmitted from the upstream device to the reader the reader may react differently.

If hardware modifications of the host are permitted, then amplitude and voltage levels could also be utilized on the Wiegand control signals by the upstream devices to communicate back to the reader while still using existing wiring. If the voltage levels stayed within the standards, then this method of communications would still be within the defined standards and, if compliance with the strict letter of the standards is not desired or required, then amplitudes and voltage levels outside of the standards may be utilized. Additionally, a reader and an upstream device can even operate according to the SIA standard when legacy backwards compatibility is desired but operate outside the defined electrical characteristics of the standard when these improvements are desired.

The data transmission of packets of data from an upstream device back to a reader via the Wiegand LEDCTL line or any of the other Wiegand control signal is described in the following in three aspects.

1. mode change protocol
2. data encoding
3. packet structure

For each aspect, there are one or more mechanisms by which the aspect can be realized in practice.

In the SIA standard, there is no defined method for upstream devices to communicate digital data to a reader, in order to, for example, change the operating characteristics of said reader. Currently it is required that a person visit the card reader and perform various maintenance procedures (*e.g.*, update software/firmware in the reader, change operating characteristics, change keys, etc.) in the presence of and with physical access to the card reader. In the present state of the art, these maintenance procedures may include entering updated data into the reader using the radio frequency (RF) communication capabilities of the reader together via a special credential, NFC-based device, or via a communications port using infrared communications. Additional less-convenient methods may be employed such as wired communications which may require removal of the reader from the wall to connect the configuring device to the reader. These maintenance procedures may also require opening the reader enclosure or removing power from the reader and then restoring power to the reader.

As it is costly to send a technician to visit every reader in a system, this method of updating readers is avoided if at all possible. One of the primary advantages of this invention is that these operations can be performed -- and performed securely -- over the Wiegand wires thus avoiding a trip to the reader. Because the cost of performing a maintenance procedure at the card reader goes from very expensive to virtually nothing, the possibility of more frequent changes to the reader configuration and operating parameters becomes possible through the two-way packet mode communication provided by embodiments of the present invention. Moreover, remote updating of readers can be

performed from anywhere in the world if there is Internet connectivity at the upstream device associated with the reader.

Another advantage offered by embodiments of the present invention is that the transmission of sensitive cardholder authentication information from the reader to the upstream devices, such as the 26-bit Wiegand format data discussed in the SIA standard, can be secured using proprietary as well as conventional and standardized security protocols that require two-way communications between the sender and the receiver. Bi-directional communications enables the ability to utilize mutual authentication, a well established mechanism commonly used to authenticate communication devices.

The present invention is generally directed toward a method, apparatus, and system that provide the additional security features described above to unidirectional security protocols. Although well suited for use in a physical access control system utilizing the Wiegand protocol, embodiments of the present invention may be suitable for use in any system utilizing a unidirectional protocol.

These and other advantages will be apparent from the disclosure of the invention(s) contained herein. The above-described embodiments and configurations are neither complete nor exhaustive. As will be appreciated, other embodiments of the invention are possible using, alone or in combination, one or more of the features set forth above or described in detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a waveform diagram for transmitting binary data over Wiegand wires in accordance with embodiments of the present invention;

Fig. 2 is a waveform diagram for timing characteristics of Wiegand data transmitted in accordance with embodiments of the present invention and as described in the SIA Standard;

Fig. 3 is a block diagram depicting a communication system in accordance with embodiments of the present invention;

Fig. 4 is a block diagram depicting a half-duplex configuration of a reader and host in accordance with at least some embodiments of the present invention;

Fig. 5 is a block diagram depicting a full-duplex configuration of a reader and host in accordance with at least some embodiments of the present invention; and

Fig. 6 is a block diagram depicting one or more data structures used in accordance with at least some embodiments of the present invention.

DETAILED DESCRIPTION

The present invention is generally directed toward a communication method, device, and system. Embodiments of the present invention address deficiencies of the prior art and may be utilized within the context of physical access control or security systems, as well as be equally efficiently utilized in a broad range of other applications that use a unidirectional communications protocol.

One compelling aspect of the present invention is that it yields so many benefits without dramatically altering the Wiegand protocol. Not only are existing deployed hardware and wiring unchanged but the size and therefore the transmission properties of the message are not significantly changed.

Obscuring Wiegand Data

There are in the art many rolling code generators. Rolling code generators are also known as pseudo-random number generators (PRNG). A rolling code generator is a function, algorithm or procedure that creates the next elements in a sequence of numbers given one or more of the previous elements together with some ancillary information such as the indices in the sequence of the elements being used.

For example, the rolling code algorithm

$$x_{i+1} = (1 + x_i + 2(g(x_i+1)-g(x_i) \bmod 2^n))$$

where

$$g(x) = x \oplus 2x+1$$

shows how to generate the next element, x_{i+1} , in a sequence given the current element, x_i . (\oplus is the logical XOR or exclusive OR operation.) Such a procedure is given an initial value, x_0 , to initiate the generation.

For use in a preferred embodiment in the context of this disclosure, the rolling code generator should be what is known in the art as cryptographically strong. There are in the art alternative definitions of cryptographically strong but to a first approximation it means that: 1) many elements are generated before the sequence starts to repeat, 2) each possible number that the generator can generate appears as often as other numbers that the generator can generate, and 3) the minimum number of distinct values in contiguous subsequences is large.

All of these criteria and others describing cryptographically strong rolling code

generators can be given strict mathematical definitions and rolling code generators satisfying these definitions can be constructed.

Which particular cryptographically strong rolling code generator is used in a particular embodiment of the invention depends on the security context in which the embodiment is to be used and on the resources available for the embodiment's implementation.

In accordance with at least some embodiments of the present invention, the rolling code generator may provide a sequence of numbers. In one embodiment of the data obfuscation, each number may be represented in binary notation; i.e., to the base 2, with a fixed number of digits (i.e., length). If, for example, the fixed number of binary digits were 6, then the number 3 would be represented by 000011. Thus, the obfuscated message produced by the rolling code generator is the same length as the original message and it yields a fixed-length sequence of 0's and 1's.

The message from the reader to the upstream device may also be a fixed-length sequence of 0's and 1's, called a format. Said format comprises a number of data fields including the unique identification of the card presented to the reader, the location of the reader, a unique identification of the reader, etc.

The contribution of the data obfuscation portion to embodiments of the present invention is to combine the 0's and 1's produced by the rolling code generator with the 0's and 1's of the format to be sent from the reader to the upstream device in such a way that the upstream device, with knowledge of the rolling code, can recover the original, un-combined format data but an attacker only in possession of the combination of rolling code and format data cannot recover the original, uncombined format data.

There are in the art many ways of performing this combination. Many of these means are known in the art as stream ciphers. In one embodiment, the rolling code generator is configured to generate a string of 0's and 1's that was exactly as long as the format data and the two binary strings are combined using the logical exclusive OR operation (XOR).

As with rolling code generators, combination mechanisms can be used in a particular embodiment of the invention. The combination used may depend on the security context in which the embodiment is to be used and on the resources available for the embodiment's implementation.

Two-Way Packet-Mode Communication

Possible System Configurations

In accordance with at least some embodiments of the present invention, two-way communications between a reader and an upstream device may be facilitated utilizing existing Wiegand wires that currently connect the reader with the upstream device and have been previously used to facilitate unidirectional communications from the reader to the upstream device. One aspect of current Wiegand wires that can be exploited to facilitate two-way communications is the fact that Wiegand wires use open collector signals. This means that a reader or upstream device can either transmit messages on the Wiegand wire or receive messages being transmitted on the Wiegand wire even though the SIA standard only describes data transmission from the reader to the upstream device. As can be seen in Figs. 4 and 5, two types of system configurations can be utilized to facilitate bi-directional data communications using Wiegand wires, namely a half-duplex configuration (Fig. 4) and a full-duplex configuration (Fig. 5).

In the full-duplex system configuration, 4 wires may be used to connect the reader to the upstream device. Two of the wires may be utilized to carry data communications from the reader to the host as per the Wiegand standard. These wires correspond to the DATA0 and/or DATA1 lines, which carry DATA0 and/or DATA1 signals, respectively. In the simplest method, two of the Wiegand signaling wires can be utilized to carry data communications from the host to the reader in the same method that is defined in the Wiegand standard. These wires may correspond to the LEDCTL signal lines, a buzzer signal line, a hold/inhibit signal, or the like. In another embodiment, these wires may be used to conduct bi-directional communications using level-based communications or modulation-based communications (*e.g.*, asynchronous serial data, FSK, PSK, ASK, *etc.*). In the full-duplex configuration, both the reader and host may be enabled to simultaneously send messages to the other device without incurring message collision problems

In a half-duplex configuration, however, unless the reader and the upstream device use a mechanism preventing them from trying to communicate with each other at the same time, message collisions resulting in data alteration may occur since the communication lines (*e.g.*, DATA0 and DATA1) between the reader and host are shared and used to support bi-directional message traffic. By nature, Wiegand communications are relatively low volume traffic and collisions will be rare. However, since there is still a statistical probability that message collisions can occur, embodiments of the present invention provide a number of different ways to enable half-duplex communications while also accounting for possible message collisions.

In accordance with at least one embodiment of the present invention, both the

reader and upstream device may be enabled to send messages to the other device at any time. When a collision is detected (*e.g.*, because a corrupted or unrecognizable message has been received) then a predefined protocol may be followed whereby, for example, the reader re-transmits its message within 5 seconds of detecting the collision and then the host transmits its message between 5 and 10 seconds after detecting the collision. In an alternative re-transmission scenario, both the reader and upstream device wait a random amount of time and retry their transmission. Collisions may be detected by any type of known error checking and correcting algorithm. If the messages contain error correction data and the message can be reliably constructed without resorting to a retransmission, then the other sender will be able to retransmit, if necessary, without the possibility of a resultant second collision.

In a preferred embodiment, the reader and upstream device operate in predefined sending and listening modes and only change their sending/listening mode upon the occurrence of a predefined event. As one example, the reader may be in a default send mode and the upstream device may be in a default listen mode. Each device may maintain its respective default mode until a predetermined event occurs (*e.g.*, a card is presented to the reader, read by the reader, and/or card data is sent to the upstream device). When the event does occur, the devices may switch to the alternative mode such that the reader goes into a listen mode and the upstream device goes into a sending mode for a predetermined amount of time after the occurrence of the event. During this window of time, the upstream device may be free to send any necessary messages to the reader since the reader is in listen mode and is otherwise prohibited from sending messages. By having synchronized, alternating, and mutually exclusive operating modes,

collisions on the Wiegand wires are avoided.

Another type of predetermined event that may initiate a change in listening/sending modes of the upstream device and reader may be the transmission of a heart beat message from the reader to the upstream device via the LEDCTL signal or other method. As discussed herein, the heart beat message transmitted from the reader to the upstream device is essentially an empty Wiegand message (because it does not actually contain card data) that is utilized to allow the reader to check-in with the upstream device. Of course, in accordance with at least some embodiments of the present invention, the heart beat message may contain a rolling code to verify the identity of the reader to the upstream device. The heart beat messages are essentially used by the reader to prove to the upstream device that it is still alive and functioning as well as insuring that the communications wires are intact and that the reader has operating power. Each time a heart beat message is transmitted from the reader to the upstream device, the devices may alternate sending and listening roles for a predetermined amount of time after the occurrence of the event. However, if the periodicity with which heart beat messages are transmitted is relatively fast such that the upstream device wouldn't be able to send a message to the reader between heart beat messages, then the operating modes of the devices may only be switched after every other, every third, every fourth, *etc.* heart beat message. The parameters used to define when the devices switch listening and sending roles may vary depending upon other system characteristics and should not be limited to the examples discussed herein.

Although the half-duplex configuration depicted above shows the connection of the LED control signals to the DATA lines as being external to the host and reader, one

skilled in the art will appreciate that these connections may also be made internally within the host and/or reader. More specifically, internal connections between the LED modules in the host and/or reader may be made to the DATA0 and/or DATA1 modules in the host and/or reader.

Mode Change Protocol

In the teachings of the current disclosure, communications between the reader and upstream systems is modal. Embodiments of the present invention contemplate at least two modes of communication. One mode is the communication of the current art according to the SIA standard. The other mode is the advanced two-way packet-mode of communication described herein. In another embodiment, one mode is the standard Wiegand communication mode and the other mode is the secure Wiegand mode.

Modal communication necessitates a method of changing from one mode to the other and then optionally back to the original mode. In the teachings of the current disclosure, either the card reader or the upstream device can initiate mode change from Wiegand-format mode to packet-mode or from legacy Wiegand mode to secure Wiegand mode (*i.e.*, the secure use of rolling codes in accordance with the Wiegand mode).

Upstream Device-Initiated Mode Change

It is desirable for communications to occur using the inventions described herein. Since a mix of readers that both support and do not support the inventions described herein may be present, the upstream device can use the out-of-band communications channel in which the timing characteristics are changed to detect which readers support the inventions described herein. Any such reader can be directed by the upstream device

to switch to these improved methods using the following methods. Note that this is very desirable because it allows a manufacturer to sell a single reader that support *both* legacy communications and these new communications methods and the improved methods will *automatically* be turned on by upstream devices that also support these improved communication methods.

As described in the SIA standard, the LEDCTL signal can be in one of two states, high or low. Each state of the LEDCTL signal is associated with the state of the illumination of an LED on the card reader. This illumination is intended to provide information about the state of the physical access control system to a human being presenting a card to the reader. Thus the state of the LEDCTL signal as currently defined in the standard and used for purpose in the field must be constant long enough to be supraliminally acquired by a human observer. Supraliminal visual acquisition time in humans is determined by many factors such as the nature of the symbol and the age of the human but the psychophysical literature generally agrees that presentation times below 10ms may be subliminal or not perceived at all.

As the visual presentation controlled by LEDCTL is not intended to be subliminal, if the state of the LEDCTL is constant for less than 10ms a reader implementing the means and methods of the current disclosure on the LEDCTL Wiegand wire can safely conclude that this is the beginning of the protocol to switch to the packet-mode of communication on LEDCTL and not a signal to change the state of the illumination of the LED. Additionally, data may be sent to the reader in a secure fashion (i.e., through obfuscation with a rolling code) within the 10 ms window.

Conversely, if the reader does not implement the means and methods of the

current disclosure on the LEDCTL Wiegand wire, presentation of a voltage level on the LEDCTL line of less than 10ms by the upstream device will either be ignored by the reader or will cause the illumination of an LED to change beneath the threshold of conscious awareness of the cardholder and therefore will not alter the understanding of the cardholder in the state of the access control system.

Thus, by the means and methods of the current disclosure, the addition of readers or upstream devices to existing physical access control systems is completely backward compatible with existing system components. A reader implementing the teachings of this disclosure will behave exactly as a reader of the current art when used with an upstream device of the current art with respect to the signals on the LEDCTL wire. The upstream device of the current art will send LEDCTL signals, levels, and/or communication data with stable times of greater than 10ms and the reader implementing the teachings of this disclosure will interpret these to be commands for changes in the illumination of an LED. Conversely, an upstream device implementing the teachings of the current disclosure sending a level change on the LEDCTL wire of less than 10ms of duration indicating a request to transition to digital data transition mode will not receive a reply from a reader in the current art and therefore will henceforth treat the reader as a reader of the current art.

In order to support the means and methods of the current disclosure, the software in a reader will not change the state of the LED immediately upon receipt of a change in the LEDCTL voltage level. Rather, upon detection of change in LEDCTL, the reader software/firmware will sample the LEDCTL line approximately 10ms later. If the voltage is still at the new level, then this is an indication from the upstream device to

change the state of illumination of the LED. If the voltage has returned to the value before the detected change then this is an indication from the upstream device to switch to the digital transmission mode. In telecommunications art, the 10ms signal is called a START signal.

A reader implementing the teachings of the current disclosure having detected a voltage level duration on the LEDCTL wire of less than 10ms sends an acknowledgement message, which may be obfuscated with a rolling code, on the DATA0 and DATA1 wires indicating that it has detected the request to change to packet-mode communication on the LEDCTL wire and has switched to this mode of reception on the LEDCTL wire.

The change back to the interpretation of signals on the LEDCTL described in the SIA standard by either the reader or the upstream device is accomplished either by sending a message in packet-mode to terminate packet-mode communication.

Furthermore, once the reader is in a secure Wiegand mode (*i.e.*, a packet transmission mode or any other secure Wiegand mode discussed herein), the reader and/or upstream device will set a flag that indicates the change to the secure Wiegand mode has been executed. In accordance with at least some embodiments of the present invention, when the reader powers up, the reader stays in this mode so that a power cycle, for example, cannot be used to attack the reader and send it back to an unsecured mode of operation. While there may be some secure way of causing a reader to go back to its initial mode of operation (*i.e.*, resetting the flag), it should not be due to a power down of the reader, which could be easily exploited by an attacker to compromise the system.

Reader-Initiated Mode Change

The DATA0/DATA1 channel from the reader to the upstream device carries digital data according to existing standards and usage so, unlike the panel-to-reader channel, it is not necessary to configure the channel for the transmission of digital data. There are circumstances however wherein which it is advantageous for the reader to signal a switch from the Wiegand format of described in the SIA standard to a more flexible packet format such as the datagrams of the Internet Protocol (IP).

This is accomplished by sending a special format message, for example a message consisting of all 1's. Such a message may be referred to as a STOP signal. The upstream device would acknowledge the change to packet mode by sending the upstream device-initiated packet-mode START signal as above.

In accordance with at least some embodiments of the present invention, the host may detect when a message has been received to determine that the line is secure. Once a message is received at the host, the host may initiate a mode change by sending a mode-change message to the reader.

Data Encoding

There are in the current art methods of encoding sequences of 0's and 1's or digital data bits on a single wire such as LEDCTL. There are also in the current art methods of forming these streams into finite-length blocks of 8-bit elements called bytes.

The blocks of digital data received on the LEDCTL wire are called frames. In the interest of simplicity and ease of implementation, a preferred embodiment would employ frames consisting of constant and fixed number of bytes in every block of data; i.e. a fixed frame length.

In the case that software/firmware in the upstream device is used to interpret the

encoding of the digital data on the LEDCTL wire (a software UART), it is advantageous that the frames be short because the reader will have to devote all of its resources to this task for example by turning off interrupts and thus will not be in a mode to receive signals on its other inputs, for example on the input that reads cards presented to it.

For the purposes envisioned for packet-mode communication using the LEDCTL line, message lengths on the order of 8 to 16 bytes are deemed sufficient. If error detection and correction (packet framing below) posed a 100% overhead, then a frame length of 32 bytes would be required. Assuming a transmission rate of 200k bits/second, such a frame would take the reader off-line for approximately $\frac{1}{2}$ of a millisecond. With a hardware UART, there is essentially no off-line time.

In alternative embodiments of the current disclosure, frames are of variable length and the data encoding methodology includes the determination of the number of bytes in the frame, message length, symbols, etc.

Packet Framing

A frame is an undifferentiated finite sequence of bytes. In order to turn the frame into a message, the values of the bytes need to be given meaning. Imputing meaning to the bytes in a frame is called packet framing and results in a packet of data. Both the upstream device and the card reader have to agree on the semantics of the bytes in the frame for a packet to be formed and for packet-mode communication to take place.

In one embodiment of the current disclosure, there is a single, fixed agreement within the access control system as to the structure of a packet of data on the LEDCTL wire. In an alternative embodiment, the only fixed aspect of the structure of the packet is an indication of what type of packet is to be found in the frame. This could, for example,

be the first byte in the frame wherein the value of this byte indicates the type of packet encoded in the following bytes.

In the case that a fixed frame length is used, the packet length may be different than the frame length, in particular the packet length may be less than the frame length. In this case the packet has to be found within the frame. One method of doing this is to reserve specific byte values to mark the beginning and end of the packet. The SLIP protocol is a method of packet framing using special byte values.

There are in the art other packet framing protocols that would be appropriate for use on two-way, packet-mode serial communication means for Wiegand wires described in the current disclosure such as the serial line internet protocol (SLIP) described in RFC 1055 and the point-to-point protocol (PPP) described in RFC 1661.

In a preferred embodiment of the current disclosure, packet framing also includes error checking and error correction using means and methods of the current art such as cyclic redundancy codes (CRC) and Hamming encoding.

Serial Line Internet Protocol (SLIP)

The following code excerpted from RFC 1055 implements a small and efficient packet framing protocol called SLIP. Due to the short frames envisioned in the application of the current disclosure, no flow control is needed or defined. SLIP can be used effectively with Van Jacobsen TCP header compression when the IP datagrams are carrying TCP packets (See IP over Wiegand below).

```
/* SLIP special character codes
*/
#define END          0300    /* indicates end of packet */
#define ESC          0333    /* indicates byte stuffing */
#define ESC_END      0334    /* ESC ESC_END means END data byte */
#define ESC_ESC      0335    /* ESC ESC_ESC means ESC data byte */

/* SEND_PACKET: sends a packet of length "len", starting at
```

```
* location "p".
*/
void send_packet(p, len)
    char *p;
    int len; {

    /* send an initial END character to flush out any data that may
     * have accumulated in the receiver due to line noise
     */
    send_char(END);

    /* for each byte in the packet, send the appropriate character
     * sequence
     */
    while(len--) {
        switch(*p) {
            /* if it's the same code as an END character, we send a
             * special two character code so as not to make the
             * receiver think we sent an END
             */
            case END:
                send_char(ESC);
                send_char(ESC_END);
                break;

            /* if it's the same code as an ESC character,
             * we send a special two character code so as not
             * to make the receiver think we sent an ESC
             */
            case ESC:
                send_char(ESC);
                send_char(ESC_ESC);
                break;

            /* otherwise, we just send the character
             */
            default:
                send_char(*p);
        }

        p++;
    }

    /* tell the receiver that we're done sending the packet
     */
    send_char(END);
}

/* RECV_PACKET: receives a packet into the buffer located at "p".
 * If more than len bytes are received, the packet will
 * be truncated.
 * Returns the number of bytes stored in the buffer.
 */
int recv_packet(p, len)
    char *p;
    int len; {
    char c;
    int received = 0;
```

```
/* sit in a loop reading bytes until we put together
 * a whole packet.
 * Make sure not to copy them into the packet if we
 * run out of room.
 */
while(1) {
    /* get a character to process
    */
    c = recv_char();

    /* handle bytestuffing if necessary
    */
    switch(c) {

        /* if it's an END character then we're done with
        * the packet
        */
        case END:
            /* a minor optimization: if there is no
            * data in the packet, ignore it. This is
            * meant to avoid bothering IP with all
            * the empty packets generated by the
            * duplicate END characters which are in
            * turn sent to try to detect line noise.
            */
            if(received)
                return received;
            else
                break;

        /* if it's the same code as an ESC character, wait
        * and get another character and then figure out
        * what to store in the packet based on that.
        */
        case ESC:
            c = recv_char();

            /* if "c" is not one of these two, then we
            * have a protocol violation. The best bet
            * seems to be to leave the byte alone and
            * just stuff it into the packet
            */
            switch(c) {
                case ESC_END:
                    c = END;
                    break;
                case ESC_ESC:
                    c = ESC;
                    break;
            }

            /* here we fall into the default handler and let
            * it store the character for us
            */
            default:
                if(received < len)
                    p[received++] = c;
            }
        }
    }
```

IP over Wiegand

In order to support Internet transport and network protocols such as TCP and UDP and application Internet protocols such as HTTP and SNMP, embodiments of the present invention may utilize an IP packet called IP-over-Wiegand.

Arbitrary protocols including proprietary protocols and industry-specific protocols can be carried in IP packets. Those familiar with the art of digital data communication will understand that the means and methods of the current disclosure include the transmission of packets that are not Internet packets but may be designed explicitly for use in physical access control systems.

The intent of the current disclosure is to cover all methods for the serial communication of digital data on the LEDCTL line in conformance to three constraints.

The first constraint is that there be no changes to the existing hardware comprising either the physical access control reader or the upstream device communicating with the reader.

The second constraint is that components implementing the means and methods of the disclosure are in full compliance with the SIA standard.

The third constraint is that card readers and upstream devices such as control upstream devices that implement the teachings of the current disclosure interoperate seamlessly with card readers and upstream devices complying with the SIA standard that do not implement the teachings of the current disclosure.

By adding hardware to either the card reader or the upstream device or by inserting additional hardware components such as gateways and translators into the physical access control system, there are alternative methods of achieving the

communication of packet data from upstream devices to card readers using Wiegand wires. Indeed there are such devices in the art.

The advantage provided by embodiments of the present invention is that two-way, packet-mode communication can be achieved on existing hardware and thus without adding hardware components to the physical access control system and without changing existing hardware or wiring in the physical access control system.

The commonly accepted and widely held view of the physical access control industry is that the Wiegand protocol described in and constrained by the SIA standard can achieve the communication of digital data in only one direction, namely from the reader to the upstream device. By describing the communication of digital data in the other direction, from the upstream device to the reader, and by defining communication between the card reader and the upstream device while maintaining conformance to the SIA standard and on existing hardware, embodiments of the present invention connect the end nodes of physical access control systems to the Internet and thereby drastically decrease their maintenance and administration costs and greatly increase their security. Additionally, a parity line may be provided to detect collisions if the readers and/or upstream device are operating in a packet mode. Thus, multiple readers can be connected to the upstream device via a single wire and the communication time on that wire may be shared among the readers.

Blind Synchronization

In accordance with at least some embodiments of the present invention, two devices may be using a synchronized PRNG to, for example, secure the communication

between them. Synchronization of the PRNG between the two devices can be lost if any number of disruptions occur at either the reader or upstream device or any intermediary device. By utilizing at least one embodiment of the present invention, the two devices can regain synchronization of the pseudo-random number sequence without opening the possibility of a replay attack on the pseudo-random number sequence.

The PRNG used to secure the communication between them is used every time they communicate and therefore is called the “fast” PRNG. The other PRNG is only used when the devices need to resynchronize the fast PRN. This second PRNG is called the “slow” PRNG.

In the current art, an element generated fast PRNG or some function of an element generated by the fast PRNG is used to resynchronize the PRNG. An attacker listening on the communication line between the two devices can capture and replay the resynchronization sequence. Thus, and in accordance with at least some embodiments of the present invention, when the fast PRNG needs to be resynchronized, the slow PRNG is stepped to the next value. This next element of the slow PRNG shared by the two devices may be used to restart the fast PRNG from some predetermined beginning point, for example the element of the slow PRNG itself or some function thereof.

Data Transfer Reduction

In accordance with at least some embodiments of the present invention, a method and system for reducing the amount of data transferred from a reader to an upstream device is provided. Although the following method will be described in relation to the transmission of Wiegand format data, one skilled in the art will appreciate that the

inventive data transmission methods described herein can be applied to other types of data transmission and security protocols.

The specific formatting of card data may have certain redundancies from card to card. For example, many cards distributed at a common location or site may be assigned the same site code. While each card has a unique card code, the site code is common among a plurality of cards used at a particular site. However, according to the SIA standard, the upstream device typically analyzes both the site code and card code transmitted from a reader (which was obtained from a card presented thereto). Accordingly, it is typically required that a reader transmit both the site code and card code to the upstream device so that the identity of the card presented to the reader can be determined.

In accordance with at least some embodiments of the present invention, the data redundancies between cards within a card population is identified and used to reduce the amount of data transmitted from the reader to the upstream device. An exemplary method of reducing data transmissions between the reader and upstream device will be described in accordance with data structures depicted in Fig. 6.

According to the SIA standard for 26-Bit Wiegand, the first bit is an even parity for the following 12 bits. Bits 2-9 are the site code and bits 10-25 are the card number. The final bit (*i.e.*, bit 26) is an odd parity over the previous 12 bits. Accordingly, the 26-bit Wiegand standard comprises at least two data fields (*i.e.*, a site code and card number data field). Data from common data fields of different cards may be identical, for example if both cards are issued the same site code or if the same card is presented to the same reader at two different times.

As can be seen in Fig. 6, when a site code or other data field is redundant between two cards, there may be an opportunity to reduce the amount of data transmitted from the reader to the upstream device. More specifically, if the reader and upstream device can maintain a synchronized accounting of the cards that have been previously presented to the reader and had their entire data set transmitted to the upstream device, then the reader may be enabled to replace data from an entire field with an indicator which indicates that the omitted data from a particular field is redundant with a previously presented card. Upon recognizing the indicator, the upstream device can reference its cache to find the redundant data from a data field of a previously presented card. Thus, instead of sending a plurality of bits of data (*e.g.*, 8 bits for the site code), the reader is enabled to send an indicator, which will be comprised of data that cannot ordinarily appear in the message. Alternatively, other methods of detecting that a field has been compressed can be employed such as the message receiver noting that the fixed length message is shorter or even including an additional field comprised of single bits indicating whether or not a field is present or has been reduced. This allows the reader to reduce the amount of data transmitted when a card currently presented to a reader comprises a field of data that matches a field of data from a previously read card.

In another more aggressive scheme, reduction of data can be utilized *within* a field. For example, if the card number field is 16 bits but only cards 1 through 100 are actually in use, the card number field will always have many high-order zero bits that can be reduced.

In accordance with at least some embodiments of the present invention, the reader may be required by internal logic to at least send certain portions of the card data

regardless of whether or not it is found in its cache. For example, if the reader reads the same card two times in a row, the reader may still be required to send at least the card number. Without such a requirement an attacker could send illicit indicators to the upstream device for all data fields that should be transmitted by the reader after the reader had previously sent valid card data. Upon receiving all of the indicators, the upstream device would simply refer to the previously read card data and allow the attacker access to the asset. Of course, the use of security techniques, some of which are described herein, in connection with the indicators would help to alleviate the risk of improperly allowing entry to an attacker that simply transmits indicators to the upstream device.

As can be appreciated by one skilled in the art, this may work for many different types of data organizational schemes used, for example, in Wiegand data transmissions. For instance, embodiments of the present invention may be utilized to reduce the amount of data transmitted in a 26-bit Wiegand data transmission scheme where three data fields (i.e., site code, card code, and parity bits) are typically transmitted from the reader to the upstream device. Alternatively, embodiments of the present invention may also be utilized in data transmission schemes that utilize significantly more data fields, such as PIV and other evolving standards, where a relatively large amount of data is transmitted from a reader to an upstream device when a card has been read by the reader. Any logical separation of data may be used to determine whether fields have been previously submitted from the reader to the upstream device

In accordance with at least some embodiments of the present invention, the reader may compare data fields of a currently read card with data fields of a card that was read immediately before the currently read card. For example, the reader may comprise a

cache for only one set of card data at a time. Thus, only a single comparison between the data fields of the currently read card and data fields of the previously read card needs to be performed. Alternatively, the reader may comprise a list of cards that have been previously read along with an order identifier (*e.g.*, last read card, second-to-last read card, third-to-last read card, *etc.*). Data fields of a currently read card may be compared to data fields from all of the other cards that are maintained in the reader's cache. A comparison may be performed for each card in the cache until a match between fields has been identified.

While utilization of multiple comparisons does increase the amount of processing required by the reader, it may further reduce the amount of data that is transmitted to the upstream device, thereby decreasing the overall traffic on the system. When the reader contains the records of multiple previously read cards and data from a currently read card is not being sent since it matched at least some data in one of the previously read cards, the reader may also need to include in its transmission of card data the identifier of the card from which the match was found. Accordingly, the upstream device should maintain a cache that is substantially consistent and synchronized with the cache of the reader.

In the event that a data transmission error occurs (*e.g.*, because of a network failure, because of a power outage at the upstream device, *etc.*), and the reader attempts to transmit less than all of the data from a currently read card (because the reader determined that at least some of the data matched data from a previously read card), the upstream device may no longer be synchronized with the reader and the instant data transmission may be determined to be erroneous by the upstream device. If such a

situation occurs, the upstream device may communicate to the reader using any of the methods described herein that it did not recognize the partial transmission and/or could not find the matching field to replace the non-transmitted field. This communication may be in the form of an error message. Alternatively, the upstream device may transmit a re-send entire data message to the reader. Upon receiving such a message from the upstream device, the reader may re-transmit all of the data from the currently read card. As an alternative reaction, the reader may clear its cache upon receiving such a message, request a re-read of the card, and transmit the entire card data. Either reader reaction will allow both the reader and upstream device to re-synchronize with one another as well as allow the upstream device to fully analyze the card data.

The present invention, in various embodiments, includes components, methods, processes, systems and/or apparatus substantially as depicted and described herein, including various embodiments, subcombinations, and subsets thereof. Those of skill in the art will understand how to make and use the present invention after understanding the present disclosure. The present invention, in various embodiments, includes providing devices and processes in the absence of items not depicted and/or described herein or in various embodiments hereof, including in the absence of such items as may have been used in previous devices or processes, e.g., for improving performance, achieving ease and/or reducing cost of implementation.

The foregoing discussion of the invention has been presented for purposes of illustration and description. The foregoing is not intended to limit the invention to the form or forms disclosed herein. In the foregoing Detailed Description for example, various features of the invention are grouped together in one or more embodiments for the purpose

of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed invention requires more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive aspects lie in less than all features of a single foregoing disclosed embodiment. Thus, the following claims are hereby incorporated into this Detailed Description, with each claim standing on its own as a separate preferred embodiment of the invention.

Moreover though the description of the invention has included description of one or more embodiments and certain variations and modifications, other variations and modifications are within the scope of the invention, e.g., as may be within the skill and knowledge of those in the art, after understanding the present disclosure. It is intended to obtain rights which include alternative embodiments to the extent permitted, including alternate, interchangeable and/or equivalent structures, functions, ranges or steps to those claimed, whether or not such alternate, interchangeable and/or equivalent structures, functions, ranges or steps are disclosed herein, and without intending to publicly dedicate any patentable subject matter.

What is claimed is:

1. A communication method, comprising:
operating a credential reader in a first mode of operation;
receiving, at the credential reader, a message from an upstream device;
determining, by the credential reader, that the message was transmitted by the upstream device; and
based on determining that the message was transmitted by the upstream device, transitioning the credential reader from the first mode of operation to a second mode of operation.
2. The method of claim 1, wherein the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol.
3. The method of claim 2, wherein the unidirectional communication protocol is the Wiegand protocol.
4. The method of claim 1, wherein the message transmitted by the upstream device comprises an alteration of a control line signal between the reader and upstream device for a predetermined amount of time.
5. The method of claim 4, wherein the predetermined amount of time is less than a human-perceivable amount of time.

6. The method of claim 1, wherein the first mode comprises a non-secure Wiegand mode and the second mode comprises a secure Wiegand mode.

7. The method of claim 1, wherein the first mode comprises a Wiegand-format mode and the second mode comprises a packet-mode.

8. A computer-readable medium comprising processor-executable instructions, the processor-executable instructions comprising:

instructions configured to cause a credential reader to operated in a first mode of operation;

instructions configured to receive a message at the reader, the message being received from an upstream device;

instructions configured to determine that the message was transmitted by the upstream device; and

instructions configured to transition the credential reader from the first mode of operation to a second mode of operation, wherein the transition from the first mode of operation to the second mode of operation occurs based on determining that the message was transmitted by the upstream device.

9. The computer-readable medium of claim 8, wherein the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol.

10. The computer-readable medium of claim 9, wherein the unidirectional communication protocol is the Wiegand protocol.

11. The computer-readable medium of claim 8, wherein the message transmitted by the upstream device comprises an alteration of a control line signal between the reader and upstream device for a predetermined amount of time.

12. The computer-readable medium of claim 11, wherein the predetermined amount of time is less than a human-perceivable amount of time.

13. The computer-readable medium of claim 8, wherein the first mode comprises a non-secure Wiegand mode and the second mode comprises a secure Wiegand mode.

14. The computer-readable medium of claim 8, wherein the first mode comprises a Wiegand- format mode and the second mode comprises a packet-mode.

15. A credential reader comprising at least one of a microprocessor and firmware that enable the reader to operate in a first mode of operation, receive a message from an upstream device, determine that the message was transmitted by the upstream device, and, in response thereto transition the credential reader from the first mode of operation to a second mode of operation, wherein the transition from the first mode of

operation to the second mode of operation occurs based on determining that the message was transmitted by the upstream device.

16. The credential reader of claim 15, wherein the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol, and wherein the unidirectional communication protocol is the Wiegand protocol.

17. The credential reader of claim 15, wherein the message transmitted by the upstream device comprises an alteration of a control line signal between the reader and upstream device for a predetermined amount of time.

18. The credential reader of claim 17, wherein the predetermined amount of time is less than a human-perceivable amount of time.

19. The credential reader of claim 15, wherein the first mode comprises a non-secure Wiegand mode and the second mode comprises a secure Wiegand mode.

20. The credential reader of claim 15, wherein the first mode comprises a Wiegand- format mode and the second mode comprises a packet-mode.

ABSTRACT

The present invention is directed toward secure access systems. Specifically, a method and system is provided that enhances the security of unidirectional communication protocols used in access control systems, such as the Wiegand protocol. The enhancements may include obfuscation of data, a two-way packet-mode communications, and blind synchronization of pseudo-random number generators.

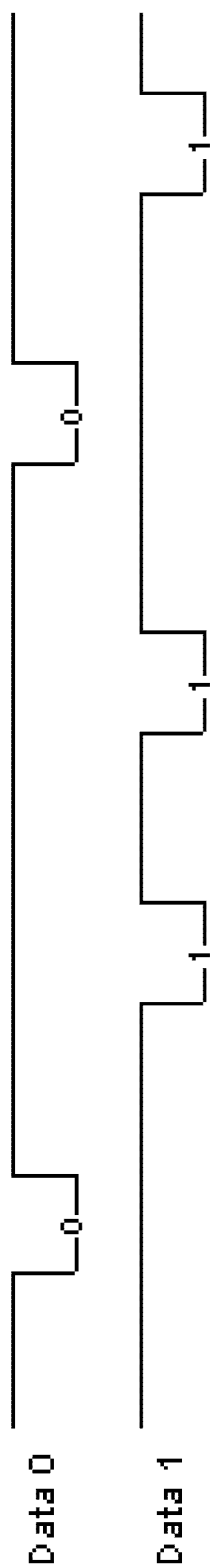


Fig. 1

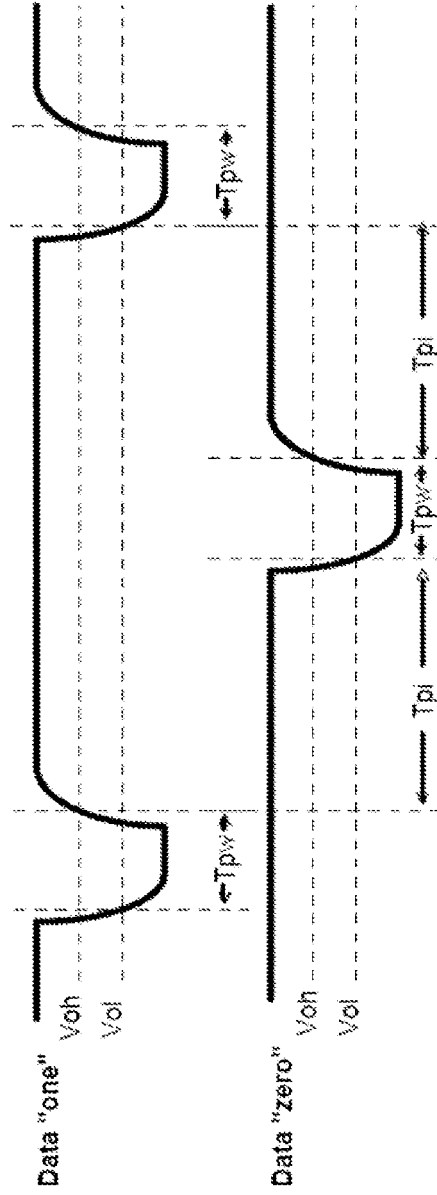


Fig. 2

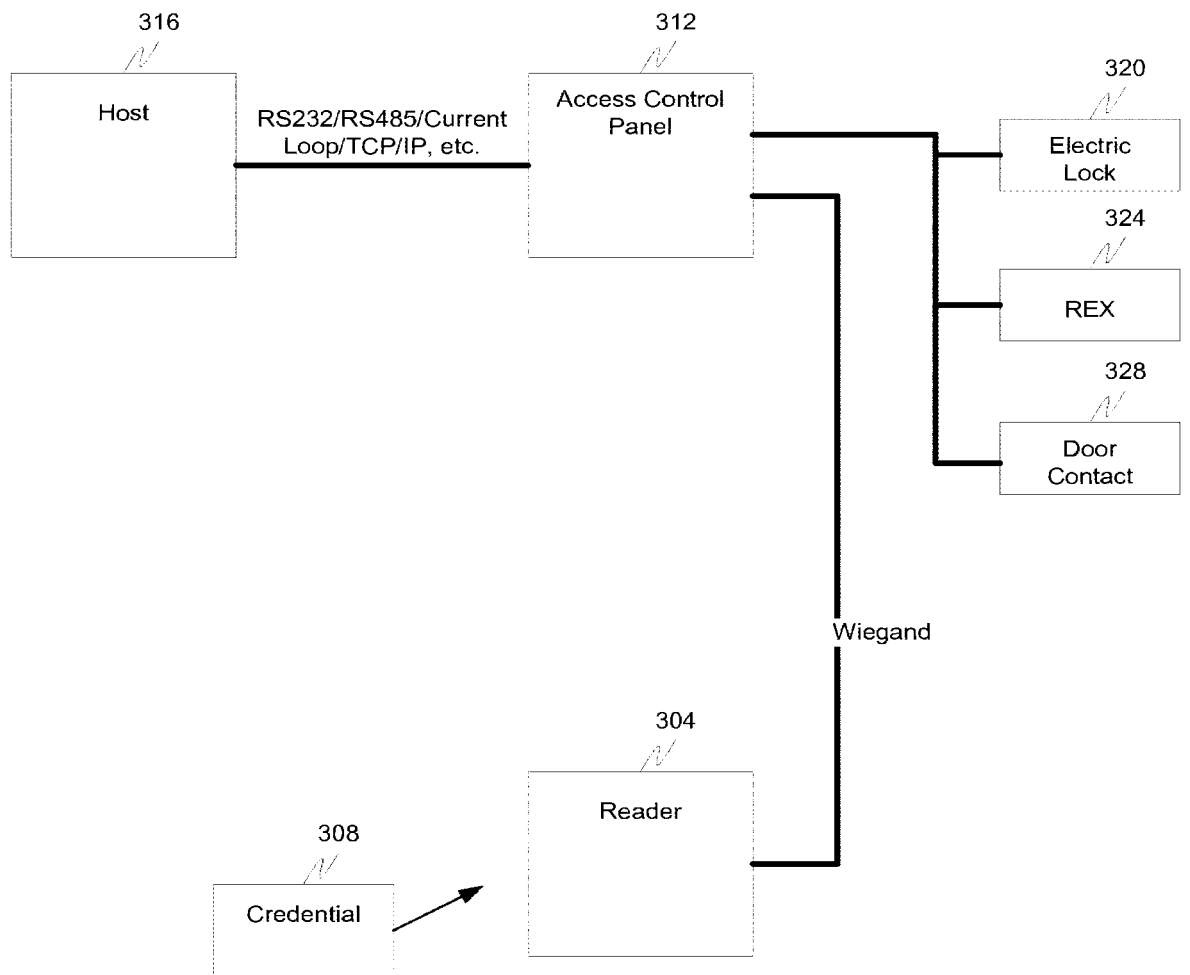


Fig. 3

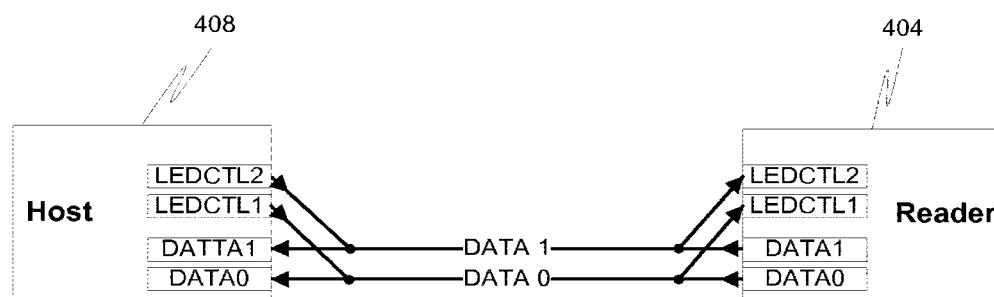


Fig. 4

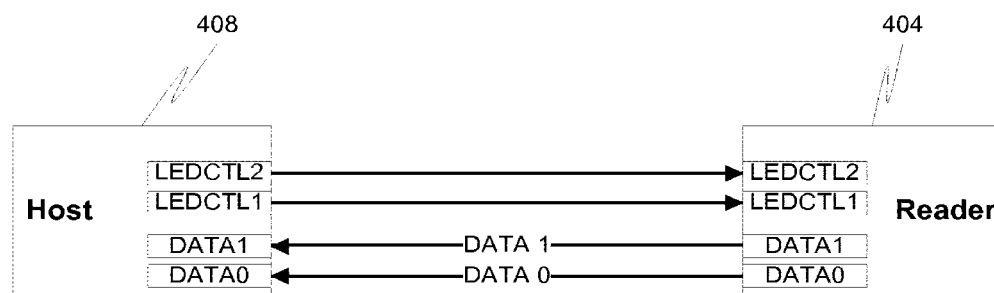


Fig. 5

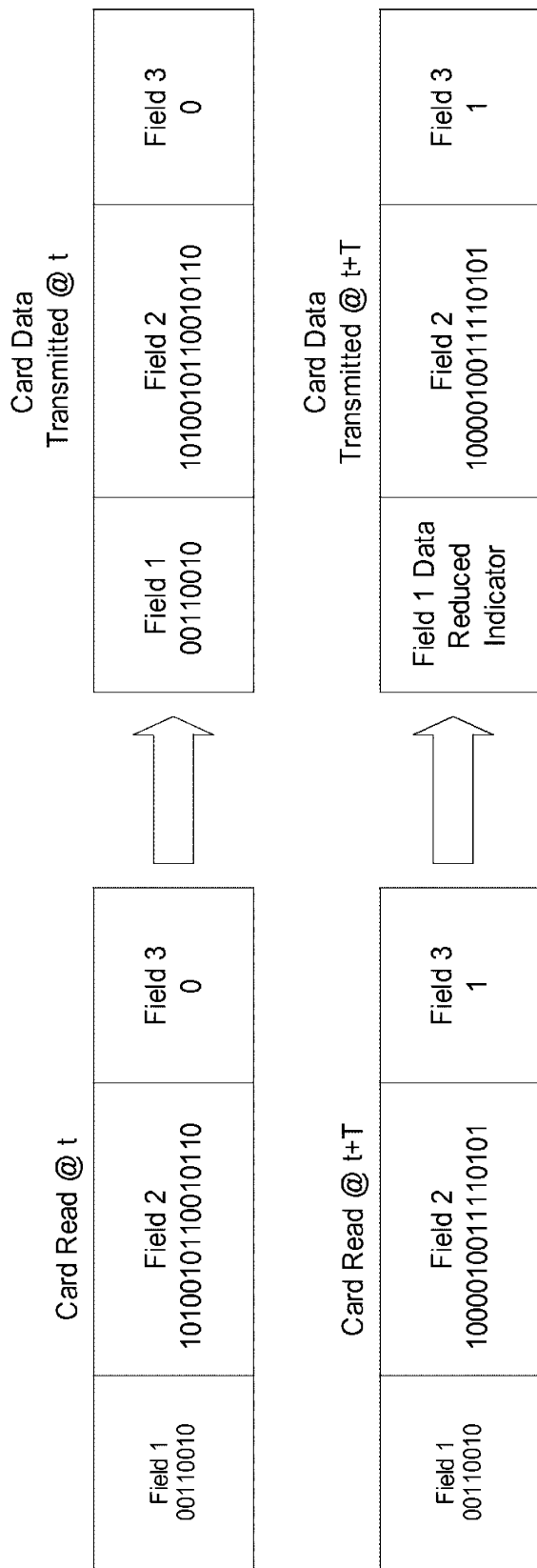


Fig. 6

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	2943AAAB-178-DIV
		Application Number	
Title of Invention	SECURE WIEGAND COMMUNICATIONS		
<small>The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.</small>			

Secrecy Order 37 CFR 5.2

<input type="checkbox"/>	Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)
--------------------------	---

Inventor Information:

Inventor 1					Remove		
Legal Name							
Prefix	Given Name		Middle Name		Family Name		Suffix
	Scott		B.		Guthery		
Residence Information (Select One) <input checked="" type="radio"/> US Residency <input type="radio"/> Non US Residency <input type="radio"/> Active US Military Service							
City	Chestnut Hill		State/Province	MA	Country of Residence ⁱ	US	
Mailing Address of Inventor:							
Address 1		2400 Beacon #208					
Address 2							
City	Chestnut Hill			State/Province	MA		
Postal Code	02467			Country ¹	US		
Inventor 2					Remove		
Legal Name							
Prefix	Given Name		Middle Name		Family Name		Suffix
	Mark				Robinton		
Residence Information (Select One) <input checked="" type="radio"/> US Residency <input type="radio"/> Non US Residency <input type="radio"/> Active US Military Service							
City	Somerville		State/Province	MA	Country of Residence ⁱ	US	
Mailing Address of Inventor:							
Address 1		897 Broadway, Apt. 2					
Address 2							
City	Somerville			State/Province	MA		
Postal Code	02144			Country ¹	US		
Inventor 3					Remove		
Legal Name							
Prefix	Given Name		Middle Name		Family Name		Suffix
	Michael		Lawrence		Davis		
Residence Information (Select One) <input checked="" type="radio"/> US Residency <input type="radio"/> Non US Residency <input type="radio"/> Active US Military Service							

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	2943AAAB-178-DIV	
		Application Number		
Title of Invention	SECURE WIEGAND COMMUNICATIONS			

City	Amherst	State/Province	NY	Country of Residence ⁱ	US
------	---------	----------------	----	-----------------------------------	----

Mailing Address of Inventor:

Address 1	12 Hummingbird Lane			
Address 2				
City	Amherst	State/Province	NY	
Postal Code	14228	Country ¹	US	

Inventor 4

Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	David		Andresky	

Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service

City	Lafayette	State/Province	CO	Country of Residence ⁱ	US
------	-----------	----------------	----	-----------------------------------	----

Mailing Address of Inventor:

Address 1	533 Whitetail Circle			
Address 2				
City	Lafayette	State/Province	CO	
Postal Code	80026	Country ¹	US	

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.

Add

Correspondence Information:Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).☐ An Address is being provided for the correspondence Information of this application.

Customer Number	22442		
Email Address	srlaw@sheridanross.com	Add Email	Remove Email

Application Information:

Title of the Invention	SECURE WIEGAND COMMUNICATIONS		
Attorney Docket Number	2943AAAB-178-DIV	Small Entity Status Claimed	<input type="checkbox"/>
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	5	Suggested Figure for Publication (if any)	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	2943AAAB-178-DIV
		Application Number	
Title of Invention	SECURE WIEGAND COMMUNICATIONS		

Publication Information:

<input type="checkbox"/>	Request Early Publication (Fee required at time of Request 37 CFR 1.219)
<input type="checkbox"/>	Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.			
Please Select One:	<input checked="" type="radio"/> Customer Number	<input type="radio"/> US Patent Practitioner	<input type="radio"/> Limited Recognition (37 CFR 11.9)
Customer Number	91935		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.			
Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Division of	12539431	2009-08-11
Prior Application Status		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12539431	non provisional of	61087941	2008-08-11
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			Add

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).			
Remove			
Application Number	Country i	Filing Date (YYYY-MM-DD)	Priority Claimed
			<input checked="" type="radio"/> Yes <input type="radio"/> No
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			Add

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	2943AAAB-178-DIV
		Application Number	
Title of Invention	SECURE WIEGAND COMMUNICATIONS		

Authorization to Permit Access:

<input checked="" type="checkbox"/> Authorization to Permit Access to the Instant Application by the Participating Offices
<p>If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.</p> <p>In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.</p> <p>In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.</p>

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.	
Applicant 1	
<p>If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.</p>	
Remove	
<input checked="" type="radio"/> Assignee	<input type="radio"/> Legal Representative under 35 U.S.C. 117
<input type="radio"/> Person to whom the inventor is obligated to assign.	<input type="radio"/> Person who shows sufficient proprietary interest
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:	
Name of the Deceased or Legally Incapacitated Inventor : <input type="text"/>	
If the Assignee is an Organization check here. <input checked="" type="checkbox"/>	
Organization Name	Assa Abloy AB

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	2943AAAB-178-DIV
		Application Number	
Title of Invention	SECURE WIEGAND COMMUNICATIONS		

Mailing Address Information:			
Address 1		Klarabergsviadukten 90 - P.O. Box 70340	
Address 2			
City		Stockholm	State/Province
Country ⁱ	SE	Postal Code	SE-107 23
Phone Number		Fax Number	
Email Address			
Additional Applicant Data may be generated within this form by selecting the Add button. Add			

Signature:Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications					
Signature	/Matthew R. Ellsworth/			Date (YYYY-MM-DD)	2012-11-29
First Name	Matthew	Last Name	Ellsworth	Registration Number	56345
Additional Signature may be generated within this form by selecting the Add button. Add					

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
13/689,088	11/29/2012		1260	2943AAAB-178-DIV	20	3

CONFIRMATION NO. 9927

22442
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

FILING RECEIPT



OC000000058617954

Date Mailed: 01/16/2013

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Scott B. Guthery, Chestnut Hill, MA;
Mark Robinton, Somerville, MA;
Michael Lawrence Davis, Amherst, NY;
David Andresky, Lafayette, CO;

Applicant(s)

ASSA ABLOY AB, Stockholm, SWEDEN

Assignment For Published Patent Application

ASSA ABLOY AB, Stockholm, SWEDEN

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a DIV of 12/539,431 08/11/2009 PAT 8358783 *
which claims benefit of 61/087,941 08/11/2008
(*)Data provided by applicant is not consistent with PTO records.

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

Projected Publication Date: To Be Determined - pending completion of Security Review

page 1 of 3

Non-Publication Request: No

Early Publication Request: No

Title

SECURE WIEGAND COMMUNICATIONS

Preliminary Class

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where

page 2 of 3

the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/689,088	11/29/2012	Scott B. Guthery	2943AAAB-178-DIV

CONFIRMATION NO. 9927

22442
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

NOTICE



Date Mailed: 01/16/2013

INFORMATIONAL NOTICE TO APPLICANT

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

The item(s) indicated below are also required and should be submitted with any reply to this notice to avoid further processing delays.

A new inventor's oath or declaration that identifies this application (e.g., by Application Number and filing date) is required. The inventor's oath or declaration does not comply with 37 CFR 1.63 in that it:

- does not state that the above-identified application was made or authorized to be made by the person executing the oath or declaration.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 13/689,088			
APPLICATION AS FILED - PART I									
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY			
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)		
BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A			N/A	390		
SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>	N/A	N/A	N/A			N/A	620		
EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A			N/A	250		
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>	20	minus 20 = *				x 62 =	0.00		
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	3	minus 3 = *				x 250 =	0.00		
APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00		
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00		
			TOTAL			TOTAL	1260		
* If the difference in column 1 is less than zero, enter "0" in column 2.									
APPLICATION AS AMENDED - PART II									
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	Minus **	=	x =		x =		
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x =		x =		
	Application Size Fee (37 CFR 1.16(s))								
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
			TOTAL ADD'L FEE			TOTAL ADD'L FEE			
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	Minus **	=	x =		x =		
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x =		x =		
	Application Size Fee (37 CFR 1.16(s))								
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
			TOTAL ADD'L FEE			TOTAL ADD'L FEE			
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.									



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/689,088	11/29/2012	Scott B. Guthery	2943AAAB-178-DIV

CONFIRMATION NO. 9927

NEW OR REVISED PPD NOTICE



22442
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

NOTICE OF NEW OR REVISED PROJECTED PUBLICATION DATE

The above-identified application has a new or revised projected publication date. The current projected publication date for this application is 05/09/2013. If this is a new projected publication date (there was no previous projected publication date), the application has been cleared by Licensing & Review or a secrecy order has been rescinded and the application is now in the publication queue.

If this is a revised projected publication date (one that is different from a previously communicated projected publication date), the publication date has been revised due to processing delays in the USPTO or the abandonment and subsequent revival of an application. The application is anticipated to be published on a date that is more than six weeks different from the originally-projected publication date.

More detailed publication information is available through the private side of Patent Application Information Retrieval (PAIR) System. The direct link to access PAIR is currently <http://pair.uspto.gov>. Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Questions relating to this Notice should be directed to the Office of Data Management, Application Assistance Unit at (571) 272-4000, or (571) 272-4200, or 1-888-786-0101.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	1	of	12	Attorney Docket Number	2943AAAB-178-DIV

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	3694757	09/26/1972	Hanna, Jr.	
	2	3842350	10/15/1974	Gross	
	3	4087626	05/02/1978	Brader	
	4	4163215	07/31/1979	Iida	
	5	4333072	06/01/1982	Beigel	
	6	4425645	01/10/1984	Weaver et al.	
	7	4519068	05/21/1985	Krebs et al.	
	8	4549264	10/22/1985	Carroll et al.	
	9	4656463	04/07/1987	Anders et al.	
	10	4688026	08/18/1987	Scribner et al.	
	11	4849927	07/18/1989	Vos	
	12	5013898	05/07/1991	Glasspool	
	13	5028918	07/02/1991	Giles et al.	
	14	5041826	08/20/1991	Milheiser	
	15	5050150	09/17/1991	Ikeda	
	16	5151684	09/29/1992	Johnsen	
	17	5166676	11/24/1992	Milheiser	
	18	5187676	02/16/1993	DeVane	
	19	5193115	03/09/1993	Vobach	
	20	5218344	06/08/1993	Ricketts	
	21	5235642	08/10/1993	Wobber et al.	
	22	5258936	11/02/1993	Gallup et al.	
	23	5343469	08/30/1994	Ohshima	
	24	5347263	09/13/1994	Carroll et al.	
	25	5357528	10/18/1994	Alon et al.	
	26	5396215	03/07/1995	Hinkle	
	27	5420928	05/30/1995	Aiello et al.	
	28	5426425	06/20/1995	Comad et al.	
	29	5446683	08/29/1995	Mullen et al.	
	30	5467082	11/14/1995	Sanderson	
	31	5491471	02/13/1996	Stobbe	
	32	5517172	05/14/1996	Chiu	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	2	of	12	Attorney Docket Number	2943AAAB-178-DIV

	33	5519381	05/21/1996	Marsh et al.	
	34	5521602	05/28/1996	Carroll et al.	
	35	5533128	07/02/1996	Vobach	
	36	5541996	07/30/1996	Ridenour	
	37	5577124	11/19/1996	Anshel et al.	
	38	5594384	01/14/1997	Carroll et al.	
	39	5600324	02/04/1997	Reed et al.	
	40	5600683	02/04/1997	Bierach et al.	
	41	5608801	03/04/1997	Aiello et al.	
	42	5680131	10/21/1997	Utz	
	43	5679945	10/21/1997	Renner et al.	
	44	5686904	11/11/1997	Bruwer	
	45	5696909	12/09/1997	Wallner	
	46	5724417	03/03/1998	Bartholomew et al.	
	47	5745037	04/28/1998	Guthrie et al.	
	48	5751808	05/12/1998	Anshel et al.	
	49	5754603	05/19/1998	Thomas et al.	
	50	5777561	07/07/1998	Chieu et al.	
	51	5802176	09/01/1998	Audebert	
	52	5825882	10/20/1998	Kowalski et al.	
	53	5844990	12/01/1998	Kokubu et al.	
	54	5848541	12/15/1998	Glick et al.	
	55	5886894	03/23/1999	Rakoff	
	56	5887176	03/23/1999	Griffith et al.	
	57	5909462	06/01/1999	Kamerman et al.	
	58	5923264	07/13/1999	Lavelle et al.	
	59	5929779	07/27/1999	MacLellan et al.	
	60	5952922	09/14/1999	Shober	
	61	5952935	09/14/1999	Mejia et al.	
	62	5954583	09/21/1999	Green	
	63	5991410	11/23/1999	Albert et al.	
	64	5995956	11/30/1999	Nguyen	
	65	6044388	03/28/2000	DeBellis et al.	
	66	6052786	04/18/2000	Tsuchida	
	67	6078888	06/20/2000	Johnson, Jr.	
	68	6079018	06/20/2000	Hardy et al.	
Examiner Signature				Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	3	of	12	Attorney Docket Number	2943AAAB-178-DIV

	69	6078251	06/20/2000	Landt et al.	
	70	6097307	08/01/2000	Utz	
	71	6154544	11/28/2000	Farris et al.	
	72	6181252	01/30/2001	Nakano	
	73	6182214	01/30/2001	Hardjono	
	74	6192222	02/20/2001	Greeff et al.	
	75	6212175	04/03/2001	Harsch	
	76	6219439	04/17/2001	Burger	
	77	6223984	05/01/2001	Renner et al.	
	78	6249866	06/19/2001	Brundrett et al.	
	79	6249212	06/19/2001	Beigel et al.	
	80	6259367	07/10/2001	Klein	
	81	6272562	08/07/2001	Scott et al.	
	82	6285761	09/04/2001	Patel et al.	
	83	6285681	09/04/2001	Kolze et al.	
	84	6304613	10/16/2001	Koller et al.	
	85	6307517	10/23/2001	Lee	
	86	6314440	11/06/2001	O'Toole et al.	
	87	6317027	11/13/2001	Watkins	
	88	6325285	12/04/2001	Baratelli	
	89	6366967	04/02/2002	Wagner	
	90	6377176	04/23/2002	Lee	
	91	6411199	06/25/2002	Geiszler et al.	
	92	6420961	07/16/2002	Bates et al.	
	93	6483427	11/19/2002	Werb	
	94	6487176	11/26/2002	Lehmann	
	95	6496595	12/17/2002	Puchek et al.	
	96	6496806	12/17/2002	Horwitz et al.	
	97	6509828	01/21/2003	Bolavage et al.	
	98	6542608	04/01/2003	Scheidt et al.	
	99	6606386	08/12/2003	Scheidt et al.	
	100	6608901	08/19/2003	Scheidt et al.	
	101	6617962	09/09/2003	Horwitz et al.	
	102	6677852	01/13/2004	Landt	
	103	6691141	02/10/2004	Schmidt	
	104	6718038	04/06/2004	Cusmario	
Examiner Signature				Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	4	of	12	Attorney Docket Number	2943AAAB-178-DIV

	105	6717516	04/06/2004	Bridgelall	
	106	6724296	04/20/2004	Hikita et al.	
	107	6810123	10/26/2004	Farris et al.	
	108	6885747	04/26/2005	Scheidt et al.	
	109	6903656	06/07/2005	Lee	
	110	6922558	07/26/2005	Delp et al.	
	111	6931533	08/16/2005	Roberts	
	112	6944768	09/13/2005	Siegel et al.	
	113	6947560	09/20/2005	Smeets et al.	
	114	6963270	11/08/2005	Gallagher, III et al.	
	115	6988203	01/17/2006	Davis et al.	
	116	6992567	01/31/2006	Cole et al.	
	117	7016925	03/21/2006	Schmidt	
	118	7026935	04/11/2006	Diorio et al.	
	119	7064665	06/20/2006	Woodall et al.	
	120	7085791	08/01/2006	Barry et al.	
	121	7118033	10/10/2006	Merkert	
	122	7120696	10/10/2006	Au et al.	
	123	7170997	01/30/2007	Petersen et al.	
	124	7190787	03/13/2007	Graunke et al.	
	125	7197279	03/27/2007	Bellantoni	
	126	7212632	05/01/2007	Scheidt et al.	
	127	7219113	05/15/2007	Bonaccio et al.	
	128	7268681	09/11/2007	Fitzgibbon	
	129	7269416	09/11/2007	Guthrie et al.	
	130	7277543	10/02/2007	Driscoll	
	131	7293698	11/13/2007	Cheng et al.	
	132	7375616	05/20/2008	Rowse et al.	
	133	7378967	05/27/2008	Sullivan et al.	
	134	7407110	08/05/2008	Davis et al.	
	135	7412056	08/12/2008	Farris et al.	
	136	7492898	02/17/2009	Farris et al.	
	137	7492905	02/17/2009	Fitzgibbon	
	138	7551081	06/23/2009	Vrba et al.	
	139	8183980	05/22/2012	Davis et al.	
	140	8358783	01/22/2013	Davis et al.	
Examiner Signature				Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	5	of	12	Attorney Docket Number	2943AAAB-178-DIV

	141	2001/0041593	11/15/2001	Asada	
	142	2001/0056534	12/27/2001	Roberts	
	143	2002/0016913	02/07/2002	Wheeler et al.	
	144	2002/0036569	03/28/2002	Martin	
	145	2002/0131595	09/19/2002	Veda et al.	
	146	2002/0184539	12/05/2002	Fukuda et al.	
	147	2003/0007473	01/09/2003	Strong et al.	
	148	2003/0014646	01/16/2003	Buddhikot et al.	
	149	2003/0055667	03/20/2003	Sgambaro et al.	
	150	2003/0074319	04/17/2003	Jaquette	
	151	2003/0081785	05/01/2003	Boneh et al.	
	152	2003/0204541	10/30/2003	Shackleford et al.	
	153	2003/0208697	11/06/2003	Gardner	
	154	2004/0069852	04/15/2004	Seppinen et al.	
	155	2004/0087273	05/06/2004	Pertti1a et al.	
	156	2004/0089707	05/13/2004	Cortina et al.	
	157	2004/0153291	08/05/2004	Kocarev et al.	
	158	2004/0162863	08/19/2004	Barry et al.	
	159	2004/0162864	08/19/2004	Nowshadi et al.	
	160	2004/0176032	09/09/2004	Kotola et al.	
	161	2004/0179684	09/16/2004	Appenzeller et al.	
	162	2004/0212493	10/28/2004	Stilp	
	163	2004/0232220	11/25/2004	Beenau et al.	
	164	2005/0002533	01/06/2005	Langin-Hooper et al.	
	165	2005/0010624	01/13/2005	Stehle	
	166	2005/0010750	01/13/2005	Ward et al.	
	167	2005/0036620	02/17/2005	Casden et al.	
	168	2005/0044119	02/24/2005	Langin-Hooper et al.	
	169	2005/0063004	03/24/2005	Silverbrook et al.	
	170	2005/0110210	05/26/2005	Soltys et al.	
	171	2005/0116813	06/02/2005	Raskar	
	172	2005/0129247	06/16/2005	Gammel et al.	
	173	2005/0127172	06/16/2005	Merkert Sr.	
	174	2005/0166040	07/28/2005	Walmsley	
	175	2005/0182946	08/18/2005	Shatford	
	176	2005/0265546	12/01/2005	Suzuki	
Examiner Signature				Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	6	of	12	Attorney Docket Number	2943AAAB-178-DIV

	177	2006/0083228	04/20/2006	Ong et al.	
	178	2006/0101274	05/11/2006	Merkert et al.	
	179	2006/0123466	06/08/2006	Davis et al.	
	180	2006/0156027	07/13/2006	Blake	
	181	2006/0174184	08/03/2006	Stroud et al.	
	182	2006/0177056	08/10/2006	Rostin et al.	
	183	2006/0179094	08/10/2006	Onaya et al.	
	184	2006/0181397	08/17/2006	Limbachiya	
	185	2006/0206554	09/14/2006	Lauter et al.	
	186	2006/0210081	09/21/2006	Zhu et al.	
	187	2006/0224901	10/05/2006	Lowe	
	188	2006/0255129	11/16/2006	Griffiths	
	189	2006/0288101	12/21/2006	Mastrodonato et al.	
	190	2006/0294312	12/28/2006	Walmsley	
	191	2007/0016942	01/18/2007	Sakai et al.	
	192	2007/0034691	02/15/2007	Davis et al.	
	193	2007/0043954	02/22/2007	Fox	
	194	2007/0057057	03/15/2007	Andresky et al.	
	195	2007/0076864	04/05/2007	Hwang	
	196	2007/0099597	05/03/2007	Arkko et al.	
	197	2007/0109101	05/17/2007	Colby	
	198	2007/0121943	05/31/2007	Dellow et al.	
	199	2007/0165847	07/19/2007	Langin-Hooper et al.	
	200	2007/0165848	07/19/2007	Reyes	
	201	2007/0178886	08/02/2007	Wang et al.	
	202	2007/0183593	08/09/2007	Yoshida et al.	
	203	2007/0195952	08/23/2007	Singanamala	
	204	2007/0214293	09/13/2007	Gangstoe et al.	
	205	2007/0269048	11/22/2007	Hsu	
	206	2007/0273497	11/29/2007	Kuroda et al.	
	207	2007/0293192	12/20/2007	De Groot	
	208	2007/0294528	12/20/2007	Shoji et al.	
	209	2007/0294531	12/20/2007	Alten	
	210	2007/0294539	12/20/2007	Shulman et al.	
	211	2007/0296817	12/27/2007	Ebrahimi et al.	
	212	2008/0001778	01/03/2008	Challener et al.	
Examiner Signature				Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	7	of	12	Attorney Docket Number	2943AAB-178-DIV

	213	2008/0005532	01/03/2008	Liao et al.	
	214	2008/0010218	01/10/2008	Zank	
	215	2008/0012690	01/17/2008	Friedrich	
	216	2008/0016363	01/17/2008	Lapstun et al.	
	217	2008/0014867	01/17/2008	Finn	
	218	2008/0032626	02/07/2008	Chen	
	219	2008/0037466	02/14/2008	Ngo et al.	
	220	2008/0046493	02/21/2008	Rosenberg	
	221	2008/0061941	03/13/2008	Fischer et al.	
	222	2008/0094171	04/24/2008	Sawhney	
	223	2008/0184349	07/31/2008	Ting	
	224	2008/0229400	09/18/2008	Burke	
	225	2009/0128392	05/21/2009	Hardacker et al.	
	226	2009/0153290	06/18/2009	Bierach	
	227	2009/0315673	12/24/2009	Huang	
	228	2010/0001840	01/17/2010	Kang et al.	

UNPUBLISHED U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-kind Code ² (if known)	Filing Date MM-DD-YYYY	Name of Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	229	13/689108	11/29/2012	Guthery et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document Country Code ³ , Number ⁴ , Kind Code ⁵ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
	230	CN 1307309	08/08/2001	BEIJING KERUIQI TECHNOLOGY DEV		(with English abstract)
	231	EP 0616429	09/21/1994	SIEMENS AG		(with English Abstract)
	232	EP 0697491	02/21/1996	NIPPON DENSO CO		
	233	EP 0843438	05/20/1998	THOMSON MULTIMEDIA SA		

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	8	of	12	Attorney Docket Number	2943AAAB-178-DIV

	234	EP 0872976	10/21/1998	UNITED TECHNOLOGIES AUTOMOTIVE		
	235	EP 0924894	06/23/1999	SIEMENS AG		(with English Abstract)
	236	EP 0949563	10/13/1999	LUCENT TECHNOLOGIES INC		
	237	EP 0956818	11/17/1999	CITICORP DEV CENTER		
	238	EP 0996928	05/03/2000	ASSURE SYSTEMS INC		
	239	EP 1148644	10/24/2001	COMM RES LAB MINISTRY OF PUBLI		
	240	EP 1251448	10/23/2002	TOO MNOGOPROFILNOE PREDPR		
	241	EP 1292882	03/19/2003	ANOTO AB		
	242	EP 1398691	03/17/2004	TOSHIBA KK		
	243	EP 1420542	05/19/2004	ST MICROELECTRONICS SRL		
	244	EP 1460573	09/22/2004	Nokia Corporation		
	245	EP 1643643	04/05/2006	MICRONAS GMBH		(with English translation)
	246	EP 1696360	08/30/2006	SAMSUNG ELECTRONICS CO LTD		
	247	EP 1043687	11/22/2006	CANON KK		
	248	GB 2256170	12/02/1992	BRANDES WILLIAM ROBERT		
	249	GB 2331825	06/02/1999	NEC CORP		
	250	JP 2002-261749	09/13/2002	MATSUSHITA ELECTRIC IND CO LTD		(with English abstract)
	251	KR 2002-0073716	09/28/2002	FIRSTECH INT INC		(with English abstract)

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	9	of	12	Attorney Docket Number	2943AAAB-178-DIV

	252	RU 2158444	10/27/2000	AJ DI SISTEMS INK		(with English abstract)
	253	RU 2195020	12/20/2002	MNOGOPROFIL NOE PRED OOO EHLSI		(with English abstract)
	254	WO 97/17683	05/15/1997	ID SYSTEMS INC		
	255	WO 99/56429	11/04/1999	IDENTIX INC		
	256	WO 01/013218	02/22/2001	Siemens Aktiengesellschaft		(with English Abstract)
	257	WO 01/13218	02/22/2001	SIEMENS AG		(with English Abstract)
	258	WO 01/18331	03/15/2001	Electec System Aktiebolag		
	259	WO 02/082367	10/17/2002	PITTHWAY CORP		
	260	WO 03/027832	04/03/2003	Intel Corporation		
	261	WO 03/042812	05/22/2003	Everbee Networks		(with English Abstract)
	262	WO 2004/010373	01/29/2004	BANQUE TEC INTERNAT PTY LTD		
	263	WO 04/010373	01/29/2004	Banque-Tec International Pty Ltd		
	264	WO 2004/039119	05/06/2004	Anzon Autodoor Limited		
	265	WO 2006/015625	08/09/2004	Telecom Italia S.P.A.		
	266	WO 05/001777	01/06/2005	SCM Microsystems GMBH		
	267	WO 2005/001777	01/06/2005	SCM MICROSYSTEMS GMBH		
	268	WO 2005/018137	02/24/2005	Securicom Pty Ltd		
	269	WO 2005/029315	03/31/2005	Globespanvirata Incorporated		
	270	WO 2005/038729	04/28/2005	SCM Microsystems, Inc.		
	271	WO 2006/032941	03/30/2006	Nokia Corporation		
	272	WO 2006/036521	04/06/2006	Qualcomm Incorporated		

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	10	of	12	Attorney Docket Number	2943AAAB-178-DIV

	273	WO 2006/126688	11/03/2006	NEC Corporation		(with English Abstract)
	274	WO 2006/123316	11/23/2006	KONINKL PHILIPS ELECTRONICS NV		
	275	WO 2007/094868	08/23/2007	MOJIX INC		
	276	WO 2007/103906	09/13/2007	Imagineer Software, Inc.		
	277	WO 2007/117315	10/18/2007	Symbol Technologies, Inc.		
	278	WO 2007/120215	10/25/2007	Imagineer Software, Inc.		
	279	WO 2008/001918	01/03/2008	Yui et al.		
	280	WO 2008/010441	01/24/2008	NEC Corporation		(with English Abstract)
	281	WO 2008/043125	04/17/2008	MICROLATCH PTY LTD		

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	282	"Access Control Standard for the 26-Bit Wiegand Reader Interface," Security Industry Association, October 17, 1996, 15 pages.	
	283	Anashin, V., "Uniformly distributed sequences over p-adic integers," Number Theoretic and Algebraic Methods in Computer Science, Moscow 1993 (A.J. van der Poorten, I.Shparlinski, and H.G. Zimmer eds., 1995), pp. 1-18, available at http://crypto.rsuh.ru/papers/anashin-paper1.pdf .	
	284	Anashin, V., "Pseudorandom number generation by p-adic ergodic transformations" (Jan. 29, 2004), available at http://arxiv.org/abs/cs.CR/0401030 .	
	285	Anashin, V., "Pseudorandom number generation by p-adic ergodic transformations: An addendum" (Feb. 26, 2004), pp. 1-9, available at http://arxiv.org/abs/cs.CR/0402060 .	
	286	ANASHIN "Non-Archimedean Ergodic Theory and Pseudorandom Generators," Oct. 07, 2007, 39 pages, available at http://arxiv.org/abs/0710.1418v1	
	287	Anashin, V., "Uniformly distributed sequences in computer algebra, or how to construct program generators of random numbers," J. Math. Sci., 89(4):1355-1390 (1998), available at http://crypto.rsuh.ru/papers/anashin-paper5.pdf .	
	288	Anashin, V., "Uniformly distributed sequences of p-adic integers," II. Discrete Math. Appl., 12(6):527-590 (2002), available at http://arXiv.org/abs/math.NT/0209407 .	
	289	Anashin, V., "Uniformly distributed sequences of p-adic integers," Mathematical Notes, 55(2):109-133 (1994), available at http://crypto.rsuh.ru/papers/anashin-paper2.pdf .	
Examiner Signature	Date Considered		

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	11	of	12	Attorney Docket Number	2943AAAB-178-DIV

290	BARKER, Cryptanalysis of Shift-Register Generated Stream Cipher Systems, Cryptographic Series No. 39, Aegean Park Press, 1984, Chapters 1-3, pages 1-38
291	BLUM, M. et al., "How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits," SIAM Journal on Computing, Nov. 1984, Vol. 13, No. 4, pp. 850-864.
292	BRIAN, M., "How Remote Entry Works," Howstuffworks.com, retrieved from http://auto.howstuffworks.com/remote-entry.htm , printed on May 19, 2005, copyright 2005, 8 pages.
293	"Condoplex - The World Leader in Developing Security and Communication Solutions," retrieved from http://web.archive.org/web/20040324112641/http://condoplexinc.com/ , publication date March 24, 2004, 1 page.
294	"Contactless Technology for Secure Physical Access: Technology and Standards Choices," Smart Card Alliance White Paper, October 2002, 36 pages.
295	DAMGARD, I., "On the Randomness of Legendre and Jacobi Sequences," Advances in Cryptology (Proceedings of Crypto '88), Lecture Notes in Computer Science (1990), pp. 163-172.
296	Data Sheet, "26 Bit Weigand Specifications," Essex Electronics Incorporated, April 1, 1998, 1 page.
297	Data Sheet, "Micro RWD EM4001 'Mag swipe' Decimal Output Version," IB Technology, May 3, 2005, pp. 1-8.
298	DAVIS, M., "Reader To Panel Authentication," Cartes 2005, Paris, France, Nov. 1, 2005, 33 pages.
299	GLASS, B., "DMCA Used In Garage Door Battle," Ziff Davis Media, retrieved from http://www.extremetech.com/print_article2/0,2533 on May 19, 2005 (Jan. 23, 2003), 1 page.
300	"Information Technology: Application Profile for Commercial Biometrical Physical Access Control," Project INCITS 1706-D, 2005, 16 pages.
301	KNEBELKAMP et al., "Latest Generation Technology for Immobilizer Systems," Texas Instruments, retrieved from www.ti.com/tiris on May 19, 2005, 11 pages.
302	LEVIN, L., "One Way Functions and Pseudorandom Generators," Combinatorica, Vol. 7(4) (1987), pp. 357-363.
303	Press Release, "Radio Frequency Identification (RFID) based immobilizer systems help to curb auto theft and reduce insurance costs," Texas Instruments, May 7, 1999, 2 pages.
304	"Technology Basics: Understanding Wiegand," HID Corporation, 2004, 5 pages.
305	WEINSTEIN, L., "DMCA: Ma Bell Would Be Proud," Wired News, Jan. 20, 2003, 27 pages.
306	Woodcock, F., et al., "p-Adic Chaos and Random Number Generation," Experimental Mathematics, Vol. 7(4), (1998), pp. 334-342.
307	KOBLITZ, N., p-Adic Number, p-Adic Analysis and Zeta Functions, Chapter 3, Building up Ω , Springer, New York, (1977), pages 52-74.
308	KUIPERS, et al., Uniform Distribution of Sequences, John Wiley & Sons (1974), 400 pages (Submitted in 3 Parts)

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	12	of	12	Attorney Docket Number	2943AAAB-178-DIV

	309	LUBY, M., Pseudorandomness and Cryptographic Applications, Princeton University Press (1996), pages ix-55
	310	Examiner's First Report for Australian Patent Application No. 2006203768, mailed November 20, 2009 (Atty. Ref. No. 2943-114-AU).
	311	Partial European Search Report for European Patent Application No. 06119388 (Atty File No. 2943-114-EP), dated January 10, 2007.
	312	European Search Report for European Patent Application No. 06119388, mailed Apr. 17, 2007 (Attorney Ref. No. 2943-114-PEP), 9 pages
	313	Official Action for European Patent Application No. 06119388, mailed Dec. 14, 2007 (Attorney Ref. No. 2943-114-PEP), 2 pages
	314	Written Opinion of the International Searching Authority for International (PCT) Patent Application No. PCT/US2009/053430 (Atty File No. 2943-178-PCT) mailed November 24, 2009.
	315	International Search Report for International (PCT) Patent Application No. PCT/US2009/053430 (Atty File No. 2943-178-PCT) mailed November 24, 2009.
	316	International Preliminary Report on Patentability for International (PCT) Patent Application No. PCT/US09/53430, mailed Feb. 24, 2011 (Attorney Ref. No. 2943-178-PCT)
	317	European Search Report and Opinion for European Patent Application No. EP09807178, dated Nov. 08, 2011 (Attorney's Ref. No. 2943-178-PEP) 6 pages
	318	Official Action for U.S. Patent Application No. 11/464,912, mailed Jun. 2, 2010 (Attorney Ref. No. 2943-114)
	319	Official Action for U.S. Patent Application No. 11/464,912, mailed Nov. 23, 2010 (Attorney Ref. No. 2943-114)
	320	Notice of Allowance for U.S. Patent Application No. 11/464,912, mailed Jan. 20, 2012 (Attorney's Ref. No. 2943-114) 5 pages
	321	Official Action for U.S. Patent Application No. 12/539,431, mailed Jan. 26, 2012 (Attorney's Ref. No. 2943-178) 7 pages
	322	Official Action for U.S. Patent Application No. 12/539,431, mailed Apr. 13, 2012 (Attorney's Ref. No. 2943-178) 13 pages
	323	Notice of Allowance for U.S. Patent Application No. 12/539,431, mailed Apr. 13, 2012 (Attorney's Ref. No. 2943-178) 13 pages

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Electronic Acknowledgement Receipt	
EFS ID:	15104867
Application Number:	13689088
International Application Number:	
Confirmation Number:	9927
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Scott B. Guthery
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Robert Roe-Pachirat
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943AAAB-178-DIV
Receipt Date:	04-MAR-2013
Filing Date:	29-NOV-2012
Time Stamp:	13:19:34
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	2943AAAB-114-EP_SR_04-17-2007.pdf	255573 b10abb800a38630434fabaf5343b792b28e8bfa	no	9

Warnings:

Information:

2	Non Patent Literature	2943AAAB-114-EP_OA_12-14-2007.pdf	91211 6c29bdce931e0b87405db17234f3cc565c184433	no	2
Warnings:					
Information:					
3		IDS_01.pdf	1058494 bb05825b9eceb5d88c4a303490c0096c9cd8e60d	yes	15
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	3	
	Information Disclosure Statement (IDS) Form (SB08)		4	15	
Warnings:					
Information:					
Total Files Size (in bytes):			1405278		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:)	Group Art Unit: 2431
Scott B. Guthery)	Confirmation No.: 9927
Serial No.: 13/689,088)	Examiner:
Filed: November 29, 2012)	
Atty. File No.: 2943AAAB-178-DIV)	<u>INFORMATION DISCLOSURE</u>
Entitled: "Secure Wiegand Communications")	<u>STATEMENT</u>
)	<i>Electronically Submitted</i>
)	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

The references cited on attached Form PTO/SB08 are being called to the attention of the Examiner.

☒ Copies of the cited non-patent and/or foreign references 312 and 313 are enclosed herewith.

☐ Copies of the cited U.S. patents and/or patent applications are enclosed herewith.

☒ Copies of the cited U.S. patents/unpublished patent applications/patent application publications are not enclosed in accordance with 37 C.F.R. § 1.98(a).

☒ Copies of the cited references 230 – 311 and 314 – 323 are not enclosed, in accordance with 37 C.F.R. § 1.98(d), because the references were cited by or submitted to the U.S. Patent and Trademark Office in prior application Serial No. 12/539,431 filed 08/11/09, which is relied upon for an earlier filing date under 35 U.S.C. § 120.

☒ To the best of applicants' belief, the pertinence of the foreign-language references is believed to be summarized in the attached English abstracts and/or in the figures, although applicants do not necessarily vouch for the accuracy of the translation.

☒ Examiner's attention is drawn to the following related applications:

- Serial No. 11/464,912 filed 08/16/06 now U.S. Patent No. 8,183,980 (Attorney's Ref. No. 2943AAAB-114)
- Serial No. 12/539,431 filed 08/11/09 now U.S. Patent No. 8,358,783 (Attorney's Ref. No. 2943AAAB-178)
- Serial No. 13/689,108 filed 11/29/12 (Attorney's Ref. No. 2943AAAB-178-DIV-2)
- Serial No. 12/002,145 filed 12/14/07 (Attorney's Ref. No. 2943AAAB-227)

☐ Other: _____

Submission of the above information is not intended as an admission that any item is citable under the statutes or rules to support a rejection, that any item disclosed represents analogous art, or that those skilled in the art would refer to or recognize the pertinence of any reference without the benefit of hindsight, nor should an inference be drawn as to the pertinence of the references based on the order in which they are presented. Submission of this statement should not be taken as an indication that a search has been conducted, or that no better art exists.

It is respectfully requested that the cited information be expressly considered during the prosecution of this application and the references made of record therein.

FEEES

<input checked="" type="checkbox"/>	<p>37 CFR 1.97(b): No fee is believed due in connection with this submission, because the information disclosure statement submitted herewith is satisfied by one of the following conditions ("X" indicates satisfaction):</p> <p><input type="checkbox"/> Within three months of the filing date of a national application other than a continued prosecution application under 37 CFR 1.53(d), or</p> <p><input type="checkbox"/> Within three months of the date of entry of the national stage as set forth in § 1.491 in an international application, or</p> <p><input checked="" type="checkbox"/> Before the mailing date of a first Office Action on the merits, or</p> <p><input type="checkbox"/> Before the mailing of a first Office action after the filing of a request for continued examination under 37 CFR 1.114.</p> <p>Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970.</p>
<input type="checkbox"/>	<p>37 CFR 1.97(c): The information disclosure statement transmitted herewith is being filed after all the above conditions (37 CFR 1.97(b)), but before the mailing date of any one of the following conditions:</p> <p>(1) a final action under 37 C.F.R. 1.113, or</p> <p>(2) a notice of allowance under 37 C.F.R. 1.311, or</p> <p>(3) an action that otherwise closes prosecution in the application.</p> <p>This Information Disclosure Statement is accompanied by:</p> <p><input type="checkbox"/> A Certification (below) as specified by 37 C.F.R. 1.97(e). Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970.</p> <p>OR</p> <p><input type="checkbox"/> Please charge Deposit Account 19-1970 in the amount of \$180.00 for the fee set forth in 37 C.F.R. 1.17(p) for submission of an information disclosure statement. Please credit any overpayment or charge any underpayment to Deposit Account 19-1970.</p>
<input type="checkbox"/>	<p>37 CFR 1.97(d): This Information Disclosure Statement is being submitted after the period specified in 37 CFR 1.97(c).</p> <p><input type="checkbox"/> This information Disclosure Statement includes a Certification (below) as specified by 37 C.F.R. 1.97(e)</p> <p>AND</p> <p><input type="checkbox"/> Applicants hereby requests consideration of the reference(s) disclosed herein. Please charge Deposit Account 19-1970 in the amount of \$180.00 under 37 C.F.R. 1.17(p). Please credit any overpayment or charge any underpayment to Deposit Account 19-1970. Election to pay the fee should not be taken as an indication that applicant(s) cannot execute a certification.</p>

Certification (37 C.F.R. 1.97(e))
(Applicable only if checked)

- ☐ The undersigned certifies that:
- ☐ Each item of information contained in this information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(1).
 - ☐ A copy of the communication from the foreign patent office is enclosed.


OR

- ☐ No item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in 37 C.F.R. 1.56(c) more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(2).

Respectfully submitted,

SHERIDAN ROSS P.C.

By:



Matthew R. Ellsworth
Registration No. 56345
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: March 7, 2013



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/689,088	11/29/2012	Scott B. Guthery	2943AAAB-178-DIV

CONFIRMATION NO. 9927

22442
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

PUBLICATION NOTICE



OC000000061099477

Title: SECURE WIEGAND COMMUNICATIONS

Publication No. US-2013-0117827-A1

Publication Date: 05/09/2013

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publicly available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <http://pair.uspto.gov/>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	1	of	2	Attorney Docket Number	2943AAAB-178-DIV

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	6084977	07/04/2000	Borza	
	2	6587032	07/01/2003	Armingaud	
	3	7771334	08/10/2010	Bailey et al.	
	4	8138923	03/20/2012	Grunwald et al.	
	5	8312540	11/13/2012	Kahn et al.	
	6	2002/0078381	06/20/2002	Farley et al.	
	7	2005/0216955	09/29/2005	Wilkins et al.	
	8	2008/0072283	03/20/2008	Relyea et al.	
	9	2009/0066509	03/12/2009	Jernstrom et al.	
	10	2010/0039220	02/18/2010	Davis	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document Country Code ³ ; Number ⁴ ; Kind Code ⁵ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
	11	EP 1209551	05/29/2002	IBM		
	12	EP 1418484	05/12/2004	Stonesoft Corp.		
	13	WO 2005/038633	04/28/2005	Vodafone Holding GMBH		(English Abstract)

NON-PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	14	Partial European Search Report for European Patent Application No. 09167708.8, mailed Dec. 4, 2009 (Atty. Ref. No. 2943-184-EP)
	15	Official Communication for European Patent Application No. 09167708.8, dated Jun. 16, 2010 (Attorney Ref. No. 2943-184-EP)
	16	Notice of Allowance for U.S. Patent Application No. 12/539,431, mailed Aug. 31, 2012 (Attorney's Ref. No. 2943-178) 8 pages

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	2	of	2	Attorney Docket Number	2943AAAB-178-DIV

	17	Official Action for U.S. Patent Application No. 12/541,480, mailed Jun. 14, 2012 (Attorney's Ref. No. 2943AAAB-184) 14 pages
	18	Official Action for U.S. Patent Application No. 12/541,480, mailed Feb. 11, 2013 (Attorney's Ref. No. 2943AAAB-184) 20 pages

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 1 209 551 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
29.05.2002 Bulletin 2002/22

(51) Int Cl.7: **G06F 1/00**

(21) Application number: **01480085.8**

(22) Date of filing: **13.09.2001**

(84) Designated Contracting States:
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR**
Designated Extension States:
AL LT LV MK RO SI

(72) Inventor: **Armingaud, François-Dominique,
Gilles**
75012 Paris (FR)

(30) Priority: **28.11.2000 EP 00480107**

(74) Representative: **de Pena, Alain**
Compagnie IBM France
Département de la Propriété Intellectuelle
06610 La Gaude (FR)

(71) Applicant: **INTERNATIONAL BUSINESS
MACHINES CORPORATION**
Armonk, NY 10504 (US)

(54) **System and method of preventing unauthorized access to computer resources**

(57) A stealth system and method that allows a resource to be practically invulnerable to fast online brute-force attacks is disclosed. The method for controlling access to a computer resource consists in performing a user authentication procedure upon receiving a request from a user to access the computer resource. Then, a password verification procedure is executed when said user request is granted. The verification procedure comprises the steps of requesting a password to the user, and comparing the entered password to an expected valid one. The next steps are to compute the number of ungranted access for the user during a predefined time interval N if the password match the expected one, and to grant access to the user only if the computed number is lower than a predetermined number K of authorized requests. Otherwise, if either the password does not match the expected one or the number of unsuccessful attempts to log is higher than the predetermined number, the access is denied to the user and a time stamp of the ungranted access is stored.

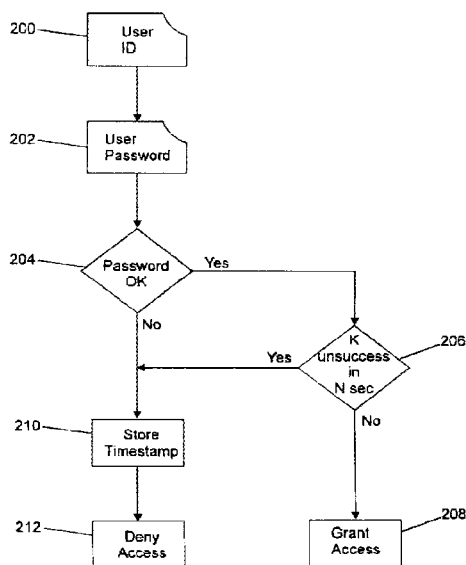


FIG.2

EP 1 209 551 A2

Description

Field of the Invention

[0001] The present invention relates to computer security and more particularly to an undetectable system and method forbidding unauthorized access to a computer resource, even when the right password is supplied by chance.

Background of the Invention

[0002] Passwords have been used for more than 40 years to restrict access of certain computer operations to a set of given authorized users. However, with the generalization of the World Wide Web and the Internet connections, it becomes frequent for a home site to be probed by hackers 3 or 4 times a day. A well-known site may be probed more than 1000 times a day. While there are 456,976 possible 6-letters passwords if only alphabetic characters in the same case are used, trying 1000 passwords a day on each of 1000 accounts would give statistically in such a case a reasonable chance to crack one password on one account every day.

[0003] In order to prevent a hacker to try all possible passwords at computer speed, two measures are generally used, either separately or in conjunction :

1. locking the user's account when more than N incorrect passwords have been supplied. Only a system administrator will then be able to unlock the account once it is locked;
2. increasing the system response delay for a user every time an incorrect password is given for that user. It is worth noting that if the delay is initially set to 1 second and doubled for every invalid attempt, the delay will be of 4,096 seconds - more than one hour - after the 12th invalid password has been supplied, which is an unbearable time for the average hacker.

[0004] But both these solutions have drawbacks, because they stay in effect after the attack is over. This allows the hackers a very easy way to induce a denial of service by saturating the system's wrong password tolerance threshold while not saturating the machine. As for example, a disgruntled employee or ex-employee could efficiently and repeatedly paralyze a whole service in a matter of minutes if he knows the list of user ids of his ex-colleagues.

[0005] U.S. Pat. N°5,559,505 issued to McNair E. Bruce on September 24, 1996 and entitled "Security system providing lockout for invalid access attempts" discloses a system for controlling access to a resource to operate such that when an attempt to access a resource using a password fails, the time interval that must elapse before a subsequent attempt at access can be successful is incremented. And by making the incre-

ments increasingly large, repeated access attempts by hackers or unauthorized users is discouraged. This solution offers an enhancement to previous point 2 by also decreasing in relatively small decrements the wait time for each successful password. Such approach aims to be "a better compromise between access control and denial" as mentioned in the description.

[0006] However, none of the prior art techniques teach, claim or even suggest a method where no information whatsoever would be provided by the system to the hacker. Such a 'silent' method, in complete opposition with previous approaches, should not provide any information useful for a hacker to detect the right password, even by a careful analysis of response times. Ideally, even a careful analysis by the hacker of unsuccessfully used passwords should be useless; indeed, the method will be almost perfect if the right password has most chances to be crossed out by the hacker as being invalid, and thus not to be tried by him/her anymore.

[0007] Accordingly, we claim to provide here a new and utterly different method which eliminates the aforementioned problems and implements a stealth solution.

Summary of the Invention

[0008] The object of the present invention is to provide a method allowing a resource to be practically invulnerable to fast online brute-force attacks. The resource may be any file server, data base, computing resource, web server or any other resource using a password protection scheme, either alone or in conjunction with other protection methods.

[0009] Another object of the invention is to deprive an hacker from any information required in order to make an efficient so-called "slow attack". A "slow attack" tries only the maximum number of allowed passwords minus one, but do it every day for every known user id, many weeks in sequence.

[0010] Another object of the present invention to offer a stealth protection method which lets any unauthorized user ignoring that the right password has been tried, or even that a protection system - other than the password, of course - is present.

[0011] It is yet another object of the invention to provide a method wherein neither the hacker nor the user will be slowed down.

[0012] Moreover, security is even based on the fact that the attacker will operate his attempts at the fastest speed he/she can, consistent or not with the idea that the real user is trying to log on - for instance through the use of a program trying different passwords at computer speed. In fact, the fastest his attempts, the better the security, and the greater the probability that he will be denied access even when, by pure chance, he/she is using the right password, and will never know it.

[0013] In a preferred embodiment, a method for controlling access to a computer resource consists in performing a user authentication procedure upon receiving

a request from a user to access the computer resource. Then, a password verification procedure is executed when said user request is granted. The verification procedure comprises the steps of requesting a password to the user, and comparing the entered password to an expected valid one. The next steps are to check the number of rejected access attempts for that user during a predefined time interval N if the given password matches the expected one and to grant access to the user only if the computed number is lower than a predetermined number K of authorized requests. Otherwise, if either the password does not match the expected one or the number of unsuccessful attempts to log is higher than the predetermined number, the access is denied to the user and a new time stamp of the ungranted access is stored.

[0014] The novel features believed to be characteristic of this invention are set forth in the appended claims. The invention itself, however, as well as these and other related objects and advantages thereof, will be best understood by reference to the following detailed description to be read in conjunction with the accompanying drawings.

Brief Description of the Drawings

[0015]

- Figure 1** is a flow chart of a prior art login sequence.
Figure 2 is a flow chart of the login sequence of the present invention.
Figure 3 shows a preferred implementation of a time stamp memory structure of the present invention.

Detailed Description of the Preferred Embodiment

[0016] The method of the present invention may be summarized as follows : a sliding time window is first chosen having a size N preferably expressed in seconds, and a number K of acceptable logon attempts within this sliding window is determined. In a preferred embodiment N is equal to 3600 seconds and K is equal to 3.

[0017] Any attempt to log in more than K times within the sliding window will result for the user (authorized or not) in a received message of the type "INVALID PASSWORD" even if the right password has been supplied. It is the main point of this invention that the hacker gets exactly the same message whether the password is right or wrong. In that way, he/she will normally cross out that password in his list in order to never try it again.

[0018] To complete this fundamental idea, one has to make sure that the hacker will never have any opportunity to try all possible passwords. If the typical size of a password is 6 case-sensitive alphanumeric characters, one has to make sure that there will be no way to try all the corresponding passwords ($62^6 = \text{about } 56 \text{ billion}$)

in a typical maximum reasonable password lifetime (say 1 year). Thus, 56 billion divided by 365 days of 24 hours would mean a rate of 1800 passwords per seconds, which is a very unlikely value for a human user. However, such unlikely attempts can be discouraged either :

- by requiring a minimum delay between two attempts, the minimum delay being compatible with human operation (two seconds for example), and rejecting his attempt otherwise. While being quite plausible in any context, this kind of message does not give the hacker any hint about the scheme use by the present invention,

or

- by enforcing a minimum delay (a two-second delay) plus or minus a random time by a programmed delay in the system, which can create the illusion that such a time is a consequence of system load. Here again, no hint is given to the hacker about the proposed scheme.

[0019] The minimum delay is an option to secure that the hacker will never have a chance to try all the passwords and thereby guess the method of the invention. However, the primary point is that in the given sliding window condition, even using the valid password results in an "Invalid password" type error message.

[0020] While a 2-seconds delay is quite acceptable for manual connections, it may be considered excessive for frequent automated operations when the context does not suggest that any attack is in progress and/or in a context where the sensitivity of data is classified as medium. In such a case, one can consider activating the 2-seconds (or any other value) delay only in an identified attack context. This will be described in detail below.

[0021] Referring now to figure 1, a basic general process for a user wanting to log a resource is shown.

[0022] On a first step 100, the system is asking for the user's name or ID. On some systems, such as the VM/CMS or TSO ones, the existence of this name is checked immediately. On others systems, like the UNIX family, this verification is deferred until the password has been entered. The present method is not linked to any particular condition of this verification.

[0023] On step 102, the system is asking for the user's password. Generally this sequence is not echoed, or not echoed as typed, for security reasons.

[0024] On next step 104, the system checks that the right password has been typed for that user if this user exists.

[0025] If the match is OK (branch YES) access is granted on step 106.

[0026] Otherwise, on step 108 the access is denied. Some systems will increase a counter in such a case allow locking the account should too many invalid log-ons be attempted.

[0027] Referring now to figure 2, the process of the present invention is now described.

[0028] On first step 200, the system asks a user willing to access a resource to type his user's name or ID. The user here can refer either to a human user or to a client computer (in which case the "user's name" may refer to a class of service rather than to a given computer ID).

[0029] On next step 202, the system asks for the user's password. This password may be seen as a given sequence of ASCII characters, printable or not. It will be either stored in a memory part of the solicited resource computer or computed from a random string issued by that computer together with the logon prompt (a "challenge/answer" password).

[0030] On next step 204, the system checks if the password matches an expected sequence. This operation is not detailed here as it is not required for the understanding of the present invention, but the skill man could refer to any known method, such as simply comparing the entered password to an existing list of valid passwords.

[0031] If the password does not match the expected sequence (branch NO), the process enters step 210 which is detailed herein below.

[0032] If the password matches the expected sequence (branch YES), a test is performed on step 206 to determine if more than K unsuccessful logons were attempted during the N last seconds. It is readily obvious that any other kind of time unit can be used, but second is generally the one used.

[0033] If no more than K unsuccessful logons were attempted during the N last seconds, access is granted on step 208. Nevertheless, the user will never be aware of the existence of the test performed on step 206.

[0034] If at least K unsuccessful logons were attempted during the last N seconds (branch YES of step 206)), then the system operates exactly the same as if the password did not match (branch NO of step 204) and the process enters step 210. It is important to note that this is the core point of the present invention, and the one which makes this method a really "stealth" one.

[0035] On step 210, whether being the result of step 204 (branch NO) or of step 206 (branch YES), a time stamp is memorized in a data structure of the resource computer able to memorized K latest unsuccessful logon attempts. In a preferred implementation, a circular buffer is used as the memory structure, but the skill man may easily devise another type of predefined class depending on which programming language is used.

[0036] As already explained, in another embodiment, the method may be enforced by the addition of a security delay. Depending on the relative importance of operation performance vs. the desired "stealthness", the security delay can be applied:

1. both for branch NO of step 204 and branch YES of step 206 which reflect a maximum stealthness with a slightly reduced performance;

2. only for branch YES of step 206 which reflect a maximum performance with a slightly reduced stealthness;

3. at the next logon time by permuting steps 204 and 206 in order to achieve both a maximum stealthness and a maximum performance when no attack is in progress. However, this option is at the expense of some extra programming to implement it in the existing logon procedures.

[0037] Finally, on step 212, access is denied with the very same error message than if the match had failed in step 204.

[0038] Figure 3 illustrates a preferred implementation of a data structure 300 to store the time stamp list of a given user. The memory 300 is a circular buffer comprising a set of at least K memory cells (300-1 to 300-k), each of which containing a time stamp (T1 to Tk). The process of the invention needs to access efficiently the Kth oldest time stamp 'Tk' at each logon, as well as to insert the current time stamp 'T1' as being the most recent one at each failed logon. The insertion of the present time stamp shifts all the others except the Kth one which is deleted.

[0039] In the preferred implementation, 'K' is chosen to be a power of 2 : in that case, a contiguous block of memory is sufficient and the "circular linking" between the memory cells is implemented by incrementing an offset and applying a binary mask to it.

[0040] However, if 'K' is not a power of 2, the binary mask can be replaced by an arithmetic modulus (mod K) operation. Alternately, a circular list may also be used.

Claims

1. A method for controlling access to a computer resource comprising the steps of:

(a) performing a user authentication procedure upon receiving a request from a user to access the computer resource (200); and

(b) performing a password verification procedure when said user request is granted, said verification procedure comprising the steps of:

(b1) requesting (202) a password to the user;

(b2) comparing (204) said password to an expected valid password ;

(c1) if said password match, computing (206) the number of ungranted access for said user during a predefined time interval

N, and

(c2) granting access (208) to said user only if said number is lower than a predetermined number K of unauthorized requests; otherwise

5

(c3) denying access (212) to said user, and storing (210) a time stamp of the ungranted access;

10

(b3) if said password does not match, denying access (212) to said user, and storing (210) a time stamp of the ungranted access.

15

2. The method of claim 1 wherein the user request (step c2) is granted after the password request (step b1).
3. The method of claim 1 or 2 wherein the user is a client computer and the computer resource is a server computer.
4. The method of claim 3 wherein the computer resource is a web server.
5. The method of anyone of claims 1 to 4 wherein the step (206) of computing the number of ungranted access is performed before the step (204) of comparing the user password.
6. The method of anyone of claims 1 to 5 wherein the number K of unauthorized requests is a power of 2.
7. The method of anyone of claims 1 to 6 further comprising a step of performing a second password verification procedure after said step 212 of denying access to said user.
8. The method of claim 7 wherein the step of performing the second password verification procedure is executed after a minimum security delay.
9. The method of claim 8 wherein said minimum delay is equal to 2 seconds.
10. A system comprising means adapted for carrying out the method according to anyone of claims 1 to 9.
11. A computer-like readable medium comprising instructions for carrying out the steps of the method of anyone of claims 1 to 9.

20

25

30

35

40

45

50

55

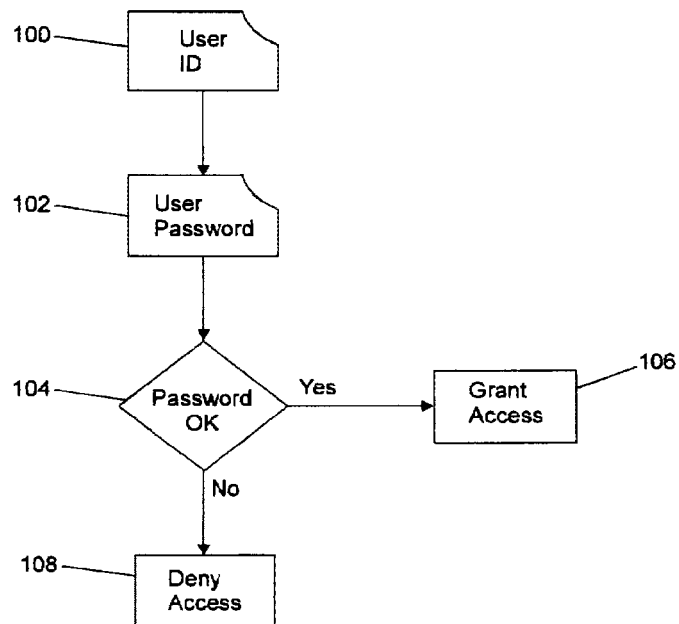


FIG.1

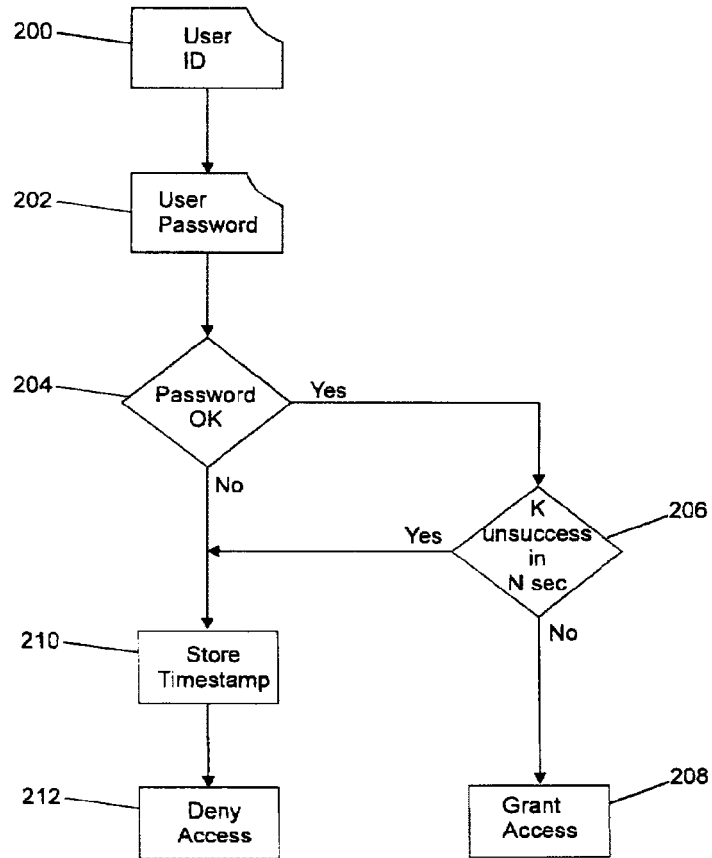


FIG.2

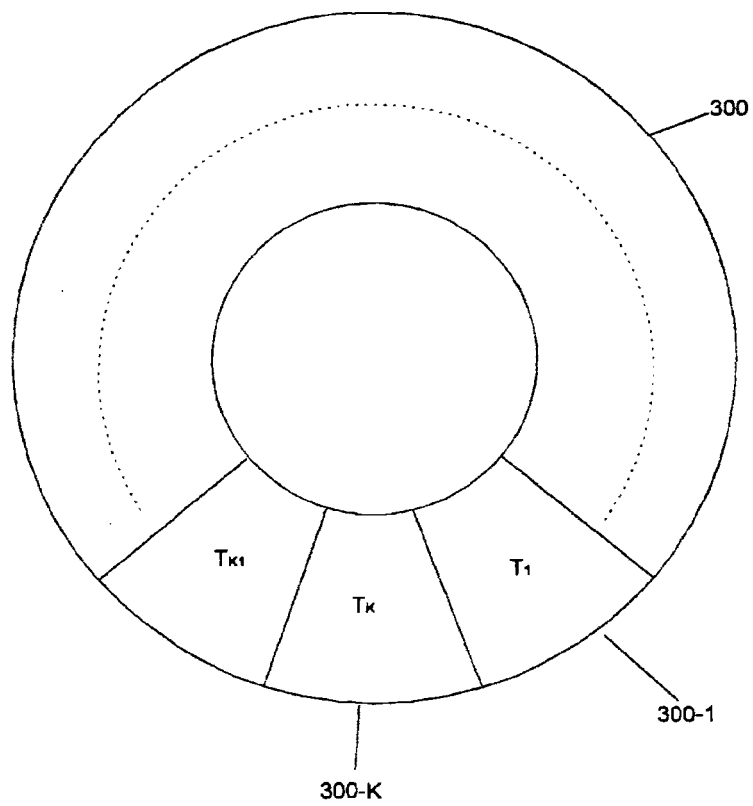


FIG.3

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 1 418 484 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
12.05.2004 Bulletin 2004/20

(51) Int Cl.7: **G06F 1/00**

(21) Application number: **03104056.1**

(22) Date of filing: **03.11.2003**

(84) Designated Contracting States:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IT LI LU MC NL PT RO SE SI SK TR**
Designated Extension States:
AL LT LV MK

(72) Inventor: **Nurmela, Kari**
02230, Espoo (FI)

(74) Representative: **Äkräs, Tapio Juhani**
Kolster Oy Ab, P.O. Box 148,
Iso Roobertinkatu 23
00121 Helsinki (FI)

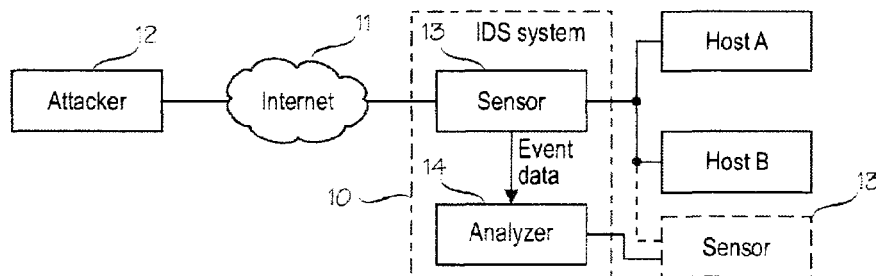
(30) Priority: **07.11.2002 US 289449**

(71) Applicant: **Stonesoft Corporation**
00210 Helsinki (FI)

(54) Event sequence detection

(57) The invention relates to event sequence detection suitable for an intrusion detection system (IDS), for example. An event sequence including two or more stages in order, each of the stages including one or more events, is defined. Also defined is a filtering function for each of the stages, each filtering function providing a TRUE indication, when one of the events belonging to the respective event is received, and a FALSE indication otherwise. Still further at least one binding function for each of the stages is defined such that a pair of binding

functions in two successive stages links the events in these two successive stages. Received event data is continuously evaluated with the filtering functions. When the evaluation results in a TRUE indication from one of the filter functions, at least one key value is derived from the received event data by the corresponding at least one binding function. Finally, it is determined that the sequence has been detected, when a TRUE indication has been obtained in each stage in a timely order and the derived key values link the detected events in the successive stages.

Fig. 1

Description

FIELD OF THE INVENTION

5 **[0001]** The present invention relates to event sequence detection for example in an intrusion detection system (IDS).

BACKGROUND OF THE INVENTION

10 **[0002]** Intrusion detection system (IDS) is a type of security management system for computers and networks. An IDS system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses *vulnerability assessment* (sometimes referred to as *scanning*), which is a technology developed to assess the security of a computer system or network.

15 **[0003]** Intrusion detection functions include:

- Monitoring and analyzing both user and system activities,
- Analyzing system configurations and vulnerabilities,
- Assessing system and file integrity,
- Ability to recognize patterns typical of attacks,
- 20 - Analysis of abnormal activity patterns, and
- Tracking user policy violations.

25 **[0004]** An IDS system is configured to generate an alarm, when an event, which is considered to be malicious, is detected. In order to decrease the amount of false positives in the event detection, correlation of the events may be taken into account. That is, also the context in which an event is detected may have an effect on whether the event is classified suspicious or not.

30 **[0005]** US Patent Application 2002/0078381, "Method and System for Managing Computer Security Information", presents one solution for real-time event sequence detection. Therein, a fusion engine "fuses" event information from multiple data sources and analyzes this information in order to detect relationships between the events that may indicate malicious behavior. According to the method presented, event data are classified into different event type categories and a ranking is assigned to each event. Then relationships between events are identified and on the basis of the relationships a mature correlation event, indicating that malicious behavior has been detected, is generated. Nevertheless, the document does not teach a specific technique for identifying the relationships nor does it provide effective way to implement event sequence detection.

SUMMARY OF THE INVENTION

35 **[0006]** Object of the invention is to provide another solution for detecting event sequences in the context of identifying intrusion attempts.

40 **[0007]** This is achieved with an invention defined in the attached independent claims. Embodiments of the invention are defined in the dependent claims.

45 **[0008]** The idea of the invention is to identify event sequences by detecting a common parameter in two or more events.

50 **[0009]** An aspect of the invention is an event sequence detection method, comprising
 defining an event sequence including two or more stages in order, each of the stages including one or more events,
 defining a filtering function for each of said stages, each filtering function providing a TRUE indication, when one of the events belonging to the respective event is received, and a FALSE indication otherwise,
 defining at least one binding function for each of the stages such that a pair of binding functions in two successive stages links the events in these two successive stages,
 continuously receiving event data,
 continuously evaluating the received event data with the filtering functions,
 when the evaluation results in a TRUE indication from one of the filter functions, deriving at least one key value from the received event data by the corresponding at least one binding function,
 determining that said sequence has been detected, when a TRUE indication has been obtained in each stage
 55 in a timely order and the derived key values link the detected events in the successive stages.

60 **[0010]** Another aspect of the invention is an event sequence detection method, comprising
 defining an event sequence including two or more stages in order, each of the stages including one or more events,
 defining a filtering function for each of said stages, each filtering function providing a TRUE indication, when one

of the events belonging to the respective event is received, and a FALSE indication otherwise,

evaluating the filtering functions with the event data,

if the filtering function of the one of the stages evaluates to TRUE, a binding function associated with the respective stage is evaluated for extracting a first key from the event data,

5 if the stage, which evaluates to TRUE, is the first stage, it is checked whether the event and the first key already exist in a table associated with the first stage, and the if checking result is negative, the event and the first key are added to the table,

10 if the stage, which evaluates to TRUE, is some other than the first stage, it is checked, whether there is an entry with the first key in the table of the previous stage, if the checking result is negative, nothing is done, and if the checking result is confirmative, another binding function associated with the current stage is evaluated for extracting a second key from the event data and the table associated with the current stage is checked for whether the event and the second key do exist in the table, and if the latter checking result is negative, the event and the second key are added to the table,

15 if the stage, which evaluates to TRUE, is the last stage, it is checked, whether there is an entry with the first key in the table of the previous stage, and if the checking result is negative, nothing is done, and if the checking result is confirmative, it is determined that a sequence of events has been detected.

[0011] A further aspect of the invention is an event sequence detection method, comprising

defining an event sequence including two or more events,

20 defining a filtering function and an associated binding function for each event, each filtering function providing a TRUE indication, when the respective event is received, and a FALSE indication otherwise,

continuously receiving event data,

continuously evaluating the received event data with the filtering functions,

25 each time when the evaluation results in a TRUE indication from one of the filter functions, registering the corresponding event and a key value derived from the received event data by the corresponding binding function,

determining the event sequence as detected, if all events of the event sequence with mutually matching key values are registered.

[0012] A further aspect of the invention is an event sequence detection method, comprising

defining an event sequence including two or more stages, each of the stages including one or more events,

30 defining a filtering function for each of said stages, each filtering function providing a TRUE indication, when one of the events belonging to the respective event is received, and a FALSE indication otherwise,

evaluating the filtering functions with the event data,

if the filtering function of the one of the stages evaluates to TRUE, a binding function associated with the respective stage is evaluated for extracting a key from the event data,

35 checking whether the key already exists in a table associated with the set of stages,

if the key is not found in the table, the event with the key is added to the table,

if the key is found in the table, it is checked whether an event for the current stage is already recorded for the key,

if no event for the current stage is already recorded for the key, the event is added to the table in connection with the key and the current stage,

checking whether the key has an event recorded for each stage, and

40 if the key has an event recorded for each stage, determining that the event sequence has been detected.

[0013] A further aspect of the invention is an event sequence detection method, comprising

defining an event sequence including two or more stages, each of the stages including one or more events,

45 defining a filtering function for each of said stages, each filtering function providing a TRUE indication, when one of the events belonging to the respective event is received, and a FALSE indication otherwise,

evaluating the filtering functions with the event data,

if the filtering function of the one of the stages evaluates to TRUE, a binding function associated with the respective stage is evaluated for extracting a key from the event data,

checking whether the key already exists in a table associated with the set of stages,

if the key is not found in the table, the event with the key is added to the table,

50 if the key is found in the table, it is checked whether an event for the current stage is already recorded for the key,

if no event for the current stage is already recorded for the key, the event is added to the table in connection with the key and the current stage,

if an event for the current stage is already recorded for the key, incrementing the number of events with this key and stage,

55 checking whether the key has a predetermined number of events recorded for each stage, and

if the key has a predetermined number of events recorded for each stage, determining that the event sequence has been detected.

[0014] A further aspect of the invention is an event sequence detector block for execution by a processor in a data

communications network environment, comprising:

a computer readable memory, and
a routine stored on a the computer readable memory and adapted to be implemented on the processor, wherein
the routine:

has a predefined event sequence including two or more stages in order, each of the stages including one or more events,
has a predefined filtering function for each of said stages, each filtering function providing a TRUE indication, when one of the events belonging to the respective event is received, and a FALSE indication otherwise,
has at least one predefined binding function for each of the stages such that a pair of binding functions in two successive stages links the events in these two successive stages,
continuously receives event data,
continuously evaluates the received event data with the filtering functions,
when the evaluation results in a TRUE indication from one of the filter functions, derives at least one key value from the received event data by the corresponding at least one binding function,
determines that said sequence has been detected, when a TRUE indication has been obtained in each stage in a timely order and the derived key values link the detected events in the successive stages.

[0015] A further aspect of the invention is an event sequence detector block for execution by a processor in a data communications network environment, comprising:

a computer readable memory, and
a routine stored on a the computer readable memory and adapted to be implemented on the processor, wherein
the routine:

has a predefined event sequence including two or more events,
has a predefined filtering function and an associated binding function for each event, each filtering function providing a TRUE indication, when the respective event is received, and a FALSE indication otherwise,
continuously receives event data,
continuously evaluates the received event data with the filtering functions,
each time when the evaluation results in a TRUE indication from one of the filter functions, registers the corresponding event and a key value derived from the received event data by the corresponding binding function,
determines the event sequence as detected, if all events of the event sequence with mutually matching key values are registered.

[0016] A further aspect of the invention is a computer readable storage medium comprising a computer program that carries out any one of the methods of the invention when executed by a computer.

[0017] A further aspect of the invention is a computer program that carries out any one of the methods of the invention when executed by a computer.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018]

Figure 1 shows an illustrative operating environment for an IDS system,
Figure 2 is a flow diagram illustrating an event sequence detection according to an embodiment of the invention, and
Figure 3 is a flow diagram illustrating an event sequence detection according to another embodiment of the invention.

DETAILED DESCRIPTION

[0019] The present invention may be embodied in program modules that run in a computing device, such as on a workstation, a personal computer, a server, or a special purpose appliance, having a processor and a memory and being connected to a data network or system to be monitored. The data network may be a fixed line network or a wireless network. The present invention may be embodied as a part of an intrusion detection system (IDS).

[0020] Intrusion detection system (IDS) is a type of security management system for computers and networks. An IDS system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within

the organization). An illustrative operating environment for an IDS system in a very simplified configuration is shown in Figure 1. The IDS system 10 is providing security functions for host servers A and B within a local network of the organization. An attacker 12 located outside the organization attempts to attack to the host A or B over the Internet 11. The IDS system may include one or more sensors 13 that notify when significant events occur that relate to the sensor's operation. The sensors can be located at any locations in the network where the system operation and traffic shall be monitored. There may various types of events that may be reported by the sensor. The events may include status messages about normal system operation. The events may also include various error and warning messages. Examples of suitable sensors include Real-Secure Network Sensor 6.5 and 7.0 from Internet Security Systems Inc (ISS), Atlanta, GA. It should be appreciated, however, that the details of the sensors, or other sources of the event data, and the specific type of the event data a p-plied by the present invention are not essential to the present invention. It is only necessary that event data is available for the event sequence detection according to the invention.

[0021] The IDS system may further include an analyzer or detector 14 that may contain the event sequence detection according to the invention. The analyzer 14 may be located on the workstation or the console of the network security personnel, for example, or alternatively at any other device or location in the network. The IDS system may further include several analysers.

[0022] An IDS system is configured to generate an alarm, when an event, which is considered to be malicious, is detected. In order to decrease the amount of false positives in the event detection, correlation of the events may be taken into account. That is, also the context in which an event is detected may have an effect on whether the event is classified suspicious or not. Event sequence detection is an important tool when trying to find out whether an attack was successful or not, and in detecting complex attack scenarios.

Event sequence detection

[0023] This section gives a formal definition of an event sequence detection according to the present invention.

[0024] The analyzer 14 receives event data or, more generally, events. Events may be received from multiple sources, such as the sensors 13. These events can contain arbitrary data, for example timestamp of the event, the situation identifier that caused generating that event record, etc. Let the sequence of events received by the analyzer 14 be E .

[0025] In accordance with the present invention, a set of filters (denoted by f_1, f_2, \dots) is provided. The filters are computable functions whose domain is the set of all events e and the range is the set $\{TRUE, FALSE\}$. That is, for each event $e \in E$ a filter f evaluates to TRUE, denoted by $f(e) = TRUE$, (i.e. the event can pass through the filter), or to FALSE, denoted by $f(e) = FALSE$ (i.e. the event is blocked by the filter). In principle a filtering function checks, if some parts of the event data match to the values or value ranges set for the function. In general level, a filtering function may be a rule to which event data is compared.

[0026] The time information, such as a timestamp of an event e is denoted by $t(e)$. For simplicity we assume that the events are received in the order defined by their timestamps or other time information. Below will be described an embodiment that processes the events in the order of receiving, neglecting the timestamps. However, in a further embodiment the analyzer can be used to sort the events in the order of increasing timestamps, if they are received in a slightly permuted order.

[0027] The last concept needed to define the event sequence detection according to the present invention is a binding function. Binding functions are denoted by $b_{x,y}^x$ or $b_{x,y}^y$, where x and y are positive integers and $x < y$. For any pair of events in the sequence, x stands for an earlier event and y for the later event (or stage as described in some embodiments below). In a special case used in the embodiments and examples below, for each binding function, it is required that $x=n-1$ and $y=n$. This means that the binding functions link two immediately consecutive events or stages. The domain of a binding function is the set of events and the range of a binding function is the set of sequences of octets (or bytes), derived or extracted or computed from the argument event. In principle, a binding function is used for finding event data pairs for which some part of a first event data has the same value than some other part of a second event data. More than one part of event data can be included in one binding function, and the parts, which are checked, may as well be the same in both events.

[0028] According to an embodiment of the present invention, an event sequence of n events is detected from the received events if and only if there exist events $e_1, e_2, \dots, e_n \in E$ such that all the following conditions are fulfilled:

- $t(e_1) < t(e_2) < \dots < t(e_n)$
- $f_1(e_1) = f_2(e_2) = \dots = f_n(e_n) = TRUE$
- $b_{1,2}^1(e_1) = b_{1,2}^2(e_2), b_{2,3}^2(e_2) = b_{2,3}^3(e_3), \dots, \text{ AND } b_{n-1,n}^{n-1}(e_{n-1}) = b_{n-1,n}^n(e_n)$
- $t(e_n) - t(e_1) \leq \text{TIME WINDOW SIZE}$

[0029] In this embodiment the binding functions links two consecutive events or stages. For example, the binding

functions $b_{1,2}^1(e_1) = b_{1,2}^2(e_2)$ are linking the first ($x=1$) and second ($y=2$) events or stages. Similarly, the binding functions $b_{2,3}^2(e_2) = b_{2,3}^3(e_3)$ are linking the second ($x=2$) and the third ($y=3$) events or stages. Thus, the intermediate events or stages have two binding functions, one for an earlier event or stage and one for later event or stage.

[0030] It is also possible to allow more general binding function conditions, but then the implementation will be more complex and the processing slower than the one required for the embodiment described above. An example of more general binding function conditions is that the binding function is linking also other than immediately neighbouring events or stages. For example, $b_{1,3}^1(e_1) = b_{1,3}^3(e_3)$ links events or stages 1 and 3.

Event group detection

[0031] If the events can arrive slightly out of order, and there is no reliable time stamp information available, the previously described method of detecting event sequences becomes less useful. Alternatively, it is possible that the order of the events may be irrelevant from the analyser point of view. In the following it is illustrated how to detect unordered event groups by modifying some parts of the event sequence detection algorithm described above. In an embodiment of the invention, we can modify the sequence detection conditions described above as follows:

[0032] An event group of n events is detected from the received events if, and only if, there exist events $e_1, e_2, \dots, e_n \in E$ such that all the following conditions are fulfilled:

- $f_1(e_1) = f_2(e_2) = \dots = f_n(e_n) = \text{TRUE}$
- $b_1(e_1) = b_2(e_2) = \dots = b_n(e_n)$
- all the events e_1, e_2, \dots, e_n have been received within a configurable time window.

[0033] Here the binding function definition is simpler, because we no more need to link two successive events but rather find a common part of all events of the group.

[0034] In the implementation level, instead of having a hash table for each stage, we can now have a single hash table, whose key is the common binding function value. The entries in the hash table have event references and expiration information. When an entry becomes "full" (it has one event reference for each filter), a group has been detected.

Event filter expressions

[0035] The following is an illustration of exemplary event filter expressions that can be used in the embodiments and examples described below. In these examples, event filter expressions (EFEs) are used both as filters and binding functions.

[0036] In these examples, event records may consist of log names and associated values. Each event may give zero or more values to each log name. Each log name may have a fixed type. Log names may be integers, but in this description we use symbolic names starting with LN_.

[0037] When an event filter expression is evaluated in the context of an event, the values of the log names in the event are investigated and the value of the event filter expression is evaluated. For example, an event can contain following log names and their values:

Event 1:	
log name	Value
LN_SITUATION_ID	999
LN_SITUATION_STRING	"Too long SMTP command was detected"
LN_IPV4_DESTINATION	10.0.0.1

[0038] Now, for example, the following event filter expressions could be evaluated in the context of Event 1:

EFE	EFE(Event 1)
defined(LN_SITUATION)	TRUE
defined(LN_SOME_OTHER)	FALSE
LN_IPV4_DESTINATION & 255.255.255.0	10.0.0.0
LN SITUATION ID == 999	TRUE

Event filter expression syntax

[0039] An event filter expression may present a combination of logical statements concerning a single event, which can be evaluated to be either true or false. The statements may refer to the symbolic log names that are present in the event. The log names may present either the value assigned to them in the event or just a logical value whether the particular log name is present in the event. A number of operations may be available to values, both log name references and literal, of different types. The expressions can also be grouped with parentheses.

[0040] The supported types may include one or more of the following:

- bool, for Boolean logical value
- int32, for 32-bit integer
- int64, for 64-bit integer
- float, for single precision floating point number
- double, for double precision floating point number
- string, for a string of characters.

[0041] The available operations are:

- defined(*log name*), returns true if the *log name* is present in the event.
- (*expr*), parentheses for expression grouping
- <, >, >=, <=, ==, !=, gives logical value of numeric or alphabetical relation
- !, logical not negates value of logical expression
- &&, ||, ->, logical *and*, *or*, and *implication* operations return Boolean value
- *log_name*, returns value assigned to the *log_name* in the event
- *literal*, literal numeric (integer or floating point) or string value
- unary -, negates numeric parameter value
- +, -, *, /, **, *add*, *subtract*, *multiply*, *divide*, and *raise to power*, to numeric values
- &, |, ^, <<, >> bitwise *and*, *or*, *xor*, and *shift* operations for integer types
- time(), returns current NTP-stamp
- get_year(int64), returns year of NTP stamp given as parameter.
- get_month(int64), returns number of month (0-11) of NTP stamp given as parameter.
- get_wday(int64), returns number of week day (0-6, 0=sunday) of NTP stamp given as parameter.
- get_mday(int64), returns day of month (1-31) of NTP stamp given as parameter.
- get_yday(int64), returns number of day of year (0-365) of NTP stamp given as parameter.
- day_time(int64) Without parameter, current time is taken as parameter.
- Literal NTP stamp value can be expressed in format YYYYMMDD.hh:mm:ss.s, for example 20020729. 15:17:27.123, means July 29 15:17 27.123s 2002 in local time zone.

[0042] Some log names may be allowed to occur more than once in single event, two special functions are meant to handle these cases. The relational expression given as parameter to these functions may be of form *LOG_NAME relational_operator literal_expression*, where relational expression may be one of <, >, >=, <=, ==, != and the log name may be of same type as the literal expression. For example: for_all(NUMERIC_LOG_NAME < 1 + 2 +3).

- for_all(*relational expression*), returns true if the *relational expression* is true for all occurrences of log name present in relational expression.
- for_any(*relational expression*), returns true if the *relational expression* is true for any occurrence of log name present in relational expression.

Further embodiments

[0043] Two illustrative further embodiments implementing the invention are presented below. In the first embodiment shown in Figure 2 it is assumed that the events are processed in the order they have happened. The events can be processed in the order they are received, or they can be sorted in the order of increasing time stamps before processing. In the latter, second, embodiment shown in Figure 3, the order in which events arrive does not matter, as long as the events arrive sufficiently close to each other. In the second embodiment the events can be processed in whatever order. In addition, both embodiments may comprise a predefined time window. In that case events are considered to be part of the same set (or sequence) of events only if they are received within the predefined time-window.

[0044] Referring now to Figure 2, in the first embodiment two or more stages (step 200) and a filtering function (e.

g. rule) for each of them (step 202) are defined. Processing of an event goes as follows:

[0045] - The filtering functions are evaluated with the received (step 204) event data (e.g. event data is compared to the filtering rules), in steps 206, 218 and 226.

[0046] - If the filtering function of the one of the stages evaluates to TRUE (e.g. event data matches filtering rule of one of the stages) in the step 206, 218 or 226, a binding function associated with the respective stage is evaluated for extracting/deriving a first key from the event data (step 208, 220 or 228, respectively).

[0047] - If the stage, which evaluates to TRUE, is the first stage (the step 206), it is checked if the event and the first key already exist in a table associated with the first stage (step 210). If not, the event and the first key are added to the table (step 212). If yes, a timestamp of the event may be updated in the table (step 216, and then the process proceeds to step 236). Otherwise (i.e. if the time stamp is not in use or not updated), nothing needs to be done (the process proceeds directly to step 236).

[0048] - If the stage, which evaluates to TRUE, is some other than the first stage or the last stage (step 218), it is checked, if there is an entry with the first key in the table of the previous stage (step 221). If not, nothing is done (the process proceeds to the step 236). If yes, another binding function associated with the current stage is evaluated for extracting a second key from the event data (step 222). Then, the table associated with the current stage is checked (224). If the event and the second key do not exist in the table, the event and the second key are added to the table (225). If the event and the second key already exist in the table, a timestamp of the event may be updated in the table (step 216). Otherwise, nothing needs to be done (the process proceeds directly to the step 236).

[0049] If the stage, which evaluates to TRUE, is the last stage (the step 226), it is checked, if there is an entry with the first key in the table of the previous stage (step 30). If not, nothing is done (the process proceeds directly to the step 236). If yes, it is determined that a sequence of events has been detected (step 232). Further, the detection may be reported and/or the related entries in the stages 1-3 be deleted (step 234).

[0050] In an embodiment of the invention, if several stages evaluate to TRUE, all such stages are processed. The processing can be arranged in ascending or descending order of the stages. If the stages are processed in ascending order, a single event can practically occur multiple times in the detected sequence (that is, a single event can evaluate to TRUE in first, second, third and so on stages of one sequence). The configuration of the stages (filtering and binding functions) naturally dictates, if this is possible in reality. If the stages are processed in descending order, all events in a detected sequence are distinct.

[0051] Finally, the entries older than the time window may be deleted (step 236).

[0052] According the second embodiment shown in Figure 3, two or more stages (step 300) and a filtering function (rule) for each of them (steps 302 and 304) are also defined. Processing of an event goes as follows:

[0053] - The filtering functions are evaluated with the received (step 306) event data (i.e. event data is compared to the filtering rules) in step 308.

[0054] - If the filtering function of a stage evaluates to TRUE (i.e. event data matches filtering rule of one of the stages), a binding function associated with the stage is evaluated for extracting a key from the event data (step 310).

[0055] - A table associated with the set of stages is checked (step 312). If the key is not found in the table, the event with the key is added to the table (step 314).

[0056] - If the key is found in the table, it is checked if an event for the current stage is recorded for the key (step 316). If yes, nothing needs to be done, and the process proceeds to step 318 (or alternatively, if it is defined that more than one event for each stage is required, the number of events with this key and stage is incremented). If not, the event is added to the table in connection with the key (step 314).

[0057] - Then it is checked if the key has an event (or alternatively, a predefined number of events) recorded for each stage (step 318), and if yes, it is determined that a set of events has been detected (step 320).

[0058] In the above embodiments there is one or two binding functions for each stage. However, any number of binding functions per stage is possible in all embodiments of the invention. Naturally, also any number of different sets of stages can be defined in accordance with the present invention.

Example

[0059] Let us now study a illustrative, fictitious example of the event sequence detection according to the invention. Let us assume that, in the network environment shown in Figure 1, we try to detect a sequence, where

1. An attacker uses an overly long SMTP command to make a buffer overflow attack to gain root access to a host A.
2. Another connection to the SMTP server on host A is not accepted, because the attacker replaced the server by a program supplied by the attacker.
3. An unauthorized connection attempt is made from a host B belonging to the same (class D) subnet as host A.

[0060] This sequence mimics a scenario where the attacker manages to gain a root access to a host by overflowing

EP 1 418 484 A2

an SMTP server buffer. However, the server remains non-functional after the overflow and any further connections are rejected. The attacker then manages to use local user information to log on another host within the same LAN and then tries to open an outbound connection that should normally not happen.

5 [0061] This sequence has 3 stages and to detect all such sequences on-the-fly, we have to store some information of prefixes, i.e. partial sequences, that can later, with additional events, form complete sequences as will be explained below.

[0062] The filters and binding functions to detect this kind of sequence could be defined as follows:

10 f_1 : LN_SITUATION_ID == 999 ("too long SMTP command")
 f_2 : LN_SITUATION_ID == 998 ("connection refused") && LN_PORT_DESTINATION == 25 (port of SMTP server)
 f_3 : LN_SITUATION_ID == 997 ("attempted unauthorized connection")
 $b_{1,2}^1$: LN_IPV4_DESTINATION
 $b_{1,2}^2$: LN_IPV4_DESTINATION
15 $b_{2,3}^2$: LN_IPV4_DESTINATION & 255.255.255.0 (compute the subnet of the destination IP address)
 $b_{2,3}^3$: LN_IPV4_SOURCE & 255.255.255.0

20 [0063] Assume that the following events are received (all in increasing timestamp order and within the configurable time window size):

Event 1:	
<i>log name</i>	<i>Value</i>
LN_SITUATION_ID	999
LN_SITUATION_STRING	"Too long SMTP command was detected"
LN_IPV4_DESTINATION	10.0.0.1
Event 2:	
<i>log name</i>	<i>Value</i>
LN_SITUATION_ID	999
LN_SITUATION_STRING	"Too long SMTP command was detected"
LN_IPV4_DESTINATION	10.0.0.15
Event 3:	
<i>log name</i>	<i>Value</i>
LN_SITUATION_ID	998
LN_SITUATION_STRING	"Attempted connection refused"
LN_PORT_DESTINATION	25
LN_IPV4_DESTINATION	10.0.0.1
Event 4:	
<i>log name</i>	<i>Value</i>
LN_SITUATION_ID	998
LN_SITUATION_STRING	"Attempted connection refused"
LN_PORT_DESTINATION	25
LN_IPV4_DESTINATION	10.254.0.5
Event 5:	
<i>log name</i>	<i>Value</i>
LN_SITUATION_ID	997
LN_SITUATION_STRING	"Attempted unauthorized connection"
LN_IPV4_SOURCE	10.0.0.254

EP 1 418 484 A2

[0064] Events 1, 3, and 5 fulfill the event sequence conditions described in the chapter **Event sequence detection** above, as can be seen by selecting e_1 = Event 1, e_2 = Event 3, and e_3 = Event 5. Now we have

$$f_1(e_1) = f_2(e_2) = f_3(e_3) = \text{TRUE}$$

$$b_{1,2}^1(e_1) = 10.0.0.1 = b_{1,2}^2(e_2)$$

$$b_{2,3}^2(e_2) = 10.0.0.0 = b_{2,3}^3(e_3)$$

[0065] The detection can be implemented in a detector or analyser using, for example, a hash table for each stage of the event sequence, except for the final stage. The hash table may contain references to the events forming a unique (according to the binding function value) prefix of length 1 on stage 1, length 2 on stage 2, and so on. The key to the table is the value of $b_{1,2}^1$ on stage 1, $b_{2,3}^2$ on stage 2, and so on.

[0066] The following example illustrates how the hash tables are updated upon receiving the five events shown above. When the first event is received, the filters are evaluated, and it is found out that only f_1 evaluates to true, so the event is considered only for stage 1. The binding function $b_{1,2}^1$ is evaluated; its value is 10.0.0.1 (LN_IPV4_DESTINATION of the received event). There is no corresponding entry in the hash table of stage 1, so one is added:

Stage 1:	
<i>key</i>	<i>references</i>
10.0.0.1	Event 1
Stage 2:	
<i>key</i>	<i>references</i>

[0067] Similarly, when Event 2 is received, another entry is added to the hash table of Stage 1: **Stage 1:**

Stage 1:	
<i>key</i>	<i>references</i>
10.0.0.1	Event 1
10.0.0.15	Event 2
Stage 2:	
<i>key</i>	<i>references</i>

[0068] When Event 3 is received, only f_2 evaluates to true, so only stage 2 is considered. Now it is first checked, whether there is an entry in the hash table of the previous stage (stage 1) with key $b_{1,2}^2$ (10.0.0.1). There is such entry (the first entry), and therefore, it is next checked whether there is already an entry in the hash table of stage 2 with key $b_{2,3}^2$. In this example, there is no such entry, and consequently, a new prefix is added:

Stage 1:	
<i>key</i>	<i>references</i>
10.0.0.1	Event 1
10.0.0.15	Event 2
Stage 2:	
<i>key</i>	<i>references</i>
10.0.0.0	Event 1, Event 3

[0069] When Event 4 is received, f_2 evaluates to true, but on the other hand, there is no entry in the hash table of the previous stage with key $b_{1,2}^2$ (10.254.0.5), and therefore, a new prefix is not added and the tables remain unchanged.

[0070] When Event 5 is received, f_3 evaluates to true. As before, it is checked whether the hash table of the previous stage (stage 2) has an entry with key $b_{2,3}^3$ (10.0.0.0). Because there is an entry with that key, it is determined that a
 5 event sequence consisting of events Event 1, Event 3, and Event 5 is detected. The analyser or detector may send or provide a respective alarm or report, for example to the operator console.

[0071] The hash table entries may be removed from the tables when the first event that the entry refers to is old enough (i.e. outside the time window). This may be implemented simply by a linked list that contains a pointer to each hash table element. The list is kept sorted so that the element that will expire next is the first element on the list. If a
 10 corresponding entry already exists in the table when adding another prefix, the expiration time of the entry may be adjusted, if the new prefix has later expiration time than the prefix that was already in the table.

[0072] It should be appreciated that, although we have concentrated on detecting a single event sequence in the above examples, several event sequences can be detected concurrently by defining multiple event sequence detection functions in the analyzer, each having a set of filters and binding functions of its own.

[0073] Thus, while the present invention has been described with reference to specific examples, which are intended to be illustrative only and not to be limiting the invention, it will be apparent to those skilled in the art that changes, additions and deletions may be made to the disclosed embodiments without departing from the spirit and scope of the invention.

Claims

1. An event sequence detection method, comprising
 25 having or defining an event sequence including two or more stages in order, each of the stages including one or more events,
 having or defining a filtering function for each of said stages, each filtering function providing a TRUE indication, when one of the events belonging to the respective event is received, and a FALSE indication otherwise,
 having or defining at least one binding function for each of the stages such that a pair of binding functions in two successive stages links the events in these two successive stages,
 30 continuously receiving event data,
 continuously evaluating the received event data with the filtering functions,
 when the evaluation results in a TRUE indication from one of the filter functions, deriving at least one key value from the received event data by the corresponding at least one binding function,
 determining that said sequence has been detected, when a TRUE indication has been obtained in each
 35 stage in a timely order and the derived key values link the detected events in the successive stages.
2. The method as claimed in claim 1, wherein said determining comprises determining that said sequence has been detected, when a TRUE indication has been obtained in each stage in a timely order and the derived key values link the detected events in the successive stages within a time window.
3. The method as claimed in claim 1 or 2, wherein said determining comprises
 40 when the filter function that provided the TRUE indication is the filter function for the first stage, registering or updating the current event with the derived key value in said first stage,
 when the filter function that provided the TRUE indication is the filter function for other than the first stage and a last stage in order in said sequence and there is a registration with one of the at least one derived key value in the previous stage in order in said sequence, registering or updating the current event or events with the at least one derived key value,
 45 when the filter function that provided the TRUE indication is the filter function for the last stage in order in said sequence and there is a registration with one of the at least one derived key value in the previous stage in order in said sequence, determining that said event sequence has been detected.
4. The method as claimed in claim 2, comprising cancelling registered event and key value older than the time window based on time information or a time stamp.
5. The method as claimed in claim 4, wherein said updating comprises updating the time information or the time stamp of an already registered event and the associated at least one key value.
6. An event sequence detection method, comprising

having or defining an event sequence including two or more stages in order, each of the stages including one or more events,

having or defining a filtering function for each of said stages, each filtering function providing a TRUE indication, when one of the events belonging to the respective event is received, and a FALSE indication otherwise,

5 evaluating the filtering functions with the event data,

if the filtering function of the one of the stages evaluates to TRUE, a binding function associated with the respective stage is evaluated for extracting a first key from the event data,

10 if the stage, which evaluates to TRUE, is the first stage, it is checked whether the event and the first key already exist in a table associated with the first stage, and the if checking result is negative, the event and the first key are added to the table,

if the stage, which evaluates to TRUE, is some other than the first stage, it is checked, whether there is an entry with the first key in the table of the previous stage, if the checking result is

15 negative, nothing is done, and if the checking result is confirmative, another binding function associated with the current stage is evaluated for extracting a second key from the event data and the table associated with the current stage is checked for whether the event and the second key do exist in the table, and if the latter checking result is negative, the event and the second key are added to the table,

if the stage, which evaluates to TRUE, is the last stage, it is checked, whether there is an entry with the first key in the table of the previous stage, and if the checking result is negative, nothing is done, and if the checking result is confirmative, it is determined that a sequence of events has been detected.

20

7. The method according to claim 6, comprising

providing the events in the tables with time information or time stamps,

updating the time information or the time stamp of the event, if the event to be added to a table already exists in the table,

25

cancelling an entry that is older than a time window.

8. An event sequence detection method, comprising

having or defining an event sequence including two or more events,

30 having or defining a filtering function and an associated binding function for each event, each filtering function providing a TRUE indication, when the respective event is received, and a FALSE indication otherwise,

continuously receiving event data,

continuously evaluating the received event data with the filtering functions,

each time when the evaluation results in a TRUE indication from one of the filter functions, registering the corresponding event and a key value derived from the received event data by the corresponding binding function,

35

determining the event sequence as detected, if all events of the event sequence with mutually matching key values are registered within a time window.

9. An event sequence detection method, comprising

40 having or defining an event sequence including two or more stages, each of the stages including one or more events,

having or defining a filtering function for each of said stages, each filtering function providing a TRUE indication, when one of the events belonging to the respective event is received, and a FALSE indication otherwise,

evaluating the filtering functions with the event data,

45

if the filtering function of the one of the stages evaluates to TRUE, a binding function associated with the respective stage is evaluated for extracting a key from the event data,

checking whether the key already exists in a table associated with the set of stages,

if the key is not found in the table, the event with the key is added to the table,

if the key is found in the table, it is checked whether an event for the current stage is already recorded for the key,

50

if no event for the current stage is already recorded for the key, the event is added to the table in connection with the key and the current stage,

checking whether the key has an event recorded for each stage, and

if the key has an event recorded for each stage, determining that the event sequence has been detected.

55

10. The method as claimed in claim 9, wherein said determining comprises determining that said sequence has been detected, when the key an event has an event recorded for each stage within a time window.

11. An event sequence detection method, comprising

having or defining an event sequence including two or more stages, each of the stages including one or more events,

having or defining a filtering function for each of said stages, each filtering function providing a TRUE indication, when one of the events belonging to the respective event is received, and a FALSE indication otherwise,

5 evaluating the filtering functions with the event data,

if the filtering function of the one of the stages evaluates to TRUE, a binding function associated with the respective stage is evaluated for extracting a key from the event data,

checking whether the key already exists in a table associated with the set of stages,

if the key is not found in the table, the event with the key is added to the table,

10 if the key is found in the table, it is checked whether an event for the current stage is already recorded for the key,

if no event for the current stage is already recorded for the key, the event is added to the table in connection with the key and the current stage,

15 if an event for the current stage is already recorded for the key, incrementing the number of events with this key and stage,

checking whether the key has a predetermined number of events recorded for each stage, and

if the key has a predetermined number of events recorded for each stage, determining that the event sequence has been detected.

20 **12.** An event sequence detector block for execution by a processor in a data communications network environment, comprising:

a computer readable memory, and

25 a routine stored on a the computer readable memory and adapted to be implemented on the processor, wherein the routine:

has a predefined event sequence including two or more stages in order, each of the stages including one or more events,

30 has a predefined filtering function for each of said stages, each filtering function providing a TRUE indication, when one of the events belonging to the respective event is received, and a FALSE indication otherwise,

has at least one predefined binding function for each of the stages such that a pair of binding functions in two successive stages links the events in these two successive stages,

continuously receives event data,

35 continuously evaluates the received event data with the filtering functions,

when the evaluation results in a TRUE indication from one of the filter functions, derives at least one key value from the received event data by the corresponding at least one binding function,

determines that said sequence has been detected, when a TRUE indication has been obtained in each stage in a timely order and the derived key values link the detected events in the successive stages.

40

13. An event sequence detector block as claimed in claim 12, wherein said routine determines that said sequence has been detected, when a TRUE indication has been obtained in each stage in a timely order and the derived key values link the detected events in the successive stages within a time window.

45 **14.** An event sequence detector block for execution by a processor in a data communications network environment, comprising:

a computer readable memory, and

50 a routine stored on a the computer readable memory and adapted to be implemented on the processor, wherein the routine:

has a predefined event sequence including two or more events,

has a predefined filtering function and an associated binding function for each event, each filtering function providing a TRUE indication, when the respective event is received, and a FALSE indication otherwise,

55 continuously receives event data,

continuously evaluates the received event data with the filtering functions,

each time when the evaluation results in a TRUE indication from one of the filter functions, registers the corresponding event and a key value derived from the received event data by the corresponding binding

function,
determines the event sequence as detected, if all events of the event sequence with mutually matching
key values are registered.

- 5 **15.** An event sequence detector block as claimed in claim 12, wherein said routine determines the event sequence
as detected, if all events of the event sequence with mutually matching key values are registered within a time
window.
- 10 **16.** A computer readable storage medium comprising a computer program that carries out the method according to
any one of claims 1 to 11 when executed by a computer.
- 15 **17.** A computer program that carries out the method according to any one of claims 1 to 11 when executed by a
computer.

15

20

25

30

35

40

45

50

55

Fig. 1

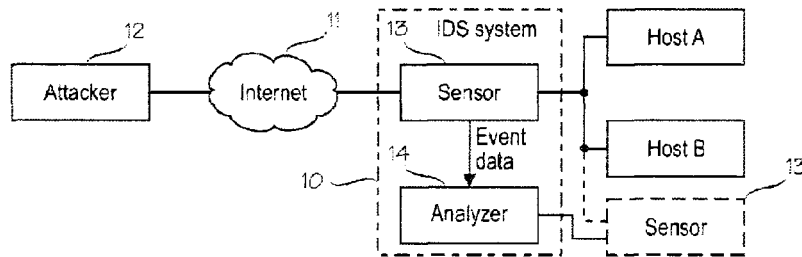
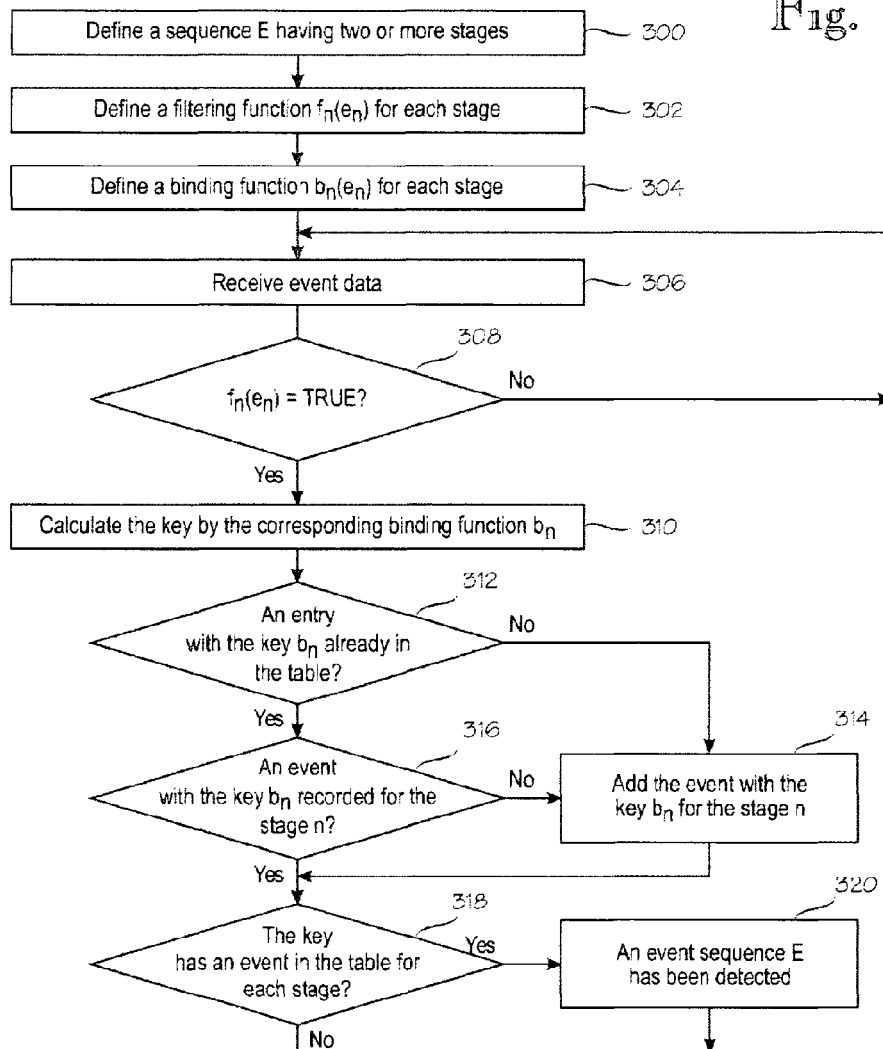
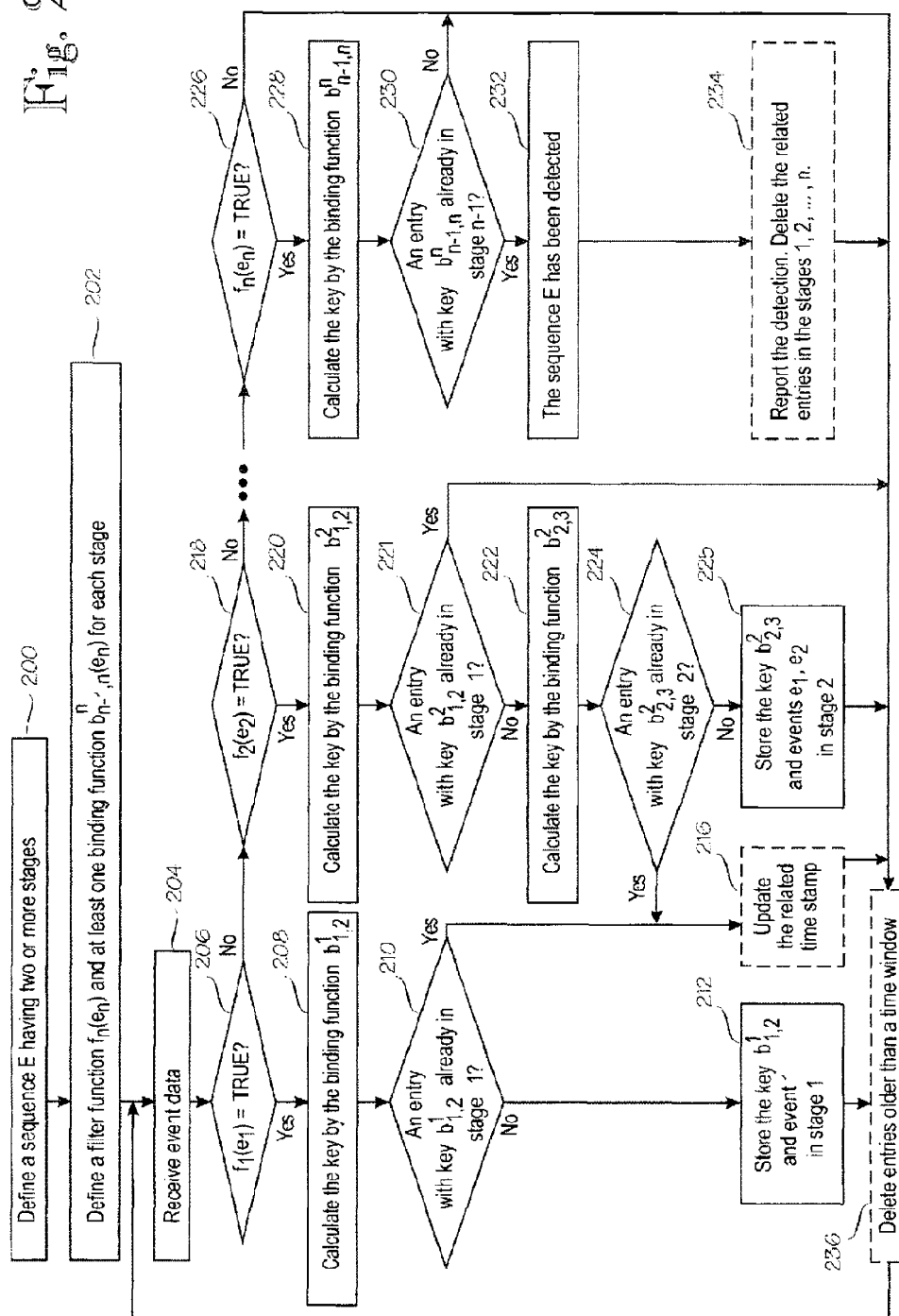


Fig. 3





DEVICE AND METHOD FOR SECURING AND MONITORING PROTECTED DATA

Publication number: WO2005038633 (A1)

Publication date: 2005-04-28

Inventor(s): DOHMANN DIERK [DE]; RUEDINGER JENS [DE] +

Applicant(s): VODAFONE HOLDING GMBH [DE]; DOHMANN DIERK [DE]; RUEDINGER JENS [DE] +

Classification:


- **international:** G06F21/00; G06F21/00; (IPC1-7): G06F1/00


- **European:** G06F21/00N1D; G06F21/00N5A3


Application number: WO2004EP11338 20041011


Priority number(s): DE20031048729 20031016

Also published as:


 EP1676191 (A1)


 DE10348729 (A1)


 CN1894644 (A)


 CN100483297 (C)


Cited documents:

 EP1209551 (A2)

 DE19839041 (A1)

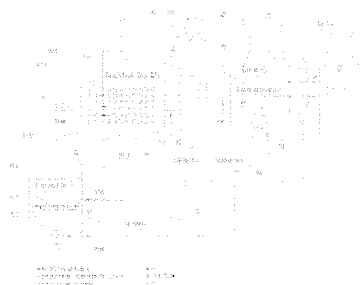
 XP002315670 (A)

 XP002315671 (A)

 XP004482668 (A)

Abstract of WO 2005038633 (A1)

The invention relates to a device (10) for securing and monitoring protected data (12) in a volatile and/or non-volatile data memory (14) of a data processing unit for the purpose of protecting them from unauthorized access. The inventive device is provided with access means (18) via which the protected data (12) in the data memory (14) can only be accessed via an authentication code (20) and/or authentication key. Means (110) detect any accesses to the protected data (12) irrespective of the input of the authentication code (20). The invention also relates to a method for securing and monitoring protected data (12) from unauthorized access using the inventive device (10).



Data supplied from the **espacenet** database — Worldwide

WAVELYNX EX. 1002, Pg. 126
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018



ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Erklärungen gemäß Regel 4.17:

- hinsichtlich der Identität des Erfinders (Regel 4.17 Ziffer i) für die folgenden Bestimmungsstaaten AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO Patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)
- hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO Patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

- hinsichtlich der Berechtigung des Anmelders, die Priorität einer früheren Anmeldung zu beanspruchen (Regel 4.17 Ziffer iii) für die folgenden Bestimmungsstaaten AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO Patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)
- Erfindererklärung (Regel 4.17 Ziffer iv) nur für US
- Erfindererklärung (Regel 4.17 Ziffer iv) nur für US

Veröffentlicht:

- mit internationalem Recherchenbericht
- vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Die Erfindung betrifft eine Einrichtung (10) zur Sicherung und Überwachung von geschützten Daten (12) in einem flüchtigen und/oder nichtflüchtigen Datenspeicher (14) einer Datenverarbeitungseinheit vor unbefugtem Zugriff, wobei Zugangsmittel (18) vorgesehen sind, über die nur mit einem Berechtigungscode (20) und/oder -schlüssel auf die geschützten Daten (12) in dem Datenspeicher (14) zugegriffen werden kann. Es sind Mittel (110) zum Erfassen von Zugriffen auf die geschützten Daten (12) unabhängig von der Eingabe des Berechtigungscode (20) enthalten. Die Erfindung betrifft ferner ein Verfahren zur Sicherung und Überwachung von geschützten Daten (12) vor unbefugtem Zugriff mit einer solchen Einrichtung (10).

5

10 **Einrichtung und Verfahren zur Sicherung und Überwachung von geschützten
Daten**

Technisches Gebiet

15 Die Erfindung betrifft eine Einrichtung zur Sicherung und Überwachung von geschützten
Daten in einem flüchtigen und/oder nichtflüchtigen Datenspeicher einer
Datenverarbeitungseinheit vor unbefugtem Zugriff, wobei

- 20 (a) Zugangsmittel vorgesehen sind, über die nur mit einem Berechtigungscode
auf die geschützten Daten in dem Datenspeicher zugegriffen werden kann,
- (b) Mittel zum Erfassen der Anzahl der Berechtigungscodeeingaben enthalten
sind,
- 25 (c) Mittel zur Beschränkung des Zugriffs auf die geschützten Daten vorgesehen
sind, wobei eine Beschränkung erfolgt, wenn die Anzahl der
Berechtigungscodeeingaben innerhalb eines bestimmten Zeitintervalls einen
diesem Zeitintervall zugeordneten Referenzwert überschreitet,

30

Ferner betrifft die Erfindung ein Verfahren zur Sicherung und Überwachung von
geschützten Daten (12) vor unbefugtem Zugriff mit einer Einrichtung (10) gemäß einem
der vorherigen Ansprüche, wobei

BESTÄTIGUNGSKOPIE

- 5
- (a) die Anzahl der Berechtigungscodeeingaben für den Zugriffe auf die geschützten Daten (12) innerhalb eines bestimmten Zeitintervalls (36) ermittelt wird und
 - (b) diese Anzahl der Versuche innerhalb des bestimmten Zeitintervalls (36) mit einem Referenzwert verglichen wird, wobei
 - 10 (c) der Zugriff auf die geschützten Daten beschränkt oder verhindert wird, wenn die Anzahl der Eingaben innerhalb des Zeitintervalls größer als der Referenzwert ist.

Stand der Technik

15

Digitale Daten werden zur Sicherung und zur Verhinderung vor unbefugten Zugriffen nach kryptographischen Verfahren geschützt. Unter Kryptographie wird grundsätzlich die Wissenschaft zur Erforschung und Realisierung von Verfahren zur Verschlüsselung bzw. Entschlüsselung von Daten verstanden, bei denen entweder das

20 Verschlüsselungsverfahren oder (bei Anwendung einheitlicher Verschlüsselungsverfahren) die verwendeten Schlüsselbegriffe geheim gehalten werden. Durch Ändern, Vertauschen oder Hinzufügen von Zeichen nach bestimmten Regeln wird ein Klartext in einen Schlüsseltext verwandelt und umgekehrt. Solche kryptographischen Verfahren sind z.B. bei der Speicherung von Daten und der Datenübertragung

25 anwendbar. Dies ist derzeit das wirksamste Mittel des Datenschutzes, um Informationen, die in falsche Hände gelangt sind, wertlos zu machen. Neben der Vertraulichkeit durch die Verschlüsselung von Klartext kann mit den Methoden der Kryptographie auch die Authentizität einer Nachricht sowie die Integrität einer Datei sichergestellt werden, wobei unter letzterem, der Integrität einer Datei, die Gewissheit zu verstehen ist, eine

30 Datei in unveränderter Form zu empfangen.

Angriffe auf kryptographisch geschützte Daten können nur durch extrem häufige Zugriffe auf die geschützten Daten erfolgen. Dabei werden die verschiedensten

kryptografischen Zeichenkombinationen ausprobiert, bis schließlich eine Kombination passt, um auf die Daten zugreifen zu können. Diese Zugriffe zur unerlaubten Entschlüsselung sind, je nach Schlüssellänge (digitaler Code) und verwendetem kryptographischen Algorithmus, sehr zeitaufwendig. Wenn ein Angreifer ausreichend
5 Zeit hat kann er theoretisch einen solchen Code knacken.

Es sind Einrichtungen, z.B. Computer, mit solchen kryptographischen Verfahren bekannt, die zur Sicherung von geschützten Daten dienen, so dass Unbefugte nicht auf die Daten zugreifen können. Die kryptographisch geschützten Daten liegen dazu
10 beispielsweise in einem flüchtigen Datenspeicher, beispielsweise einem RAM (= Random Access Memory) oder einem nichtflüchtigen Datenspeicher, vor, z. B. Festplatte, CD-ROM und EPROM (= Erasable Programmable Read Only Memory). Nur mit einem geeigneten digitalen Code kann auf die Daten zugegriffen werden. Der Code kann beispielsweise auf einem Magnetstreifen oder einem Chip einer "Scheckkarte"
15 gespeichert sein und wird mittels geeigneten Lesegeräts für den Zugriff auf die geschützten Daten ausgewertet. Erst wenn die Codeüberprüfung erfolgreich war, d.h. die Daten können nun insbesondere mit dem Schlüsselcode entschlüsselt werden. Dann kann auf die Daten zugegriffen werden. Bei anderen Einrichtungen muss der Schlüsselcode über eine Tastatur eingegeben werden. Probleme können bei solchen Einrichtungen
20 entstehen, indem ein Unbefugter beliebig oft versuchen kann, den Schlüsselcode zu knacken. Mit dem Schlüsselcode hat er schließlich unautorisierten Zugriff auf die geschützten Daten und kann unter Umständen erheblichen Schaden damit anrichten.

Das deutsche Patent DE 198 39 041 C2 beschreibt ein Verfahren zum Identifizieren und
25 Darstellen von Zuständen eines Fehlbedienungszählers. Der Fehlbedienungszähler ist auf einem intelligenten Datenträger installiert. Bei einer definierten Anzahl von Fehlversuchen bei der Eingabe eines Identifikationsmerkmals wird der Zugriff auf den intelligenten Datenträger automatisch gesperrt. Eine Anpassung an den Benutzer bei der Eingabe des Identifikationsmerkmals erfolgt nicht.

30

Aus der europäischen Patentanmeldung EP 1 209 551 A2 ist ein Verfahren bekannt, um den Zugriff auf einem Computer zu kontrollieren. Dabei wird ein Passwort überprüft. Der Zugriff wird nur erlaubt, wenn das Passwort gültig ist. Wird eine bestimmte Anzahl

bei der Eingabe eines falschen Passworts innerhalb eines Zeitintervalls erreicht, so wird der Zugang verhindert. Nachteil bei diesem Verfahren ist, dass sich die Passworteingabe nicht an das Verhalten von Benutzern anpasst. Beispielsweise bei älteren Menschen oder Kindern besteht vermehrt die Gefahr, dass wiederholt falsche Passworte innerhalb eines
5 Zeitintervalls eingegeben werden.

Bisher gibt ein Anwender eine PIN (= Personal Identification Number) oder ein alphanumerischen Code als Berichtigungscode für den Zugang zu den geschützten Daten oder Funktionen ein. Damit war er autorisiert, auf die geschützten Daten oder Funktionen
10 zugreifen zu können. Bei Mobilfunkendgeräten wird eine PIN zur Identifikation eingegeben. Diese Identifikation wird mit der SIM-Karte abgeglichen. Wenn die PIN korrekt war, wird der Benutzer des Mobilfunkendgeräts in ein Mobilfunknetz eingebucht. In diesem Mobilfunknetz gilt er fortan weitestgehend als autorisiert.

15 Hacker, damit sind solche Personen gemeint, die aus unterschiedlichsten Motiven versuchen an geschützte Daten heranzukommen. Die Hacker handeln zumeist einerseits aus einer kriminellen Energie heraus, z.B. um an einen Bankzugang heranzukommen oder um Werksspionage bzw. Sabotage zu betreiben, andererseits aus einer rein sportlichen Natur heraus.

20 Für einen Hacker besteht nun theoretisch die Möglichkeit auch ohne die SIM-Karte auf die geschützten Daten oder Funktionen zuzugreifen. Mit geeigneten Equipment kann er versuchen über andere Kanäle, beispielsweise mit einem weiteren Mobilfunkendgerät und einer bereits autorisierten SIM-Karte auf die geschützten Daten zu zugreifen. Dafür
25 benötigt er nicht notwendigerweise die PIN.

Offenbarung der Erfindung

30 Aufgabe der Erfindung ist es daher, eine Einrichtung zu schaffen, die die Nachteile des Standes der Technik vermeidet und verhindert, dass ein Angriff auf die geschützten Daten durch beliebige Versuche erfolgen kann, die sich aber an den Bedürfnissen der Benutzer orientiert.

Erfindungsgemäß wird die Aufgabe dadurch gelöst, dass bei einer Einrichtung zur Sicherung von geschützten Daten der eingangs genannten Art,

5 (d) Mittel vorgesehen sind, mit denen unabhängig von der Eingabe des Berechtigungscode die Anzahl der Zugriffe auf die geschützten Daten und/oder Funktionen in dem flüchtigen bzw. nichtflüchtigen Datenspeicher innerhalb eines bestimmten Zeitintervalls ermittelt wird.

10 Weiterhin wird die Aufgabe durch ein Verfahren der eingangs genannten Art mit einer Einrichtung gelöst, bei dem

(d) unabhängig von der Eingabe des Berechtigungscode die Anzahl der Zugriffe auf die geschützten Daten und/oder Funktionen in dem flüchtigen bzw.
15 nichtflüchtigen Datenspeicher innerhalb eines bestimmten Zeitintervalls ermittelt wird.

Die Erfindung beruht auf dem Prinzip, die Anzahl der Zugriffe auf die geschützten Daten innerhalb eines Zeitintervalls zu überwachen. Es wird bei der vorliegenden Erfindung
20 davon ausgegangen, dass ein berechtigter Benutzer durchaus auch Fehler bei der Eingabe des Berechtigungscode macht. Durch die vorgeschlagene Maßnahme wird verhindert, dass ein Unberechtigter beliebige Versuche hat, den Berechtigungscode zu ermitteln. Die erfindungsgemäße Einrichtung liefert dem berechtigten Benutzer zudem ein Zeitfenster, in dem er mit einer bestimmten Häufigkeit auf die geschützten Daten zugreifen kann.
25 Dafür ist erforderlich, dass die Zugriffe auf die geschützten Daten in dem Zeitintervall gezählt werden. Dabei kann sich das System geschickt an den Benutzer anpassen. Jemand der üblicherweise z. B. fünf Zugriffe während eines Zugangsvorgangs zu den verschlüsselten Daten benötigt, wird auch weiterhin fünf Zugriffe innerhalb eines Zeitintervalls haben, da sich die Einrichtung an den Benutzer anpasst.

30 Dies erfolgte, indem ein Referenzwert sich an vorherigen Zeitintervallen orientiert, in denen der Benutzer auf die geschützten Daten zugegriffen hat. Weicht das

Zugriffsverhalten von vorherigen Zeitintervallen ab, so wird der Zugang zu den gesicherten Daten beschränkt bzw. vollständig verhindert.

5 Ein vorteilhafter Aspekt der Erfindung ist, dass die Datenverarbeitungseinheit einen Taktgeber für den Arbeitstakt enthält, wobei das Zeitintervall durch eine bestimmte Anzahl von Taktzyklen des Taktgebers vorgebbbar ausgebildet ist. Diese Maßnahme kann ein Gerät weitestgehend von externen Zeitgebern unabhängig machen, da die Anzahl der Taktzyklen ein Zeitintervall bestimmen.

10 Als vorteilhafte Ausgestaltung der Erfindung hat sich ferner erwiesen, wenn die Mittel zur Erfassung der Zugriffe auf die geschützten Daten einen Zähler enthalten, welcher die Anzahl der Zugriffe innerhalb des Zeitintervalls zählt. Anhand des Zählerstandes kann überprüft werden, ob noch ein weiterer Zugriff auf die geschützten Daten möglich ist, oder ob jegliche Zugangsmöglichkeit zunächst gesperrt wird.

15 Eine bevorzugte Ausbildung der Erfindung ergibt sich dadurch, dass Mittel zum Zurücksetzen des Zählers vorgesehen sind, welche den Zähler bei einem berechtigten Zugriff auf Null setzen. Damit kann der Zähler beispielsweise nach Ablauf einer vordefinierten Zeitspanne zurückgesetzt werden, um die Möglichkeit zu haben, erneut auf die geschützten Daten zugreifen zu können. Vorteilhafterweise sind die Mittel zur Beschränkung der Zugriffe auf die geschützten Daten dynamisch eingestellt. Dadurch kann die Beschränkung ggf. auf bestimmte Benutzerprofile angepasst werden. Bei Personen, bei denen häufiger auf die geschützten Daten zugegriffen wird, wird die Anzahl der erlaubten Zugriffe auf die geschützten Daten innerhalb des Zeitintervalls für
20 die Anzahl der möglichen Zugriffe höher liegen, als bei Personenkreisen, bei denen eine solche hohe Anzahl nicht vorkommt. Es ist daher vorteilhaft, wenn die Mittel zur Beschränkung der Zugriffe auf die geschützten Daten auf einen Anwender einstellbar ausgebildet sind.

25 30 Eine weitere vorteilhafte Ausgestaltung der Erfindung ergibt sich dadurch, dass der Datenspeicher auf einer SIM-Karte vorgesehen ist. Damit lässt sich eine solche Einrichtung auch beispielsweise in Mobilfunkendgeräten oder Telematikgeräten in geeigneter Weise verwenden. Dabei sind Mobilfunkendgeräte und Telematikgeräte

vorteilhafterweise als Datenverarbeitungseinheit ausgebildet. Alternativ dazu ist die Datenverarbeitungseinheit in einer weiteren Ausgestaltung der Erfindung als Computer ausgebildet. Eine bevorzugte Ausbildung der Erfindung ergibt sich durch Alarmmittel, welche bei Überschreiten einer Anzahl von unberechtigten oder Fehlzugriffen ein Alarmsignal erzeugen. Damit kann signalisiert werden, dass unter Umständen ein Unbefugter sich an den geschützten Daten zu schaffen macht.

In einer Ausgestaltung des erfindungsgemäßen Verfahrens wird die Anzahl der Zugriffe auf die geschützten Daten innerhalb eines bestimmten Zeitintervalls mit einem Zähler erfasst. Durch diese Maßnahme wird erreicht, dass die Anzahl der Zugriffe festgehalten werden, um bei Überschreiten einer Anzahl in dem Zeitintervall ein Ereignis eintreten zu lassen. Ein solches Ereignis besteht in einer weiteren bevorzugten Ausbildung des erfindungsgemäßen Verfahrens zur Sicherung und Überwachung von geschützten Daten, nämlich, wenn der Zugriff auf die geschützten Daten beschränkt wird. Dies erfolgt z.B. bei Überschreitung eines Referenzwertes für die Anzahl der Zugriffe auf die geschützten Daten innerhalb eines bestimmten Zeitintervalls.

Weiterhin kann in einer besonderen Ausgestaltung des erfindungsgemäßen Verfahrens der Zähler zum Zählen der Anzahl der Zugriffe bei einem korrekten Zugriff zurückgesetzt werden. Dadurch ist gewährleistet, dass nach Fehlzugriffen ein Berechtigter wieder auf die geschützten Daten zugreifen kann.

Unterschiedliche Benutzer haben ein eigenes Benutzerprofil. So kann es sein, dass beispielsweise im Fall von Mobilfunkendgeräten z.B. ältere Personen und ggf. Kinder eine höhere Fehlerquote beim Zugriff auf die geschützten Daten haben. Es ist daher eine vorteilhafte Ausgestaltung, wenn die Anzahl der Zugriffe für die Beschränkung eingestellt und/oder an einen Anwender angepasst werden kann.

Eine vorteilhafte Ausbildung des erfindungsgemäßen Verfahrens ergibt sich ferner, wenn die Anzahl der Zugriffe für die Beschränkung über ein Netzwerk, insbesondere Mobilfunknetzwerk, eingestellt und/oder an einen Anwender angepasst wird. Damit muss der Anwender mit seiner Einrichtung nicht notwendigerweise zu einem Service gehen, der ihm die Einrichtung auf seine Bedürfnisse einstellt.

Eine bevorzugte Ausgestaltung des erfindungsgemäßen Verfahrens zur Sicherung von geschützten Daten vor unbefugtem Zugriff ergibt sich ferner dadurch, dass bei Überschreiten eines Wertes für die Anzahl der Zugriffe auf die geschützten Daten ein
5 geeignetes Alarmsignal erzeugt wird. Vorteilhafterweise ist das Alarmsignal für den auf die geschützten Daten Zugreifenden nicht erkennbar. Dadurch kann der Unberechtigte ggf. auf "frischer Tat" gefasst werden.

In einer geeigneten Ausgestaltung des erfindungsgemäßen Verfahrens wird bei
10 Überschreiten eines Wertes für die Anzahl der Zugriffe auf die geschützten Daten der weitere Zugriff innerhalb eines Zeitintervalls auf die Daten verweigert. Damit wird Zugang auf die geschützten Daten nur für einen bestimmten Zeitraum gesperrt, so dass es beispielsweise "Hacker-Programme" von Unberechtigten schwer haben, in ein solches System einzubrechen. Sie können nämlich nicht beliebig viele Versuche starten, sondern
15 müssen immer wieder den Zeitraum abwarten, bis sie erneut wieder auf die geschützten Daten zugreifen können.

Weitere Vorteile ergeben sich aus dem Gegenstand der Unteransprüche sowie der
20 Zeichnung mit der dazugehörigen Beschreibung.

Kurze Beschreibung der Zeichnung

Fig. 1 zeigt in einer Prinzipskizze eine erfindungsgemäße Einrichtung zur
25 Sicherung und Überwachung von geschützten Daten.

Bevorzugtes Ausführungsbeispiel

30 In Fig. 1 wird in einer Prinzipskizze ein bevorzugtes Ausführungsbeispiel einer erfindungsgemäßen Einrichtung 10 zur Sicherung und Überwachung von geschützten Daten 12 dargestellt. Die geschützten Daten 12 befinden sich in einem Datenspeicher 14 der Einrichtung 10 und sind durch gekreuzte Schraffur gekennzeichnet. Die Daten 12

liegen nach einem kryptographischen Verfahren in codierter bzw. verschlüsselter Form vor. Der Datenspeicher 14 ist im vorliegenden Ausführungsbeispiel ein nichtflüchtiger Speicher, der auch auf eine SIM-Karte (= Subscriber Identification Modul) vorgesehen sein kann.

5

Die erfindungsgemäße Einrichtung 10 befindet sich im vorliegenden Ausführungsbeispiel in einer nicht explizit dargestellten Datenverarbeitungseinheit, beispielsweise einem Computer oder einem vergleichbaren prozessorgesteuerten Gerät, wie Mobilfunkendgeräte oder Telematikgeräte mit üblichen standardisierten Schnittstellen 16, die für den Datenzugriff ausgebildet sind.

10

Über Zugangsmittel 18, beispielsweise eine Computertastatur, kann ein Berechtigungscode 20 als ein digitaler Schlüssel eingegeben werden, der darum symbolisch als Schlüssel dargestellt ist. Der Berechtigungscode 20 wird an eine Prüfeinheit 22 geleitet. Die Prüfeinheit 22 befindet sich wiederum in einem Berechtigungsapparat 23. Eine Dechiffriereinheit 26 decodiert bei korrektem Berechtigungscode 20 die geschützten Daten 12 des Datenspeichers 14 und gibt sie an eine Ausgabeschnittstelle 28. Der Berechtigungscode 26 kann unter Umständen ganz oder teilweise für die Dechiffrierung der geschützten Daten 12 durch die Dechiffriereinheit 26 erforderlich sein.

15

20

An der Ausgabeschnittstelle 28 kann beispielsweise ein nicht dargestellter Monitor, Drucker oder ein anderer Computer bzw. Speicherlaufwerk vorgesehen sein, um die entschlüsselten Daten 12 darzustellen oder zu speichern. Die Daten- bzw. Berechtigungscodeübertragung zwischen den einzelnen Einheiten 18, 22, 26, bzw. Schnittstellen 16, 28 erfolgt über einen Datenbus 30. Die Steuerung der Abläufe in der Einrichtung 10 erfolgen mit Hilfe eines Prozessors 32 (CPU), der mit einem Taktgeber 34 getaktet wird.

25

Der Taktgeber 34 dient ferner dazu, ein Zeitmaß 36 für den Berechtigungsapparat 23 zu definieren. Eine mittels Stellmittel 38 einstellbare Anzahl von Taktzyklen des Taktgebers 34 bildet ein Zeitintervall. Ein Zähler 40 zählt die Versuche der unkorrekten Eingaben für den Berechtigungscode 20, um an die geschützten Daten 12 gelangen zu können.

30

Wenn innerhalb eines eingestellten Zeitintervalls 36 eine vorgegebene Anzahl von Zugriffen für die Eingabe durch die Prüfeinheit 22 festgestellt wird, werden keine weiteren Zugriffe über diese Schnittstelle 16 auf die geschützten Daten 12 mehr
5 zugelassen. Dieser Referenzwert für die Anzahl der möglichen Zugriffe berechnet sich aus Zeitintervallen 36, vorheriger Eingabeversuche. Beispielsweise, indem die durchschnittliche Anzahl von früheren Berechtigungscodeeingaben pro Zeitintervall 36 festgehalten wird. Durch die Verwendung eines Referenzwertes, der sich aus früheren Eingabeversuchen berechnet, wird eine höhere Flexibilität für den Benutzer erzielt.

10

Vordergründig wird aber vor allem verhindert, dass insbesondere Computerprogramme von unberechtigten Benutzern verschiedenste Codekombinationen austesten, bis der richtige Berechtigungscode erreicht wird. Durch die Beschränkung der Zugriffe wird ein "Hacken" des Berechtigungscodees 20 nahezu verhindert. Der Zugriff auf die geschützten
15 Daten 12 wird bei Überschreiten der vorgegebenen Anzahl für die Eingabe des Berechtigungscodees 20 innerhalb des Zeitintervalls 36 für einen bestimmten Zeitraum oder sogar vollständig gesperrt. Dabei kann auch ein Alarmsignal erzeugt werden, um zu signalisieren, dass die Anzahl der Fehlversuche zur Eingabe des Berechtigungscodees überschritten wurde

20

Lediglich ein "Administrator" kann mit einer geeigneten "Reset-Funktion" 42 den Zähler 40 für die Fehlversuche ggf. zurückstellen. Alternativ wird der Zähler 40 nach Ablauf einer vordefinierten Zeitspanne zurückgestellt. Die Zeitspanne für die Zugangsbeschränkung kann auch dynamisch auf die möglichen Benutzergewohnheiten
25 eingestellt werden.

Ein Hacker 100 kann beispielsweise zum Zwecke der Spionage oder Sabotage versuchen, über eine weitere Schnittstelle 102 auf die geschützten Daten 12 zu gelangen und zwar unabhängig von der zuvor beschriebenen Berechtigungscodeeingabe. Um die geschützten
30 Daten 12 zu dechiffrieren muss er jedoch Dechiffrieralgorithmus 104 kennen. Um diesen herauszubekommen wird er über Datenbus 106 auf die geschützten Daten 12 zugreifen. Dabei liegt Häufigkeit der Zugriffe pro Zeitintervall 108 wahrscheinlich erheblich höher, als es bei einem berechtigten Anwender der Fall ist. Um die Zugriffe auf die geschützten

Daten zu kontrollieren ist eine Kontrolleinheit 110 vorgesehen. Die Kontrolleinheit 110 enthält einen Zähler 112, der die Anzahl der Zugriffe auf die geschützten Daten 12 zählt. Ferner enthält die Kontrolleinheit 110 Stellmittel 114. Mit den Stellmitteln 114 wird über den Taktgeber 34, ein Zeitmaß 116 für die Kontrolleinheit 110 festgelegt. Eine mittels
5 Stellmittel 114 einstellbare Anzahl von Taktzyklen des Taktgebers 34 bildet ein Zeitintervall 108. Ein Zähler 118 zählt die Anzahl der Zugriffe auf die geschützten Daten 12.

Wenn innerhalb eines eingestellten Zeitintervalls 108 eine vorgegebene Anzahl von
10 Zugriffen für die Eingabe durch Prüfeinheit 120 festgestellt wird, werden keine weiteren Zugriffe die geschützten Daten 12 mehr zugelassen. Dieser Referenzwert für die Anzahl der möglichen Zugriffe berechnet sich aus Zeitintervallen 108, vorheriger Zugriffe. Beispielsweise, indem die durchschnittliche Anzahl von früheren Zugriffen auf die geschützten Daten 12 pro Zeitintervall 108 festgehalten wird. Durch die Verwendung
15 eines Referenzwertes, der sich aus früheren Zugriffen pro Zeitintervall berechnet, wird eine höhere Flexibilität für den Benutzer erzielt.

Stellt die Prüfeinheit 120 fest, dass die Anzahl der Zugriffe auf die geschützten Daten erhöht sind, wird ein Alarm 122 ausgelöst. Sind die Zugriffe innerhalb eines
20 Zeitintervalls unterhalb eines Referenzwertes, wird der Zähler 112 zurückgesetzt.

Der "Administrator" kann mit der "Reset-Funktion" 42 auch den Zähler 112 für die Zugriffe auf die geschützten Daten 112 zurückstellen. Alternativ wird der Zähler 112 nach Ablauf einer vordefinierten Zeitspanne zurückgestellt.

Patentansprüche

5

1. Einrichtung (10) zur Sicherung und Überwachung von geschützten Daten (12) in einem flüchtigen und/oder nichtflüchtigen Datenspeicher (14) einer Datenverarbeitungseinheit vor unbefugtem Zugriff, wobei

10

- (a) Zugangsmittel (18) vorgesehen sind, über die nur mit einem Berechtigungscode (20) auf die geschützten Daten (12) in dem Datenspeicher (14) zugegriffen werden kann,

15

- (b) Mittel (23) zum Erfassen der Anzahl der Berechtigungscodeeingaben enthalten sind,

20

- (c) Mittel (23, 26) zur Beschränkung des Zugriffs auf die geschützten Daten (12) vorgesehen sind, wobei eine Beschränkung erfolgt, wenn die Anzahl der Berechtigungscodeeingaben innerhalb eines bestimmten Zeitintervalls (36) einen diesem Zeitintervall zugeordneten Referenzwert überschreitet,

dadurch gekennzeichnet, dass

25

- (d) Mittel (110) vorgesehen sind, mit denen unabhängig von der Eingabe des Berechtigungscode (20) die Anzahl der Zugriffe auf die geschützten Daten (12) und/oder Funktionen in dem flüchtigen bzw. nichtflüchtigen Datenspeicher (14) innerhalb eines bestimmten Zeitintervalls (108) ermittelt wird.

30

2. Einrichtung (10) zur Sicherung und Überwachung von geschützten Daten (12) in einem Datenspeicher (14) einer Datenverarbeitungseinheit vor unbefugtem Zugriff nach Anspruch 1, **gekennzeichnet** durch Mittel (120) zur Bestimmung eines

Referenzwertes aus der Anzahl der Zugriffe auf die geschützten Daten (12) und/oder Funktionen pro Zeitintervall (108) vorheriger Zeitintervalle (108).

3. Einrichtung (10) zur Sicherung und Überwachung von geschützten Daten (12) in
5 einem Datenspeicher (14) einer Datenverarbeitungseinheit vor unbefugtem Zugriff nach einem der Ansprüche 1 oder 2, **dadurch gekennzeichnet, dass** die Datenverarbeitungseinheit einen Taktgeber (34) für den Arbeitstakt enthält, wobei das Zeitintervall (108) durch eine bestimmte Anzahl von Taktzyklen des Taktgebers (34) vorgebar ausgebildet ist.
- 10 4. Einrichtung (10) zur Sicherung und Überwachung von geschützten Daten (12) in einem Datenspeicher (14) einer Datenverarbeitungseinheit vor unbefugtem Zugriff nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** die Mittel (110) zur Erfassung der Zugriffe auf die geschützten Daten 12 einen Zähler (112)
15 enthalten, welcher die Anzahl der Zugriffe innerhalb des Zeitintervalls (108) zählt.
5. Einrichtung (10) zur Sicherung und Überwachung von geschützten Daten (12) in einem Datenspeicher (14) einer Datenverarbeitungseinheit nach Anspruch 4,
20 **dadurch gekennzeichnet, dass** Mittel (42) zum Zurücksetzen des Zählers (112) vorgesehen sind, welche den Zähler (112) bei einem berechtigten Zugriff auf Null setzen.
6. Einrichtung (10) zur Sicherung und Überwachung von geschützten Daten (12) in
25 einem Datenspeicher (14) einer Datenverarbeitungseinheit nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet, dass** Mittel (110) zur Beschränkung der Zugriffe auf die geschützten Daten (12) dynamisch eingestellt sind.
7. Einrichtung (10) zur Sicherung und Überwachung von geschützten Daten (12) in
30 einem Datenspeicher (14) einer Datenverarbeitungseinheit nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet, dass** Mittel (110) zur Beschränkung der Zugriffe auf die geschützten Daten (12) auf einen Anwenderprofil einstellbar ausgebildet sind.

- 5
8. Einrichtung (10) zur Sicherung und Überwachung von geschützten Daten (12) in einem Datenspeicher (14) einer Datenverarbeitungseinheit nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet, dass** der Datenspeicher (14) auf einer SIM-Karte vorgesehen ist.
- 10
9. Einrichtung (10) zur Sicherung und Überwachung von geschützten Daten (12) in einem Datenspeicher (14) einer Datenverarbeitungseinheit nach einem der Ansprüche 1 bis 8, **dadurch gekennzeichnet, dass** die Datenverarbeitungseinheit als Mobilfunkendgerät oder Telematikendgerät ausgebildet ist.
- 15
10. Einrichtung (10) zur Sicherung und Überwachung von geschützten Daten (12) in einem Datenspeicher (14) einer Datenverarbeitungseinheit nach einem der Ansprüche 1 bis 9, **dadurch gekennzeichnet, dass** die Datenverarbeitungseinheit als Computer ausgebildet ist.
- 20
11. Einrichtung (10) zur Sicherung und Überwachung von geschützten Daten (12) in einem Datenspeicher (14) einer Datenverarbeitungseinheit nach einem der Ansprüche 1 bis 10, **dadurch gekennzeichnet, dass** Alarmmittel (112) vorgesehen sind, welche bei Überschreiten eines Referenzwertes für die Anzahl der Zugriffe auf die geschützten Daten (12) ein Alarmsignal erzeugen.
- 25
12. Verfahren zur Sicherung und Überwachung von geschützten Daten (12) vor unbefugtem Zugriff mit einer Einrichtung (10) gemäß einem der vorherigen Ansprüche, wobei
- 30
- (a) die Anzahl der Berechtigungscodeeingaben für den Zugriffe auf die geschützten Daten (12) innerhalb eines bestimmten Zeitintervalls (36) ermittelt wird und
- (b) diese Anzahl der Versuche innerhalb des bestimmten Zeitintervalls (36) mit einem Referenzwert verglichen wird, wobei

- (c) der Zugriff auf die geschützten Daten beschränkt oder verhindert wird, wenn die Anzahl der Eingaben innerhalb des Zeitintervalls größer als der Referenzwert ist,

5 **dadurch gekennzeichnet, dass**

- (d) unabhängig von der Eingabe des Berechtigungscode (20) die Anzahl der Zugriffe auf die geschützten Daten (12) und/oder Funktionen in dem flüchtigen bzw. nichtflüchtigen Datenspeicher (14) innerhalb eines bestimmten Zeitintervalls (108) ermittelt wird.

10 13. Verfahren zur Sicherung und Überwachung von geschützten Daten (12) vor unbefugtem Zugriff nach Anspruch 12, **dadurch gekennzeichnet, dass** ein Referenzwert sich aus der Anzahl der Zugriffe auf die geschützten Daten (12) vorheriger Zeitintervalle (108) berechnet.

15 14. Verfahren zur Sicherung und Überwachung von geschützten Daten (12) vor unbefugtem Zugriff nach Anspruch 13, **dadurch gekennzeichnet, dass** der Zugriff auf die geschützten Daten (12) beschränkt wird, wenn die Anzahl der Zugriffe auf die geschützten Daten (12) innerhalb eines bestimmten Zeitintervalls (108) einen Referenzwert überschreitet.

20 15. Verfahren zur Sicherung und Überwachung von geschützten Daten (12) vor unbefugtem Zugriff nach einem der Ansprüche 12 bis 14, **dadurch gekennzeichnet, dass** der Zähler (112) zum Zählen der Anzahl Zugriffe auf die geschützten Daten (12), bei einem korrekten Zugriff, zurückgesetzt wird.

25 16. Verfahren zur Sicherung und Überwachung von geschützten Daten (12) vor unbefugtem Zugriff nach einem der Ansprüche 12 bis 15, **dadurch gekennzeichnet, dass** die mögliche Anzahl der Zugriffe auf die geschützten Daten (12) für die Beschränkung eingestellt und/oder an ein Anwenderprofil angepasst wird.

17. Verfahren zur Sicherung und Überwachung von geschützten Daten (12) vor unbefugtem Zugriff nach einem der Ansprüche 12 bis 16, **dadurch gekennzeichnet, dass** die mögliche Anzahl der Zugriffe für die Beschränkung über ein Netzwerk, insbesondere Mobilfunknetzwerk, eingestellt und/oder an einen Anwenderprofil angepasst wird.
18. Verfahren zur Sicherung und Überwachung von geschützten Daten (12) vor unbefugtem Zugriff nach einem der Ansprüche 12 bis 17, **dadurch gekennzeichnet, dass** bei Überschreiten eines Referenzwertes für die Anzahl der Zugriffe auf die geschützten Daten (12) ein geeignetes Alarmsignal erzeugt wird.
19. Verfahren zur Sicherung und Überwachung von geschützten Daten (12) vor unbefugtem Zugriff nach Anspruch 18, **dadurch gekennzeichnet, dass** das Alarmsignal zur Erzeugung einer Abwehrmaßnahme ausgewertet wird.
20. Verfahren zur Sicherung und Überwachung von geschützten Daten (12) vor unbefugtem Zugriff nach Anspruch 19, **dadurch gekennzeichnet, dass** die Abwehrmaßnahmen in einem Strecken der Antwortzeit bestehen.
21. Verfahren zur Sicherung und Überwachung von geschützten Daten (12) vor unbefugtem Zugriff nach einem der Ansprüche 19 oder 20, **dadurch gekennzeichnet, dass** die Abwehrmaßnahmen in einem Verfälschen eines Ergebnisses bestehen.
22. Verfahren zur Sicherung und Überwachung von geschützten Daten (12) vor unbefugtem Zugriff nach einem der Ansprüche 12 bis 21, **dadurch gekennzeichnet, dass** das Alarmsignal für den auf die geschützten Daten (12) Zugreifenden nicht erkennbar ist.
23. Verfahren zur Sicherung und Überwachung von geschützten Daten (12) vor unbefugtem Zugriff nach einem der Ansprüche 12 bis 23, **dadurch gekennzeichnet, dass** bei Überschreiten eines Wertes für die Anzahl Zugriffe

weitere Zugriff innerhalb eines Zeitintervalls (36) auf die Daten (12) verweigert wird.

- 5 24. Verfahren zur Sicherung und Überwachung von geschützten Daten (12) vor unbefugtem Zugriff nach einem der Ansprüche 12 bis 24, **dadurch gekennzeichnet, dass** bei Überschreiten eines Wertes für die Anzahl Zugriffe der weitere Zugriff auf die geschützten Daten (12) für einen Zeitraum beschränkt ist.

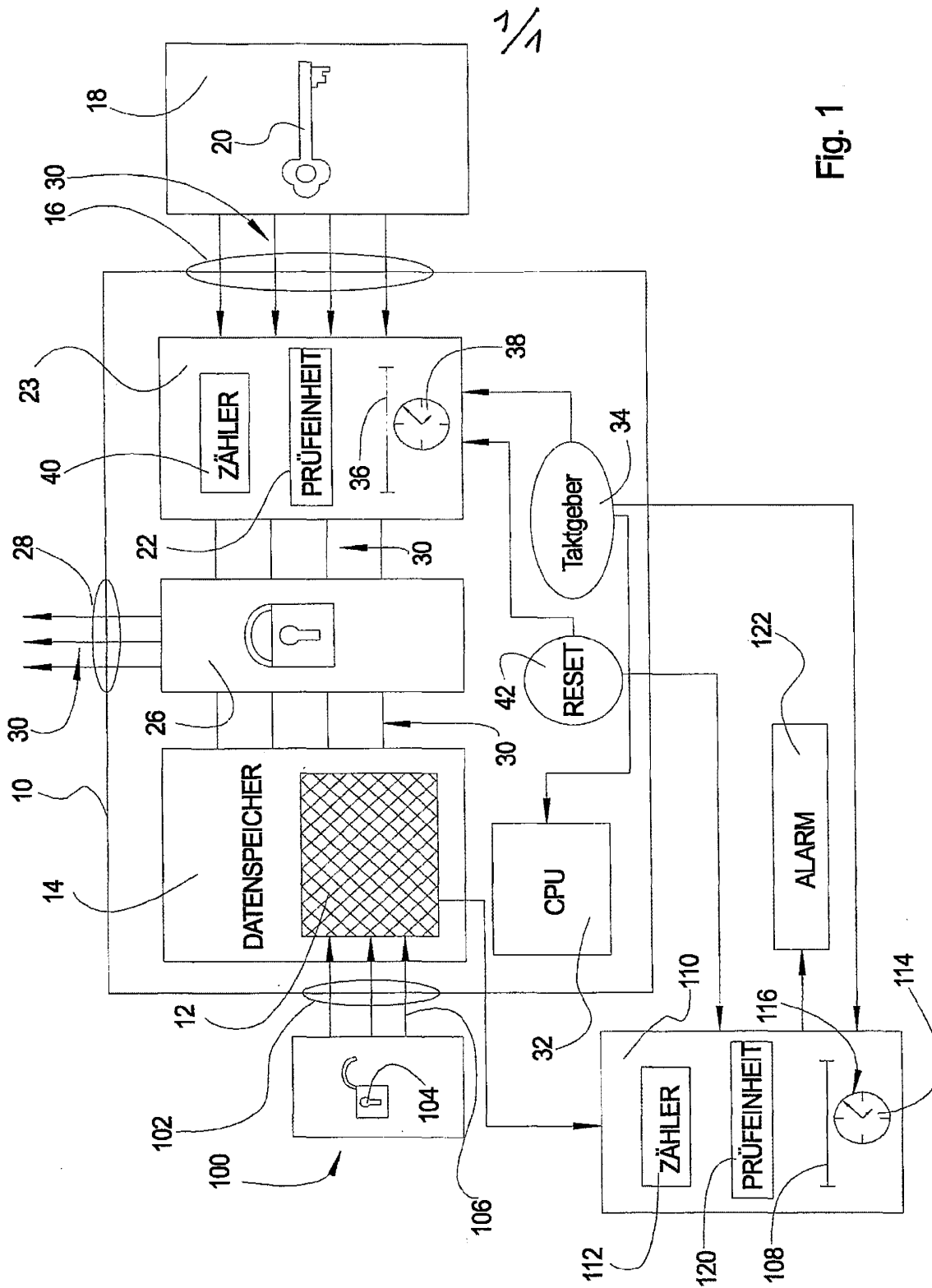


Fig. 1

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/EP2004/011338

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 209 551 A (INTERNATIONAL BUSINESS MACHINES CORPORATION) 29 May 2002 (2002-05-29) cited in the application	1-5, 8-15, 18-24
Y	abstract paragraph '0003! - paragraph '0007! paragraph '0013! paragraph '0016! paragraph '0018! paragraph '0028! - paragraph '0036! ----- -/-	6, 7, 16, 17

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *Z* document member of the same patent family

Date of the actual completion of the international search

1 February 2005

Date of mailing of the international search report

17/02/2005

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2260 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3010

Authorized officer

Kleiber, M

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/011338

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	F. MONROSE, M.K. REITER, S. WETZEL: "Password hardening based on keystroke dynamics" INTERNATIONAL JOURNAL OF INFORMATION SECURITY, vol. 1, no. 2, 26 October 2001 (2001-10-26), pages 69-83, XP002315670 abstract page 70, column 1, paragraph 3 - paragraph 4 page 70, column 2, paragraph 1 -----	6,7,16, 17
A	DE 198 39 041 A1 (INTERNATIONAL BUSINESS MACHINES CORP., ARMONK) 2 March 2000 (2000-03-02) cited in the application the whole document -----	1-24
A	"Handbuch zum ChipCard Center Desktop" "Online!" 1999, SMART PAY SYSTEMS, ELTVILLE, GERMANY, XP002315671 Retrieved from the Internet: URL: http://www.smartpaysystems.de/service/download/handbuch/hbcenter.pdf Abschnitte 1.5, 2.2, 3.1.1, 3.1.3, 3.1.4 abstract -----	1-24
P,A	GUVEN A ET AL: "Understanding users' keystroke patterns for computer access security" COMPUTERS & SECURITY, ELSEVIER SCIENCE PUBLISHERS, AMSTERDAM, NL, vol. 22, no. 8, December 2003 (2003-12), pages 695-706, XP004482668 ISSN: 0167-4048 the whole document -----	6,7,16, 17

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP2004/011338

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 1209551	A	29-05-2002	EP 1209551 A2	29-05-2002
			US 2002108046 A1	08-08-2002
DE 19839041	A1	02-03-2000	EP 0982693 A2	01-03-2000
			JP 2000076134 A	14-03-2000

Form PCT/ISA/210 (patent family annex) (January 2004)

INTERNATIONALER RECHERCHENBERICHT

Internationales Abdruckzeichen

PCT/EP2004/011338

A. KLASIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 1 209 551 A (INTERNATIONAL BUSINESS MACHINES CORPORATION) 29. Mai 2002 (2002-05-29) in der Anmeldung erwähnt	1-5, 8-15, 18-24
Y	Zusammenfassung Absatz '0003! - Absatz '0007! Absatz '0013! Absatz '0016! Absatz '0018! Absatz '0028! - Absatz '0036! ----- -/-	6,7,16, 17

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

A Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

E älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

L Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

O Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

P Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

Z Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

1. Februar 2005

Absendedatum des internationalen Recherchenberichts

17/02/2005

Name und Postanschrift der internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3010

Bevollmächtigter Beauftragter

Kleiber, M

Formblatt PCT/ISA/210 (Blatt 2) (Januar 2004)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2004/011338

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	F. MONROSE, M.K. REITER, S. WETZEL: "Password hardening based on keystroke dynamics" INTERNATIONAL JOURNAL OF INFORMATION SECURITY, Bd. 1, Nr. 2, 26. Oktober 2001 (2001-10-26), Seiten 69-83, XP002315670 Zusammenfassung Seite 70, Spalte 1, Absatz 3 - Absatz 4 Seite 70, Spalte 2, Absatz 1 -----	6,7,16, 17
A	DE 198 39 041 A1 (INTERNATIONAL BUSINESS MACHINES CORP., ARMONK) 2. März 2000 (2000-03-02) in der Anmeldung erwähnt das ganze Dokument -----	1-24
A	"Handbuch zum ChipCard Center Desktop" 'Online! 1999, SMART PAY SYSTEMS, ELTVILLE, GERMANY, XP002315671 Gefunden im Internet: URL: http://www.smartpaysystems.de/service/download/handbuch/hbcenter.pdf Abschnitte 1.5, 2.2, 3.1.1, 3.1.3, 3.1.4 Zusammenfassung -----	1-24
P,A	GUVEN A ET AL: "Understanding users' keystroke patterns for computer access security" COMPUTERS & SECURITY, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, Bd. 22, Nr. 8, Dezember 2003 (2003-12), Seiten 695-706, XP004482668 ISSN: 0167-4048 das ganze Dokument -----	6,7,16, 17

Formblatt PCT/3A/210 (Fortsetzung von Blatt 2) (Januar 2004)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2004/011338

im Recherchenbericht angeführtes Patentedokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 1209551 A	29-05-2002	EP 1209551 A2	29-05-2002
		US 2002108046 A1	08-08-2002
DE 19839041 A1	02-03-2000	EP 0982693 A2	01-03-2000
		JP 2000076134 A	14-03-2000

Formblatt POT/ISA/210 (Anhang Patentfamilie) (Januar 2004)

Electronic Acknowledgement Receipt	
EFS ID:	15780157
Application Number:	13689088
International Application Number:	
Confirmation Number:	9927
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Scott B. Guthery
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Robert Roe-Pachirat
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943AAAB-178-DIV
Receipt Date:	15-MAY-2013
Filing Date:	29-NOV-2012
Time Stamp:	11:06:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		IDS_02.pdf	186821	yes	5
			886e4cc24aede0e139f388189f37ea5e60da6bfe		

Multipart Description/PDF files in .zip description					
Document Description			Start	End	
Transmittal Letter			1	3	
Information Disclosure Statement (IDS) Form (SB08)			4	5	
Warnings:					
Information:					
2	Foreign Reference	EP1209551A2.pdf	348220	no	8
			e8f87ecf01e67b4a6e3f13bba7a1ff600c85129		
Warnings:					
Information:					
3	Foreign Reference	EP1418484A2.pdf	923300	no	16
			d0df8ceb7cef03744c67e5b1be520d96e339de3f		
Warnings:					
Information:					
4	Foreign Reference	WO2005038633A1.pdf	1231066	no	27
			a72ea51fb105fc65caaaddd541216f97ff6a2041		
Warnings:					
Information:					
5	Non Patent Literature	2943-184-EP_09167708_SR.pdf	181077	no	6
			40f9679c7a4f6aeaff5d3479309a6b3ca4d6efc		
Warnings:					
Information:					
6	Non Patent Literature	2943AAAB-178_NOA_08-31-2012.pdf	435031	no	8
			6686520f9940a28d52c8927ee054924d7f953967		
Warnings:					
Information:					
7	Non Patent Literature	2943AAAB-184_OA_06-14-2012.pdf	480761	no	14
			4f347ebee8629a8be5a4e985bb03172095ad80b0		
Warnings:					
Information:					
8	Non Patent Literature	2943AAAB-184_OA_02-11-2013.pdf	761939	no	20
			65ce0dfb7cd2d3e6ef52061b7bb26ba9d6dbec04		
Warnings:					
Information:					

9	Non Patent Literature	2943-184-EP_OA_6-16-2010. pdf	125281 de32d101715f81cde04b4ac58fabea280d1 dcd98	no	4
Warnings:					
Information:					
Total Files Size (in bytes):					4673496
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:)	Group Art Unit: 2431
Scott B. Guthery)	Confirmation No.: 9927
Serial No.: 13/689,088)	Examiner:
Filed: November 29, 2012)	
Atty. File No.: 2943AAAB-178-DIV)	<u>SUPPLEMENTAL</u>
Entitled: "Secure Wiegand Communications")	<u>INFORMATION DISCLOSURE</u>
)	<u>STATEMENT</u>
)	<i>Electronically Submitted</i>

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

The references cited on attached Form PTO/SB08 are being called to the attention of the Examiner.

- ☒ Copies of the cited non-patent and/or foreign references are enclosed herewith.
- ☐ Copies of the cited U.S. patents and/or patent applications are enclosed herewith.
- ☒ Copies of the cited U.S. patents/patent application publications are not enclosed in accordance with 37 C.F.R. § 1.98(a).
- ☐ Copies of the cited references are not enclosed, in accordance with 37 C.F.R. § 1.98(d), because the references were cited by or submitted to the U.S. Patent and Trademark Office in prior application Serial No. _____ filed _____, which is relied upon for an earlier filing date under 35 U.S.C. § 120.
- ☒ To the best of applicants' belief, the pertinence of the foreign-language references is believed to be summarized in the attached English abstracts and/or in the figures, although applicants do not necessarily vouch for the accuracy of the translation.
- ☒ Examiner's attention is drawn to the following related applications:
- Serial No. 12/541,480 filed 08/14/09 (Attorney's Ref. No. 2943AAAB-184)
- ☐ Other: _____

Submission of the above information is not intended as an admission that any item is citable under the statutes or rules to support a rejection, that any item disclosed represents analogous art, or that those skilled in the art would refer to or recognize the pertinence of any reference without the benefit of hindsight, nor should an inference be drawn as to the pertinence

of the references based on the order in which they are presented. Submission of this statement should not be taken as an indication that a search has been conducted, or that no better art exists.

It is respectfully requested that the cited information be expressly considered during the prosecution of this application and the references made of record therein.

FEES

<input checked="" type="checkbox"/>	<p>37 CFR 1.97(b): No fee is believed due in connection with this submission, because the information disclosure statement submitted herewith is satisfied by one of the following conditions ("X" indicates satisfaction):</p> <p><input type="checkbox"/> Within three months of the filing date of a national application other than a continued prosecution application under 37 CFR 1.53(d), or</p> <p><input type="checkbox"/> Within three months of the date of entry of the national stage as set forth in § 1.491 in an international application, or</p> <p><input checked="" type="checkbox"/> Before the mailing date of a first Office Action on the merits, or</p> <p><input type="checkbox"/> Before the mailing of a first Office action after the filing of a request for continued examination under 37 CFR 1.114.</p> <p>Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970.</p>
<input type="checkbox"/>	<p>37 CFR 1.97(c): The information disclosure statement transmitted herewith is being filed after all the above conditions (37 CFR 1.97(b)), but before the mailing date of any one of the following conditions:</p> <p style="padding-left: 40px;">(1) a final action under 37 C.F.R. 1.113, or</p> <p style="padding-left: 40px;">(2) a notice of allowance under 37 C.F.R. 1.311, or</p> <p style="padding-left: 40px;">(3) an action that otherwise closes prosecution in the application.</p> <p>This Information Disclosure Statement is accompanied by:</p> <p><input type="checkbox"/> A Certification (below) as specified by 37 C.F.R. 1.97(e). Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970.</p> <p style="text-align: center;">OR</p> <p><input type="checkbox"/> Please charge Deposit Account 19-1970 in the amount of \$180.00 for the fee set forth in 37 C.F.R. 1.17(p) for submission of an information disclosure statement. Please credit any overpayment or charge any underpayment to Deposit Account 19-1970.</p>
<input type="checkbox"/>	<p>37 CFR 1.97(d): This Information Disclosure Statement is being submitted after the period specified in 37 CFR 1.97(c).</p> <p><input type="checkbox"/> This information Disclosure Statement includes a Certification (below) as specified by 37 C.F.R. 1.97(e)</p> <p style="text-align: center;">AND</p> <p><input type="checkbox"/> Applicants hereby requests consideration of the reference(s) disclosed herein. Please charge Deposit Account 19-1970 in the amount of \$180.00 under 37 C.F.R. 1.17(p). Please credit any overpayment or charge any underpayment to Deposit Account 19-1970. Election to pay the fee should not be taken as an indication that applicant(s) cannot execute a certification.</p>

Certification (37 C.F.R. 1.97(e))
(Applicable only if checked)

- ☐ The undersigned certifies that:
- ☐ Each item of information contained in this information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(1).
 - ☐ A copy of the communication from the foreign patent office is enclosed.

OR

- ☐ No item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in 37 C.F.R. 1.56(c) more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(2).

Respectfully submitted,

SHERIDAN ROSS P.C.

By: /Matthew R. Ellsworth/
Matthew R. Ellsworth
Registration No. 56345
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: May 15, 2013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:)	Group Art Unit: Not Yet Assigned
)	
GUTHERY et al.)	Examiner: Not Yet Assigned
)	
Serial No.: 13/689,088)	Confirmation No.: 9927
)	
Filed: November 29, 2012)	
)	
Atty. File No.: 2943AAAB-178-DIV)	
)	
For: "SECURE WIEGAND)	
COMMUNICATIONS")	
)	

RESPONSE TO INFORMATIONAL NOTICE TO APPLICANT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Madam:

In response to the Informational Notice to Applicant mailed January 16, 2013, in connection with the above-identified application, enclosed for filing is a Declaration. Although Applicant believes that no fees are due in connection with the filing of this paper, please charge any fees deemed necessary, or credit any overpayment to Deposit Account No. 19-1970.

Respectfully submitted,

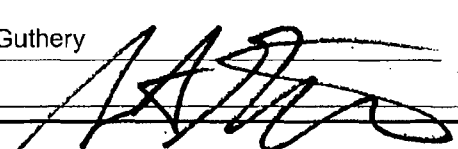
SHERIDAN ROSS P.C.

Date: May 16, 2013

By: /Matthew R. Ellsworth/
Matthew R. Ellsworth
Reg. No. 56,345
Telephone: 303-863-2989

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

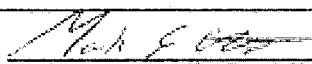
Title of Invention	SECURE WIEGAND COMMUNICATIONS
<p>As the below named inventor, I hereby declare that:</p> <p>This declaration is directed to: <input type="checkbox"/> The attached application, or <input checked="" type="checkbox"/> United States application or PCT international application number <u>13/689,088</u> filed on <u>2012-11-29</u>.</p> <p>The above-identified application was made or authorized to be made by me.</p> <p>I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.</p> <p>I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.</p> <p style="text-align: center;">WARNING:</p> <p>Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.</p> <p>LEGAL NAME OF INVENTOR</p> <p>Inventor: <u>Scott B. Guthery</u> Date (Optional): <u>2/4/13</u></p> <p>Signature: </p> <p>Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.</p>	

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

Title of Invention	SECURE WIEGAND COMMUNICATIONS
<p>As the below named inventor, I hereby declare that:</p> <p>This declaration is directed to: <input type="checkbox"/> The attached application, or <input checked="" type="checkbox"/> United States application or PCT international application number <u>13/689,088</u> filed on <u>2012-11-29</u>.</p> <p>The above-identified application was made or authorized to be made by me.</p> <p>I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.</p> <p>I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.</p> <p style="text-align: center;">WARNING:</p> <p>Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.</p> <p>LEGAL NAME OF INVENTOR</p> <p>Inventor: <u>Mark Robinton</u> Date (Optional): <u>3/8/13</u></p> <p>Signature: <u></u></p> <p>Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.</p>	

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

Title of Invention	SECURE WIEGAND COMMUNICATIONS
<p>As the below named inventor, I hereby declare that:</p> <p>This declaration is directed to: <input type="checkbox"/> The attached application, or <input checked="" type="checkbox"/> United States application or PCT international application number <u>13/689,088</u> filed on <u>2012-11-29</u></p> <p>The above-identified application was made or authorized to be made by me.</p> <p>I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.</p> <p>I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.</p> <p style="text-align: center;">WARNING:</p> <p>Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.</p> <p>LEGAL NAME OF INVENTOR</p> <p>Inventor: <u>Michael Lawrence Davis</u> Date (Optional): <u>2/4/2013</u> Signature: <u>Michael J Davis</u></p> <p>Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.</p>	

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

Title of Invention	SECURE WIEGAND COMMUNICATIONS
<p>As the below named inventor, I hereby declare that:</p> <p>This declaration is directed to: <input type="checkbox"/> The attached application, or <input checked="" type="checkbox"/> United States application or PCT international application number <u>13/689,088</u> filed on <u>2012-11-29</u>.</p> <p>The above-identified application was made or authorized to be made by me.</p> <p>I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.</p> <p>I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.</p> <p style="text-align: center;">WARNING:</p> <p>Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.</p>	
<p>LEGAL NAME OF INVENTOR</p> <p>Inventor: <u>David Andresky</u> Date (Optional): <u>2/12/2013</u></p> <p>Signature: <u>David Andresky</u></p>	
<p>Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.</p>	

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt	
EFS ID:	15794035
Application Number:	13689088
International Application Number:	
Confirmation Number:	9927
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Scott B. Guthery
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Leslie Roberts
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943AAAB-178-DIV
Receipt Date:	16-MAY-2013
Filing Date:	29-NOV-2012
Time Stamp:	13:21:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant Response to Pre-Exam Formalities Notice	RESPONSE_INFORMATIONAL_NOTICE.pdf	74320 6eadbdc4e50bf39eb96cf564db4e830de7355e8c	no	1

Warnings:

Information:

2	Oath or Declaration filed	DECLARATION.pdf	566346	no	4
			ad520be1142cbe9d8d5776a406e71c38418cf5b1		
Warnings:					
Information:					
Total Files Size (in bytes):				640666	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2432
				Examiner Name	Cordelia P K Zecher
Sheet	1	of	1	Attorney Docket Number	2943AAAB-178-DIV

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document Country Code ³ ; Number ⁴ ; Kind Code ⁵ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶

NON-PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	1	Official Action for European Patent Application No. 09167708.8, dated Apr. 17, 2013 (Attorney's Ref. No. 2943AAAB-184-EP) 4 pages
	2	Official Action for U.S. Patent Application No. 12/541,480, mailed Jun. 05, 2013 (Attorney's Ref. No. 2943AAAB-184) 22 pages

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Electronic Acknowledgement Receipt	
EFS ID:	16649745
Application Number:	13689088
International Application Number:	
Confirmation Number:	9927
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Scott B. Guthery
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Robert Roe-Pachirat
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943AAAB-178-DIV
Receipt Date:	21-AUG-2013
Filing Date:	29-NOV-2012
Time Stamp:	16:35:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		IDS_03_2943AAAB-178-DIV.pdf	150574 5a49d370af3d249ae608e417fdab0970442b041d	yes	4

Multipart Description/PDF files in .zip description					
Document Description			Start	End	
Transmittal Letter			1	3	
Information Disclosure Statement (IDS) Form (SB08)			4	4	
Warnings:					
Information:					
2	Non Patent Literature	2943AAAB-184-EP_OA_04-17-2013.pdf	123813	no	4
			d424f33724a86f67378557bebb62ce078a420e8		
Warnings:					
Information:					
3	Non Patent Literature	2943AAAB-184_OA_06-05-2013.pdf	864140	no	22
			2850cb3369beb47a02835a50f6eb730236ee2a9		
Warnings:					
Information:					
Total Files Size (in bytes):			1138527		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:)	Group Art Unit: 2432
Scott B. Guthery)	Confirmation No.: 9927
Serial No.: 13/689,088)	Examiner: Cordelia P K Zecher
Filed: November 29, 2012)	
Atty. File No.: 2943AAAB-178-DIV)	<u>SUPPLEMENTAL</u>
Entitled: "Secure Wiegand Communications")	<u>INFORMATION DISCLOSURE</u>
)	<u>STATEMENT</u>
)	<i>Electronically Submitted</i>

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

The references cited on attached Form PTO/SB08 are being called to the attention of the Examiner.

- ☒ Copies of the cited non-patent and/or foreign references are enclosed herewith.
- ☐ Copies of the cited U.S. patents and/or patent applications are enclosed herewith.
- ☐ Copies of the cited U.S. patents/patent application publications are not enclosed in accordance with 37 C.F.R. § 1.98(a).
- ☐ Copies of the cited references are not enclosed, in accordance with 37 C.F.R. § 1.98(d), because the references were cited by or submitted to the U.S. Patent and Trademark Office in prior application Serial No. _____ filed _____, which is relied upon for an earlier filing date under 35 U.S.C. § 120.
- ☐ To the best of applicants' belief, the pertinence of the foreign-language references is believed to be summarized in the attached English abstracts and/or in the figures, although applicants do not necessarily vouch for the accuracy of the translation.
- ☐ Examiner's attention is drawn to the following related applications:
Serial No. _____ filed _____ (Attorney Ref. No. _____)
Serial No. _____ filed _____ (Attorney Ref. No. _____)
- ☐ Other: _____

Submission of the above information is not intended as an admission that any item is citable under the statutes or rules to support a rejection, that any item disclosed represents analogous art, or that those skilled in the art would refer to or recognize the pertinence of any reference without the benefit of hindsight, nor should an inference be drawn as to the pertinence

of the references based on the order in which they are presented. Submission of this statement should not be taken as an indication that a search has been conducted, or that no better art exists.

It is respectfully requested that the cited information be expressly considered during the prosecution of this application and the references made of record therein.

FEES

<input checked="" type="checkbox"/>	<p>37 CFR 1.97(b): No fee is believed due in connection with this submission, because the information disclosure statement submitted herewith is satisfied by one of the following conditions ("X" indicates satisfaction):</p> <p><input type="checkbox"/> Within three months of the filing date of a national application other than a continued prosecution application under 37 CFR 1.53(d), or</p> <p><input type="checkbox"/> Within three months of the date of entry of the national stage as set forth in § 1.491 in an international application, or</p> <p><input checked="" type="checkbox"/> Before the mailing date of a first Office Action on the merits, or</p> <p><input type="checkbox"/> Before the mailing of a first Office action after the filing of a request for continued examination under 37 CFR 1.114.</p> <p>Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970.</p>
<input type="checkbox"/>	<p>37 CFR 1.97(c): The information disclosure statement transmitted herewith is being filed after all the above conditions (37 CFR 1.97(b)), but before the mailing date of any one of the following conditions:</p> <p style="padding-left: 40px;">(1) a final action under 37 C.F.R. 1.113, or</p> <p style="padding-left: 40px;">(2) a notice of allowance under 37 C.F.R. 1.311, or</p> <p style="padding-left: 40px;">(3) an action that otherwise closes prosecution in the application.</p> <p>This Information Disclosure Statement is accompanied by:</p> <p><input type="checkbox"/> A Certification (below) as specified by 37 C.F.R. 1.97(e). Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970.</p> <p style="text-align: center;">OR</p> <p><input type="checkbox"/> Please charge Deposit Account 19-1970 in the amount of \$180.00 for the fee set forth in 37 C.F.R. 1.17(p) for submission of an information disclosure statement. Please credit any overpayment or charge any underpayment to Deposit Account 19-1970.</p>
<input type="checkbox"/>	<p>37 CFR 1.97(d): This Information Disclosure Statement is being submitted after the period specified in 37 CFR 1.97(c).</p> <p><input type="checkbox"/> This information Disclosure Statement includes a Certification (below) as specified by 37 C.F.R. 1.97(e)</p> <p style="text-align: center;">AND</p> <p><input type="checkbox"/> Applicants hereby requests consideration of the reference(s) disclosed herein. Please charge Deposit Account 19-1970 in the amount of \$180.00 under 37 C.F.R. 1.17(p). Please credit any overpayment or charge any underpayment to Deposit Account 19-1970. Election to pay the fee should not be taken as an indication that applicant(s) cannot execute a certification.</p>

Certification (37 C.F.R. 1.97(e))
(Applicable only if checked)

- ☐ The undersigned certifies that:
- ☐ Each item of information contained in this information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(1).
 - ☐ A copy of the communication from the foreign patent office is enclosed.

OR

- ☐ No item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in 37 C.F.R. 1.56(c) more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(2).

Respectfully submitted,

SHERIDAN ROSS P.C.

By: /Matthew R. Ellsworth/
Matthew R. Ellsworth
Registration No. 56345
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: August 21, 2013



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/689,088	11/29/2012	Scott B. Guthery	2943AAB-178-DIV	9927
22442	7590	01/17/2014	EXAMINER	
Sheridan Ross PC 1560 Broadway Suite 1200 Denver, CO 80202			LEMMA, SAMSON B	
			ART UNIT	PAPER NUMBER
			2432	
			NOTIFICATION DATE	DELIVERY MODE
			01/17/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

c-docket@sheridanross.com

Office Action Summary	Application No. 13/689,088	Applicant(s) GUTHERY ET AL.	
	Examiner SAMSON LEMMA	Art Unit 2432	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 11/29/2012.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

- 5) ☒ Claim(s) 1-20 is/are pending in the application.
5a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 6) ☐ Claim(s) ____ is/are allowed.
- 7) ☒ Claim(s) 1-5, 8-12 and 15-18 is/are rejected.
- 8) ☒ Claim(s) 6, 7, 13, 14, 19 and 20 is/are objected to.
- 9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

- 10) ☐ The specification is objected to by the Examiner.
- 11) ☒ The drawing(s) filed on 11/29/2012 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

- a) ☐ All b) ☐ Some** c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 3) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) | Paper No(s)/Mail Date. ____. |
| Paper No(s)/Mail Date ____. | 4) <input type="checkbox"/> Other: ____. |

DETAILED ACTION

1. This office action is in response to an application No. 13/689,088 filed on November 29, 2012. Claims 1-20 are submitted for examination and claims 1, 8 and 15 are independent.

Priority

2. This application filed on 11/29/2012 is a division of application No. 12/539,4312, filed on 08/11/2019, now US Patent No. 8358783 and claims priority from provisional application No. 61087941, filed on 08/11/2008. Therefore, the effective filling date for the subject matter defined in the pending claims of this application is **August 11, 2008**.

Information Disclosure Statement

3. The submitted information disclosure statements (IDS), have been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

Drawings

4. The drawings filed on November 29, 2012 are accepted.

Specification

5. The specification filed on November 29, 2012 is also accepted.

Double Patenting

6. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).
A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).
Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).
7. Claims 1-20 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-27 of the U.S. Patent No. 8,358,783 B2 (hereinafter refereed as '783 Patent.) Although the conflicting claims are not identical, they are not patentably distinct from each other.

The following is referring to the independent claims 1, 8 and 15

- As per independent claims 1, 8 and 15,
Independent claim 1, 8 and 15 of the instant application and claim 1, and 18, of the '783 patent recite similar limitation. The above independent claim, namely independent claims 1, 8 and 15 of the instant/present application would have been obvious over independent claims 1 and 18, of the '783 patent because each and every element of the above independent

claims 1, 8 and 15 of the present application is anticipated by the corresponding independent claims 1 and 18 of the '783 patent.

The following is applicable to the dependent claims 2-7, 9-14, and 16-20

- As per dependent claims 2-7, 9-14 and 16-20, Dependent Claims 2-7, 9-14 and 16-20 of the instant application and claims **2-17 and 19-27 of the '783 patent** further recite similar/equivalent limitation of the same subject matter. Thus, the above dependent claims, namely dependent claims 2-7, 9-14 and 16-20 of the instant/present application would have been obvious over dependent claims 2-17 and 19-27, of the '783 patent because each and every element of the above dependent claims 2-7, 9-14 and 16-20, of the present application is anticipated by the corresponding dependent claims 2-17 and 19-27 of the '783 patent.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 5, 12 and 18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 5, 12 and 18 recites the limitation, "human perceivable amount of time" and this limitation is a relative term which renders the claim indefinite. The term "human perceivable amount of time" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. For this reason the office could not determine the scope of this claim and appropriate correction is required.

Claim Rejections - 35 USC § 101

10. 35 U.S.C. 101 reads as follows:
- Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.
11. **Claims 1-14** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.
12. **Independent claim 1** is rejected under 35 U.S.C. 101 because the method steps recited in independent claim 1 are could be done or completely performed mentally, verbally and are directed merely to an abstract idea.
- Machine-or-Transformation test (1st test)**

Based on Supreme Court precedent and recent Federal Circuit decisions, a 35 U.S.C § 101 process is tested the following machine or transformation test (1) is it tied to a particular machine or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. In re Bilski et al, 88 USPQ 2d 1385 CAFC (2008); Diamond v. Diehr, 450 U.S. 175, 184 (1981); Parker v. Flook, 437 U.S. 584, 588 n.9 (1978); Gottschalk v. Benson, 409 U.S. 63, 70 (1972); Cochrane v. Deener, 94 U.S. 780,787-88 (1876).

An example of a method claim that would not qualify as a statutory process would be a claim that recited purely mental steps or abstract idea. Thus, one way to qualify as a § 101 statutory process, the claim should positively recite the particular machine to which it is tied, for example by identifying the apparatus that accomplishes the method steps, or positively recite the subject matter that is being transformed, for example by identifying the material that is being changed to a different state.

Here however, applicant's method steps: recited in independent claim 1, are broad enough that the steps could be done or completely performed mentally, verbally or without a machine nor is any transformation apparent.

(2nd or subsequent test)

Since a claimed method recited in independent claim 1 do not meet or failed to meet the above machine-or-transformation test, examiner further raises a question whether or not the method claim is directed to the an abstract idea.

As it is indicated above, it is found that method steps recited in claims 6 and 16 are purely mental steps or abstract idea. Thus claim 1 is rejected under 35 U.S.C. 101 because the method steps recited in independent claim 1 are broad enough that the steps could be done or completely performed mentally, verbally and are directed merely to an abstract idea to form the basis of statutory subject matter under 35 U.S.C. 101. See MPEP § 2106 IV. B. 1(a).

13. Dependent claims 2-7 are rejected under 35 U.S.C. 101 because the method steps recited in these dependent claims are broad enough that the steps could be done or completely performed mentally, verbally and are directed merely to an abstract idea.

 14. Claims 8-14 are directed to a computer readable medium for storing computer program instructions...” Examiner asserts that this particular limitation such as “computer readable medium” can be broadly or reasonably interpreted as being just a signal. In view of this interpretation and understanding, the office asserts that the claim does not fall within the statutory classes listed in 35 USC 101. See MPEP § 2106 IV. B. 1(a).
- Note: Replacing the limitation “computer readable medium” with “non-transitory computer-readable medium” would overcome this particular ground of rejection.

Claim Rejections - 35 USC § 102

15. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

16. Claims 1-5, 8-12 and 15-18 are rejected under 35 U.S.C. 102(e) as being anticipated by **Davis, Michael** (hereinafter referred as **Davis**) (International Publication No. EP1760985) (Published on 03/07/2007)

17. **As per independent claims 1, 8 and 15 Davis discloses a communication method** [See at least figure 1], **comprising:**
operating a credential reader in a first mode of operation [See at least on paragraph 0043, 0045, figure 1 and 2 the reader 112]; **receiving, at the credential reader, a message from an upstream device** [See at least paragraph 0043 and 0045 and figure 1-2, see the message that is received from the control panel 104 at the reader 112, the control panel 104 meets the limitation, “upstream device”];

determining, by the credential reader, that the message was transmitted by the upstream device [See at least paragraphs 0043 and 0045, Figure 1 and 2]; **and based on determining that the message was transmitted by the upstream device, transitioning the credential reader from the first mode of operation to a second mode of operation** [See at least paragraph 0045, “the control panel could inform the reader to change how it is working...with a prompting signal send via an LED control signal].

18. **As per dependent claims 2 and 9 Davis discloses a method as applied to claims above. Furthermore Davis discloses the method , wherein the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol.**[See at least paragraph 0043, “the communications protocol between the control panel 104 and the reader 112 is typically considered unidirectional...”]
19. **As per dependent claims 3, 10 and 16 Davis discloses a method as applied to claims above. Furthermore Davis discloses the method , wherein the unidirectional communication protocol is the Wiegand protocol.**[See at least paragraph 0009 and 0043, “Wiegand”]
20. **As per dependent claims 4-5, 11-12 and 17-18 Davis discloses a method as applied to claims above. Furthermore Davis discloses the method wherein the message transmitted by the upstream**

device comprises an alteration of a control line signal between the reader and upstream device for a predetermined amount of time. [Paragraph 0013 incorporates the reference US patent No, 6988203/WO 02/082367 to Davis et al and its equivalent International publication WO 02/082367 on page 11, lines 1-17 discloses this feature]

Conclusion

Allowable Subject Matter

21. Claims 6-7, 13-14 and 19-20 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.
22. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private

Art Unit: 2432

PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/SAMSON LEMMA/

Primary Examiner, Art Unit 2432

Application/Control Number: 13/689,088
Art Unit: 2432

Page 12

Notice of References Cited	Application/Control No. 13/689,088		Applicant(s)/Patent Under Reexamination GUTHERY ET AL.	
	Examiner SAMSON LEMMA		Art Unit 2432	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-8,183,980	05-2012	Davis et al.	340/5.8
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N	EP 1760985 A2	03-2007	European Patent	DAVIS et al.	
	O	WO 2008043125 A1	04-2008	World Intellect	BROWN, PERRY ANDREW	
	P	WO 02082367 A1	10-2002	World Intellect	DAVIS M et al.	
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

U.S. Patent and Trademark Office
PTO-892 (Rev. 01-2001)

Notice of References Cited

Part of Paper No. 12142013



(11) **EP 1 760 985 A2**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
07.03.2007 Bulletin 2007/10

(51) Int Cl.:
H04L 29/06 (2006.01) G06K 19/10 (2006.01)

(21) Application number: **06119388.4**

(22) Date of filing: **23.08.2006**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK YU

(72) Inventors:
• **Davis, Michael L.**
AMHERT, NY 14228 (US)
• **Hulusi, Tam**
IRVINE, CA 92618 (US)

(30) Priority: **31.08.2005 US 713528**
16.08.2006 US 464912

(74) Representative: **Grosfillier, Philippe**
Andre Roland S.A.
Intellectual Property Services
Avenue Tissot 15
P.O. Box 1255
1001 Lausanne (CH)

(71) Applicant: **Assa Abloy Identification Technology Group AB**
107 23 Stockholm (SE)

(54) **Device authentication using a unidirectional protocol**

(57) The present invention is directed toward secure access systems. Specifically, a method and system is provided that allows a control panel (104) of a secure

access system to verify the authenticity and fidelity of a reader (112) within the secure access system by utilizing a rolling code agreed upon by the reader and the control panel.

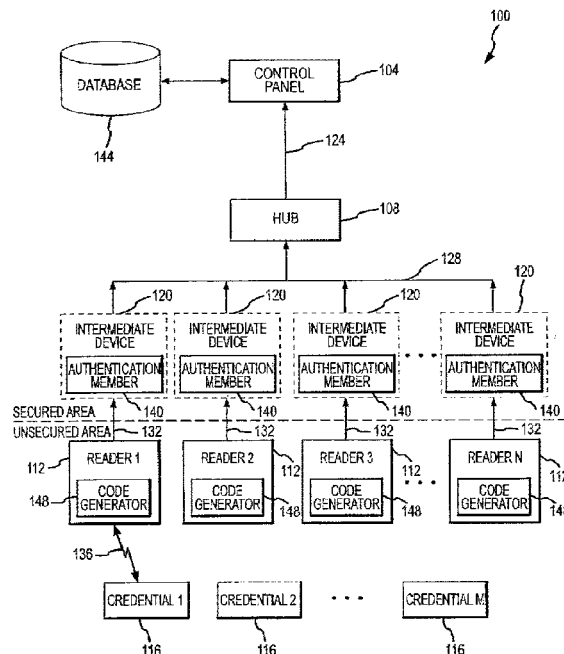


FIG.1

EP 1 760 985 A2

Description

[0001] This application claims benefit of United States Provisional Patent Application serial number 60/713,528, filed August 31, 2005, which is herein incorporated by this reference in its entirety.

FIELD OF THE INVENTION

[0002] The present invention is generally directed to authentication of a reader in a secure access system. More specifically, the present invention provides a reader signal protocol used to protect and differentiate authorized, authentic readers from non-authorized, non-authentic readers in a secure access system.

BACKGROUND

[0003] Limiting or securing access to designated or sensitive areas is an important issue. As such, there is a current focus on technological systems for controlling access to designated areas in both the private and public venues. Such systems must be made highly impervious to attack by those wishing to gain unauthorized access to the secured area.

[0004] In access control systems, Radio Frequency Identification Devices (RFIDs) or other security credentials are typically used to store data that uniquely identify a holder of the RFID device or the holder's access authorizations. In order to gain access to an asset, such as a building, room, safe, computer, files, information, etc., a holder presents the RFID device to a reader that reads the data and subsequently transmits the data to a panel, processor, or a host system where a decision is made to either grant access to the subject asset or not. There are also readers that combine the functionality of a panel/host and the physical reader into a single unit that makes the access decision. This type of device is sometimes referred to as a stand-alone reader.

[0005] Attention has been focused on the security mechanisms employed by RFID cards to protect and secure the data exchange between the RFID device and the reader. Some of these techniques include the use of cryptography, mutual key authentication, secure channels, and even protection of the chip on the RFID device against physical and electrical attacks. However, little attention has been given to ensuring the integrity of the communications between the reader and its host/control panel as well as insuring the integrity of the reader itself.

[0006] A working assumption thus far has been that RFID device readers are trustworthy devices, when in fact this may not be the case. In many building access control applications, a reader is mounted on the unsecured side of a door in a location that is not under continuous scrutiny. In such a case, compromise of a single reader could result in a compromise of RFID device security if any secret information, such as keys, authorization codes and the like, were somehow extracted from

the reader.

[0007] In addition, without knowing the authenticity of the reader an unauthorized or rogue reader could be used to replace an existing legitimate reader in a security system. This rogue reader can actually be any reader or data reply device capable of outputting data in the same format as the replaced reader.

[0008] In the access control industry, one of the most popular communication protocols used between a reader and a panel is the Wiegand protocol. Due to its popularity, the Wiegand protocol has become a de-facto industry standard. It is estimated that the majority of today's access control panels support the Wiegand protocol as the primary method to connect readers to the panel. It should be noted that several companies use their own proprietary communications protocols, but they still support the Wiegand protocol due to its popularity and widespread use. Because of this, a variety of non-RFID machine readable ID readers and other devices have standardized on the Wiegand protocol. Examples of these readers support smart card, proximity, magnetic stripe, bar code, barium ferrite, etc. There are also keypads, biometric devices, wireless Wiegand protocol extenders, protocol converters, and even robots that utilize the Wiegand protocol. The Security Industry Association (SIA) also recognizes the Wiegand protocol as an important standard in the access control industry. The Wiegand protocol has become so important that it has been published as an industry standard.

[0009] The Wiegand protocol is essentially a unidirectional protocol that only provides for data transmission from a reader to an upstream device (e.g., a control panel, host, or processor). Although there is a signal sent back from the upstream device to the reader, this signal is essentially a logic signal used to convey status to a cardholder by controlling a reader's LED. A superset of the Wiegand protocol adds additional logic signals to control an audible device in the reader and provides for additional reader LED colors. These are not bi-directional protocols because substantive data is still sent in only one direction. The host cannot give the reader a command. Only simple signals are sent from the host to the reader.

[0010] As popular as the Wiegand protocol has become, it has shortcomings. Examples of these shortcomings include the fact that the Wiegand protocol is susceptible to electrical noise, has distance limitations, and only allows data to be sent from a reader to an upstream device. Without bidirectional capabilities, it is very difficult to implement a modem protocol that provides for reader authentication.

[0011] Another issues is that the Wiegand protocol allows "party line" connections so that it is very easy to connect one or more additional devices to communication wires to monitor the communications between a card reader and a host in an attempt to harvest data streams to be used to compromise the system. Once a rogue device has been connected to monitor communications between the reader and control panel, an attacker could

merely note when the door has been unlocked and flag the most recent data stream as one that will open the door. Then, whenever illicit entry is desired, the attacker could just "replay" that data stream causing the door to unlock. The attacker need not even remove the device from the communication wires because the Wiegand communications utilize an "open collector" electrical interface, which allows both the monitoring of messages and generation of messages from that same connection.

[0012] There is typically little stopping an attacker from harvesting one or more valid messages to gain illicit entry using different cardholder's data so that no suspicions are aroused. Accessibility to the Wiegand communications wires is increased by the fact that a reader is typically located on the unsecured side of a wall or door and, because of the nature of access control, may be at a location that is not under continuous observation or scrutiny. Making matters worse, many access control readers do not employ a tamper mechanism so that the removal of a reader to access the internal wiring or even to replace the reader with another compromised reader or illicit Wiegand generating device is undetectable.

[0013] There have been some attempts to address the shortcomings of the Wiegand protocol. One example of an extension to the Wiegand protocol is described in U.S. Patent No. 6,988,203 to Davis et al., the contents of which are hereby incorporated herein by this reference. The '203 patent describes appending additional bits to the Wiegand data stream. This provides supplementary information from the reader to the upstream device as well as a CRC or other type of error detection and/or correction bits covering all of the data in the transmission. The '203 patent further describes transmitting data back to the reader from the upstream device via an LED control line.

[0014] Additionally, in PCT Application No. WO 2005/038729 to Merkert, which is herein incorporated by this reference, an access system that includes a signal generator located between a reader and a control panel is described. The reader utilizes a dynamic timing element that ensures a replay attack cannot be used to gain unauthorized access to an asset. The reader stamps any signal sent therefrom with a time stamp indicating when the message was generated. Then the control panel reads the time stamp to ensure that the message is authentic. An attempt to harvest a signal and resubmit that signal again at a later time will result in the control panel determining the signal is invalid. To ensure channel security between system elements, encryption and/or digital signatures are used. Unfortunately, this solution does not overcome most of the Wiegand deficiencies.

[0015] For instance, there is no way in the currently existing solutions that allows the control panel to continually monitor each reader in order to verify the fidelity of each reader. Thus, leaving open the possibility of having a valid reader replaced with a rogue reader without the system or system operator becoming aware of such actions.

SUMMARY

[0016] The present invention is generally directed toward a method, apparatus, and system that allows for authentication of readers in a secure access system. Although well suited for use in an access system utilizing the Wiegand protocol, embodiments of the present invention may be suitable for use in any system utilizing a unidirectional protocol.

[0017] In accordance with embodiments of the present invention, a method of checking authenticity of devices in a secure access system utilizing a unidirectional communication protocol is provided. The method comprises the steps of reading a credential with a reader, the reader generating a first message that includes credential data associated with the credential and a first code, transmitting the first message to an upstream device, and the upstream device analyzing the credential data in order to determine the authenticity of the credential and further analyzing the first code in order to determine the authenticity of the reader.

[0018] A valid reader employing the above-described method will be able to verify its authenticity to the upstream device by sending a valid code. A reader that is not enabled to generate a valid code may be identified by the upstream device as defective and/or fraudulent. By requiring the reader to send a valid code along with credential data, the upstream device can be confident that the reader is valid and has not been tampered with.

[0019] In accordance with further embodiments of the present invention, a method of maintaining a secure access system that utilizes a unidirectional communication protocol is provided. The method comprises the steps of providing a downstream device that is operable to transmit a valid rolling code as a part of a message and further providing an upstream device that is operable to receive the message and analyze the rolling code. The method can continue by determining a required first time of check in and requiring the downstream device to transmit a first message including a first valid rolling code at a first time related to the required time of check in. The method may then determine a required second time of check in that is after the required first time of check in, and require the downstream device to transmit a second message including a second valid rolling code at a second time related to the required second time of check in.

[0020] By requiring a downstream device to check in with the upstream device at a particular time schedule, the upstream device can continually update the state of the system. In other words, the upstream device can determine fairly quickly, depending on the amount of time between required check in times, whether a downstream device has been tampered with, replaced, and/or is malfunctioning. If the time between required check in messages is very short, like one second or less, it becomes very difficult for an attacker to perform any action that would interrupt communications between the upstream device and the downstream device.

[0021] In one embodiment of the present invention, certain thresholds may be set at the upstream device that allows for missed messages due to noise or the like. For example, a threshold of N missed messages may be allowed for a particular downstream device. Thus, if a downstream device misses one predetermined check in time, it is not necessarily identified as malfunctioning or having been tampered with. Rather, the downstream device is allowed to miss up to N check-ins, which may or may not be consecutive, before an error determination is made.

[0022] In accordance with other embodiments of the present invention, a secure access system utilizing a unidirectional communication protocol is provided. The system comprises a credential, a reader that is operable to read credential data from the credential upon presentation of the credential to the reader, generate a message including the credential data and rolling code data, and to transmit the message, and an upstream device that is operable to receive the message and upon receiving the message is operable to analyze the credential data in order to determine the authenticity of the credential and to analyze the rolling code data in order to determine the authenticity of the reader.

[0023] In accordance with still further embodiments of the present invention a device adapted for use in a secure access system utilizing a unidirectional communication protocol is provided. The device comprises an input that is adapted to receive a message from a reader, where the message includes a rolling code, an authentication member operable to determine the authenticity of the reader based upon an analysis of the rolling code, and an output operable to transmit the message to an upstream device in response to the authentication member determining the authenticity of the reader is valid.

[0024] The device may be an intermediate device that is used only to monitor the authenticity of readers in a given system. The intermediate device may also be adapted to analyze credential data received from the reader in order to make a determination about the authenticity of a credential that was presented to the reader. The intermediate device may be employed in order to ensure that communications between a rogue reader and a control panel do not occur, thus protecting the control panel from potentially harmful signals. This provides a provision for updating legacy systems with embodiments of the present invention without requiring the replacement of a reader or host.

[0025] These and other advantages will be apparent from the disclosure of the invention(s) contained herein. The above-described embodiments and configurations are neither complete nor exhaustive. As will be appreciated, other embodiments of the invention are possible using, alone or in combination, one or more of the features set forth above or described in detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0026]

Fig. 1 is a diagram depicting an exemplary system for authenticating credentials with legitimate readers in accordance with embodiments of the present invention;

Fig. 2 is a block diagram depicting an exemplary reader and control panel utilizing a unidirectional data transfer protocol in accordance with embodiments of the present invention;

Fig. 3 is a flow chart depicting a method of generating a message for transmission to an upstream device in accordance with embodiments of the present invention;

Fig. 4 is a flow chart depicting a method of receiving and processing a message at an upstream device in accordance with embodiments of the present invention;

Fig. 5 is a flow chart depicting a method of transmitting a message in order to verify authenticity of downstream device to an upstream device in accordance with embodiments of the present invention;

Fig. 6 is a flow chart depicting logic within an exemplary upstream device in order to verify the authenticity of downstream devices in a secure access system in accordance with embodiments of the present invention; and

Fig. 7 is a block diagram depicting a data structure that can be used by both the upstream and downstream device in order to maintain a secure access system in accordance with embodiments of the present invention.

DETAILED DESCRIPTION

[0027] The present invention is generally directed toward a reader authentication method, device, and system. The invention advantageously addresses deficiencies of the prior art and may be utilized within the context of access control or security systems, as well as be equally efficiently utilized in a broad range of other applications using a unidirectional communications protocol where interactive computerized data acquisition techniques are used, both contactless or requiring a physical contact with a carrier of pre-programmed information (e.g., monitoring moving objects, tracking inventory, verifying credit cards, and the like).

[0028] Fig. 1 depicts an access network 100 used to verify the identity of at least one credential. In one embodiment of the present invention, the system 100 comprises a control panel 104, a hub 108, a plurality of readers 1121-n, and a plurality of credentials 1161-m such that n and m are integers wherein $n \geq 1$, $m \geq 1$, and typically m is greater than n. The plurality of readers 1121-n may include readers 112 of the same type, as well as readers of different types. For example, a subset of the plurality

of readers 1121-n may be legacy readers (e.g. readers using older transmission protocols). Whereas another subset of the plurality of readers 1121-n may be new readers utilizing more secure protocols including the protocols described herein.

[0029] Additionally, the system 100 may further comprise intermediate devices 120 connected between a reader 112 and the control panel 104. In the depicted embodiment, the readers 112 are coupled to an intermediate device 112 through interface 132. The intermediate devices 120 are coupled to the hub 108 through interface 128 and the hub is coupled to the control panel 104 via interfaces 124. In an alternate embodiment (not shown), the readers 112 may be coupled to the respective inputs/outputs of the control panel 104 without a device, like the hub 108 or intermediate device 120, existing there between. Interfaces 124, 128, and 132 between the readers 112, the intermediate devices 120, the hub 108, and the control panel 104 are generally unidirectional interfaces, which may selectively be implemented in a form of wired, wireless, fiber-optic communication links, or combinations thereof.

[0030] As can be appreciated by one of skill in the art, the interfaces 124, 128, and 132 may be implemented utilizing buses or other types of connections. For example, the I/O ports may be one or more of a USB port, parallel port, serial port, Small Computer Systems Interface (SCSI) port, modem, Ethernet, and/or an RF interface. The protocols used to communicate between the control panel 104 and the readers 112 may include one or more of the TCP/IP protocol, RS 232, RS 485, Current Loop, Power of Ethernet (POE), Bluetooth, ZigBee, GSM, WiFi, and other communication methods and protocols known in the art.

[0031] An exemplary intermediate device 120 comprises an input that is adapted to receive signals via interface 132, an output that is adapted to transmit signals via interface 128, and an authentication member 140. The authentication member 140 is operable to determine the authenticity of one or more readers 112 associated with the intermediate device 120 (e.g., determine whether the reader 112 is valid or not), based upon a rolling code that is transmitted from the reader 112 to the intermediate device 120.

[0032] The control panel 104 may be a general-purpose computer adapted for multi-task data processing and suitable for use in a various settings (e.g., commercial, industrial, residential, and the like). A memory of the control panel 104 comprises software program(s) containing a database of records for the system 100. Alternatively, a database 144 may be separated from the control panel 104. The database 144 whether integral to the control panel 104, separate from the control panel 104, or both, maintains records associated with the readers 112, credentials 116 and their respective holders or users, algorithm(s) for acquiring, decoding, verifying, and modifying data contained in the readers 112, algorithm(s) for testing authenticity and validity of the credentials

116, and algorithm(s) for implementing actions based on the results of these tests. The database 144 may further comprise a list of valid rolling codes and their corresponding required time of check in and/or algorithm(s) for generating valid rolling codes and comparing them with rolling codes received from a downstream device.

[0033] As used herein, in reference to an individual or an object associated with a credential 116, the terms a "holder" and a "user" are used interchangeably.

[0034] Each reader 112 is adapted for exchanging information with the control panel 104 and for requesting data from the credential 116 placed in the active zone of the reader. The reader 112 may also be adapted for processing at least a portion of the data acquired from the credential 116. Alternatively, processing of the acquired data may be performed using the control panel 104 exclusively. In one embodiment, the reader 112 generates signals facilitating execution of the results of interrogating the credential 116 (e.g., engages/disengages a locking mechanism, allows/disallows movement of a monitored article, temporarily disables itself, activates an alarm system, updates a database, and the like). Alternatively, the control panel 104 may generate such signals.

[0035] In accordance with embodiments of the present invention, a stand-alone reader 112 may be utilized to perform the functionality of both the reader 112 and the control panel 104. This stand-alone reader may include, or have access to, the database that contains data used to determine the authenticity of a credential and/or algorithm(s) used to make the determination of authenticity of the credential 116. A determination of authenticity for a credential is made at the receiving point rather than having to transmit data across a network from the reader to a control panel 104 in order to make a determination of authenticity. The stand-alone reader is further operable to execute instructions based upon the analysis of the credential 116.

[0036] Specific configurations of the control panel 104 are determined based on and compliant with computing and interfacing capabilities of the readers 112 and/or the hub 108.

[0037] At least a portion of the plurality of readers 112 further comprise a code generator 148. The code generator 148 is used by the reader 112 to generate a code, possibly a rolling code, in order to verify its authenticity to an upstream device. The code generator 148 may comprise a table, sequence, or data structure of valid rolling codes that the reader 112 can work through as update signals are generated. The code generator 148 may also comprise a code generating algorithm that creates a valid code based on certain criteria.

[0038] Interface 136 represents the communication interface that exists between a reader 112 and a credential 116. Interface 128 may represent an RF communication interface, a biometric communication interface, a keypad, a magnetic communication interface, an optical communication interface, or combinations thereof.

[0039] In operation a credential 116, for example a credential, is brought into an active zone of the reader 112 in order to establish the communication interface 136. For a credential, a Radio Frequency (RF) communication interface 136 between the reader 112 and the credential is typically automatically established when the credential is brought within an active zone of a reader/interrogator 112. The active zone of an RF reader 112 is defined as a three dimensional space where the intensity of RF signals emitted by the reader 112 exceeds a threshold of sensitivity of the credential and the intensity of RF signals emitted by the credential exceeds a threshold of sensitivity of the reader 112. When a credential is presented to most readers, such a communication interface 136 is established and the reader 112 and credential begin transmitting data back and forth.

[0040] The credential 116 may also be implemented in a number of other machine readable devices including, but not being limited to, contact smart card, a contactless smart card, a proximity card, a magnetic stripe card, a barium ferrite card, a bar code, a Wiegand card, a PDA, a cellular phone and any other type of device used to store and transmit data relating a particular application. The active zone for each type of credential 116 may vary based upon the type of communications used between the reader 112 and the credential 116. For example, a magnetic stripe card is placed in the active zone of the reader 112 when it is swiped through the reader 112. As can be appreciated by one of skill in the art, the interface 128 is created upon presentation of the credential 116 to the reader 112 such that communications between the two is facilitated.

[0041] The reader 112 takes the information that it retrieves from the credential 116 and generates a signal to send to the control panel 104. In generating the signal the reader 112 creates a credential part of the signal and a rolling code part of the signal. The code generator 148 is typically operable to generate the code part of the signal. The credential data relates to the credential that was read (e.g., user name, social security number, title, access permissions, key, password, manufacturer ID, site code, customer code, unique ID, etc.) The code data or rolling code data is a number, letter, dataset, and/or identifier chosen from possibly a list of potential rolling codes. The rolling code sent from a valid reader 112 may possibly be a code previously agreed upon by the control panel 104 and reader 112. The reader 112 and control panel 104 may cycle through and agree upon a number of valid rolling codes as time progresses in order to provide a more secure system.

[0042] Once the control panel 104 receives the signal from the reader 112, the control panel 104 will analyze the credential data from the signal to determine if the credential 116 is authorized to gain access to the asset associated with the reader 112. Additionally, the control panel 104 will analyze the rolling code portion of the signal to determine if the reader 112 is authorized to send commands and has not been tampered with. In an alter-

native configuration, the signal is sent from the reader 112 to the intermediate device 120 where the rolling code data is analyzed by the authentication member 140 in order to determine if the reader 112 is still valid and has not been tampered with. The intermediate device 120 then forwards the signal on to the control panel 104 for verification of the credential 116. In still a further configuration, the reader 112 generates a signal containing only the credential data and forwards that signal on to the intermediate device 120. The intermediate device 120 then generates rolling code data and incorporates that into the signal from the reader 112. The intermediate device 120 then forwards the signal on to the control panel 104 for verification of the credential and rolling code data. As can be appreciated, any upstream device within the system 100 may perform the verification of the credential data and/or the rolling code data generated by a downstream device. However, it is advantageous to have the reader 112 verified by a device that resides in a secured area rather than an unsecured area so that the device verifying the authenticity of the reader 112 may not be as easily compromised.

[0043] Referring now to Fig. 2 a typical Wiegand protocol reader 112 and control panel 104 will be described. As noted above, the control panel 104 is located in a secure area remote from the Wiegand reader 112. The reader 112 may receive its power from the control panel 104 via the channel 204. The reader 112 is accessible to a user attempting to obtain access to an asset, like the secure area. In order to gain access, a user presents his/her credential (e.g., smart card, RFID tag, magnetic stripe card, bar code card, PDA, cellphone, or the like) to the reader 112. The information received at the reader 112 is transmitted from the reader 112 to the control panel 104 via the data channels 208 and/or 212. The control panel 104 evaluates the information to determine whether the credential is authorized to gain access to an asset associated with reader 112. Depending upon the results of the evaluation, the control panel 104 either performs a valid credential action (e.g., unlocks a door, unlocks a file, turns on a computer, opens a door, etc.) or performs an invalid credential action (e.g., no action, denies access, sounds an alarm, notifies security personnel, etc.) Additionally the control panel 104 may send a signal to the reader 112 via the data channel 216 to flash a light on/off indicating to the credential holder the results of the evaluation. The communications protocol between the control panel 104 and the reader 112 is typically considered unidirectional because most often substantive data is sent from the reader 112 to the control panel 104 and not from the control panel 104 to the reader 112.

[0044] Referring now to Fig. 3 a method of generating a signal for transmission to an upstream device will be described in accordance with at least some embodiments of the present invention. Initially, the method begins when a credential, like an RFID device, is presented to and read by a reader 112 (step 304). The reader 112 processes the received signal and determines what credential

data is contained therein (step 308). Examples of credential data include, user name, social security number, title, access permissions, key, password, manufacturer ID, site code, customer code, and a unique ID. Once the credential data has been determined, a rolling code is determined and generated by the code generator 148 (step 312). A rolling code is generally selected from a list of rolling codes. After a predetermined amount of time the next rolling code from the list of rolling codes is selected by the reader 112. Alternatively, an algorithm for generating a proper code based upon certain criteria may be used. For example, a choosing algorithm for a rolling code may be created based upon the time of day, the number of credentials previously read at a given reader 112, the number of messages transmitted from the reader to the upstream device, a reader unique ID, reader manufacturer identification number, *etc.* If the reader 112 sends the wrong rolling code, then the control panel 104 will know something is wrong with the reader 112. The reader 112 and control panel 104 generally have their copies of the rolling code (or rolling code selection algorithms) synchronized upon installation. However, as can be appreciated by one of skill in the art, the reader 112 and control panel 104 may have their rolling codes synchronized based upon other known methods.

[0045] Alternatively, a valid rolling code may be generated arbitrarily, as long as the control panel 104 is in synchronization with the reader 112 in determining what the next valid code is in a rolling code sequence. For example, the reader 112 may use a pseudorandom code generator and the control panel 104 may use an exact copy of the generator. The system may be initiated such that each generator determines, creates, and agrees upon the same valid rolling code as each continues to operate properly. For example, the reader 112 and the control panel 104 may use a previously agreed upon sequence or list of valid rolling codes. The control panel 104, at any random time, may change the order in which the code generator 148 goes through the list. The control panel 104 could inform the reader 112 to change how it is working through the list with a prompting signal send via an LED control signal, or may do so through an interruption to the power supply of the reader 112. This ensures that the code generator 148 does not necessarily have to go through a finite list of valid rolling codes in the same order until a new list of codes is provided to the code generator 148. Rather, the same list may be used for a relatively longer amount of time and a higher level of security can be maintained.

[0046] In an alternative embodiment, data received from the credential 116 may dictate what sequence the rolling code should follow. For example, when a first type of credential 116 is read, the reader 112 may use a first rolling code selection algorithm or select a rolling code from a first list of rolling codes. When a second type of credential 116 is read by the reader 112, the reader may change to a different rolling code selection algorithm and/or list of rolling codes. When the reader 112 switches

from one rolling code selection algorithm to another, it should indicate to the upstream device that such a switch has been made. Alternatively, the upstream device may recognize that a second type of credential 116 has been read and automatically knows to switch to a different rolling code selection algorithm.

[0047] Of course different algorithms may be used in a similar fashion. The code generator 148 may use a first algorithm to generate valid codes, then upon receiving a prompting signal from an upstream device, like a control panel 104, a different algorithm is used by the code generator 148. Furthermore, data used by the algorithm to compute a valid rolling code may be changed in an analogous way.

[0048] Once the rolling code data and credential data have been determined, the reader 112 generates a message containing both the credential data and rolling code data (step 316). In step 320, it is determined if the signal containing the message is to be encrypted. If the signal is not to be encrypted, then the reader 112 transmits the message (step 332). However, if the message is to be encrypted, then an encryption key is determined (step 324). Thereafter, the message is encrypted using the encryption key (step 328). By encrypting the message, the communications between the reader 112 and the control panel 104 becomes more secure. Even if someone is harvesting signals sent from the reader 112 to the control panel 104, they must know the encryption/decryption key and decrypt the message before any substantive information about the message can be determined. Essentially, the encryption of the message makes it more difficult for an attacker to steal a valid rolling code and valid credential data.

[0049] In step 332, the message, whether encrypted or not, is transmitted. Then, if the rolling code is based upon the number of sent messages from a particular reader 112, the reader increments to the next rolling code in the valid rolling code sequence (step 336). A valid rolling code may depend on the time of day or the amount of time the reader 112 has been operational. In this case, the rolling code is not necessarily updated after a message is transmitted. In one embodiment, a list of valid rolling codes, for example rolling codes A, B, C, D, and E may be used. The reader 112 starts by appending rolling code A to the first message it generates and transmits to the control panel 104. The next rolling code the reader 112 transmits may be rolling code B, then rolling code C and so on. Once the reader 112 has went through the entire list of rolling codes, it may start over by appending rolling code A to the next message it generates. Alternatively, the reader may append rolling code D after it has appended rolling code E and work through the list of rolling codes that way. As long as the reader 112 follows the predetermined rolling code selection protocol, it will continue to generate valid rolling codes. Using a list of a select number of rolling codes provides for an inexpensive implementation of the present invention. However, a persistent attacker may eventually discover the finite

list of rolling codes thus jeopardizing the secure access system 100. In order to create a more secure access system, valid rolling codes may be generated based on predetermined algorithms using previously agreed upon criteria.

[0050] As can be appreciated by one of skill in the art, the reader 112 is not the only device that may be used to generate a signal containing both rolling code data and credential data. If there are other devices present in an unsecured area, those devices may be required to generate rolling code data in order to guarantee their validity, and the validity of devices connected thereto to the control panel 104. These devices may include credentials 116, intermediate devices 120, and/or any other downstream device.

[0051] Referring now to Fig. 4, a method of receiving and processing a signal containing credential and/or rolling code data will be described in accordance with at least some embodiments of the present invention. The method begins when a message is received at an upstream device like a control panel 104 (step 404). The control panel 104 determines if the message has been encrypted, or should have been encrypted at step 408. If the message has been encrypted, then the encryption key is determined (step 412). Using the encryption key, the control panel 104 decrypts the message (step 416). Once the message has been decrypted, or never was encrypted, the reader 112 separates the credential data from the rolling code data (step 420). It is not necessary to separate the credential data from the rolling code data literally. As long as the control panel 104 knows where the credential data ends and the rolling code data starts.

[0052] Once the credential data has been separated from the rolling code data, the control panel 104 compares the received rolling code to the required code. The required code may be maintained at the control panel 104 or in the database 144 separate from the control panel 104. In step 428 it is determined if the received code matches the required rolling code. If the received code does not match the required code, then the control panel 104 determines that a valid reader did not generate the signal or a valid reader has been tampered with. In response to determining that there is a problem with the reader 112, the control panel 104 performs invalid reader logic (step 432). An invalid reader logic action may include, sounding an alarm, notifying security/maintenance personnel that a reader is defective, not opening a door, disabling a reader by discontinuing power supply thereto, and other appropriate actions associated with determining that a reader is not valid and as are dictated by the particular circumstances. However, if the reader 112 was valid and did generate a valid rolling code, the credential data is analyzed in step 436. If the credential data is determined to be invalid, then the control panel 104 performs invalid credential logic (step 440). An invalid credential logic action may include actions similar to invalid reader logic actions. Different actions may be taken by the control panel 104 in response to determining

that a credential is invalid including, taking no action and/or controlling an LED on the reader notifying the holder of the credential that access has not been granted. However, if the control panel 104 can verify both the rolling code data and credential data, then the control panel 104 performs valid message logic (step 444). A valid message logic action may include opening/unlocking a door, unlocking a computer, disabling an alarm, *etc.* Then if valid rolling codes are based on a list of rolling codes, the control panel 104 increments to the next valid code in the rolling code sequence (step 448). If the validity of the reader 112 could not be determined in step 428 then the control panel 104 typically does not increment to the next valid code in the rolling code sequence. However, if the reader 112 was valid, but the credential could not be authenticated, then a valid reader 112 will expect to increment to the next code in the rolling code sequence. Because of this, the control panel 104 should also increment to the next code in the rolling code sequence so that the valid reader 112 and control panel 104 continue to agree upon a valid rolling code.

[0053] Referring now to Fig. 5, a method of continually sending an update message from a unidirectional communications protocol device to an upstream device will be described in accordance with at least some embodiments of the present invention. Initially, the downstream device, for example a reader 112, will determine an initial code in the rolling code sequence (step 504). Then the upstream device determines the periodicity with which it needs to receive a valid code from a downstream device, for example a reader 112. Most of these determinations may be made upon installation of the reader 112 or may be based upon other synchronization techniques known in the art. A valid reader 112 is informed of the required check in period and determines how often it needs to transmit a valid code to the upstream device (step 508). The downstream device waits until it is time to send an update signal in step 512. If the required amount of time has not passed since the last update message, the downstream device continues to wait at step 512. Once it becomes time to transmit the message, the downstream device generates and transmits a message to the upstream device (step 516). The transmitted message contains the valid code in the rolling code sequence. The valid code is sent to the upstream device to verify to the upstream device that the downstream device is still operational. Once the downstream device has sent the message containing the valid rolling code, the downstream device updates to the next code in the rolling code sequence (step 520).

[0054] A downstream device may be required to send in an update signal every second or fraction of a second for example. Having such a short period between update signals may preclude an attacker from cutting the connection between the upstream device and the downstream device as any interruption in communication may be discovered due to the high frequency of required updates. However, in order to conserve bandwidth, a lower

frequency of update may be required.

[0055] As noted above a reader 112, intermediate device 120, hub 108, or control panel 104 may be considered an upstream and/or downstream device depending on where it resides in relation to other devices in the system. A first control panel 104 may be connected to a master control panel. The first control panel 104 may be required to update its status to the master control panel in which case the first control panel 104 would be considered the downstream device and the master control panel would be considered the upstream device.

[0056] Referring now to Fig. 6 a method of ensuring that a downstream device is updated and valid will be described in accordance with at least some embodiments of the present invention. Initially, the period with which a downstream device is required to "check-in" is determined (step 604). Then, the number of acceptable missed messages or "check-ins" is determined (step 608). For a more secure system, the number of acceptable missed messages may be set to a very low number, i. e. zero, one, or two. In less secure systems the number of acceptable missed messages may be set higher, giving the system a higher tolerance to missed messages.

[0057] Once the required update rate and number of acceptable missed messages is determined, a variable representing elapsed time is set equal to zero (step 612). During this system initialization a variable representing the number of missed messages is set equal to zero (step 616). Then as time progresses the upstream device waits to receive a signal from a downstream device. When the predetermined amount of time between required updates has passed (step 620), the upstream device determines if it has received a valid rolling code (step 624). The upstream device may require the downstream device to "check-in" right on the required time. Alternatively, a downstream device may only be required to transmit a valid code once every period. In the latter configuration, if a downstream device sends a message in response to reading a credential and appends a valid rolling code with that message, the upstream device may not require another update message from the downstream device during that time span. However, if the upstream device does require the downstream device to transmit a valid rolling code on the required time, even if the downstream device already sent a message with a valid rolling code earlier in the time period, the downstream device will be required to transmit another valid rolling code at the predetermined time or in a predetermined time window.

[0058] If the upstream device does receive a valid rolling code at step 624 for that time period, then the method returns to step 612 and the variable representing elapsed time is set equal to zero. If the upstream device does not receive a valid rolling code (e.g. no check-in signal is received or the check-in signal included an invalid rolling code), then the variable representing the number of missed messages is incremented by one (step 628). In step 632, it is determined if the number of missed check-in messages is greater than the acceptable number of

missed messages. If the threshold for missed check-in messages has not been realized, then the method returns to step 620 to wait for the next required check in time or time window. If the threshold for missed check-in messages has been exceeded then the upstream device determines that there is a problem with the downstream device, typically a reader, and performs the required steps to notify personnel that the subject downstream device is malfunctioning (step 636).

[0059] Referring now to Fig. 7, a data structure employed by both an upstream device and downstream device will be described in accordance with at least some of the embodiments of the present invention. The data structure may be in the form of a list of valid rolling codes or a rolling code sequence 700. The rolling code sequence 700 comprises a rolling code data field 704 and a required check in time field 708. One copy of the rolling code sequence 700 is maintained in the upstream device that will be determining the authenticity of a downstream device. The rolling code sequence 700 may alternatively be maintained in the database 144 and referenced by the upstream device when analyzing a message that includes a rolling code. In addition to maintaining the rolling code sequence 700 in the upstream device, the rolling code sequence 700 is maintained in the downstream device. This ensures that both the upstream and valid downstream device "agree" on a valid rolling code. The rolling code sequence 700 may be employed in a system 100 that utilizes a unidirectional protocol because substantive data typically cannot be sent from upstream device to the downstream device. Therefore, each device in the system 100 can utilize the rolling code sequence 700 to determine a valid rolling code without engaging in bilateral communications. In the event that a fraudulent reader not having the rolling code sequence 700 attempts to send a message to the upstream device, the upstream device will be able to determine that the downstream device is either fraudulent or malfunctioning.

[0060] The rolling code sequence 700 may comprise up to x rolling codes or rolling code generation variables that are required to be transmitted at a check in time up to k periods after the first check in time, where x and k are typically greater than one.

[0061] Each rolling code in the rolling code data field 704 may be a unique predetermined rolling code. Alternatively, an algorithm may use the data stored in the rolling code data field 704 in order to generate a valid rolling code. The upstream device will expect rolling code A from a downstream device at time T in order to determine the authenticity of the downstream device. Then at a time later than time T, the upstream device will expect rolling code B. Since a valid downstream device will have the rolling code sequence 700, it will know what rolling code to send and when to send it. A fraudulent reader on the other hand will not have access to the rolling code sequence 700 and thus will not be able to send a valid rolling code to the upstream device at the required time. This will result in the upstream device determining that the

downstream device is not valid or is not functioning properly. A valid rolling code generally includes the next rolling code to be sent in the rolling code sequence. As can be appreciated, a less noise sensitive system may be created that identifies more than one rolling code as a valid rolling code. For example, an upstream device may accept the next rolling code up to X more rolling codes in the rolling code sequence. This valid rolling code buffer can be implemented to provide some level of resistance to one or more rolling codes being missed due to noise or other factors.

[0062] In an alternative configuration, a prompt signal may be sent from the upstream device to the downstream device asking for the next valid rolling code in the rolling code sequence 700. The prompting signal may be sent via the LED control signal in the case of the Wiegand protocol. When the prompt signal is received at the downstream device, the next rolling code is chosen in the sequence of rolling codes 700. This particular configuration is beneficial in that a predetermined period of reply does not necessarily need to be employed. Rather, a prompt signal may be sent randomly from an upstream device to a downstream device. In order for the downstream device to prove its authenticity to the upstream device, it should generate a valid rolling code and transmit it back to the upstream device.

[0063] As can be appreciated by one of skill in the art, the relationship of an upstream device and a downstream device is generally defined by the flow of credential information. The downstream device transmits credential information to an upstream device, which may further forward the information to another upstream device or analyze the information to determine an authenticity of the downstream device. Downstream devices are not limited to a reader 112, but rather may include an intermediate device 120, a credential 116, and/or a control panel 104. Moreover, upstream devices are not limited to control panels 104, but also may include a reader 112, an intermediate device 120, and/or a credential 116.

[0064] The present invention, in various embodiments, includes components, methods, processes, systems and/or apparatus substantially as depicted and described herein, including various embodiments, subcombinations, and subsets thereof. Those of skill in the art will understand how to make and use the present invention after understanding the present disclosure. The present invention, in various embodiments, includes providing devices and processes in the absence of items not depicted and/or described herein or in various embodiments hereof, including in the absence of such items as may have been used in previous devices or processes, e.g., for improving performance, achieving ease and/or reducing cost of implementation.

[0065] The foregoing discussion of the invention has been presented for purposes of illustration and description. The foregoing is not intended to limit the invention to the form or forms disclosed herein. In the foregoing Detailed Description for example, various features of the

invention are grouped together in one or more embodiments for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed invention requires more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive aspects lie in less than all features of a single foregoing disclosed embodiment. Thus, the following claims are hereby incorporated into this Detailed Description, with each claim standing on its own as a separate preferred embodiment of the invention.

[0066] Moreover though the description of the invention has included description of one or more embodiments and certain variations and modifications, other variations and modifications are within the scope of the invention, e.g., as may be within the skill and knowledge of those in the art, after understanding the present disclosure. It is intended to obtain rights which include alternative embodiments to the extent permitted, including alternate, interchangeable and/or equivalent structures, functions, ranges or steps to those claimed, whether or not such alternate, interchangeable and/or equivalent structures, functions, ranges or steps are disclosed herein, and without intending to publicly dedicate any patentable subject matter.

Claims

1. A method of maintaining a secure access system that uses a unidirectional communication protocol, the secure access system comprising at least one credential, at least one reader, and a device upstream of said reader, comprising:

reading a credential with a reader;
said reader generating a first message comprising credential data associated with said credential and a first code;
transmitting said first message to an upstream device; and
said upstream device, analyzing said credential data in order to determine the authenticity of said credential and further analyzing said first code in order to determine the authenticity of said reader.

2. The method of claim 1, further comprising:

said reader generating a second message comprising a second code, wherein said second code is different from said first code;
transmitting said second message to an upstream device; and
said upstream device analyzing said second code in order to determine the authenticity of said reader.

3. The method of claim 2, wherein said second message is generated a predetermined amount of time after said first message is generated.
4. The method of claim 2, wherein said second message is generated in response to receiving a prompting signal from said upstream device.
5. The method of claim 1, wherein said first message is encrypted by said reader prior to transmitting said first message to said upstream device and decrypted by said upstream device prior to analyzing said first message.
6. The method of claim 1, wherein a code selection algorithm is used to generate said first code.
7. The method of claim 6, wherein said code selection algorithm generates said first code based upon at least one of time of day, total operation time of said reader, a reader unique ID, number of cards read, and a reader manufacturer ID.
8. The method of claim 6, wherein said code selection algorithm generates said first code based upon a number of messages previously transmitted from said reader to said upstream device.
9. The method of claim 1, wherein said first code is a unique code chosen from a rolling code list.
10. The method of claim 9, further comprising:
 - said upstream device accessing a second list that corresponds to said rolling code list;
 - said upstream device comparing said first code to one or more valid codes from said second list; determining that said first code matches a valid code; and
 - in response to said upstream device determining that said first code matches said valid code, said upstream device determining that the authenticity of said reader is valid.
11. The method of claim 1, wherein said transmitting utilizes a Wiegand protocol.
12. The method of claim 1, wherein said credential is machine readable and comprises at least one of an RFID device, a contact smart card, a contactless smart card, a proximity card, a magnetic stripe card, a barium ferrite card, a bar code, a Wiegand card, a PDA, and a cellular phone.
13. The method of claim 1, wherein credential data is at least one of a user name, a social security number, a title, access permissions, a key, a password, a manufacturer ID, site code, customer code, and a unique ID.
14. The method of claim 1, wherein said upstream device is at least one of a control panel, a host computer, a processor, a database, and an intermediate device.
15. The method of claim 1, wherein said reader comprises a second device that generates the codes.
16. The method of claim 15, wherein said second device is integral with a housing of said reader.
17. A method of maintaining a secure access system that uses a unidirectional communication protocol, comprising:
 - providing a downstream device associated with at least one interrogator device that is operable to transmit a rolling code as a part of a message;
 - providing an upstream device that is operable to receive said message and analyze said rolling code;
 - requiring said downstream device to transmit a first message comprising a first valid rolling code at a first time; and
 - requiring said downstream device to transmit a second message comprising a second valid rolling code at a second time.
18. The method of claim 17, wherein at least one of said first and second is a window of time in which said downstream device is required to transmit said message.
19. The method of claim 17, wherein at least one of said first and second message is time stamped in order to verify to said upstream device that said at least one of said first and second message was transmitted at their respective required time.
20. The method of claim 17, further comprising, determining a required first and second time of check in.
21. The method of claim 20, wherein at least one of said first and second time is before at least one of said required first and second time of check in.
22. The method of claim 20, wherein at least one of said first and second time related is after at least one of said required first and second time of check in.
23. The method of claim 17, wherein in response to said downstream device not transmitting at least one of said first and second valid rolling codes, determining that said downstream device is at least one of fraudulent and malfunctioning.

24. The method of claim 17, wherein in response to said downstream device not transmitting said first rolling code, determining that said downstream device is at least one of fraudulent and malfunctioning.
25. The method of claim 24, wherein in response to determining that said downstream device is at least one of fraudulent and malfunctioning, performing an invalid reader logic action.
26. The method of claim 25, wherein said invalid reader logic action is at least one of sounding an alarm, notifying security/maintenance personnel that said downstream device is defective, not opening a door, and disabling said downstream device.
27. A secure access system utilizing a unidirectional communication protocol, comprising:
- a credential;
 - a reader that is operable to read credential data from said credential upon presentation of said credential to said reader, generate a message comprising some or all of said credential data and code data, and to transmit said message;
 - an upstream device that is operable to receive said message and upon receiving said message is operable to analyze said credential data in order to determine the authenticity of said credential and to analyze said code data in order to determine the authenticity of said reader.
28. The system of claim 27, wherein said message is encrypted by said reader prior to transmitting said message to said upstream device and decrypted by said upstream device prior to analyzing said message.
29. The system of claim 28, wherein a key is used to encrypt and decrypt said message.
30. The system of claim 27, wherein the code is a rolling code.
31. The system of claim 30, wherein a code selection algorithm is used to generate said rolling code.
32. The system of claim 31, wherein said code selection algorithm generates said rolling code based upon at least one of time of day, total operation time of said reader, a reader unique ID, and a reader manufacturer ID.
33. The system of claim 31, wherein said code selection algorithm generates said first code based upon the number of messages previously transmitted from said reader to said upstream device.
34. The system of claim 30, wherein said rolling code is a unique code chosen from a rolling code list.
35. The system of claim 34, wherein said upstream device is further operable to access a list corresponding to said rolling code list, compare said rolling code to a valid code from said list, determine that said first code matches said valid code, and in response to determining that said first code matches said valid code, determine that the authenticity of said reader is valid.
36. The system of claim 27, wherein said message is transmitted by said reader utilizing a Wiegand protocol.
37. The system of claim 27, wherein said credential is at least one of an RFID device, magnetic stripe card, bar code, barium ferrite card, and smart card.
38. The system of claim 27, wherein said upstream device is an intermediate device.
39. The system of claim 27, wherein said upstream device is a control panel.
40. A device adapted for use in a secure access system utilizing a unidirectional communication protocol, comprising:
- an input adapted to receive messages from a reader, wherein at least a portion of said messages comprise a code;
 - an authentication member operable to determine the authenticity of said reader based upon an analysis of said code; and
 - an output operable to transmit said message to an upstream device, wherein said message is transmitted to said upstream device in response to said authentication member determining the authenticity of said reader is valid.
41. The device of claim 40, wherein at least a portion of said messages are encrypted prior to being received at said input, and wherein said authentication member is operable to decrypt said message prior to said analysis of said code.
42. The device of claim 40, wherein said authentication member is further operable to encrypt said message after said analysis of said code and prior to being transmitted at said output.
43. The device of claim 40, wherein said authentication member comprises a valid rolling code sequence and wherein said valid rolling code sequence is used by said authentication member to analyze said code.

44. The device of claim 40, wherein said authentication member transmits a prompting signal to said reader that prompts said reader to generate a message comprising a code.
45. The device of claim 40, wherein said message further comprises credential data that is related to a credential and wherein said authentication member is further operable to determine the authenticity of said credential based on said credential data.
46. A device for use in a secure access system that uses a unidirectional communication protocol, wherein said device is operable to read credential data from a credential, comprising:
- a code generator that is operable to generate a first message comprising credential data associated with a credential that is used to determine the authenticity of said credential and a first code that is used to determine the authenticity of said device; and
- an output for transmitting said first message to an upstream device.
47. The device of claim 46, wherein said code generator is further operable to generate a second message comprising a second code, wherein said second code is different from said first code.
48. The device of claim 47, wherein said second message is generated a predetermined amount of time after said first message is generated.
49. The device of claim 47, wherein said second message is generated in response to receiving a prompting signal from said upstream device.
50. The device of claim 46, wherein said first message is encrypted by said code generator prior to transmitting said first message to said upstream device.
51. The device of claim 46, wherein said code generator comprises a code selection algorithm.
52. The device of claim 51, wherein said code selection algorithm generates said first code based upon at least one of time of day, total time of operation, a reader unique ID, and a reader manufacturer ID.
53. The device of claim 51, wherein said code selection algorithm generates said first code based upon a number of messages previously transmitted from said device to said upstream device.
54. The device of claim 51, wherein said code selection algorithm changes in response to receiving a prompting signal from said upstream device.
55. The device of claim 46, wherein said code generator comprises a rolling code list.
56. The device of claim 55, wherein said code generator changes how the rolling code list is used in response to receiving a prompting signal from said upstream device.
57. The device of claim 56, wherein said prompting signal is transmitted randomly from said upstream device.
58. The device of claim 46, wherein said upstream device comprises a reader and wherein a credential comprises said code generator.

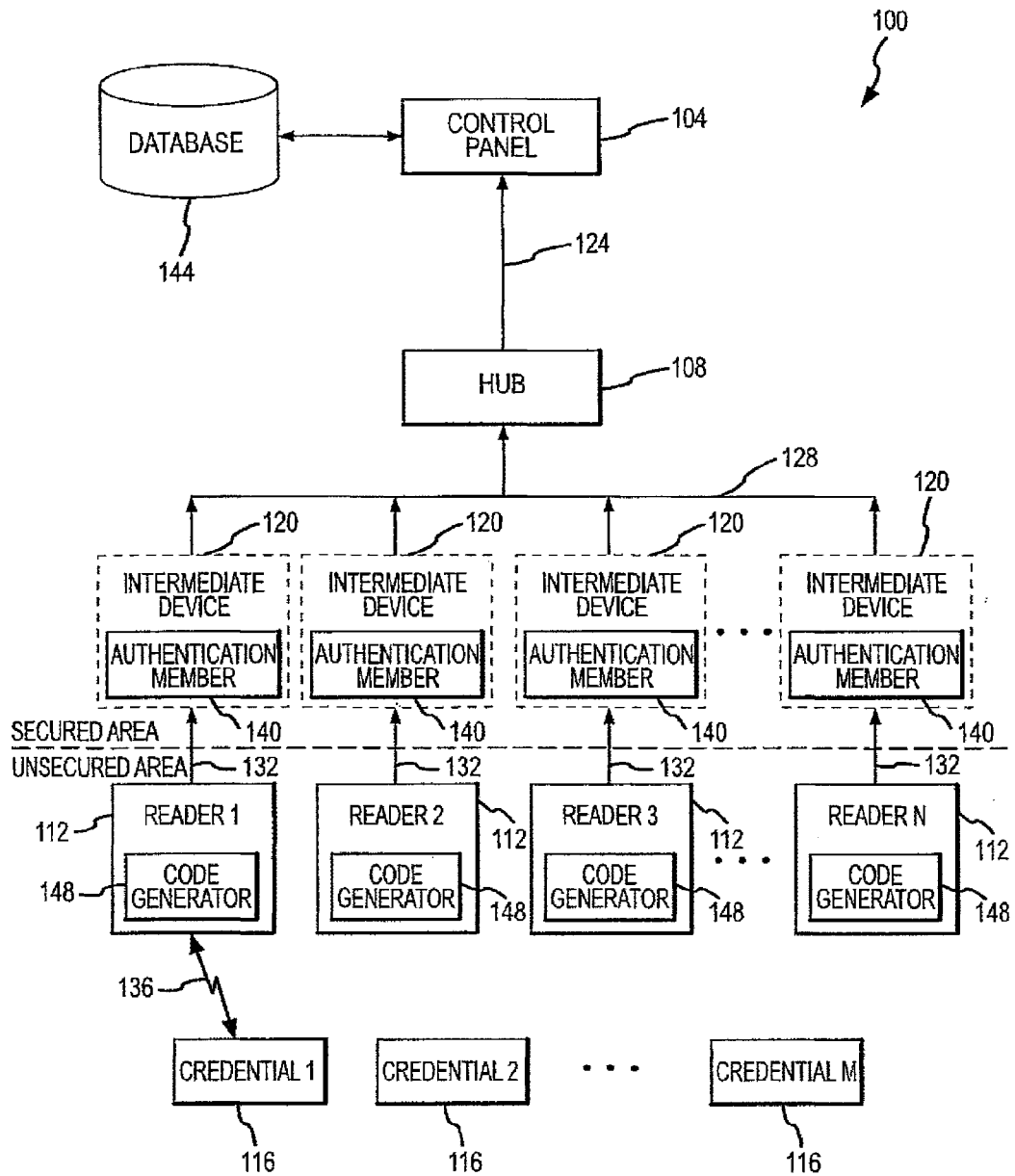


FIG.1

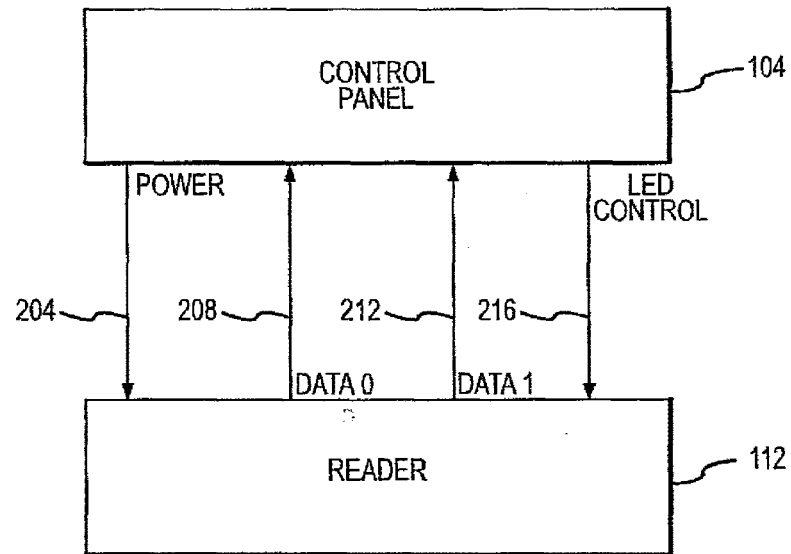


FIG.2
PRIOR ART

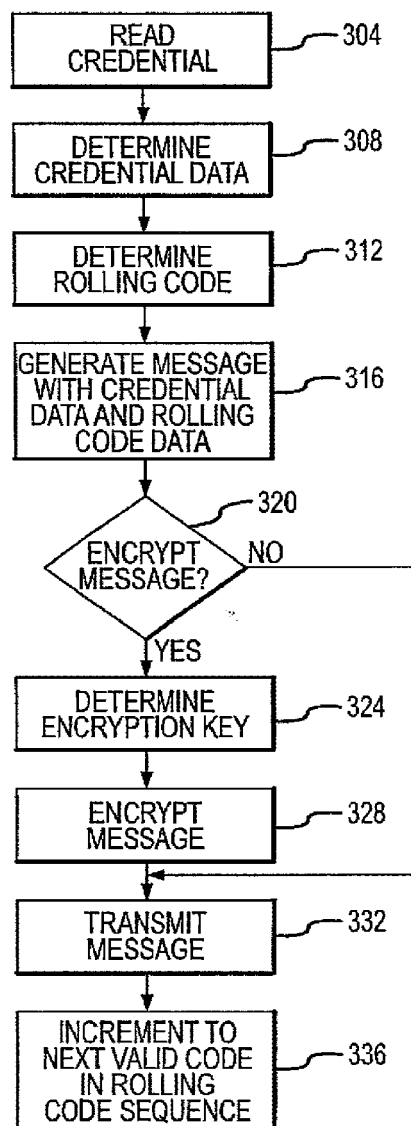
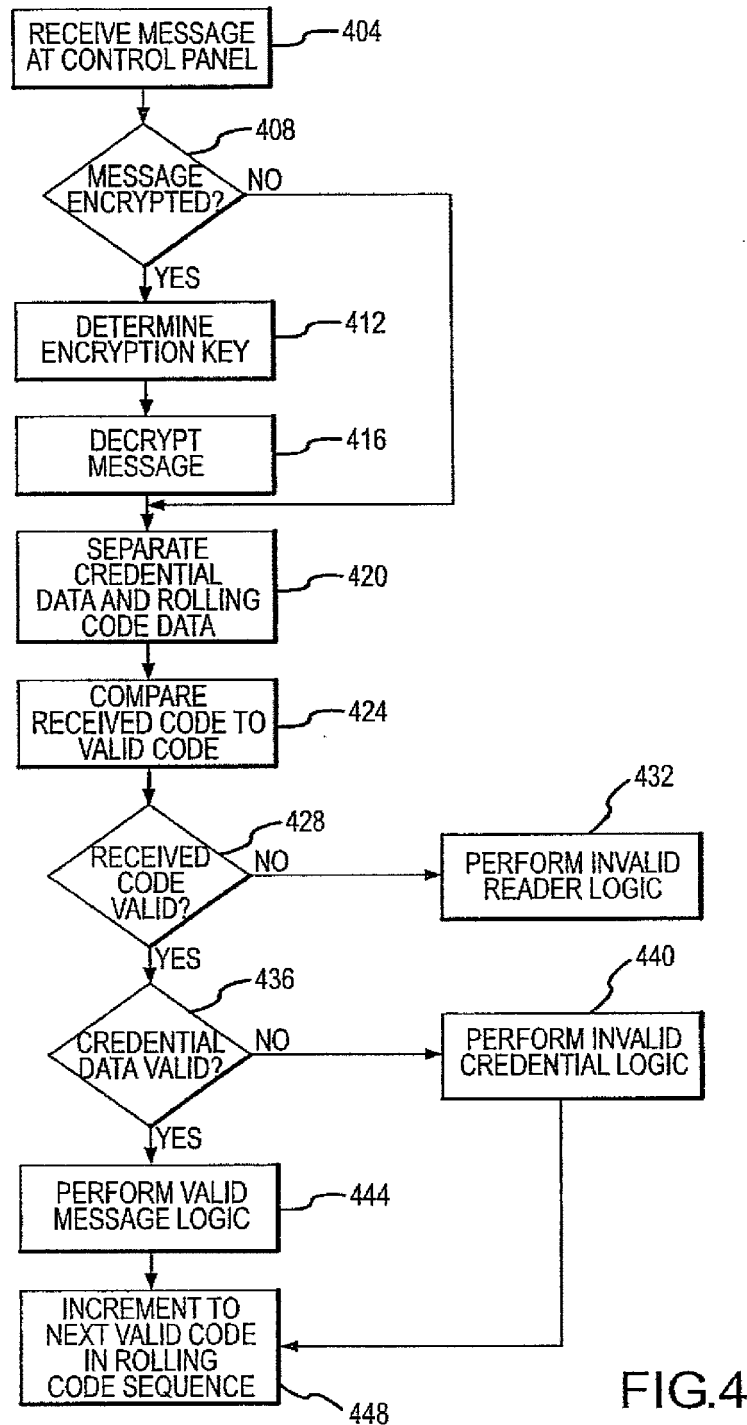


FIG.3



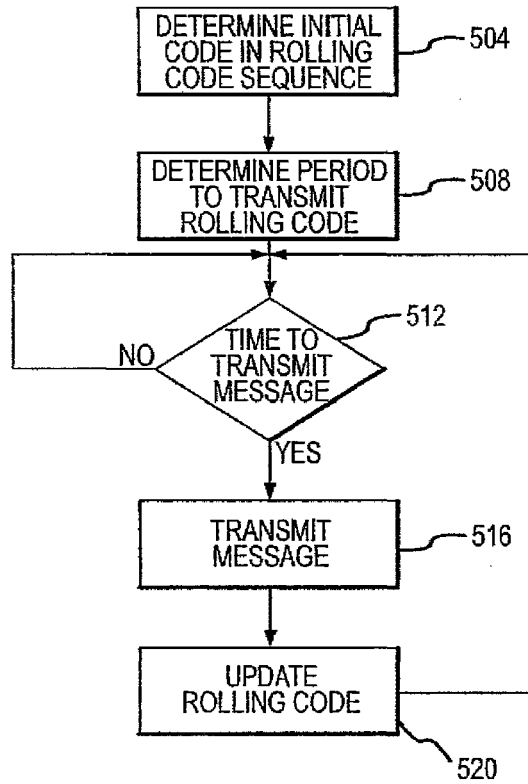


FIG.5

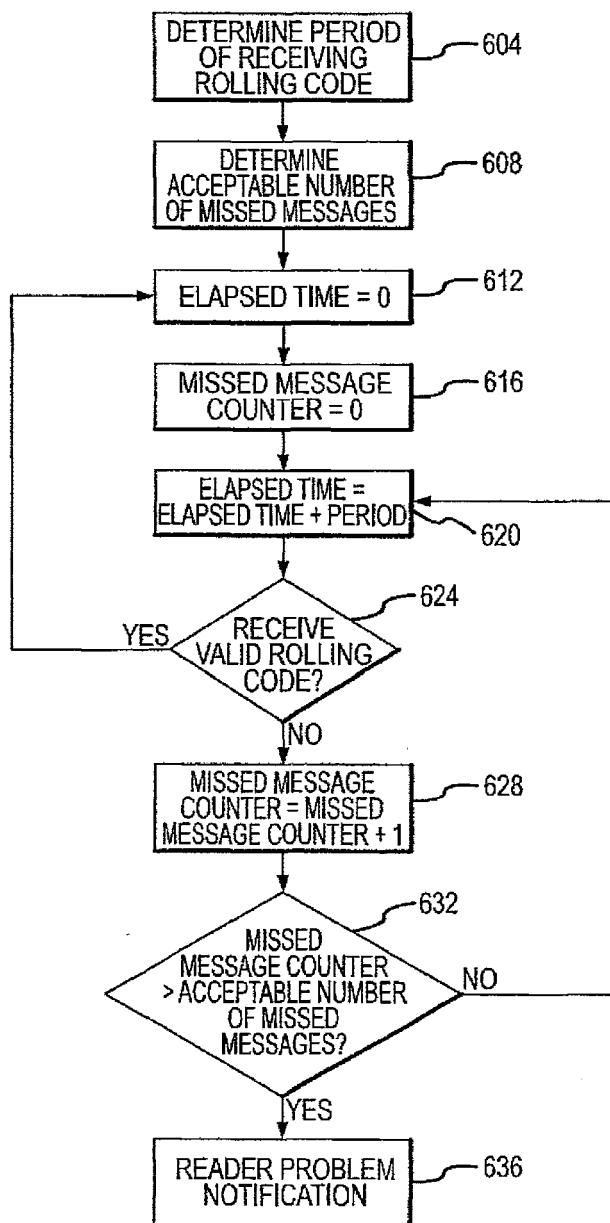


FIG.6

700

704

708

ROLLING CODE	REQUIRED CHECK IN TIME
A	T
B	T + PERIOD
C	T + (2 * PERIOD)
• • •	• • •
X	T + (k * PERIOD)

FIG.7

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 71352805 P [0001]
- US 6988203 B, Davis [0013]
- WO 2005038729 A, Merkert [0014]

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
17 April 2008 (17.04.2008)

(10) International Publication Number
WO 2008/043125 A1

(51) International Patent Classification:
H04L 9/32 (2006.01)

(74) Agent: **SPRUSON & FERGUSON**; GPO Box 3898, Sydney, NSW 2001 (AU).

(21) International Application Number:
PCT/AU2007/000311

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(22) International Filing Date: 13 March 2007 (13.03.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2006905707 13 October 2006 (13.10.2006) AU

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(71) Applicant (*for all designated States except US*): **MICROLATCH PTY LTD** [AU/AU]; Unit 13, 145-147 Forest Road, Hurstville, NSW 2220 (AU).

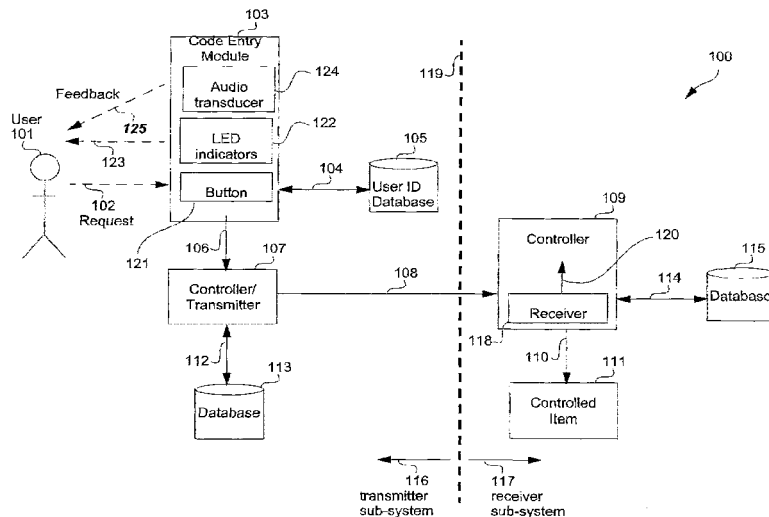
(72) Inventor; and

(75) Inventor/Applicant (*for US only*): **BROWN, Perry, Andrew** [AU/AU]; 67 Bredon Avenue, West Pennant Hills, NSW 2125 (AU).

Published:

— with international search report

(54) Title: A SECURE WIRELESS REMOTE ENTRY SYSTEM



(57) Abstract: A system (100) for providing secure access to a controlled item (111) is disclosed. The system (100) comprises a transmitter subsystem (116) comprising means for storing a Wiegand protocol identifier, means for receiving a request, means for generating a code from a sequence of codes based on the Wiegand identifier, upon receiving the request, means for encoding the code and the Wiegand protocol identifier, and means for transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier. The system (100) also comprises a receiver sub-system (117) comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item (111) dependent upon the code and the Wiegand protocol identifier.

WO 2008/043125 A1

A SECURE WIRELESS REMOTE ENTRY SYSTEM

Field of the Invention

The present invention relates to secure access systems and, in particular, to systems using wireless transmission of security code information.

5

Background

Fig. 1 shows a prior art arrangement for providing secure access. A user 401 makes a request, as depicted by an arrow 402, directed to a code entry module 403. The module 403 is typically mounted on the external jamb of a secure door. The request 402 is typically a secure code of some type which is compatible with the code entry module 10 403. Thus, for example, the request 402 can be a sequence of secret numbers directed to a keypad 403. Alternately, the request 402 may be a biometric signal from the user 401 directed to a corresponding biometric sensor 403. One example of a biometric signal is a fingerprint. Other physical attributes that can be used to provide biometric signals include voice, retinal or iris pattern, face pattern, palm configuration and so on.

15

The code entry module 403 conveys the request 402 by sending a corresponding signal, as depicted by an arrow 404, to a controller 405 which is typically situated in a remote or inaccessible place. The controller 405 authenticates the security information provided by the user 401 by interrogating a database 407 as depicted by an arrow 406. If the user 401 is authenticated, and has the appropriate access privileges, then the controller 20 405 sends an access signal, as depicted by an arrow 408, to a device 409 in order to provide the desired access. The device 409 can, for example, be the locking mechanism of a secure door, or can be an electronic lock on a personal computer (PC) which the user 401 desires to access. A proximity card can also be used to emit the request 402, in which case the code entry module 403 has appropriate functionality.

- 2 -

Although the request 402 can be made secure, either by increasing the number of secret digits or by using a biometric system, the communication infrastructure in **Fig. 1** is typically less secure. The infrastructure of the arrangement 400 is generally hardwired, with the code entry module 403 generally being mounted on the outside jamb of a secured door. In such a situation, the signal path 404 can be over a significant distance in order to reach the controller 405. The path 404 represents one weak point in the security system 400, providing an unauthorised person with relatively easy access to the information being transmitted between the code entry module 403 and the controller 405. Such an unauthorised person can, given this physical access, decipher the communicated information between the code entry module 403 and the controller 405. This captured information can be deciphered, replayed in order to gain the access which rightfully belongs to the user 401, or to enable modification for other subversive purposes.

Some current systems as depicted in **Fig. 1** utilise a serial communication protocol called “Wiegand” for communication between the code entry module 403 and the controller 405. The Wiegand protocol is a simple one-way data protocol. In one known arrangement for providing secure access that uses Wiegand, the signal 404 conveyed by the code entry module 403 to the controller 405 comprises a twenty four (24) bit Wiegand protocol identifier. The Wiegand protocol can be modified by increasing or decreasing the bit count to ensure uniqueness of the protocol among different security companies. However, the Wiegand protocol does not secure the information being sent between the code entry module 403 and the controller 405. The Wiegand protocol provides no protection against interception of the signal 404 nor injection of messages into the signal 404.

More advanced protocols are known to overcome the vulnerability of the Wiegand protocol over the long distance route 404. For example, one known

- 3 -

arrangement for providing secure access is that distributed by Microchip Technology Inc ("the Microchip arrangement"). The Microchip arrangement is also traded under the Trade Mark, "Keeloq". The Microchip arrangement comprises multiple transmitters similar to the code entry module 403 and a receiver similar to the controller 405 described
5 above. The code entry modules 403 of the Microchip arrangement typically reside within an insecure environment and the controller 405 resides within a secure environment. Again, authentication is based upon the transmission of a secure code in the form of a radio frequency (RF) signal over an insecure signal path similar to the signal path 404.

In the Microchip arrangement, there are typically 2^{32} different codes which may
10 be transmitted by the code entry module 403 to the controller 405. The code entry module 403 will generate one of these secure codes from a distinct sequence, advancing progressively through the sequence on each transmission. The sequence of codes is unique for each code entry module 403 and will exhibit no apparent pattern. The transmitted code should also not include a code from any of the 2^{15} previously transmitted
15 codes. In order to identify each code entry module 403 and a corresponding unique sequence of codes, each code entry module 403 is assigned a unique Microchip (Keeloq) serial number, which is typically twenty eight (28) bits in length. This serial number is included within each code transmission. Access will be granted by the controller 405, if a correct code is received from the code entry module 403. At any instant, the controller
20 405 will only accept a range of sixteen (16) codes from each code entry module's 403 sequence. Following receipt of a valid code, the sixteen code range is adjusted to coincide with the next sixteen (16) codes expected from the particular code entry module 403. This allows up to sixteen (16) transmissions to be damaged/lost before the controller 405 and the code entry module 403 become partially unsynchronised. In order to recover
25 from a partial synchronisation loss, the controller 405 typically accepts as valid, two

- 4 -

consecutive codes from the 2^{15} possible codes in advance of the most recently validated code from the code entry module 403.

The Microchip arrangement achieves “unpredictability” of its codes by means of a secret “key” (typically sixty four (64) bits in length) which is known by both the code entry module 403 and the controller 405. The code entry module 403 encodes the code for transmission using an invertible encryption algorithm, customised through the application of the secret key and the Microchip (Keeloq) serial number. Accordingly, a simple ascending numerical sequence may be transformed into apparently random, uncorrelated codes, with a code sequence unique for each particular code entry module 403.

Conventionally, initial synchronisation has been established between the code entry module 403 and the controller 405 of the Microchip arrangement, by instructing the controller 405 to accept a current transmission unconditionally, without regard to the transmitted code’s position within the sequence. This instruction is made through physical operation of a switch or similar mechanism located within the controller 405, while transmission is in progress. This requirement for physical operation is used to demonstrate to the controller 405 that the code entry module 103 has independent credentials for accessing the secure area, thus authorising synchronisation. Accordingly, this conventional method of synchronisation creates a weakness in the Microchip arrangement, which may be exploited by any fraudster who is be able to gain access to the secure environment of the controller 403 and synchronise a code entry module 403.

Summary

It is an object of the present invention to substantially overcome, or at least ameliorate, one or more disadvantages of existing arrangements.

- 5 -

According to one aspect of the present invention there is provided a system for providing secure access to a controlled item, the system comprising:

a transmitter subsystem:

means for storing a Wiegand protocol identifier;

5 means for receiving a request;

means for generating a code from a sequence of codes based on the Wiegand identifier, upon receiving the request;

means for encoding the code and the Wiegand protocol identifier;

and

10 means for transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier; and

a receiver sub-system comprising;

means for receiving the transmitted secure access signal; and

15 means for providing conditional access to the controlled item dependent upon said code and said Wiegand protocol identifier.

According to another aspect of the present invention there is provided a transmitter sub-system for operating in a system for providing secure access to a controlled item, the system comprising a receiver sub-system comprising means for receiving a secure access signal transmitted by the transmitter sub-system, and means for
20 providing conditional access to the controlled item dependent upon information conveyed in the secure access signal, wherein the transmitter subsystem comprises:

means for storing a Wiegand protocol identifier;

means for receiving a request;

25 means for generating a code from a sequence of codes based on the Wiegand protocol identifier, upon receiving the request;

- 6 -

means for encoding the code and the Wiegand protocol identifier; and

means for transmitting said secure access signal comprising the code and the encoded Wiegand protocol identifier embedded therein.

According to still another aspect of the present invention there is provided a
5 receiver sub-system for operating in a system for providing secure access to a controlled
item, the system comprising transmitter subsystem comprising means for storing a
Wiegand protocol identifier, means for receiving a request, means for generating a code
from a sequence of codes based on said Wiegand identifier, upon receiving the request,
means for encoding the code and the Wiegand identifier, and means for transmitting a
10 secure access signal comprising the code and the encoded Wiegand protocol identifier,
wherein the receiver sub-system comprises:

means for receiving the transmitted secure access signal comprising the
code and the encoded Wiegand protocol identifier; and

means for providing conditional access to the controlled item dependent
15 upon said code and said Wiegand protocol identifier.

According to still another aspect of the present invention there is provided a
method for providing secure access to a controlled item, the method comprising the steps
of:

receiving a request;

20 generating a code from a sequence of codes based on a Wiegand identifier, upon
receiving the request;

encoding the code and the Wiegand protocol identifier;

transmitting a secure access signal comprising the code and the encoded
Wiegand protocol identifier to a controller of said controlled item; and

- 7 -

providing conditional access to the controlled item dependent upon said code and said Wiegand identifier.

According to still another aspect of the present invention there is provided a computer program product having a computer readable medium having a computer
5 program recorded therein for directing a processor to provide secure access to a controlled item, said computer program product comprising:

code for receiving a request;

code for generating a code from a sequence of codes based on a Wiegand identifier, upon receiving the request;

10 code for encoding the code and the Wiegand protocol identifier;

code for transmitting a secure access signal comprising the code and the Wiegand encoded protocol identifier to a controller of said controlled item, wherein said controller provides conditional access to the controlled item dependent upon said code and said Wiegand identifier.

15 According to still another aspect of the present invention there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to transmit a secure access signal in a system for providing secure access to a controlled item, said computer program product comprising:

20 code for receiving a request;

code for generating a code from a sequence of codes based on a Wiegand identifier, upon receiving the request;

code for encoding the code and the Wiegand protocol identifier; and

code for transmitting said secure access signal comprising the code and the
25 encoded Wiegand protocol identifier to a controller of said controlled item, wherein said

- 8 -

controller provides conditional access to the controlled item dependent upon said code and said Wiegand identifier.

According to still another aspect of the present invention there is provided a method of enrolling a biometric signature into a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising means for storing a Wiegand protocol identifier, means for receiving a request, means for generating a code from a sequence of codes based on the Wiegand identifier, means for encoding the code and the Wiegand protocol identifier, and means for transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier, and a receiver subsystem comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon said code and said Wiegand protocol identifier, said method comprising the steps of:

receiving a biometric signal; and
storing a biometric signature in the database, as a representation of the biometric signal, if the database of biometric signatures is empty; and
classifying the stored biometric signature as an administrator, thereby enrolling the received biometric signature.

According to still another aspect of the present invention there is provided an apparatus for enrolling a biometric signature into a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising means for storing a Wiegand protocol identifier, means for receiving a request, means for generating a code from a sequence of codes based on the Wiegand identifier, means for encoding the code and the Wiegand protocol identifier, and means for transmitting a secure access signal

- 9 -

comprising the code and the encoded Wiegand protocol identifier, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon said code and said Wiegand protocol identifier, said apparatus comprising:

- 5 receiving means for receiving a biometric signal; and
- storage means for storing the biometric signature in the database, as a representation of the biometric signal, if the database of biometric signatures is empty; and
- classification means for classifying the stored biometric signature as an
- 10 administrator, thereby enrolling the received biometric signature.

 According to still another aspect of the present invention there is provided a computer program product having a computer readable medium having a computer program recorded therein for enrolling a biometric signature into a database of biometric signatures in a system for providing secure access to a controlled item, the system

15 comprising said database of biometric signatures, a transmitter subsystem comprising means for storing a Wiegand protocol identifier, means for receiving a request, means for generating a code from a sequence of codes based on the Wiegand identifier, means for encoding the code and the Wiegand protocol identifier, and means for transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier,

20 and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon said code and said Wiegand protocol identifier, said program comprising:

- code for receiving a biometric signal representing a biometric signature; and
- code for storing the biometric signature in the database, as a representation of the
- 25 biometric signal, if the database of biometric signatures is empty; and

- 10 -

code for classifying the stored biometric signature as an administrator, thereby enrolling the received biometric signature.

Other aspects of the invention are also disclosed.

Brief Description of the Drawings

5 Some aspects of the prior art and one or more embodiments of the present invention are described with reference to the drawings, in which:

Fig. 1 shows a prior art arrangement for providing secure access;

Fig. 2 is a functional block diagram of an arrangement for providing secure access according to the present disclosure;

10 **Fig. 3** shows an example of a method of operation of a sub-system of **Fig. 2** comprising a code entry module, according to one embodiment;

Fig. 4 shows an example of a method of operation of the (fixed) control device of **Fig. 2**;

Fig. 5 is a schematic block diagram of the arrangement in **Fig. 2**; and

15 **Fig. 6** shows a method of operation of the sub-system of **Fig. 2** comprising the code entry module, according to another embodiment;

Fig. 7 shows an access process relating to the example of **Fig. 6**;

Fig. 8 shows one enrolment process relating to the example of **Fig. 6**; and

Fig. 9 shows another enrolment process relating to the example of **Fig. 6**.

Detailed Description including Best Mode

20 It is to be noted that the discussions contained in the "Background" section relating to prior art arrangements relate to discussions of documents or devices which form public knowledge through their respective publication and/or use. Such should not be interpreted as a representation by the present inventor(s) or patent applicant that such documents or devices in any way form part of the common general knowledge in the art.

- 11 -

Where reference is made in any one or more of the accompanying drawings to steps and/or features, which have the same reference numerals, those steps and/or features have for the purposes of this description the same function(s) or operation(s), unless the contrary intention appears.

5 **Fig. 2** is a functional block diagram of an arrangement 100 for providing secure access according to the present disclosure. The arrangement 100 may also be referred to as a system comprising sub-systems 116 and 117. The arrangement of **Fig. 2** comprises a code entry module 103. The code entry module 103 is preferably a Microchip (Keeloq) code entry module, as described above, which is modified as described below. However,
10 a person skilled in the art would appreciate that any other suitable type of code entry module may be used.

In the arrangement 100 of Fig. 2, a user 101 makes a request, as depicted by an arrow 102, to a controller/transmitter 107 configured within a code entry module 103. The code entry module 103 comprises a button 121 and the request 102 takes the form of
15 a button press. A signal, as depicted by arrow 106, generated by the button press is sent to the controller/transmitter 107. Upon receiving the signal 106, the controller/transmitter 107 is configured to generate a code. In particular, the controller/transmitter 107 is configured to generate one of the 2^{32} different codes. However, the controller/transmitter 107 may be configured to generate any suitable number of different codes. The code
20 entry module 103 will generate one of these codes from a distinct sequence, advancing progressively through the sequence on each request 102 being received. The sequence of codes is unique for each code entry module 103. Accordingly, upon receiving the signal 106, the controller/transmitter 107 checks, as depicted by an arrow 112, the current code in a database 113. The controller 107 then generates a new code in the sequence of codes
25 for the code entry module 103.

- 12 -

In order to identify each code entry module 103 and the corresponding unique sequence of codes, each code entry module 103 of the present disclosure is assigned a different serial number. In the described arrangement, the Microchip (Keeloq) serial number, which is typically twenty eight (28) bits in length, is replaced by a Wiegand protocol identifier. The Wiegand protocol identifier is typically twenty four (24) bits in length. Each code entry module 103 has a different Wiegand protocol identifier. Prior to replacing the Microchip (Keeloq) serial number with the Wiegand identifier, the Wiegand protocol identifier is encoded using an invertible twenty four (24) bit encryption algorithm. Examples of encryption algorithms that may be used to encode the Wiegand protocol identifier include the Rivest, Shamir, & Adleman (RSA) algorithm, the Public Key Infrastructure (PKI) algorithm, the Data Encryption Standard (DES), Blowfish and the International Data Encryption Algorithm (IDEA). The encryption algorithm used to encode the Wiegand protocol identifier is known only to the code entry module 103 and to a receiver 118, as seen in Fig. 2, which will be described below.

The encoded Wiegand protocol identifier is inserted into bits zero (0) to twenty three (23) of the normal Microchip (Keeloq) serial number address space for the code entry module 103. The remaining four bits (i.e., bits twenty four (24) to twenty seven (27)) of the Microchip (Keeloq) serial number are set to a predetermined fixed value (e.g., a series of '1's) indicating that the Microchip (Keeloq) serial number has been replaced by an encoded Wiegand protocol identifier. The Wiegand protocol identifier is allocated entirely within a predetermined ($1/16^{\text{th}}$) portion of the normal Microchip (Keeloq) code entry module (or transmitter) address space for the code entry module 103. A person skilled in the art would appreciate that the Wiegand protocol identifier may be inserted into any suitable bits of the normal Microchip (Keeloq) serial number address space for

- 13 -

the code entry module 103. Further, any bits may be used to indicate that the Microchip (Keeloq) serial number has been replaced by the Wiegand protocol identifier.

Each code entry module 103 has a Wiegand protocol identifier allocated to the code entry module 103 prior to the code entry module 103 being distributed to the user 101 for use. The Wiegand protocol identifier may be stored in the database 113. Prior to the code entry module 103 being distributed to the user 101, the code entry module 103 is also allocated a secret "key" (typically sixty four (64) bits in length) which is known by both the code entry module 403 and the receiver 118. Again, the secret key may be stored in the database 113 on the transmitter sub-system 116. The secret key may also be stored in a database 115 on the receiver sub-system 117.

Upon generating the new code in the sequence of codes for the code entry module 103, the controller 107 sends the updated code, this being referred to as an access signal, as depicted by an arrow 108 to the receiver 118. Prior to the new code being sent to the controller 109, the new code is preferably encoded by the controller 107 using one of the encryption algorithms described above with the encryption algorithm being customised through the application of the secret key and the Wiegand protocol identifier. The encoded Wiegand protocol identifier number for the code entry module 103 is also included within the access signal 108.

The receiver 118 receives the access signal 108 and firstly determines that the four bit fixed portion of the address space for a Microchip (Keeloq) serial number correctly indicates that the serial number has been replaced by an encoded Wiegand protocol identifier. If the receiver 118 determines that the four bit fixed portion does not indicate that the Microchip (Keeloq) serial number has been replaced by an encoded Wiegand protocol identifier then the receiver 118 rejects the access signal 108. Otherwise, the receiver 118 decodes the code included in the access signal 108, using the

- 14 -

encryption algorithm that was used by the code entry module 103 to encode the code. The receiver also decodes the Wiegand protocol identifier using the encryption algorithm that was used by the code entry module 103 to encode the Wiegand protocol identifier.

Based on the decoded Wiegand protocol identifier, the receiver 118 identifies the
5 sequence of codes being used by the code entry module 103 and tests the code received in the access signal 108 against the most recent previously received code for the code entry module 103, this code having been stored in the database 115, this testing being depicted by an arrow 114. As will be described in detail below, the codes are stored in the database 115 in a hash table, or similar data structure. The receiver 118 uses the Wiegand
10 protocol identifier received with the access signal 108 and linear probing for accessing the codes stored in the hash table in order to test the code received in the access signal 108.

If the code within the received access signal 108 is found to be the next code in the sequence for the received Wiegand protocol identifier, then, the receiver 118 provides a signal 120, in Wiegand format, to the controller 109. The signal 120 includes the
15 decoded Wiegand identifier. In response to the signal 120, the controller 109 sends a command, as depicted by an arrow 110, to a controlled item 111. The controlled item 111 may be a door locking mechanism on a secure door, or an electronic key circuit in a personal computer (PC) that is to be accessed by the user 101.

It is noted that the receiver 118 receives the transmitted access signal 108 and
20 converts it into a form that the controller 109 can use, as depicted by the arrow 120. As the Wiegand protocol identifier is allocated entirely within a predetermined portion of the normal address space for Microchip (Keeloq) code entry modules (or transmitters) of the code entry module 103, the receiver 118 may be a conventional Microchip (Keeloq) receiver. However, such a conventional Microchip (Keeloq) receiver is modified so as to

- 15 -

use the Wiegand protocol identifier received with the access signal 108 for accessing the codes stored in the hash table.

The sub-system 117 maintains a unique sequence of codes for each of the code entry modules that the receiver 118 may encounter. Each of these code entry modules has a unique Wiegand protocol identifier corresponding to one of the sequences. The total number of possible code entry modules, each having a unique Wiegand identifier, and accordingly, the total number of unique code sequences, is 2^{24} (i.e., more than 16 million). A person skilled in the relevant art would appreciate that more or less code sequences may be possible. Each of these code sequences is stored in the database 115.

10 In order to provide sufficient access for the receiver 118 to the stored codes, the codes are stored in a hash table or similar data structure within the database 115, as described above. The receiver 118 may use a “hash table with linear probing” algorithm, as described above, to access the codes within the data structure. This allows the codes to be stored within a physical storage area of a size proportional to the number of active code entry modules. Such a hash table algorithm also requires the selection of a “hash function.” The 24 bit Wiegand protocol identifier may be used as this hash function.

The code entry module 103 may also incorporate at least one mechanism for providing feedback to the user 101. This mechanism may, for example, take the form of one or more Light Emitting Diodes (LEDs) 122 which can provide visual feedback, depicted by an arrow 123 to the user 101. Alternately or in addition the mechanism can take the form of an audio signal provided by an audio transducer 124 providing audio feedback 125.

The codes generated by the code entry module 103 may be referred to as “rolling codes”. Rolling codes provide a substantially non-replayable, non-repeatable and encrypted radio frequency data communications scheme for secure messaging. These

- 16 -

codes use inherently secure protocols and serial number ciphering techniques which in the present disclosure hide the clear text values required for authentication between the key fob (transmitter) sub-system 116 and the receiver/controller 118/109.

As described above, the rolling codes generated by the code entry module 103
5 use a different code variant each time the transmission of the access signal 108 occurs. This is achieved by encrypting the data from the controller 107 with an encryption algorithm, as described above, and ensuring that successive transmissions of the access signal 108 are modified using a code and/or a look-up table or hash table known to both the transmitter sub-system 116 and the receiver sub-system 117. Using this approach,
10 successive transmissions are modified, resulting in a non-repeatable data transfer, even if the information from the controller 107 remains the same. The modification of the code in the access signal 108 for each transmission significantly reduces the likelihood that an intruder can access the information and replay the information to thereby gain entry at some later time.

As described above, based on the Wiegand protocol identifier, the receiver 118
15 identifies the sequence of codes being used by the code entry module 103 and tests the code received in the access signal 108 against the most recent previously received code for the code entry module 103, this code having been stored in the database 115, this testing being depicted by the arrow 114. If the incoming code forming the access signal
20 108 is found "not to be" the next code in the sequence for that code entry module 103, then the receiver 118 stores the Wiegand protocol identifier received in the access signal 108. The receiver 118 also then stores another code which is the next code expected in the sequence (the "expected next code") for the code entry module 103 (i.e., as identified by the Wiegand protocol identifier) after the code that was received in the access signal 108.
25 The receiver 118 also starts a timer for a predetermined time. If another access signal 108

- 17 -

is received from the same code entry module 103 within the predetermined time and the code in the access signal 108 exactly matches the “expected next code” as previously stored, then the receiver 118 provides the signal 120 in the Wiegand format to the controller 109. The receiver 118 also stores a flag in the database 115 indicating that the receiver 118 and the code entry module 103 are “synchronised”. Accordingly, the code entry module 103 and the receiver 118 may be synchronised provided the code entry module 103 can generate two consecutive “in sequence” codes.

The above method of synchronising the code entry module 103 and the receiver 118 is particularly advantageous over conventional Microchip (Keeloq) secure access arrangements using conventional Microchip (Keeloq) code entry modules (or transmitters), which require physical operation of a switch mechanism in a receiver. The arrangement 100 described above can maintain security without the need to demonstrate physical access during synchronisation, since the arrangement 100 guarantees the authenticity of the code entry module 103, and hence the authenticity of the resultant Wiegand protocol identifiers.

The sub-system in Fig. 2 falling to the left hand side, as depicted by an arrow 116, of a dashed line 119 may be implemented in a number of different forms. The sub-system 116 may for example be incorporated into a remote fob (which is a small portable device carried by the user 101), or alternately may be mounted in a protected enclosure on the outside jamb of a secured door. The sub-system 116 communicates with the sub-system 117 on the right hand side of the dashed line 119 via the wireless communication channel used by the access signal 108. The sub-system 117 is typically located in an inaccessible area such as a hidden roof space or alternately in a suitable protected area such as an armoured cupboard. The location of the sub-system 117 must of course be consistent with reliable reception of the wireless access signal 108.

- 18 -

Although typically the communication channel uses a wireless transmission medium, there are instances where the channel used by the access signal 108 may use a wired medium. This is particularly the case when the transmitter sub-system 116 is mounted in an enclosure on the door jamb rather than in a portable key fob.

5 In the event that the sub-system 116 is implemented as a remote fob, the combination of the Wiegand identifier and the strongly encrypted wireless communication provides a particularly significant advantage over conventional secure access arrangements. The remote key fob arrangement allows easy installation, since the wired communication path 404 (see **Fig. 1**) is avoided. Other existing wiring elements of
10 the present systems 400 may be used where appropriate.

Fig. 3 shows the method of operation of the sub-system 116 of **Fig. 2** comprising the code entry module 103. The process 200 commences with a testing step 201 in which the code entry module 103 checks whether a request 102 is being received. If this is not the case, then the method 200 is directed in accordance with a NO arrow back to the step
15 201 in a loop. If, on the other hand, the request 102 has been received, then the method 200 is directed in accordance with a YES arrow to a step 202. In the step 202, the controller/transmitter 107 checks, as depicted by an arrow 112, the current code in the database 113. Then at the next step 203, the controller/transmitter 107 generates a new code in the sequence of codes for the code entry module 103 according to the Wiegand
20 protocol identifier allocated to the code entry module 103.

At the next step 204, the newly generated code is encoded by the controller/transmitter 107 using one of the encryption algorithms described above, with the encryption algorithm being customised through the application of the secret key and the Wiegand protocol identifier. The Wiegand identifier is also encrypted at step 204,
25 using one of the encryption algorithms described above. In the subsequent step 205, the

- 19 -

controller 107 sends the appropriate access signal 108 to the receiver 109. The access signal comprises the encoded code and the encoded Wiegand protocol identifier. The process 200 is then directed in accordance with an arrow 206 back to the step 201.

Fig. 4 shows the method of operation of the control sub-system 117 of **Fig. 2**.

5 The process 300 commences with a testing step 301 which continuously checks whether the access signal 108 has been received from the controller/transmitter 107. The step 301 is performed by the receiver 118. As long as the access signal 108 is not received the process 300 is directed in accordance with a NO arrow in a looping manner back to the step 301. When the access signal 108 is received, the process 300 is directed from the
10 step 301 by means of a YES arrow to a step 302. In the step 302, if the receiver 118 determines that the four bit fixed portion following the Wiegand protocol identifier included in the received access signal 108 correctly indicates that the serial number has been replaced by an encoded Wiegand protocol identifier, then the process 300 is directed from the step 302 by means of a YES arrow to a step 303. Otherwise, the process 300 is
15 directed in accordance with a NO arrow in a looping manner back to the step 301.

At step 303, the receiver 118 decodes the code included in the access signal 108, using the encryption algorithm that was used to encode the code. The receiver 118 also decodes the Wiegand protocol identifier included in the signal 108. Then at step 304, the receiver 118 identifies the sequence of codes being used by the code entry module 103,
20 based on the Wiegand protocol identifier, and tests the code received in the access signal 108 against the most recent previously received code for the code entry module 103, this code having been stored in the database 115. If the incoming code forming the access signal 108 is found to be the next code in the sequence corresponding to the Wiegand protocol identifier included in the access signal 108, then the process 300 is directed from
25 the step 304 by means of a YES arrow to a step 305. In step 305, the receiver 118

- 20 -

provides the signal 120 in the Wiegand format to the controller 109. The signal 120 comprises the Wiegand protocol identifier.

In a subsequent step 308, the controller 109 sends a control signal 110 to the controlled item 111 (for example opening a secured door). The process 300 is then
5 directed from the step 308 as depicted by an arrow 308 back to the step 301.

Returning to the testing step 304, if the incoming code forming the access signal 108 is found “not to be” the next code in the sequence corresponding to the Wiegand protocol identifier included in the received access signal 108, then the process 300 is directed from the step 304 by means of the NO arrow to step 306. At step 306, the
10 receiver 118 determines what the next code in the sequence corresponding to the Wiegand protocol identifier after the code that was received in the access signal 108 at step 301. This next code is the “next expected code” as described above. Then at the next step 309, the receiver 118 stores the code entry module’s 103 Wiegand protocol identifier and the code determined at step 306 (i.e., the next expected code) in the database 115. The
15 receiver 118 also starts a timer to time out for a predetermined time (e.g., ten (10) seconds).

In a subsequent step 310, if another access signal 108 is received from the same code entry module 103 (i.e., the access signal 108 contains the encoded Wiegand protocol identifier corresponding to the code entry module 103) within the predetermined time,
20 then the process 300 is directed from the step 310 by means of the YES arrow to step 311. Otherwise, the process 300 is directed from the step 310 by means of the NO arrow back to step 301. At step 311, if the incoming code included in the access signal 108 received at step 310 is found to be the code stored at step 309 (i.e., the next expected code), then the process 300 is directed from the step 311 by means of a YES arrow to step 307.
25 Otherwise, the process 300 is directed from the step 311 by means of the NO arrow back

- 21 -

to step 301. Accordingly, the code entry module 103 and the receiver 118 may be synchronised provided the code entry module 103 can generate two consecutive “in sequence” codes.

One of the advantages of the arrangement 100 described above is that security system upgrades may be made without replacing the Wiegand compatible controller 109. Accordingly, existing systems as are described in **Fig. 1** may be upgraded by replacing the code entry module 403 and the transmission path 404, leaving the other components of the system 400 (ie., the controller 405, the code database 407, and the controlled item 409, together with existing wiring 408 and 406), largely intact. Minor programming modifications may however be necessary to the receiver 118 so that the receiver 118 uses the Wiegand protocol identifier to interrogate the hash table stored in the database 115. When upgrading systems in this manner, the sub-system 116 may either be used in a remote fob configuration, or may be placed in a secure housing on an external door jamb.

In the code entry module 103 described above, the code entry module 103 comprises a button 121 and the request 102 takes the form of a button press. In another embodiment as described below, the code entry module 103 may comprise a biometric sensor (not shown), either in place of the button 121 or as well as the buttons 121, and the request 102 may take a form which corresponds to the nature of the biometric sensor in the module 103.

In accordance with the further embodiment described below of the arrangement 100, the button 121 is replaced by a biometric sensor which will be referred to below as the “biometric sensor 121”. If the biometric sensor 121 in the code entry module 103 is a fingerprint sensor, then the request 102 typically takes the form of a thumb press on a sensor panel (not shown) on the code entry module 103. In this instance, the code entry module 103 would interrogate, as depicted by an arrow 104, a user identity database 105.

- 22 -

Thus, for example, if the request 102 is the thumb press on the biometric sensor 121 then the user database 105 contains biometric signatures for authorised users against which the request 102 can be authenticated. If the identity of the user 101 is authenticated successfully, then the code entry module 103 sends the signal 106 to the
5 controller/transmitter 107. Then, as at step 202, in response to receiving the signal 106, the controller/transmitter 107 checks, as depicted by the arrow 112, the current code in the database 113. The controller/transmitter 107 then generates a new code in the sequence of codes for the code entry module 103, as at step 203. As described above, the newly generated code is encrypted by the controller/transmitter 107 using one of the
10 encryption algorithms described above. The controller 107 then sends the appropriate access signal 108 to the receiver 109, as at step 205.

The biometric signature database 105 is shown in **Fig. 2** to be part of the transmitter sub-system 116. However, in an alternate arrangement, the biometric signature database 105 may be located in the receiver sub-system 117, in which case the communication 104
15 between the code entry module 103 and the signature database 105 may also be performed over a secure wireless communication channel such as the one used by the access signal 108. In the event that the secure access arrangement 100 is being applied to providing secure access to a PC, then the secured PC may store the biometric signature of the authorised user in internal memory, and the PC may be integrated into the receiver
20 sub-system 117 of **Fig. 2**.

In addition to authenticating the user 101, the biometric sensor 121 in the code entry module 103 in conjunction with the controller 107 may also check other access privileges of the user 101. These access privileges may be contained in the database 105 which may be located either locally in the remote key fob, or in the receiver sub-system
25 117 as previously described. In one example, Tom Smith may firstly be authenticated as

- 23 -

Tom Smith using the thumb press by Tom on the biometric sensor panel (not shown). After Tom's personal biometric identity is authenticated, the transmitter sub-system 116 may check if Tom Smith is in fact allowed to use the particular door secured by the device 111 on weekends. Thus the security screening offered by the described
5 arrangement may range from simple authentication of the user's identity, to more comprehensive access privilege screening.

The incorporation of the biometric sensor 121 into the code entry module 103 in the form of a remote key fob also means that if the user 101 loses the remote key fob, the user need not be concerned that someone else can use the code entry module 103. Since
10 the finder of the lost key fob will not be able to have his or her biometric signal authenticated by the biometric sensor 121 in the code entry module 103, the lost key fob is useless to anyone apart from the rightful user 101.

The transmitter sub-system 116 is preferably fabricated in the form of a single integrated circuit (IC) to reduce the possibility of an authorised person bypassing the
15 biometric sensor 121 in the code entry module 103 and directly forcing the controller 107 to emit the access signal 108.

The incorporation of the biometric sensor 121 into the code entry module 103, as described above, allows the user 101 to be validated. In this manner, the transmissions of the access signal 108 containing the encrypted code and Wiegand protocol identifier may
20 be limited to occur for only authorised users. The incorporation of the biometric sensor 121 into the code entry module 103, also allows the security of the arrangement of **Fig. 2** to be maintained without the reliance on the physical security of the code entry modules. However, the incorporation of the biometric sensor 121 also creates the need for a method of allowing the enrolment of the user's biometrics.

- 24 -

Fig. 6 shows another process 700 of operation of the arrangement 100 of **Fig. 2** where the code entry module 103 incorporates the biometric sensor 121, in accordance with the further embodiment. In this further embodiment, the process 700 is performed instead of the process 200 of **Fig. 3**. The code entry module 103 incorporating the biometric sensor 121 is allocated a range of Wiegand protocol identifiers rather than just one Wiegand protocol identifier as with the first embodiment described above. The Wiegand protocol identifier in this range are distinct from those allocated to other code entry modules sharing the same “secret” key as described above. The Wiegand protocol identifier being used at any particular time is referred to as the “current” Wiegand protocol identifier.

The process 700 commences with a step 701 that determines if a biometric signal has been received by the biometric sensor 121 in the code entry module 103. If not, then the process 700 follows a NO arrow back to the step 701. If however a biometric signal has been received, then the process 700 follows a YES arrow to a step 702 that determines if the user ID database 105 in **Fig. 2** is empty. This would be the case, for example, if the code entry module is new and has never been used, or if the user 101 has erased all the information in the database 105 (as will be described in detail below).

If the database 105 is empty, then the process 700 is directed by an arrow 703 to 706 in **Fig. 8** which depicts a process 800 dealing with the enrolment or the administration function for loading relevant signatures into the database 105. If on the other hand the database 105 is not empty, then the process 700 is directed to a step 704 that determines if the biometric signal that has been received is an administrator’s biometric signal.

The arrangement 100 comprising the code entry module 103 incorporating the biometric sensor 121 may accommodate at least three classes of user, namely

- 25 -

administrators, (ordinary) users, and duress users. The administrators have the ability to amend data stored, for example, in the database 105, while the ordinary users preferably do not have this capability. The first user of the code entry module 103, whether this is the user who purchases the module, or the user who programs the module 103 after all
5 data has been erased from the database 105, is automatically categorised as an administrator. This first administrator may direct the arrangement 100 to either accept further administrators, or alternately to only accept further ordinary users.

Although the present description refers to “users”, in fact it is “fingers” which are the operative entities in operation of the arrangement 100 where the biometric sensor
10 121 is a fingerprint sensor. In this event, a single user may enrol two or more of his or her own fingers as separate administrators or (ordinary) users of the arrangement 100, by storing corresponding fingerprints for corresponding fingers in the database 105 via the enrolment process 800 (see **Fig. 8**).

Some class overlap is possible. Thus a stored biometric signature can belong to
15 an administrator in the duress class.

The first administrator may provide control information to the code entry module 103 by providing a succession of finger presses to the biometric sensor 121, providing that these successive presses are of the appropriate duration, the appropriate quantity, and are input within a predetermined time. In one arrangement, the control information is
20 encoded by either or both (a) the number of finger presses and (b) the relative duration of the finger presses. If the successive finger presses are provided within this predetermined time, then the controller 107 accepts the presses as potential control information and checks the input information against a stored set of legal control signals.

One example of a legal control signal can be expressed as follows:

25 “Enrol an ordinary user” -> dit, dit, dit, dah

- 26 -

where “dit” is a finger press of one second’s duration (provided by the user 101 in response to the feedback provided by the Amber LED as described below), and “dah” is a finger press of two second’s duration.

In the event that a legitimate sequence of finger presses are not delivered within
5 the predetermined time, then the presses are considered not to be control information and merely to be presses intended to provide access to the controlled item 111. Legitimate control sequences are defined in Read Only Memory (ROM) in the controller 107.

The code entry module 103 has feedback signalling mechanisms 122,
implemented for example by a number of LEDs 122 and an audio transducer 124,
10 implemented by an audio transducer. The LEDs 122 and the audio transducer 124 are used by the controller to signal the state of the code entry module 103 to the user 101, and to direct the administration process. Thus, in one example, three LEDs, being Red, Amber and Green are provided.

When the Amber LED is flashing, it means “Press the sensor”. When the Amber
15 LED is steady ON, it means “Maintain finger pressure”. When the Amber LED is OFF, it means “Remove finger pressure”. When the arrangement 100 enters the enrolment state (depicted by the process 800 in **Fig. 8**), then the audio transducer 124 emits the “begin enrolment” signal (*dit dit dit dit*) and the Red LED flashes. Enrolment of a normal user (according to the step 807 in **Fig. 8**) is signalled by the OK audio signal (*dit dit*) and a
20 single blink of the Green LED.

Returning to the step 704, if the step determines that the biometric signal received is an administrator’s signal, then the process 700 is directed by a YES arrow to 706 in **Fig. 8** as depicted by the arrow 703. If on the other hand, the step 704 indicates that the received biometric signal does not belong to an administrator then the process
25 700 is directed by a NO arrow to 707 in **Fig. 7**.

- 27 -

Fig. 7 shows the access process 600 by which a biometric signal 102 (see **Fig. 2**) is processed in order to provide access to the controlled item 111, or to take other action. Entering the process at 707 from **Fig. 6**, the process 600 proceeds to a step 602 that compares the received biometric signal to biometric signatures stored in the database 105.

5 A following step 603 determines if the received signal falls into the “duress” category. Biometric signals in this category indicate that the user 101 is in a coercive situation where, for example, an armed criminal is forcing the user 101 to access the secure facility (such as a bank door). If the step 603 determines that the received biometric signal is in the duress class, then a following step 604 prepares a “duress” bit for incorporation into

10 the code access signal 108. The aforementioned duress bit is an access attribute of the biometric signal 102. Thereafter the process 600 proceeds to a step 605.

Modules used in the code entry module for producing the rolling code enable a number of user defined bits to be inserted into the access signal 108, and these bits may be used to effect desired control functions in the receiver sub-system 117. The disclosed

15 arrangement 100 utilises four such user bits, namely (a) to indicate that the user belongs to the duress category, (b) to indicate a “battery low” condition, or other desired system state or “telemetry” variable, for the code entry module 103, (c) to indicate that the biometric signal represents a legitimate user in which case the secure access to the controlled item 111 is to be granted, or (d) to indicate that the biometric signal is

20 unknown, in which case the controller 109 in the receiver sub-system 117 sounds an alert tone using a bell (not shown) or the like.

Returning to **Fig. 7**, if the step 603 determines that the biometric signal is not in the duress class, then the process 600 proceeds according to a NO arrow to the step 605. The step 605 determines if the code entry module 103 has a low battery condition, in

25 which event the process 600 proceeds according to a YES arrow to a step 606 that

- 28 -

prepares a telemetry bit for insertion into the access signal 108. The aforementioned telemetry bit is an access attribute of the biometric signal 102. Thereafter, the process proceeds to a step 607.

If the step 605 determines that telemetry signalling is not required, then the process 600 proceeds according to a NO arrow to the step 607. The step 607 checks the biometric signal against the biometric signatures in the database 105. If the received biometric signal matches a legitimate signature in the database 105, then the process 600 is directed to a step 608 that prepares an "access" bit for insertion into the access signal 108. This access bit directs the controller 109 in the receiver sub-system 117 to provide access to the controlled item 111. The aforementioned access bit is an access attribute of the biometric signal 102. The process 600 then proceeds to a step 610.

If the step 607 determines that the biometric input signal does not match any legitimate biometric signatures in the database 105, then the process 600 proceeds according to a NO arrow to a step 609 that prepares an "alert" bit for insertion into the access signal 108. The aforementioned alert bit is an access attribute of the biometric signal 102. This alert bit directs the controller 109 (a) not to provide access to the controlled item 111, and (b) to provide an alert tone, like ringing a chime or a bell (not shown), to alert personnel in the vicinity of the receiver sub-system 117 that an unauthorised user is attempting to gain access to the controlled item 111. The alert bit may also cause a camera mounted near the controlled item 111 to photograph the unauthorised user for later identification of that person. The camera may be activated if the person attempting to gain access is unauthorised, and also if the person attempting to gain access is authorised but uses a duress signature.

An optional additional step (not shown) may prepare an identification field for insertion into the access signal 108. This sends, to the receiver sub-system 117, ID

- 29 -

information that the receiver sub-system 117 may use to construct an audit trail listing which users, having signatures in the database 105, have been provided with access to the controlled item 111.

The process 600 is then directed to the step 610, where the controller/transmitter 107 checks, as depicted by an arrow 112 in **Fig. 2**, the current code in the database 113. Then at the next step 613, the controller/transmitter 107 generates a new code in the sequence of codes for the code entry module 103 according to the current Wiegand protocol identifier. At the next step 615, the newly generated code is encoded by the controller 107 using one of the encryption algorithms described above, with the encryption algorithm being customised through the application of the secret key and the current Wiegand protocol identifier. The Wiegand identifier is also encoded at step 204, using one of the encryption algorithms described above. In the subsequent step 617 the controller/transmitter 107 sends the appropriate access signal 108 to the receiver 109. The access signal 108 includes the encoded code and the current encoded Wiegand protocol identifier. Also, in the embodiment of Figs. 7 to 9, the access signal 108 also includes the various user defined bits. The process 200 is then directed in accordance with an arrow 611 to 705 of Fig. 6.

Fig. 8 shows a process 800 for implementing various enrolment procedures. The process 800 commences at 706 from **Fig. 6** after which a step 801 determines if the biometric signal is a first administrator's signal (which is the case if the database 105 is empty). If this is the case, then the process 800 is directed to a step 802 that stores a biometric signature, representing the received biometric signal, in the database 105. From a terminology perspective, this first administrator, or rather the first administrator's first finger (in the event that the biometric sensor 121 is a fingerprint sensor), is referred to as the "superfinger". Further administrator's fingers are referred to as admin-fingers, and

- 30 -

ordinary users fingers are referred to merely as “fingers”. The reason that someone would enrol more than one of their own fingers into the system is to ensure that even in the event that one of their enrolled fingers is injured, the person can still operate the system using another enrolled finger.

5 It is noted that the step 802, as well as the steps 805, 807 and 809 involve sequences of finger presses on the biometric sensor 121 in conjunction with feedback signals from the LEDs 122 and/or the audio speaker 124. The process 800 then proceeds to a step 810 that determines if further enrolment procedures are required. If this is the case, then the process 800 proceeds by a YES arrow back to the step 801. If no further
10 enrolment procedures are required, then the process 800 proceeds by a NO arrow to 705 in **Fig. 6**.

 Returning to the step 801, if the biometric signal is not a first administrator’s signal, then the process 800 proceeds by a NO arrow to a step 803. The step 803 determines if a further administrator signature is to be stored. It is noted that all signatures
15 stored in the database are tagged as belonging to one or more of the classes of administrator, ordinary user, and duress users. If a further administrator signature is to be stored, then the process 800 proceeds by a YES arrow to the step 802 that stores the biometric signal as a further administrator’s signature.

 If a further administrator’s signature is not required, then the process 800
20 proceeds according to a NO arrow to a step 804 that determines if a duress signature is to be stored. If this is the case then the process 800 follows a YES arrow to a step 805 that stores a duress signature. The process 800 then proceeds to the step 810. If however the step 804 determines that a duress signature is not required, then the process 800 proceeds by a NO arrow to step 806.

- 31 -

The step 806 determines if a further simple signature (i.e., belonging to an ordinary user) is to be stored. If a further simple signature is to be stored, then the process 800 proceeds by a YES arrow to the step 807 that stores a representation of the received biometric signal as a further ordinary signature.

5 If a further simple signature is not required, then the process 800 proceeds according to a NO arrow to a step 808 that determines if any or all signatures are to be erased from the database 105. The determination of whether all signatures are to be erased from the database 105 at step 808 may be made based on an “erase all” control (not shown) incorporated into the code entry module 103. If any or all signatures are to
10 be erased from the database 105 then the process 800 follows a YES arrow to a step 809 that erases the desired signatures.

 If all of the signatures in the database 115 are erased at step 809, the controller/transmitter 107 changes the current Wiegand protocol identifier to a previously unused value from the range of Wiegand protocol identifiers allocated to the code entry
15 module 103. If no previously unused values from the range of Wiegand protocol identifiers allocated to the code entry module 103 are available, then the code entry module 103 is completely non-functional and the process 800 concludes at step 809 and will not return to 705 of Fig. 6.

 If all of the signatures in the database 115 are erased at step 809, the database
20 115 will be determined to be empty at a subsequent execution of step 702 of the process 700. Further, the code entry module 103 will appear as completely new to the receiver 118 and any existing synchronisation between the code entry module 103 and the receiver 118 will be revoked. That is, the flag in the database 115 indicating that the receiver 118 and the code entry module 103 are “synchronised” will be reset to indicate that the code
25 entry module 103 and the receiver 118 are not synchronised. In the instance that

- 32 -

synchronisation is revoked as described above, the code entry module 103 and the receiver 118 may be synchronised provided the code entry module 103 can generate two consecutive “in sequence” codes or through physical operation of a switch mechanism as described above.

5 If the code entry module 103 is still functional (i.e., there are still unused values from the range of Wiegand protocol identifiers allocated to the code entry module 103) following step 809, then the process 800 then proceeds to the step 810.

Further, if the step 804 determines that no signatures are to be erased, then the process 800 proceeds by a NO arrow to the step 810.

10 **Fig. 9** shows another enrolment process relating to the example of **Fig. 6**. The process 900 commences at 706 from **Fig. 6** after which a step 901 determines if the received biometric signal comes from the first administrator. If this is the case, then the process 900 proceeds according to a YES arrow to a step 902. The step 902 emits an “Enrolment” tone and flashes the green LED once only. Thereafter, a step 905 reads the
15 incoming biometric signal which is provided by the user as directed by the Amber LED. When the Amber LED flashes continuously, this directs the user to “Apply Finger”. When the Amber LED is in a steady illuminated state, this directs the user to “Maintain Finger Pressure”. Finally, when the amber LED is off, this directs the user to “Remove Finger”.

20 Returning to the step 901, if the incoming biometric signal does not belong to the first administrator, then the process 900 proceeds according to a NO arrow to a step 903. The step 903 emits an “Enrolment” tone, and flashes the Red LED in an on-going fashion. Thereafter, the process 900 proceeds according to an arrow 904 to the step 905.

Following the step 905, a step 906 determines whether the incoming biometric
25 signal is legible. If this is not the case, then the process 900 proceeds according to a NO

- 33 -

arrow to a step 907. The step 907 emits a “Rejection” tone, after which the process 900 is directed, according to an arrow 908 to 705 in **Fig. 6**. Returning to the step 906, if the incoming biometric signal is legible, then the process 900 follows a YES arrow to a step 909. The step 909 determines whether the finger press exceeds a predetermined time. If this is not the case, then the process 900 follows a NO arrow to a step 910 which stores a representation of the biometric signal, which in the present case is stored as a fingerprint signature. Thereafter the process 900 follows an arrow 911 to 705 in **Fig. 6**.

Returning to the step 909 if the finger press does exceed the predetermined period, then the process follows a YES arrow to a step 912. The step 912 erases any or all relevant signatures depending upon the attributes of the incoming biometric signal. Thus, for example, if the incoming biometric signal belongs to an ordinary user, then the ordinary user’s signature in the database 105 is erased by the step 912. If, on the other hand, the incoming biometric signal belongs to the first administrator, then all the signatures in the database 105 are erased. Administrators who are not the first administrator may be granted either the same powers as the first administrator in regard to erasure of signatures, or can be granted the same powers as ordinary user in this respect.

Again, the determination of whether all signatures are to be erased from the database 105 at step 912 may be made based on an “erase all” control (not shown) incorporated into the code entry module 103. Further, if all of the signatures in the database 115 are erased at step 912, the controller/transmitter 107 changes the current Wiegand protocol identifier to a previously unused value from the range of Wiegand protocol identifiers allocated to the code entry module 103. If no previously unused values from the range of Wiegand protocol identifiers allocated to the code entry module 103 are available, then the code entry module 103 is completely non-functional and the process 900 concludes at step 912 and will not return to 705 of Fig. 6.

If the code entry module 103 is still functional (i.e., there are still unused values from the range of Microchip (Keeloq) serial numbers allocated to the code entry module 103) following step 912, then the process 900 follows an arrow 913 to 705 in **Fig. 6**.

Fig. 5 is a schematic block diagram of the arrangement 100 in **Fig. 2**. The disclosed secure access methods are preferably practiced using the arrangement 100 in the form of a computer system, such as that shown in **Fig. 5** wherein the processes of **Figs. 3-4** and **6-9** may be implemented as software, such as application program modules executing within the arrangement 100. In particular, the described method steps are effected by instructions in the software that are carried out under direction of the respective controller 107 and controller 109 (and receiver 118) in the transmitter and receiver sub-systems 116 and 117. The instructions may be formed as one or more code modules, each for performing one or more particular tasks. The software may also be divided into two separate parts, in which a first part performs the provision of secure access methods and a second part manages a user interface between the first part and the user. The software may be stored in a computer readable medium, including the storage devices described below, for example. The software is loaded into the transmitter and receiver sub-systems 116 and 117 from the computer readable medium, and then executed under direction of the respective controllers 107 and 109 (and receiver 118). A computer readable medium having such software or computer program recorded on it is a computer program product. The use of the computer program product in the computer preferably effects an advantageous apparatus for provision of secure access.

The following description is directed primarily to the transmitter sub-system 116, however the description applies in general to the operation of the receiver sub-system 117. The arrangement 100 is formed, having regard to the transmitter sub-system 116, by the controller module 107, input devices such as the button 121 (or biometric sensor in

- 35 -

the case of the further embodiment), output devices including the LED display 122 and the audio device 124. A communication interface/transceiver 1008 is used by the controller module 107 for communicating to and from a communications network 1020. Although **Fig. 2** shows the transmitter sub-system 116 communicating with the receiver sub-system 117 using a direct wireless link for the access signal 108, this link used by the access signal 108 can be effected over the network 1020 forming a tandem link comprising 108-1020-108'. The aforementioned communications capability may be used to effect communications between the transmitter sub-system 116 and the receiver sub-system 117 either directly or via the Internet, and other network systems, such as a Local Area Network (LAN) or a Wide Area Network (WAN).

The controller module 107 typically includes at least one processor unit 1005, and a memory unit 1006, for example formed from semiconductor random access memory (RAM) and read only memory (ROM). The controller module 107 also includes a number of input/output (I/O) interfaces including an audio-video interface 1007 that couples to the LED display 122 and audio speaker 124, an I/O interface 1013 for the button 121, and the interface 1008 for communications. The components 1007, 1008, 1005, 1013 and 1006 of the controller module 107 typically communicate via an interconnected bus 1004 and in a manner which results in a conventional mode of operation of the controller 107 known to those in the relevant art.

Typically, the application program modules for the transmitter sub-system 116 are resident in the memory 1006 iROM, and are read and controlled in their execution by the processor 1005. Intermediate storage of the program and any data fetched from the bio sensor 121 and the network 1020 may be accomplished using the RAM in the semiconductor memory 1006. In some instances, the application program modules may be supplied to the user encoded into the ROM in the memory 1006. Still further, the

- 36 -

software modules can also be loaded into the transmitter sub-system 116 from other computer readable media, say over the network 1020. The term "computer readable medium" as used herein refers to any storage or transmission medium that participates in providing instructions and/or data to the transmitter sub-system 116 for execution and/or processing. Examples of storage media include floppy disks, magnetic tape, CD-ROM, a hard disk drive, a ROM or integrated circuit, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the transmitter sub-system 116. Examples of transmission media include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

As described above, the code entry module 103 incorporating the biometric sensor 121 is allocated a range of Wiegand protocol identifiers. In still another arrangement, the code entry module 103 may comprise a plurality of buttons similar to the button 121 shown in Fig. 2. In this instance, each of these buttons may have a different Wiegand protocol identifier, with each Wiegand identifier having a unique sequence of codes. Accordingly, pressing different ones of the buttons will result in different codes being sent by the code entry module 103.

As described above, the encoded Wiegand protocol identifier is inserted into bits zero (0) to twenty three (23) of the normal Microchip (Keeloq) serial number address space for the code entry module 103. The remaining four bits (i.e., bits twenty four (24) to twenty seven (27)) of the Microchip (Keeloq) serial number are set to a predetermined fixed value (e.g., a series of '1's) indicating that the Microchip (Keeloq) serial number has been replaced by an encoded Wiegand protocol identifier. Alternatively, two or more of the remaining four bits may be used to indicate user groups. In this instance,

the code entry module 103 will only be accepted by the receiver 118 if the code entry module 103 and the receiver 118 are in the same user group. In one example, bits twenty six (26) and twenty seven (27) may be set to '1', while the remaining two bits (i.e., bits twenty four (24) and twenty five (25)) are set to a user group number.

Code entry modules may also be allocated to different user groups by using a different secret key, as described above, in each of the code entry modules. For example, one or more of the code entry modules may be allocated a particular secret key indicating one user group and one or more other code entry modules may be allocated a different secret key indicating a different user group.

10 **Industrial Applicability**

It is apparent from the above that the arrangements described are applicable to the security industry.

The foregoing describes only some embodiments of the present invention, and modifications and/or changes can be made thereto without departing from the scope and spirit of the invention, the embodiments being illustrative and not restrictive.

The arrangement 100 may also be used to provide authorised access to lighting systems, building control devices, exterior or remote devices such as air compressors and so on. The concept of “secure access” is thus extendible beyond mere access to restricted physical areas.

Claims

1. A system for providing secure access to a controlled item, the system comprising:
- 5 a transmitter subsystem:
- means for storing a Wiegand protocol identifier;
- means for receiving a request;
- means for generating a code from a sequence of codes based on the Wiegand identifier, upon receiving the request;
- 10 means for encoding the code and the Wiegand protocol identifier;
- and
- means for transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier; and
- a receiver sub-system comprising;
- 15 means for receiving the transmitted secure access signal; and
- means for providing conditional access to the controlled item dependent upon said code and said Wiegand protocol identifier.
2. A system according to claim 1, wherein the sequence of codes is unique to the
- 20 transmitter sub-system.
3. A system according to claim 1, wherein the Wiegand protocol identifier is unique to the transmitter sub-system and to the sequence of codes.

- 39 -

4. A system according to claim 1, wherein the Wiegand protocol identifier is unique to the transmitter sub-system.
5. A system according to claim 1, wherein the secure access signal is configured to indicate that the secure access signal comprises the Wiegand protocol identifier.
6. A system according to claim 1, wherein the code is encrypted using a key allocated to the transmitter sub-system.
- 10 7. A system according to claim 1, said receiver sub-system further comprising means for identifying the sequence of codes based on the Wiegand protocol identifier included in the received secure access signal.
8. A system according to claim 1, said receiver sub-system further comprising means for testing the code included in the received secure access signal to determine if the code is a next code in the sequence of codes.
- 15 9. A system according to claim 1, wherein said request is generated based on a button press.
- 20 10. A system according to claim 1, wherein said transmitter sub-system comprises a plurality of buttons.
11. A system according to claim 10, wherein each of said buttons has a different associated Wiegand protocol identifier.
- 25

12. A system according to claim 1, wherein said request is a biometric signal.
13. A system according to claim 12, further comprising a database comprising one or
5 more biometric signatures.
14. A system according to claim 13, wherein the transmitter sub-system further
comprises means for populating said database of biometric signatures.
- 10 15. A system according to claim 12, wherein a range of Wiegand protocol identifiers
are allocated to the transmitter sub-system.
16. A system according to claim 12, wherein a current Wiegand protocol identifier is
changed upon one or more of the biometric signatures in a database associated with the
15 system being erased.
17. A system according to claim 12, wherein the biometric signal is responsive based
on one of voice, retinal pattern, iris pattern, face pattern, and palm configuration.
- 20 18. A system according to claim 1, wherein the controlled item is one of:
a locking mechanism of a door; and
an electronic lock on a Personal Computer (PC).
19. A transmitter sub-system for operating in a system for providing secure access to
25 a controlled item, the system comprising a receiver sub-system comprising means for

- 41 -

receiving a secure access signal transmitted by the transmitter sub-system, and means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal, wherein the transmitter subsystem comprises:

means for storing a Wiegand protocol identifier;

5 means for receiving a request;

means for generating a code from a sequence of codes based on the Wiegand protocol identifier, upon receiving the request;

means for encoding the code and the Wiegand protocol identifier; and

10 means for transmitting said secure access signal comprising the code and the encoded Wiegand protocol identifier embedded therein.

20. A transmitter sub-system according to claim 19, wherein the sequence of codes is unique to the transmitter sub-system.

15 21. A transmitter sub-system according to claim 19, wherein the Wiegand protocol identifier is unique to the transmitter sub-system and to the sequence of codes.

22. A transmitter sub-system according to claim 19, wherein the Wiegand protocol identifier is unique to the transmitter sub-system.

20

23. A transmitter sub-system according to claim 19, wherein the secure access signal is configured to indicate that the secure access signal comprises the Wiegand protocol identifier.

- 42 -

24. A transmitter sub-system according to claim 19, wherein the code is encoded using a key allocated to the transmitter sub-system.

25. A transmitter sub-system according to claim 19, said receiver sub-system further
5 comprising means for identifying the sequence of codes based on the Wiegand protocol included in the received secure access signal.

26. A transmitter sub-system according to claim 19, said receiver sub-system further comprising means for testing the code included in the received secure access signal to
10 determine if the code is a next code in the sequence of codes.

27. A transmitter sub-system according to claim 19, wherein said request is generated based on a button press.

15 28. A transmitter sub-system according to claim 19, wherein said transmitter sub-system comprises a plurality of buttons.

29. A transmitter sub-system according to claim 28, wherein each of said buttons has a different associated Wiegand protocol identifier.

20

30. A transmitter sub-system according to claim 19, wherein said request is a biometric signal.

31. A transmitter sub-system according to claim 30, further comprising a database
25 comprising one or more biometric signatures.

32. A transmitter sub-system according to claim 31, wherein the transmitter sub-system further comprises means for populating said database of biometric signatures.

5 33. A transmitter sub-system according to claim 30, wherein a range of Wiegand protocol identifiers are allocated to the transmitter sub-system.

34. A transmitter sub-system according to claim 33, wherein a current Wiegand protocol identifier is changed upon one or more of the biometric signatures in a database
10 associated with the system being erased.

35. A transmitter sub-system according to claim 30, wherein the biometric signal is responsive based on one of voice, retinal pattern, iris pattern, face pattern, and palm configuration.

15

36. A transmitter sub-system according to claim 19, wherein the controlled item is one of:

a locking mechanism of a door; and

an electronic lock on a Personal Computer (PC).

20

37. A receiver sub-system for operating in a system for providing secure access to a controlled item, the system comprising transmitter subsystem comprising means for storing a Wiegand protocol identifier, means for receiving a request, means for generating a code from a sequence of codes based on said Wiegand identifier, upon receiving the
25 request, means for encoding the code and the Wiegand identifier, and means for

- 44 -

transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier, wherein the receiver sub-system comprises:

means for receiving the transmitted secure access signal comprising the code and the encoded Wiegand protocol identifier; and

5 means for providing conditional access to the controlled item dependent upon said code and said Wiegand protocol identifier.

38. A method for providing secure access to a controlled item, the method comprising the steps of:

10 receiving a request;

generating a code from a sequence of codes based on a Wiegand identifier, upon receiving the request;

encoding the code and the Wiegand protocol identifier;

15 transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier to a controller of said controlled item; and

providing conditional access to the controlled item dependent upon said code and said Wiegand identifier.

39. A computer program product having a computer readable medium having a
20 computer program recorded therein for directing a processor to provide secure access to a controlled item, said computer program product comprising:

code for receiving a request;

code for generating a code from a sequence of codes based on a Wiegand identifier, upon receiving the request;

25 code for encoding the code and the Wiegand protocol identifier;

- 45 -

code for transmitting a secure access signal comprising the code and the Wiegand encoded protocol identifier to a controller of said controlled item, wherein said controller provides conditional access to the controlled item dependent upon said code and said Wiegand identifier.

5

40. A computer program product having a computer readable medium having a computer program recorded therein for directing a processor to transmit a secure access signal in a system for providing secure access to a controlled item, said computer program product comprising:

10 code for receiving a request;

code for generating a code from a sequence of codes based on a Wiegand identifier, upon receiving the request;

code for encoding the code and the Wiegand protocol identifier; and

code for transmitting said secure access signal comprising the code and the encoded Wiegand protocol identifier to a controller of said controlled item, wherein said controller provides conditional access to the controlled item dependent upon said code and said Wiegand identifier.

41. A method of enrolling a biometric signature into a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising means for storing a Wiegand protocol identifier, means for receiving a request, means for generating a code from a sequence of codes based on the Wiegand identifier, means for encoding the code and the Wiegand protocol identifier, and means for transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier,

25

- 46 -

and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon said code and said Wiegand protocol identifier, said method comprising the steps of:

receiving a biometric signal; and

5 storing a biometric signature in the database, as a representation of the biometric signal, if the database of biometric signatures is empty; and

classifying the stored biometric signature as an administrator, thereby enrolling the received biometric signature.

10 42. A method according to claim 41, wherein:

if the database of biometric signatures is not empty, and if a predefined succession of finger presses to the biometric sensor are made, the method comprises a further step of:

enrolling one of a further administrator and an ordinary user.

15

43. An apparatus for enrolling a biometric signature into a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising means for storing a Wiegand protocol identifier, means for receiving a request, means for
20 generating a code from a sequence of codes based on the Wiegand identifier, means for encoding the code and the Wiegand protocol identifier, and means for transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon
25 said code and said Wiegand protocol identifier, said apparatus comprising:

- 47 -

receiving means for receiving a biometric signal; and

storage means for storing the biometric signature in the database, as a representation of the biometric signal, if the database of biometric signatures is empty; and

5 classification means for classifying the stored biometric signature as an administrator, thereby enrolling the received biometric signature.

44. A computer program product having a computer readable medium having a computer program recorded therein for enrolling a biometric signature into a database of
10 biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising means for storing a Wiegand protocol identifier, means for receiving a request, means for generating a code from a sequence of codes based on the Wiegand identifier, means for encoding the code and the Wiegand protocol identifier, and means
15 for transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon said code and said Wiegand protocol identifier, said program comprising:

20 code for receiving a biometric signal representing a biometric signature; and
 code for storing the biometric signature in the database, as a representation of the biometric signal, if the database of biometric signatures is empty; and
 code for classifying the stored biometric signature as an administrator, thereby enrolling the received biometric signature.

25

400

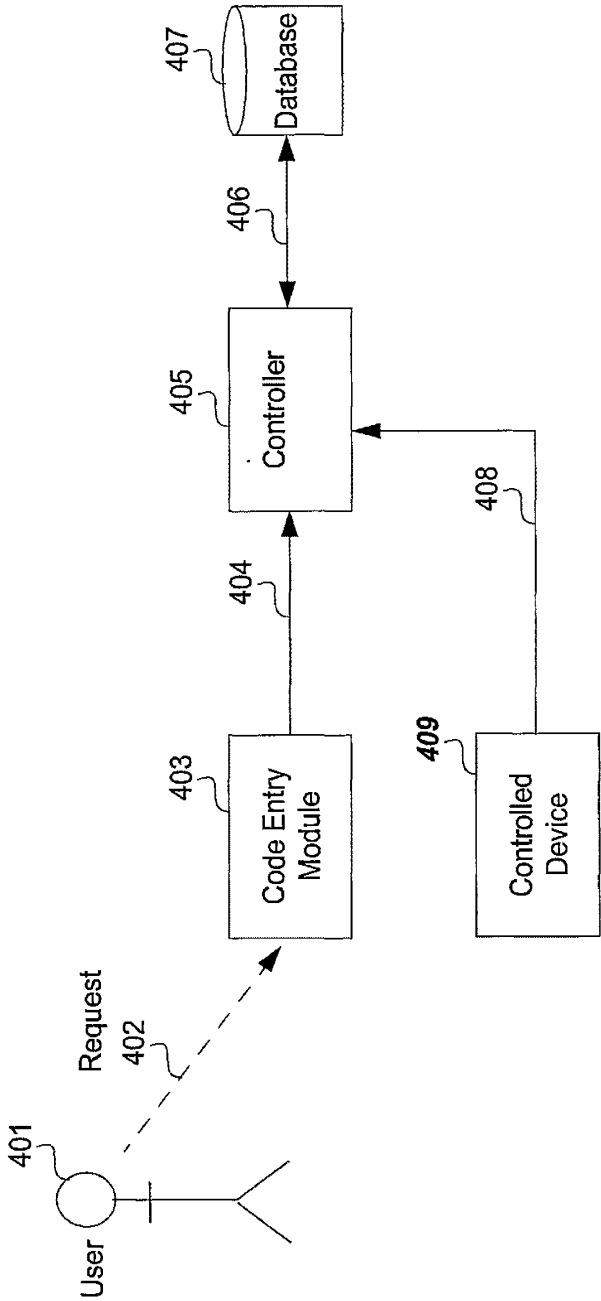


Fig. 1
(prior art)

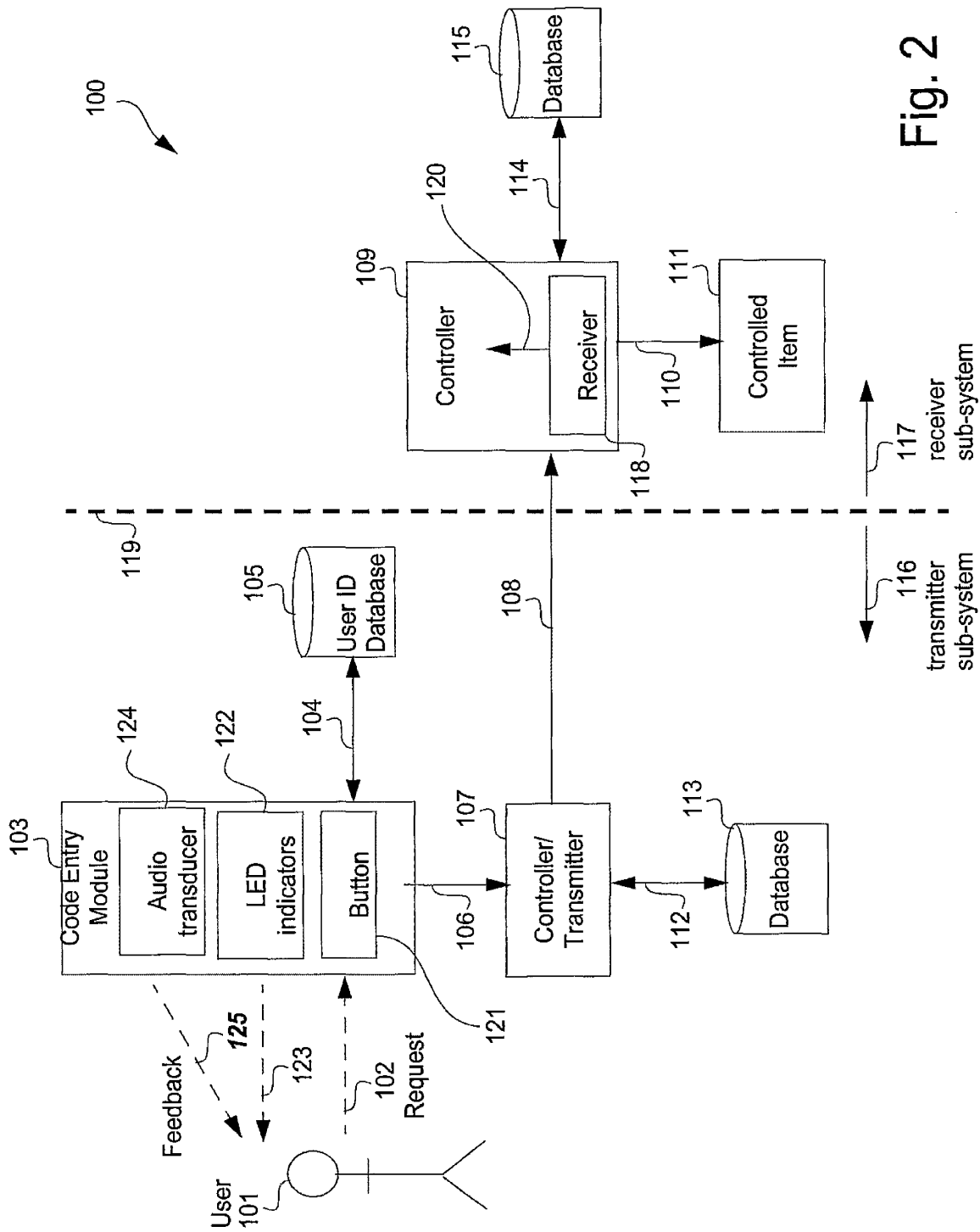


Fig. 2

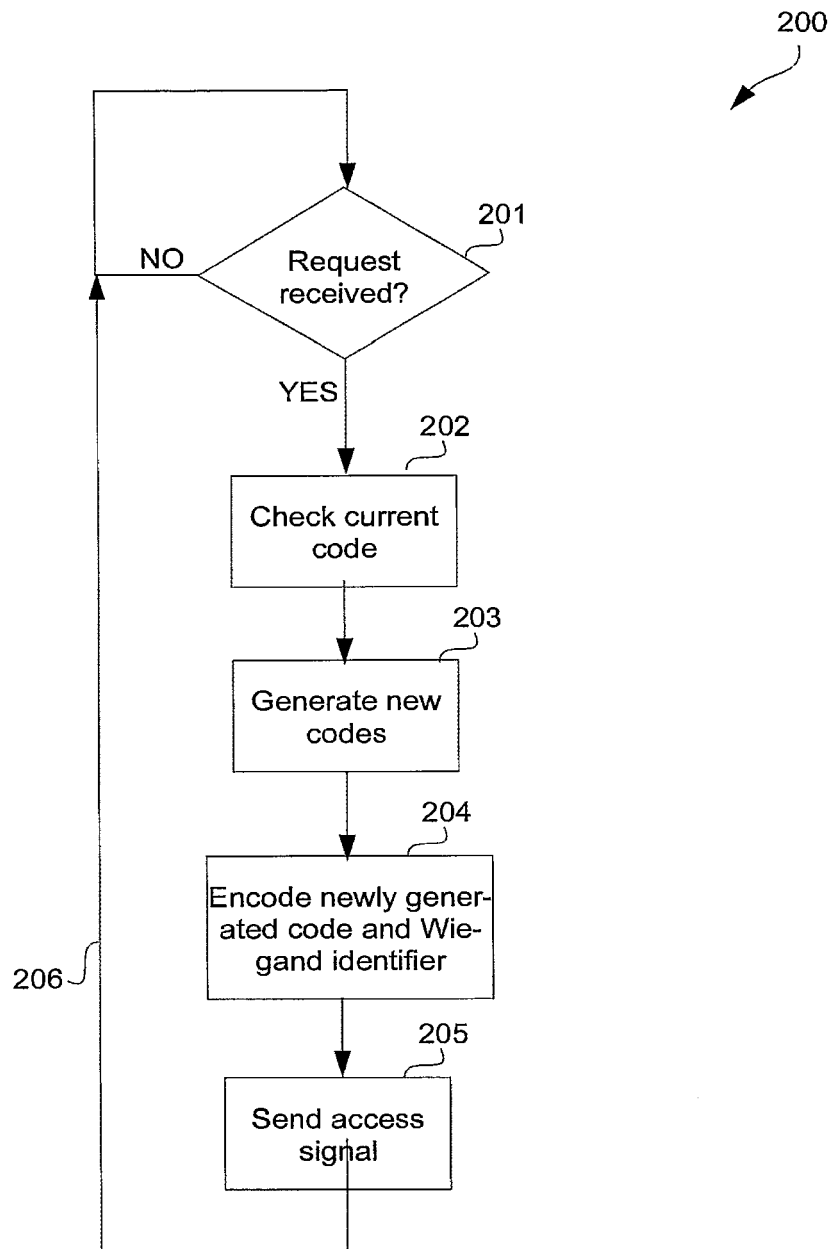
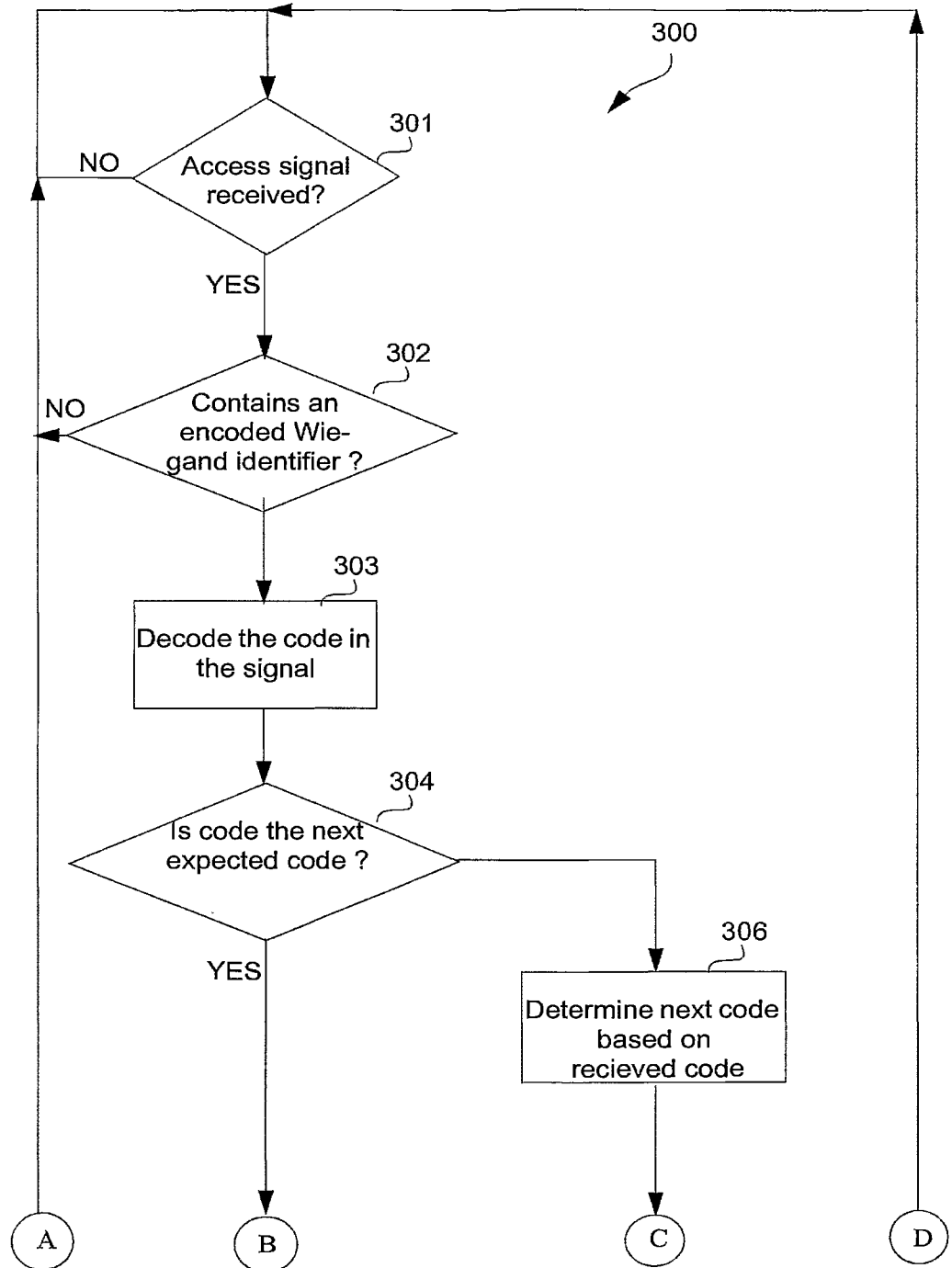


Fig. 3



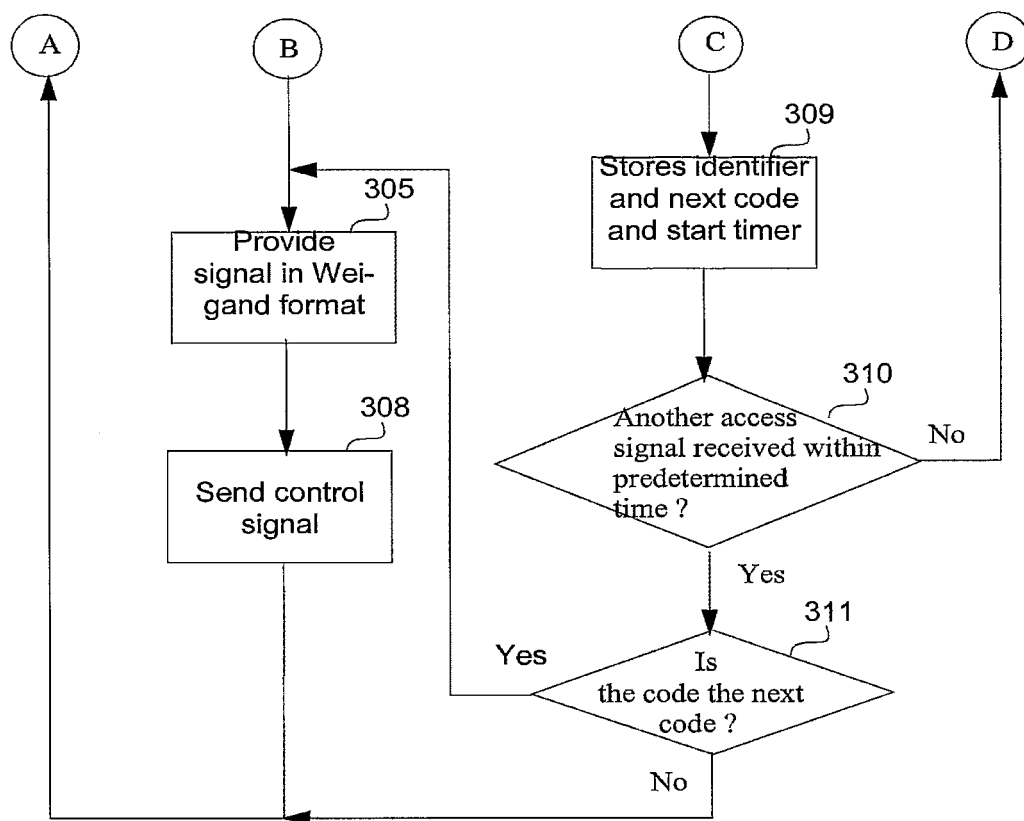


Fig. 4[A:B]

6/11

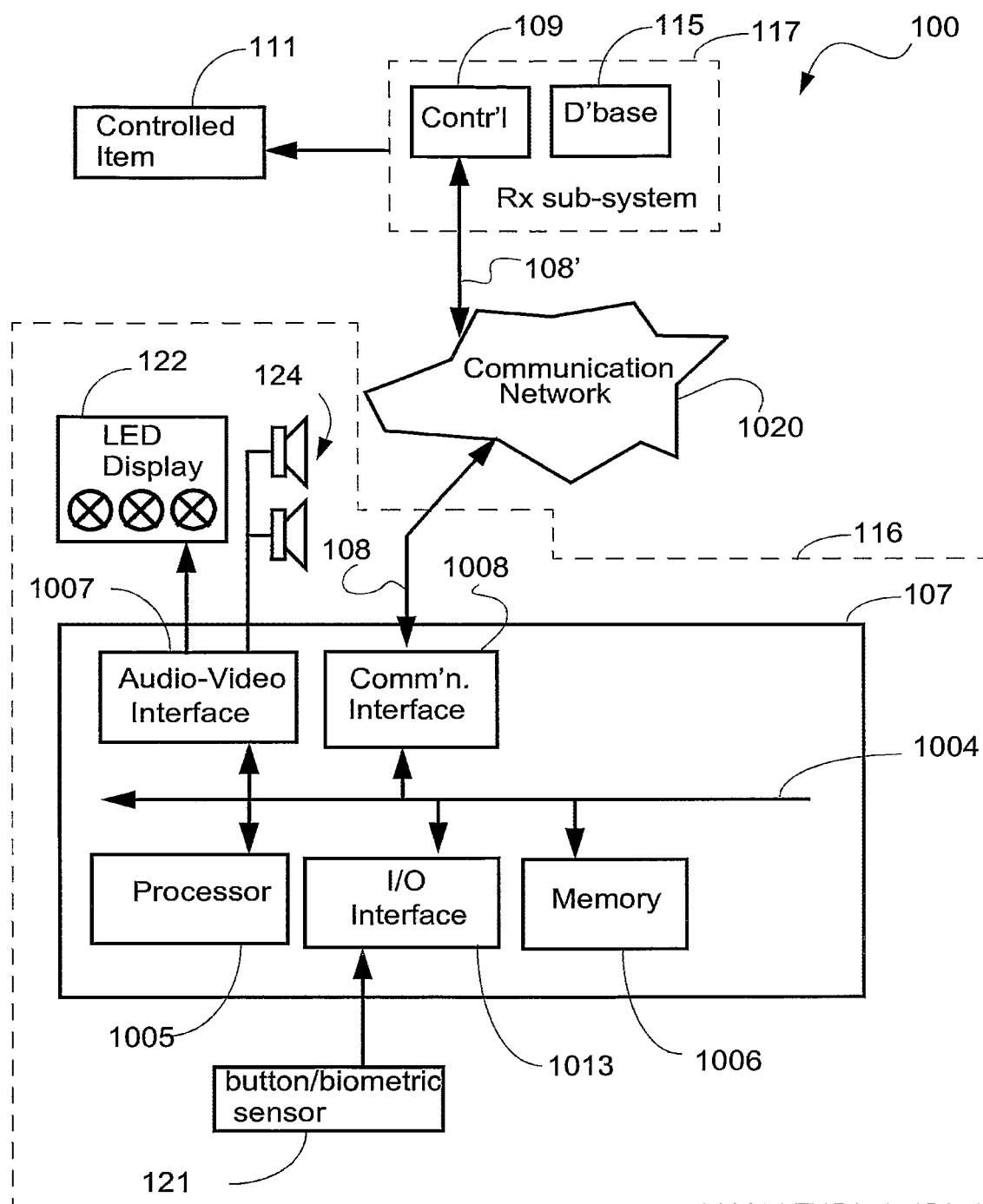


Fig. 5

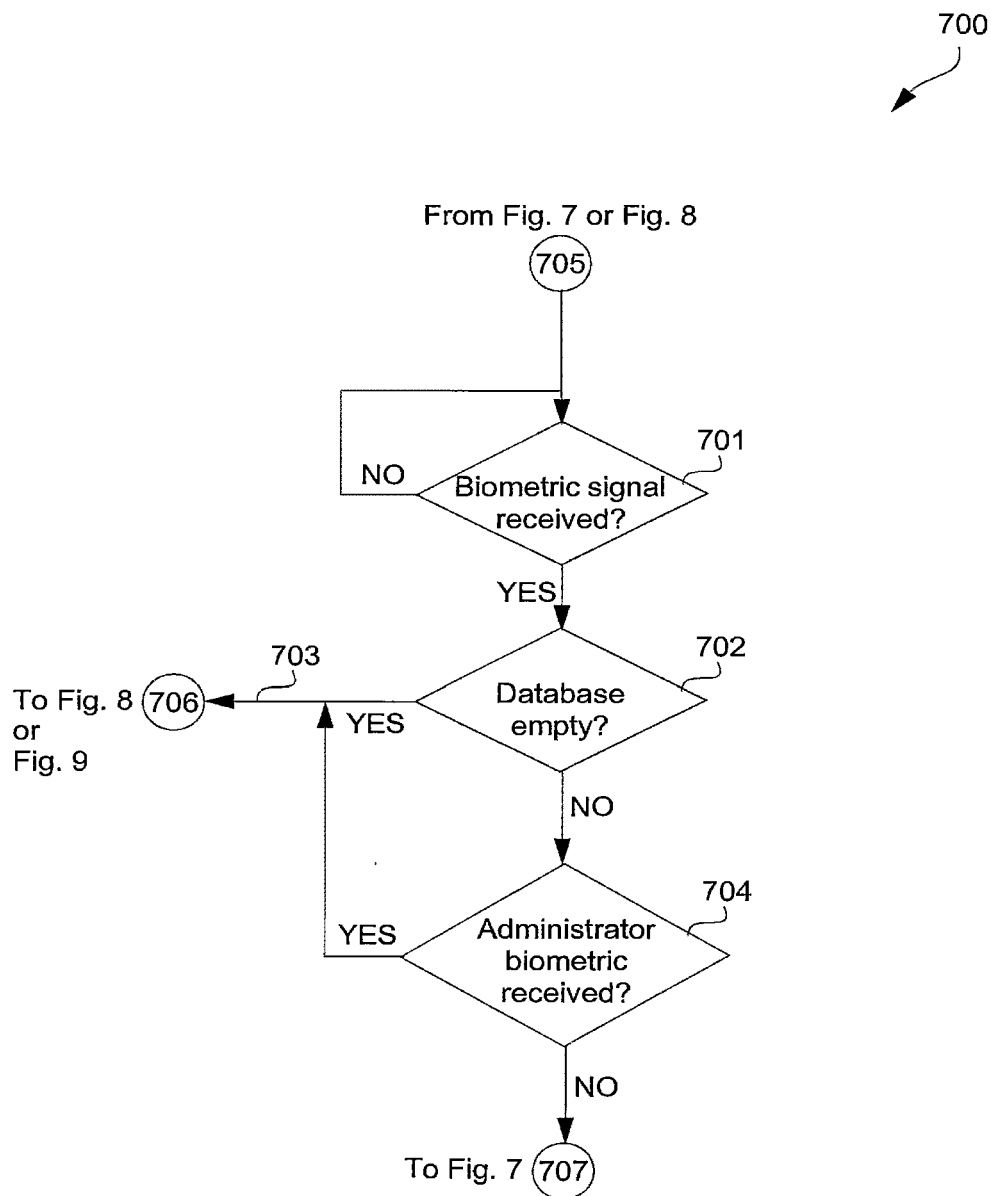
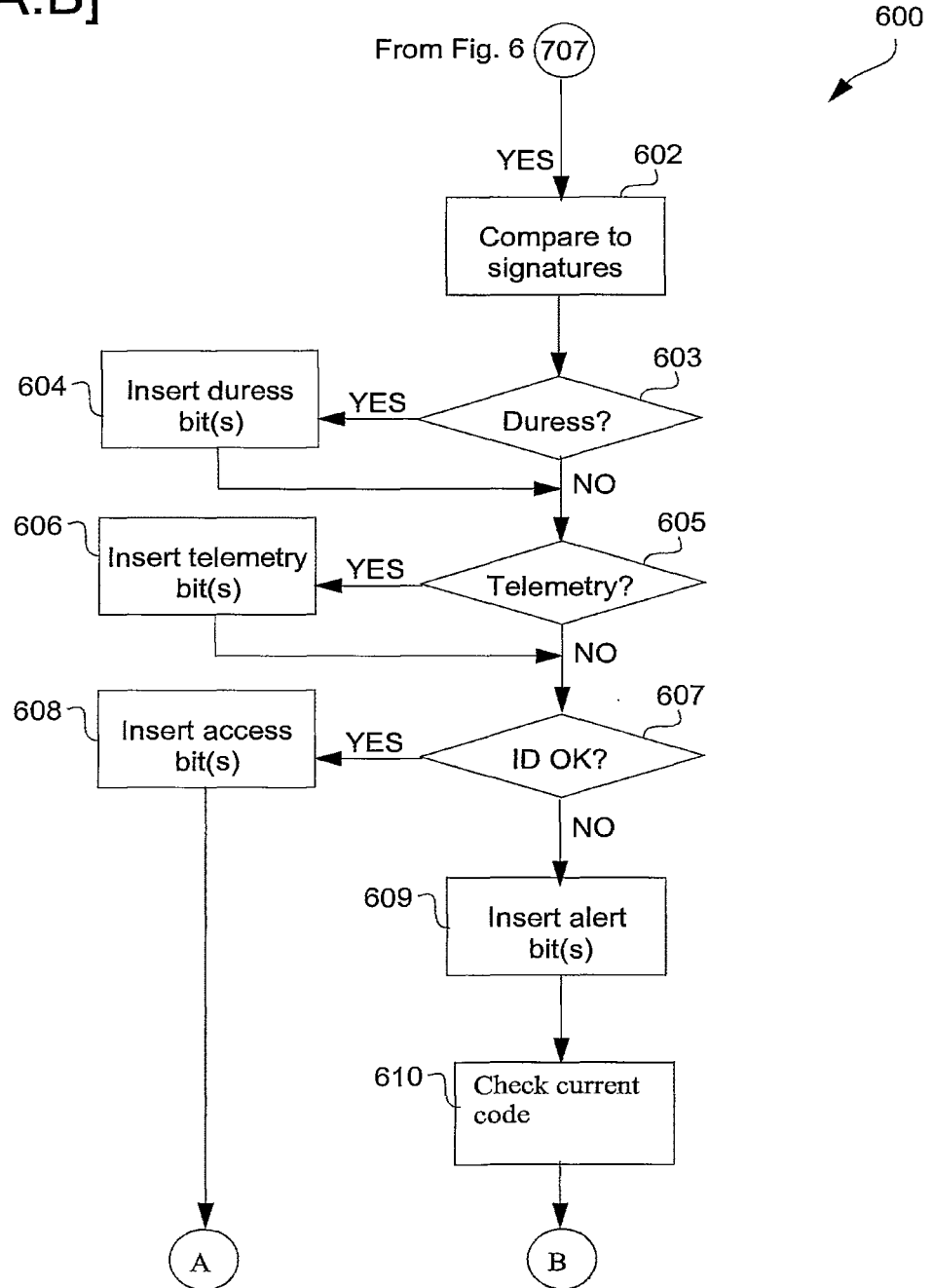


Fig. 6

Fig. 7[A:B]



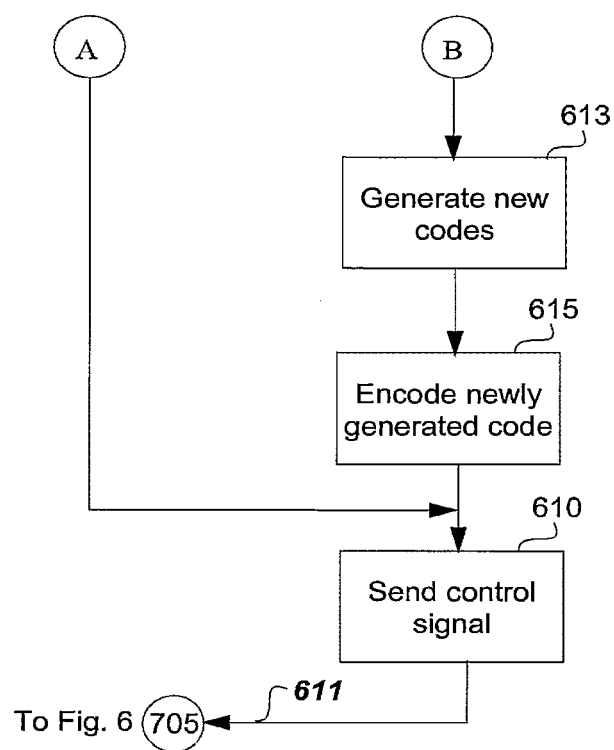


Fig. 7[A:B]

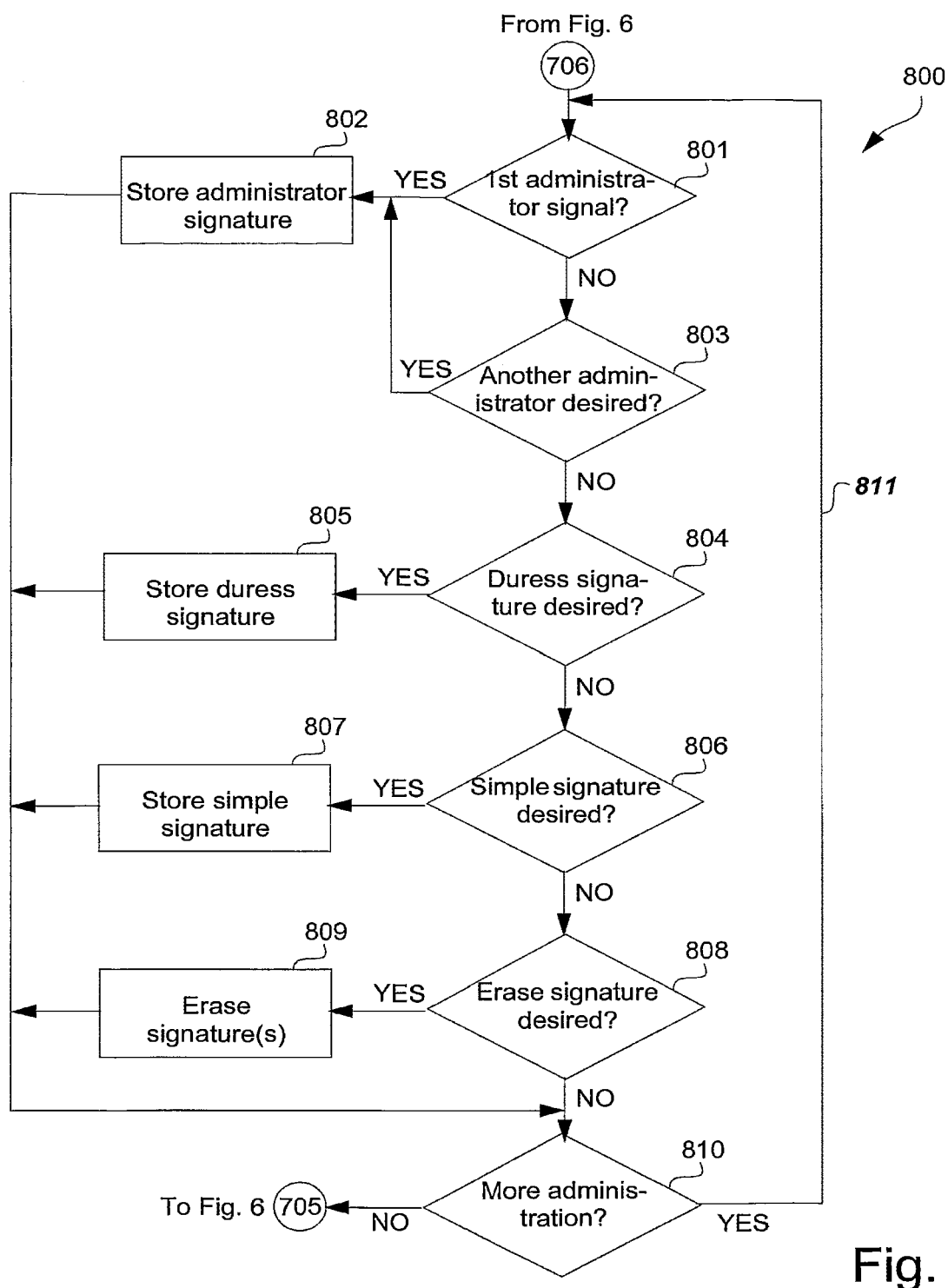


Fig. 8

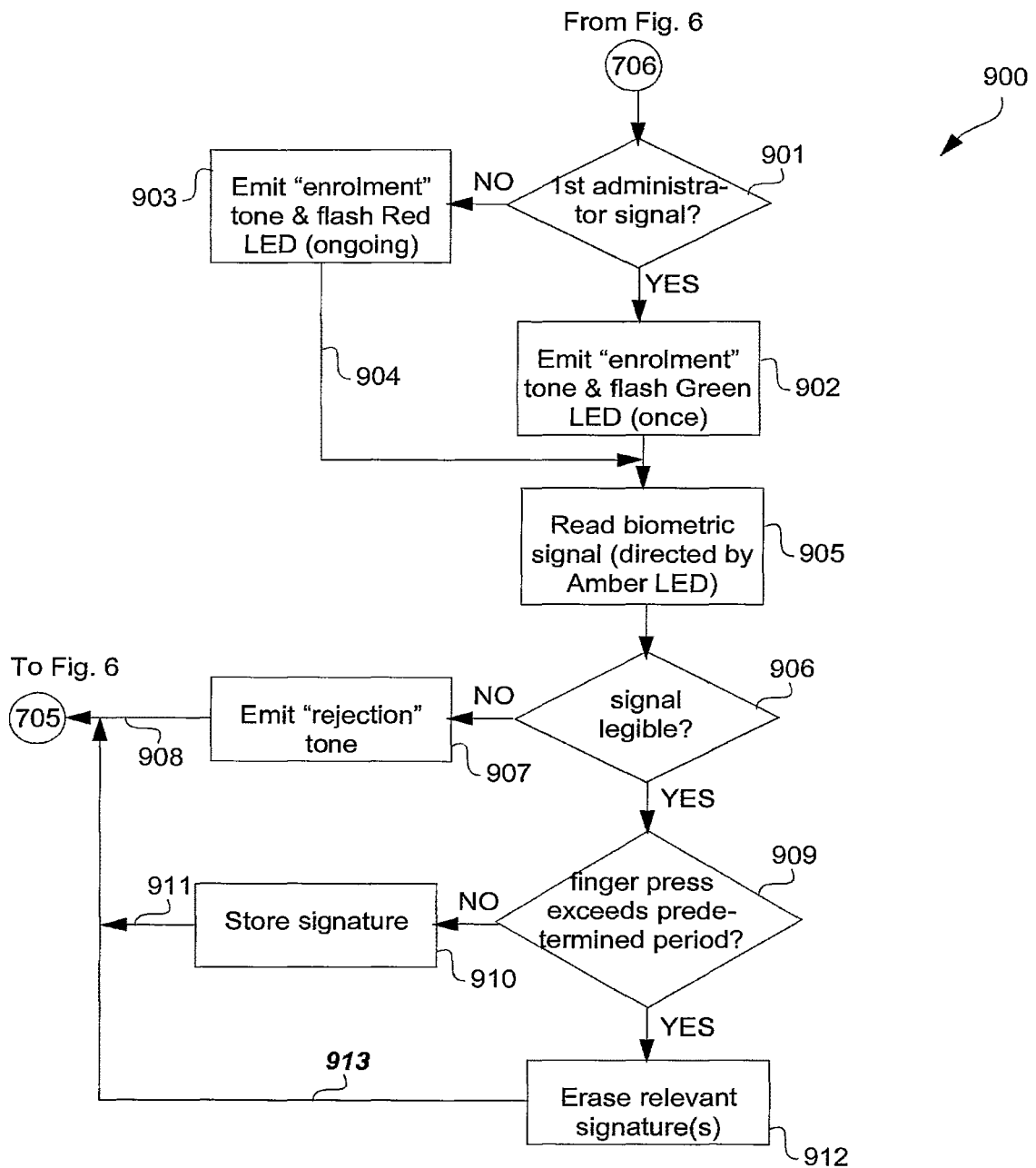


Fig. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2007/000311

A. CLASSIFICATION OF SUBJECT MATTER		
Int. Cl.		
H04L 9/32 (2006.01)		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols)		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPOQUE Internal : TEXTE (access, code, fixed, rolling, Wiegand, Kceloq and like terms)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2005/018137 A1 (SECURICOM (NSW) PTY LTD) 24 February 2005 Abstract, page 2 lines 13-18, page 16 line 18 to page 17 line 24, claim 41, figures	1-40
Y	WO 2004/039119 A1 (ANZON AUTODOOR LIMITED) 6 May 2004 Abstract, figure 2, claims 7-9	1-40
Y	US 6484260 B1 (SCOTT et al.) 19 November 2002 Abstract, column 3 lines 4-19, column 9 lines 38-53, claims	1-40
Y	US 6154544 (FARRIS et al.) 28 November 2000 Abstract, column 2 line 65 to column 3 line 27, claims	1-40
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C <input checked="" type="checkbox"/> See patent family annex		
* Special categories of cited documents:		
"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention	
"E" earlier application or patent but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone	
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art	
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family	
"P" document published prior to the international filing date but later than the priority date claimed		
Date of the actual completion of the international search 04 May 2007	Date of mailing of the international search report - 9 MAY 2007	
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustalia.gov.au Facsimile No. (02) 6285 3929	Authorized officer DALE SIVER AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : (02) 6283 2196	

INTERNATIONAL SEARCH REPORT

International application No.

PCT/AU2007/000311

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6882729 B2 (ARLING et al.) 19 April 2005 Column 7 line 1 to column 8 line 67, claim 51	1-40
Y	US 2002/0034303 A1 (FARRIS et al.) 21 March 2002 Whole document, especially paragraphs 10,11,37,38, claims	1-40
P,X	AU 2006203768 A1 (ASSA ABLOY IDENTIFICATION TECH. GROUP AB) Published 15 March 2007, Priority 31 August 2005	1,19,37,40
Y	US 6956460 B2 (TSUI) 18 October 2005 Whole document	1-40
Y	US 6956495 B2 (KLEIN et al.) 18 October 2005 Abstract, column 1 line 60 to column 2 line 23, column 5 lines 12-62	1-40
A	US 2005/0195066 A1 (VANDRUNEN et al.) 8 September 2005 Abstract, paragraphs 9,26,34,35	1
A	US 6026165 (MARINO et al.) 15 February 2000 Abstract, figure 3	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/AU2007/000311

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member			
WO	2005018137	AU	2004301168	CA	2535434
		EP	1661298	CN	1836399
WO	2004039119	AU	2003267878		
US	6484260	AU	37610/99	GB	2353386
US	6154544	AU	59213/96	WO	9956429
		CA	2193846	BR	9606663
		EP	0771498	CA	2493715
		US	6810123	US	6690796
		US	2002191794	US	2002034303
		US	2004243813	US	2004066936
		WO	2004017167	WO	9637063
US	6882729	AU	2003259786	CA	2503660
		US	2004117632	EP	1579626
		AU	59213/96	US	2004056034
		CA	2193846	AU	2003265424
		EP	0771498	BR	9606663
		US	6690796	CA	2493715
		US	2002034303	GB	2407901
		US	2004066936	US	6154544
		WO	9637063	US	6980655
				US	2002191794
				US	2003118187
				US	2004243813
				US	2006109978
				WO	2004017167
AU	2006203768	CA	2556843	EP	1760985
US	6956460	AU	2003235585	US	2007046424
		US	2003193448	CA	2507869
US	6956495	US	2002175827	US	2003189530
US	2005195066	AU	2005222330	WO	03060850
		US	7193502	CA	2558398
US	6026165	US	6167137	EP	1725994
				WO	2005088562
Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.					
END OF ANNEX					

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
17 October 2002 (17.10.2002)

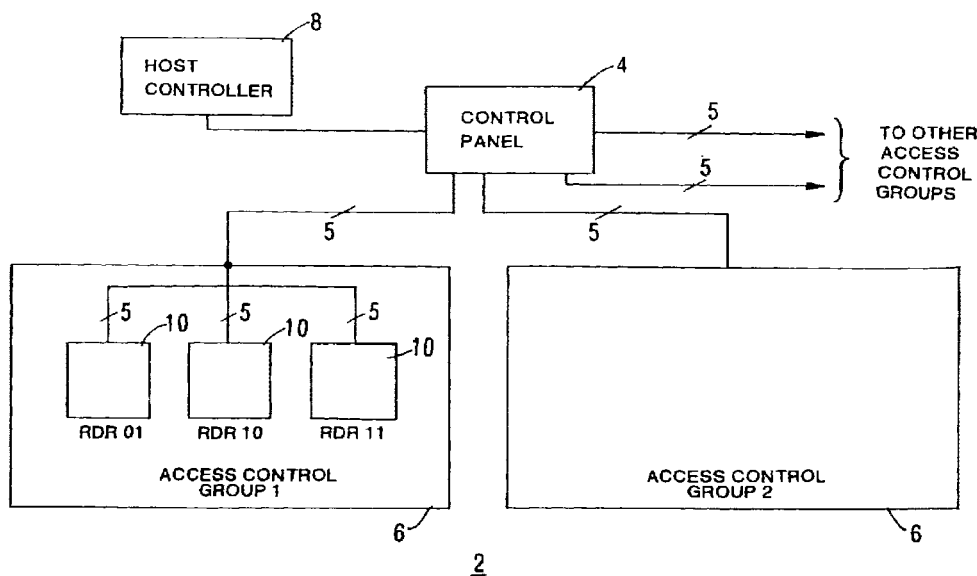
PCT

(10) International Publication Number
WO 02/082367 A1

- (51) International Patent Classification⁷: G06K 19/06, 7/10 (74) Agent: BARKUME, Anthony, R.; 20 Gateway Lane, Manorville, NY 11949 (US).
- (21) International Application Number: PCT/US02/10554 (81) Designated States (*national*): AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CO, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (22) International Filing Date: 6 April 2002 (06.04.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 09/828,395 6 April 2001 (06.04.2001) US (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- (71) Applicant (*for all designated States except US*): PITTWAY CORPORATION [US/US]; 200 South Wacker Drive, Suite 700, Chicago, IL 60606 (US).
- (72) Inventors: DAVIS, Michael [US/US]; 12 Hummingbird Lane, Amherst, NY 14228 (US). HULUSI, Tam [US/US]; 16 Harborview Drive, Northport, NY 11768 (US).
- Published:
— with international search report
before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

[Continued on next page]

(54) Title: SYSTEM AND METHOD OF EXTENDING COMMUNICATIONS WITH THE WIEGAND PROTOCOL



(57) Abstract: An extension of the industry standard Wiegand protocol (2) for enabling two way extended communication, enhanced error detection, encryption, multiple reader capability, and enhanced information regarding the embedded data stream between a Wiegand device such as a card reader (10) and a control panel (4) on the existing 5-wire bus structure without requiring the modification to the existing infrastructure.

WO 02/082367 A1



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD OF EXTENDING COMMUNICATIONS WITH THE
WEIGAND PROTOCOL

TECHNICAL FIELD

This application relates to access control systems, and in particular to a system and method for utilizing an existing Wiegand infrastructure to support readers and panels with extended data communications functionality.

BACKGROUND ART

Access control systems are used for controlling automated access to protected premises, typically through doorways, without requiring in-person security personnel. Typically, a device such as a card reader is positioned near a doorway of a secure area such as a computer room. A person desiring to enter the secure area must present to the reader a card having user data that can be read by the reader. The reader will transmit the user data via a hardwired bus to a control system typically consisting of numerous control panels ultimately connected back to a host computer, which will decide based on certain rules if that person should be allowed to enter the premises at that door. For example, the host computer may be programmed to let certain users in at only certain times of the day, such as normal working hours, or it may be programmed to allow certain users in at all times, or it may be programmed to disallow entry to certain users. If the host computer determines that access should be allowed, it will send a command that will, for example, activate a relay that will open a door strike mechanism, thusly allowing entry by the user that presented the card.

One technology in prevalent use for many years is the Wiegand protocol, which utilizes five wires to communicate data and provide power to a dedicated card reader as well known in the art. The five wires are for power, ground, DATA0, DATA1, and LEDCTL. The DATA1 line is a reader output that delivers pulses that are interpreted as binary ones. The DATA0 line is a reader output that delivers pulses that are interpreted as binary zeros. The LEDCTL line is the panel output that determines the state of the LED contained on the reader (off, red, green, or amber). The Wiegand standard protocol well known in the art and is described in detail in "Access Control Standard Protocol for the 26-Bit Wiegand Reader Interface," by the Security Industry Association. The data bits of the transmission from the reader to the panel typically consists of one or more parity bits and numerous data bits, as described in the aforementioned standard. The definition of the data bits are left to the system designer. For example, one data format uses the first 8 bits as a site code (0-255), and the next 16 bits as the card number (0-65,535).

Certain problems exist with the Wiegand protocol, however. For example, the Wiegand protocol is a one-way protocol, since the reader can send data to the panel but the panel cannot send any data to the reader except to control the door mechanism and a status LED. The ability to detect errors is weak because most Wiegand formats only include a leading and trailing parity bit, and wire runs up to 500 feet in an electrically noisy area enhances the possibility of a data transmission error. Further, if the panel detects a data transmission error, there is no way at the present time for it to signal the error detection back to the reader (to obtain a retransmission). The reader has no method of signaling additional information except the

ability to control the reader LED. Moreover, there is no way to attach multiple Wiegand readers in a party-line connection scheme and determine which reader generated the data. Finally, there exists no security (such as encryption) between the reader and the panel.

It is therefore an object of the invention to provide a methodology and system for extending the functionality of the Wiegand protocol such that improved readers and panels may be implemented, without requiring rewiring of the existing Wiegand infrastructure in use today.

It is a further object of the invention to provide such a methodology and system for extending the Wiegand protocol while still allowing prior art Wiegand readers to communicate with the panel, such that existing system can be upgraded with certain readers while still allowing existing readers to function in their original manner.

It is a further object of the invention to provide such a methodology and system for extending the Wiegand protocol that will allow improved functionality in the reader such that the user can provide different types of data inputs to the panel.

DISCLOSURE OF THE INVENTION

Thus, provided is an improvement on the existing Wiegand system, wherein the first major difference is that additional bits are appended to the data stream, which provide supplementary information from the reader (which may or may not be related to a card read) as well as a CRC or other type of error detection and/or correction bits covering all of the data in the transmission. A second

major improvement is that the LEDCTL line controlled by the panel is now used to transmit data back to the reader.

As a result of this invention, described herein, no additional wires are required to be connected between the panel and the reader, thus preserving the existing Wiegand infrastructure while providing increased functionality. The panel computer will require no changes to its interface (or other) hardware; only the firmware needs to be modified in accordance with the invention. Messages can be customized by users in accordance with the extended protocol set forth herein.

The Wiegand extension can be turned on or off, so that if a panel does not support the extension, it is not used and the reader behaves as an existing prior art device.

Thus, in accordance with the present invention, provided is an access control security system including a control panel and a plurality of access control groups. Each access control group is interconnected to the control panel on an independent multi-wire Wiegand data bus. Each access control group includes at least one access interface unit that has data output means for transmitting data onto the data bus to the control panel, data input means for receiving data via the data bus from the control panel, and processing means. The processing means interoperates with the data output means and the data input means, and operates data transfers over the data bus. In particular, the processing means is adapted to generate a data message for transmission onto the data bus via the data output means, wherein the data message has a Wiegand message field in accordance with the existing Wiegand protocol, as well as an extended data field. The extended data field can include a

status information field indicative of a status condition of the access interface unit. Data transfers are made to the control panel using the electrical and information content of the Wiegand protocol via the Data "0" and Data "1" output signals. Data transfers are made by the control panel using the electrical characteristics of the Wiegand protocol via the LEDCTL input signal as a serial protocol.

The access interface unit further includes user ID reading means for reading an ID device. For example, the ID reading means may be configured to read an access control card, a data transponder, a data-carrying key fob, or biometric data from a user. The processing means interoperates with the ID reading means, and the extended data field includes an information field indicative of a property of an ID read by the ID reading means.

In the system of the present invention, an access control group may include more than one access interface units, in which case the extended data field then includes address information uniquely identifying each access interface unit in an access control group.

The processing means may be adapted to utilize an error detection algorithm such as a CRC as a function of data contained within the extended data field.

The access interface unit may further include user input means (such as pushbutton) for accepting user input functions (such as a door bell), and the status condition of the access interface unit may indicate a function input by a user via the user input means.

The access interface unit may also include external status input means for accepting external status data from an external device coupled thereto, and the status information field of the extended data field then will include the external status data. For example, the external device may be adapted to measure temperature, in which case the external status data is the measured temperature. The external device may also be adapted to detect a change in light incident thereon, or it may be adapted to detect physical tampering with the access interface unit.

The processing means may be further adapted to generate supervision data on a periodic basis, and the status information field could then include the supervision data.

BRIEF DESCRIPTION OF THE DRAWING

Fig. 1 is a block diagram of the system of the preferred embodiment.

Fig. 2 is an illustration of the extended Wiegand data protocol of the present invention.

Fig. 3 is a block diagram of the Wiegand reader of the preferred embodiment.

BEST MODE FOR CARRYING OUT THE INVENTION

Figure 1 illustrates a system block diagram of the preferred embodiment of the present invention. The access control system 2 includes a control panel 4 which is used to communicate via several 5-wire buses to various access control groups 6. A host controller 8 provides master data processing and control for one or more control panels 4 as illustrated. Thus, depending on the topology and layout of a building or campus under control, the system 2 can be

adapted via various combinations of control panels 4 and access control groups 6.

Each access control group 6 contains up to three access interface units (card readers) 10, as shown in access control group 1 in Figure 1. Since two address bits are used in the extended protocol described herein, four different addresses are possible. Address 00 is reserved for a broadcast message in the preferred embodiment, so addresses 01, 10 and 11 are useable for discrete readers 10. In the prior art, each 5-wire bus could only communicate with one such card reader 10 since addressing was not possible under the standard Wiegand protocol. Multiple card readers tied to the same 5-wire bus are useful, for example, in situations where it is desired to place one reader on one side of a door and another reader on the other side of the door, thus controlling access in both directions with the same 5-wire interface.

A block diagram of each access interface unit (card reader) 10 is shown in Figure 3. A Wiegand transmitter 12, Wiegand receiver 14, and power supply circuit 16 are all shown; these operate functionally the same as in prior art Wiegand devices well known in the art. The transmitter 12 and receiver 14 are connected to the DATA1, DATA0, and LEDCTL wires of the standard Wiegand interface as known in the art. Also shown in Figure 3 is an RF transmitter/receiver 26, which is known in the art and which is used for reading an access control card when presented thereto.

A tamper and temperature sensing interface 18 is shown in Figure 3, which allows connection of the reader 10 to external tamper and temperature sensing devices. By

using a temperature sensor, temperature data may be transmitted back to the control panel 4 with the extended data field. Likewise, by using a tamper sensor, an alarm may be sent to the control panel in the event that someone attempts to alter or destroy the reader 10, and such activity is sensed by the tamper sensor. These types of sensors are well known in the art and need not be described in detail herein.

Also provided is a button/switch interface 20, which is connected to one or more buttons and/or switches that may reside on the housing of the reader 10. These buttons can be programmed to indicate virtually anything that may be desired by the system designer; for example a doorbell function described further below is easily attained by using a doorbell button with the extended protocol. This allows a person without an access card (e.g. a building visitor) to signal that he desires attention at the reader 10 by simply pressing the doorbell button. The doorbell status would be transmitted to the control panel without requiring the use of additional wires as in the prior art.

Also shown in Figure 3 is LED control block 22, which is used to drive one or more LEDs associated with the reader 10. While the prior art Wiegand systems relied on the LEDCTL wire for this function, the extended protocol allows more data to be communicated to the reader 10, thus providing more sophisticated LED (or other) outputs as desired.

Processor 24 is used to read data from the external sources, formulate data to be transferred over the 5-wire interface, and run all other functions that may be required by the reader 10 of the present invention.

In the preferred embodiment, the extended Wiegand protocol adds an additional 18 bits to the prior art (basic) Wiegand data transmission, although of course any amount of extension bits could be added as desired. The first two bits are used for address data to determine which Wiegand reader (also referred to as a Wiegand generator or an access interface unit) generated the data in a party-line configuration in a given access control group, where there is more than one reader available for communications. The next 8 bits contain an information field (message number), and the last eight bits contain a CRC of all preceding bits including the basic Wiegand data. If the panel determines that there is an error in the received Wiegand data (i.e. due to a CRC error),* then it can request the reader to retransmit as described herein. The extended protocol is shown in Figure 2.

The address field (first two bits) is used to distinguish among multiple Wiegand readers sharing the same Wiegand 5-wire bus. In the preferred embodiment, address 00 is reserved for broadcast messages, and addresses 01, 10, and 11 are used to distinguish among multiple readers. An address of 00 is the default when multiple-unit addressing is not used.

Since the electrical characteristics of the Wiegand interface call for open-collector drivers, multiple readers can be attached to the same Wiegand bus. Note that with the robust error checking enabled by the present invention, any attempt by multiple Wiegand generators to talk at the same time (so-called "collisions") will be detected, and then the panel will send out a "rebroadcast

message" request using either address 00 or one-by-one to each of the active generators.

In the preferred embodiment, there are seven groups of messages; each is used for different Wiegand generators. For example, these categories include security/access control, time & attendance, parking, etc. Group zero is reserved for messages common to all group, and group 7 is reserved for error messages.

Data transfer from panel to reader

In accordance with the invention, the panel may send data to a reader using an asynchronous serial data stream via the LEDCTL wire at 1200 baud, 8 data bits, 1 stop bit, no parity. All fields in this instance are one byte long. The first byte of a command is divided into two sub-fields. The first two bits are the address field (00-11), and the last six bits contain the command code (000000-111111). The following commands are available in the preferred embodiment:

COMMAND SENT BY PANEL		WIEGAND GENERATOR RESPONSE
00h <CRC>	0 = retransmit last Wiegand data transmission <CRC> = 8-bit CRC	Retransmits last Wiegand data message
01h <address> <CRC>	1=Return value of selected parameter address <address> = 00 thru FF <CRC> = 8-bit CRC	Parameter value of desired address is transmitted back via the Wiegand extension
02h <address> <data> <CRC>	2= set value of selected parameter address <address> = 00 thru FF <data> = 00 thru FF <CRC> = 8-bit CRC	Acknowledgement that data was written is transmitted via the Wiegand extension
03h <LEDCTL> <seconds> <CRC>	3=Turn on LED <LEDCTL> = simulation of LED control signals <# of seconds to keep LED on> <CRC> = 8-bit CRC	Acknowledgement is transmitted via the Wiegand extension

The panel system in the preferred embodiment is able to switch a Wiegand generator from the basic protocol to the extended protocol as follows. Note that this procedure will typically be run when the panel is initialized. The panel will drop the LEDCTL signal low three times within a one-second interval. The Wiegand generator starts an interval timer when the first pulse is received, and then checks to see if it receives two additional pulses within the one-second period from the first pulse. If it receives exactly three pulses as described, then it sends the Wiegand extension message "Capable of Using the Wiegand Extension" in message group 0. The panel then will send out the "Use Wiegand Extension" command to the Wiegand generator, and the Wiegand generator sends the "Command received and executed" message in group 0 and sets a flag in non-volatile memory to use the Wiegand extension (even if power is lost and subsequently restored).

Pushbutton Emulation

In another aspect of the invention, the reader includes one or more push buttons or other types of input devices on the housing that can be used to provide additional information to the panel. Rather than utilize separately added wires for pushbutton functions as in the prior art, this invention utilizes the Wiegand extension protocol to transmit the button data to the panel. Moreover, in this invention, buttons can be required to be pressed before a card will be accepted; button status is reported along with card data in the same Wiegand extension transmission, multiple buttons can be pressed to signify different functions, and buttons may have changeable legends

on the housing (since their functionality is easily reprogrammed).

Since the status of the buttons on the housing is reported using the extended Wiegand protocol described herein, no additional wires are required to be added to existing 5-wire Wiegand infrastructure.

A reader can be programmed to report the status of a button without requiring a card to be read. For example, a doorbell function may be emulated in this way, so that a visitor can press the button, causing a doorbell message to be sent to the panel. This can then alert a security person in the area that a visitor who does not have a card needs attention at that entry point. This eliminates the need to provide a separate, dedicated doorbell wiring system as in the prior art.

In addition, the arming and disarming functions of the related security system can now be easily implemented. That is, a user can arm or disarm the security system upon presentation of a valid card authorized for that function.

Similarly, legends such R and C can be used with separate buttons that would be pressed by a user leaving or entering a facility, who would then present the card for identification purposes. This enables the system to keep track of who is in the building at any given time.

A duress or panic condition could be used for example if a person presses a certain combination of buttons upon presentment of the card for entry.

Panel operating parameters can be modified by button presses along with presentment of an authorized card.

CRC

The CRC field contains an 8-bit CRC of all of the preceding Wiegand data and the extended data field. CRC technology is well known in the art and need not be repeated herein.

We claim:

1. An access control security system comprising:
 - a) a control panel;
 - b) a plurality of access control groups, each access control group interconnected to the control panel on an independent multi-wire data bus, each access control group comprising:
 - an access interface unit comprising:
 - data output means for transmitting data onto the data bus to the control panel,
 - data input means for receiving data via the data bus from the control panel,
 - processing means, interoperating with the data output means and the data input means, for operating data transfers over the data bus, the processing means adapted to generate a data message for transmission onto the data bus via the data output means, the data message comprising a Wiegand message field in accordance with the Wiegand protocol and an extended data field.
2. The system of claim 1 wherein the extended data field comprises a status information field indicative of a status condition of the access interface unit.
3. The system of claim 1 wherein the access interface unit further comprises user ID reading means for reading an ID device.

4. The system of claim 3 wherein the ID reading means is configured to read an access control card.
5. The system of claim 3 wherein the ID reading means is configured to read a data transponder.
6. The system of claim 3 wherein the ID reading means is configured to read a data-carrying key fob.
7. The system of claim 3 wherein the ID reading means is configured to read biometric data from a user.
8. The system of claim 3 wherein the processing means interoperates with the ID reading means, and wherein the extended data field further comprises an information field indicative of a property of an ID read by the ID reading means.
9. The system of claim 1 wherein at least one access control group comprises a plurality of access interface units, and wherein the extended data field comprises address information uniquely identifying each access interface unit in an access control group.
10. The system of claim 1 wherein the processing means is further adapted to utilize an error detection algorithm as a function of data contained within the extended data field.
11. The system of claim 10 wherein the error detection algorithm is a cyclic redundancy check (CRC), and wherein the extended data field is appended with the CRC.
12. The system of claim 2 wherein the access interface unit further comprises user input means for accepting user input

functions, and wherein the status condition of the access interface unit indicates a function input by a user via the user input means.

13. The system of claim 12 wherein the input means comprises at least one pushbutton.

14. The system of claim 13 wherein the function of the pushbutton is a door bell function.

15. The system of claim 2 wherein the access interface unit comprises external status input means for accepting external status data from an external device coupled thereto, and wherein the status information field of the extended data field comprises the external status data.

16. The system of claim 15 wherein the external device is adapted to measure temperature, and wherein the external status data comprises the measured temperature.

17. The system of claim 15 wherein the external device is adapted to detect a change in light incident thereon, and wherein the external status data comprises data indicative of a change in light.

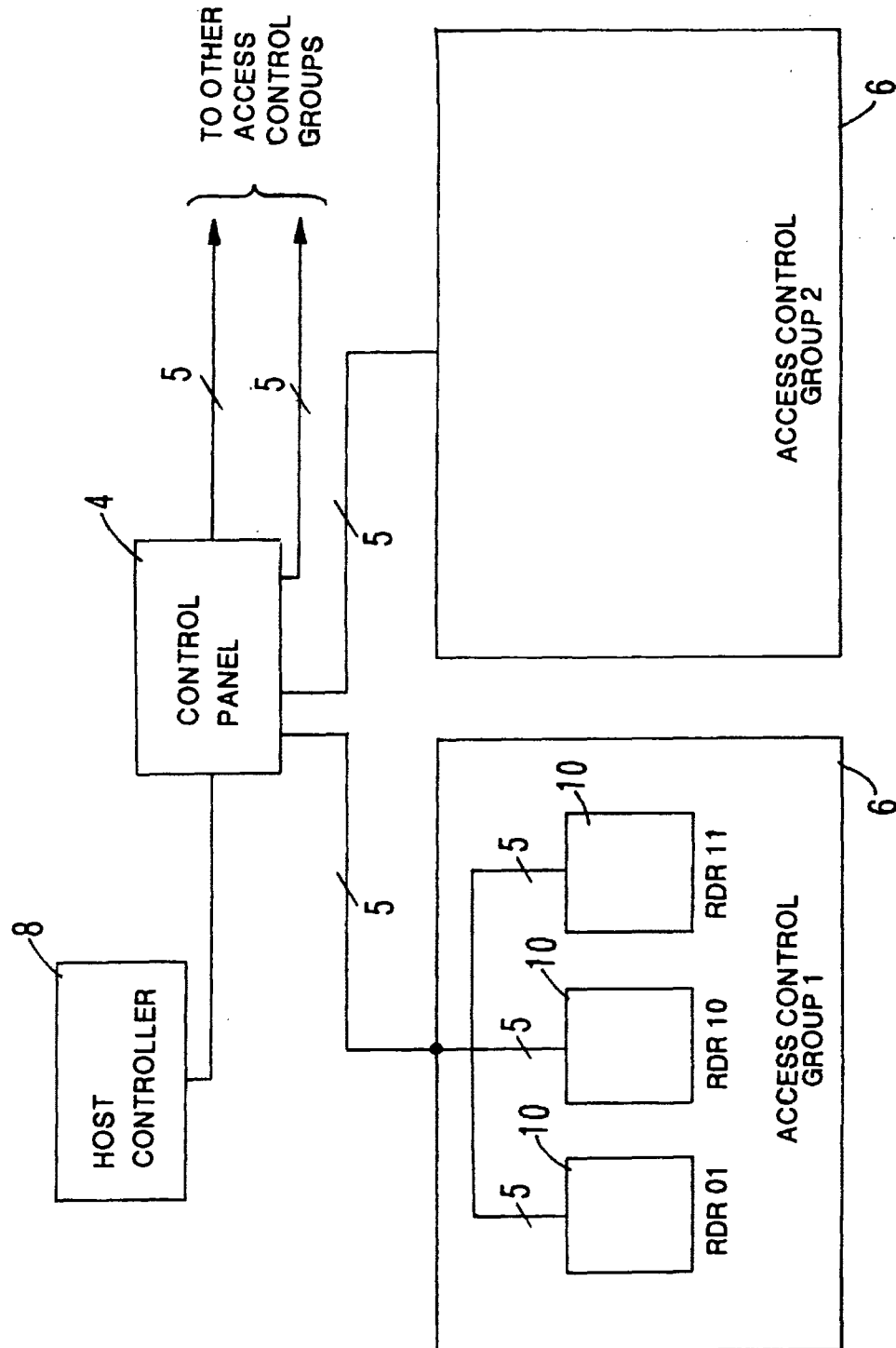
18. The system of claim 15 wherein the external device is adapted to detect physical tampering with the access interface unit, and wherein the external status data comprises a tamper indication.

19. The system of claim 2 wherein the processing means is further adapted to generate supervision data on a periodic basis, and wherein the status information field comprises the supervision data.

20. The system of claim 2 wherein the processing means is further adapted to detect a malfunction of the access interface unit, and wherein the status information field comprises data indicative of a malfunction.

21. The system of claim 1 wherein data transfers are made to the control panel using the electrical and information content of the Wiegand protocol via the Data "0" and Data "1" output signals.

22. The system of claim 1 wherein data transfers are made by the control panel using the electrical characteristics of the Wiegand protocol via the LEDCTL input signal as a serial protocol.



2

FIG.1

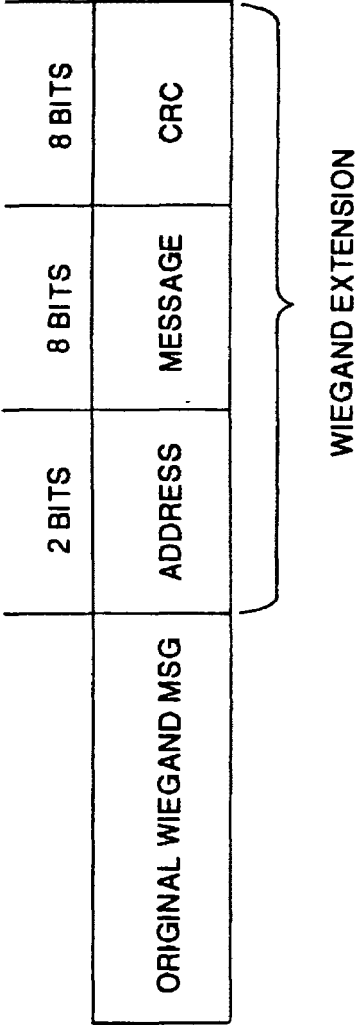


FIG.2

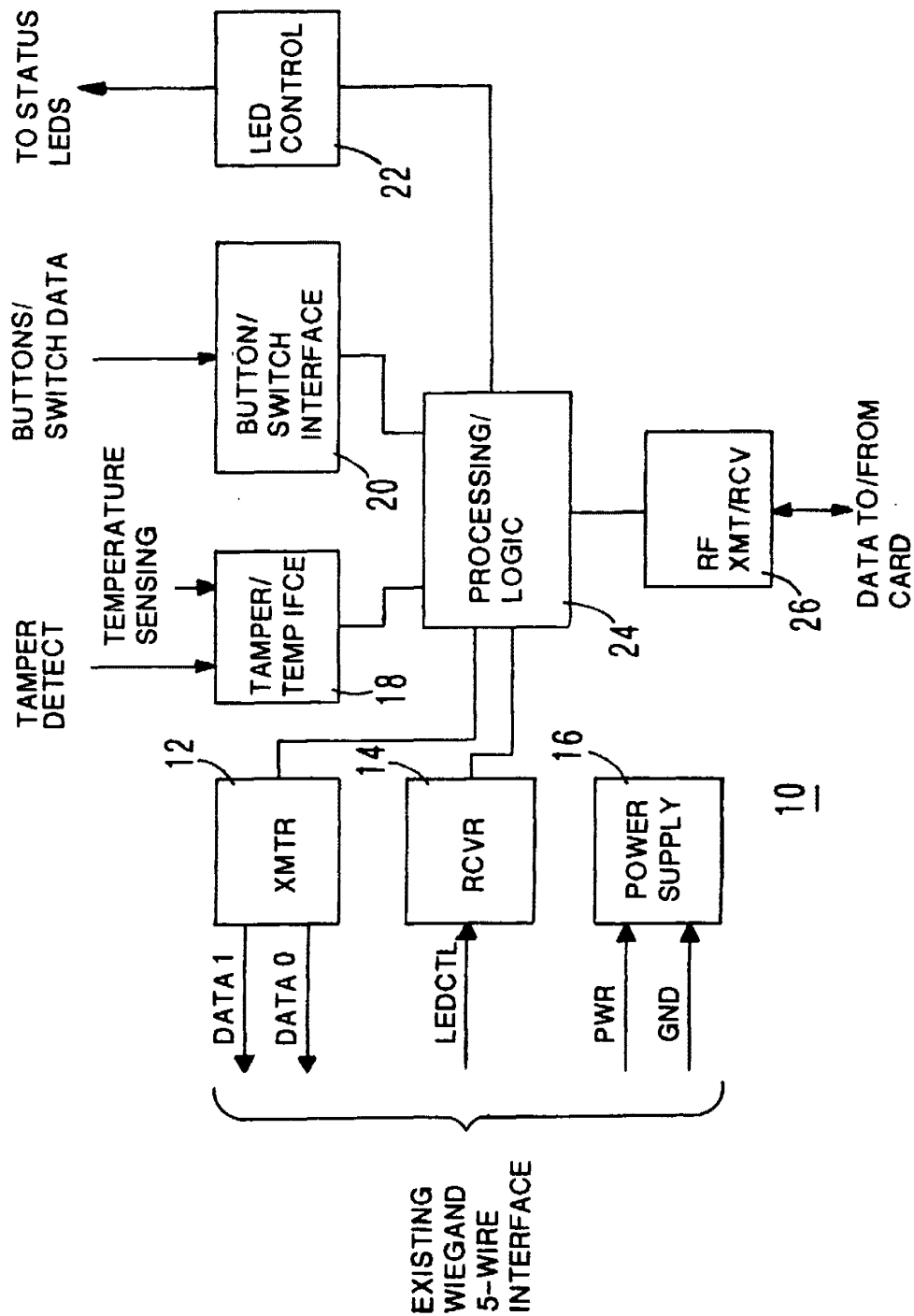


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/10554

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06K 19/06, 7/10

US CL : 235/ 381, 382, 382.5, 492, 486, 441, 375, 380, 384; 705/13, 41, 43, 44

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 235/ 381, 382, 382.5, 492, 486, 441, 375, 380, 384; 705/13, 41, 43, 44

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,517,172 A (CHIU) 14 May 1996 (05.14.1996), the entire document.	1-22
Y	US 5,491,471 A (STOBBE) 13 February 1996 (13.02.1996), the entire document.	1-22
A	US 5,166,676 A (MILHEISER) 24 November 1992 (24.11.1992), the entire document.	1-22
A	US 5,028,918 A (GILES et al) 02 July 1991 (02.07.1991), the entire document.	1-22
Y,E	US 6,411,199 B1 (GEISZLER et al) 25 June 2002 (25.06.2002), the entire document.	1-22

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

24 July 2002 (24.07.2002)

Date of mailing of the international search report

05 SEP 2002

Name and mailing address of the ISA/US

Commissioner of Patents and Trademarks

Box PCT

Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

Le, Thien M.

Telephone No. (703) 308-0956

Reese Paster

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/10554

Continuation of B. FIELDS SEARCHED Item 3:

USPTO APS EAST


search terms: Wiegand, protocol, card\$1, reader\$1, two-way\$1, 5-wire\$2 bus\$3, interface, panel

Form PCT/ISA/210 (second sheet) (July 1998)

EAST Search History**EAST Search History (Prior Art)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	4	("8358783")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/12/16 13:37
L2	2	("8358783").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/12/16 13:37
L3	2849	(380/270).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/12/16 13:56
L4	401	(380/260).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/12/16 13:56
L5	1454	(380/46).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/12/16 13:56
L6	2	(ep-1760985-\$.did.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/12/16 13:56
L7	2	(WO-2008043125-\$.did.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/12/16 13:57
L8	4528	(726/5).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/12/16 14:08
L9	73	(WIEGAND WITH protocol) and reader	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/12/16 14:08
L10	13	9 and ("713"/\$).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/12/16 14:08
L11	13	9 and ("726"/\$).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/12/16 14:08
L12	3	9 and ("380"/\$).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/12/16 14:08

12/ 16/ 2013 2:09:02 PM**C:\Users\slemma\Documents\EAST\Workspaces\13181890.wsp**

<p align="center"><i>Index of Claims</i></p> 	Application/Control No. 13689088	Applicant(s)/Patent Under Reexamination GUTHERY ET AL.
	Examiner SAMSON LEMMA	Art Unit 2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant			<input type="checkbox"/> CPA			<input type="checkbox"/> T.D.			<input type="checkbox"/> R.1.47		
CLAIM		DATE									
Final	Original	12/14/2013									
	1	✓									
	2	✓									
	3	✓									
	4	✓									
	5	✓									
	6	O									
	7	O									
	8	✓									
	9	✓									
	10	✓									
	11	✓									
	12	✓									
	13	O									
	14	O									
	15	✓									
	16	✓									
	17	✓									
	18	✓									
	19	O									
	20	O									

Receipt date: 08/21/2013

13689088 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2432
				Examiner Name	Cordelia P K Zecher
Sheet	1	of	1	Attorney Docket Number	2943AAAB-178-DIV

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document Country Code ³ ; Number ⁴ ; Kind Code ⁵ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶

NON-PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	1	Official Action for European Patent Application No. 09167708.8, dated Apr. 17, 2013 (Attorney's Ref. No. 2943AAAB-184-EP) 4 pages
	2	Official Action for U.S. Patent Application No. 12/541,480, mailed Jun. 05, 2013 (Attorney's Ref. No. 2943AAAB-184) 22 pages

Examiner Signature	/Samson Lemma/	Date Considered	12/16/2013
--------------------	----------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Receipt date: 03/04/2013

13689088 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	1	of	12	Attorney Docket Number	2943AAAB-178-DIV

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	3694757	09/26/1972	Hanna, Jr.	
	2	3842350	10/15/1974	Gross	
	3	4087626	05/02/1978	Brader	
	4	4163215	07/31/1979	Iida	
	5	4333072	06/01/1982	Beigel	
	6	4425645	01/10/1984	Weaver et al.	
	7	4519068	05/21/1985	Krebs et al.	
	8	4549264	10/22/1985	Carroll et al.	
	9	4656463	04/07/1987	Anders et al.	
	10	4688026	08/18/1987	Scribner et al.	
	11	4849927	07/18/1989	Vos	
	12	5013898	05/07/1991	Glasspool	
	13	5028918	07/02/1991	Giles et al.	
	14	5041826	08/20/1991	Milheiser	
	15	5050150	09/17/1991	Ikeda	
	16	5151684	09/29/1992	Johnsen	
	17	5166676	11/24/1992	Milheiser	
	18	5187676	02/16/1993	DeVane	
	19	5193115	03/09/1993	Vobach	
	20	5218344	06/08/1993	Ricketts	
	21	5235642	08/10/1993	Wobber et al.	
	22	5258936	11/02/1993	Gallup et al.	
	23	5343469	08/30/1994	Ohshima	
	24	5347263	09/13/1994	Carroll et al.	
	25	5357528	10/18/1994	Alon et al.	
	26	5396215	03/07/1995	Hinkle	
	27	5420928	05/30/1995	Aiello et al.	
	28	5426425	06/20/1995	Comad et al.	
	29	5446683	08/29/1995	Mullen et al.	
	30	5467082	11/14/1995	Sanderson	
	31	5491471	02/13/1996	Stobbe	
	32	5517172	05/14/1996	Chiu	
Examiner Signature	/Samson Lemma/			Date Considered	12/16/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Receipt date: 03/04/2013

13689088 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	2	of	12	Attorney Docket Number	2943AAAB-178-DIV

	33	5519381	05/21/1996	Marsh et al.	
	34	5521602	05/28/1996	Carroll et al.	
	35	5533128	07/02/1996	Vobach	
	36	5541996	07/30/1996	Ridenour	
	37	5577124	11/19/1996	Anshel et al.	
	38	5594384	01/14/1997	Carroll et al.	
	39	5600324	02/04/1997	Reed et al.	
	40	5600683	02/04/1997	Bierach et al.	
	41	5608801	03/04/1997	Aiello et al.	
	42	5680131	10/21/1997	Utz	
	43	5679945	10/21/1997	Renner et al.	
	44	5686904	11/11/1997	Bruwer	
	45	5696909	12/09/1997	Wallner	
	46	5724417	03/03/1998	Bartholomew et al.	
	47	5745037	04/28/1998	Guthrie et al.	
	48	5751808	05/12/1998	Anshel et al.	
	49	5754603	05/19/1998	Thomas et al.	
	50	5777561	07/07/1998	Chieu et al.	
	51	5802176	09/01/1998	Audebert	
	52	5825882	10/20/1998	Kowalski et al.	
	53	5844990	12/01/1998	Kokubu et al.	
	54	5848541	12/15/1998	Glick et al.	
	55	5886894	03/23/1999	Rakoff	
	56	5887176	03/23/1999	Griffith et al.	
	57	5909462	06/01/1999	Kamerman et al.	
	58	5923264	07/13/1999	Lavelle et al.	
	59	5929779	07/27/1999	MacLellan et al.	
	60	5952922	09/14/1999	Shober	
	61	5952935	09/14/1999	Mejia et al.	
	62	5954583	09/21/1999	Green	
	63	5991410	11/23/1999	Albert et al.	
	64	5995956	11/30/1999	Nguyen	
	65	6044388	03/28/2000	DeBellis et al.	
	66	6052786	04/18/2000	Tsuchida	
	67	6078888	06/20/2000	Johnson, Jr.	
	68	6079018	06/20/2000	Hardy et al.	
Examiner Signature	/Samson Lemma/			Date Considered	12/16/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Receipt date: 03/04/2013

13689088 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	3	of	12	Attorney Docket Number	2943AAAB-178-DIV

	69	6078251	06/20/2000	Landt et al.	
	70	6097307	08/01/2000	Utz	
	71	6154544	11/28/2000	Farris et al.	
	72	6181252	01/30/2001	Nakano	
	73	6182214	01/30/2001	Hardjono	
	74	6192222	02/20/2001	Greeff et al.	
	75	6212175	04/03/2001	Harsch	
	76	6219439	04/17/2001	Burger	
	77	6223984	05/01/2001	Renner et al.	
	78	6249866	06/19/2001	Brundrett et al.	
	79	6249212	06/19/2001	Beigel et al.	
	80	6259367	07/10/2001	Klein	
	81	6272562	08/07/2001	Scott et al.	
	82	6285761	09/04/2001	Patel et al.	
	83	6285681	09/04/2001	Kolze et al.	
	84	6304613	10/16/2001	Koller et al.	
	85	6307517	10/23/2001	Lee	
	86	6314440	11/06/2001	O'Toole et al.	
	87	6317027	11/13/2001	Watkins	
	88	6325285	12/04/2001	Baratelli	
	89	6366967	04/02/2002	Wagner	
	90	6377176	04/23/2002	Lee	
	91	6411199	06/25/2002	Geiszler et al.	
	92	6420961	07/16/2002	Bates et al.	
	93	6483427	11/19/2002	Werb	
	94	6487176	11/26/2002	Lehmann	
	95	6496595	12/17/2002	Puchek et al.	
	96	6496806	12/17/2002	Horwitz et al.	
	97	6509828	01/21/2003	Bolavage et al.	
	98	6542608	04/01/2003	Scheidt et al.	
	99	6606386	08/12/2003	Scheidt et al.	
	100	6608901	08/19/2003	Scheidt et al.	
	101	6617962	09/09/2003	Horwitz et al.	
	102	6677852	01/13/2004	Landt	
	103	6691141	02/10/2004	Schmidt	
	104	6718038	04/06/2004	Cusmario	
Examiner Signature	/Samson Lemma/			Date Considered	12/16/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Receipt date: 03/04/2013

13689088 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	4	of	12	Attorney Docket Number	2943AAAB-178-DIV

	105	6717516	04/06/2004	Bridgelall	
	106	6724296	04/20/2004	Hikita et al.	
	107	6810123	10/26/2004	Farris et al.	
	108	6885747	04/26/2005	Scheidt et al.	
	109	6903656	06/07/2005	Lee	
	110	6922558	07/26/2005	Delp et al.	
	111	6931533	08/16/2005	Roberts	
	112	6944768	09/13/2005	Siegel et al.	
	113	6947560	09/20/2005	Smeets et al.	
	114	6963270	11/08/2005	Gallagher, III et al.	
	115	6988203	01/17/2006	Davis et al.	
	116	6992567	01/31/2006	Cole et al.	
	117	7016925	03/21/2006	Schmidt	
	118	7026935	04/11/2006	Diorio et al.	
	119	7064665	06/20/2006	Woodall et al.	
	120	7085791	08/01/2006	Barry et al.	
	121	7118033	10/10/2006	Merkert	
	122	7120696	10/10/2006	Au et al.	
	123	7170997	01/30/2007	Petersen et al.	
	124	7190787	03/13/2007	Graunke et al.	
	125	7197279	03/27/2007	Bellantoni	
	126	7212632	05/01/2007	Scheidt et al.	
	127	7219113	05/15/2007	Bonaccio et al.	
	128	7268681	09/11/2007	Fitzgibbon	
	129	7269416	09/11/2007	Guthrie et al.	
	130	7277543	10/02/2007	Driscoll	
	131	7293698	11/13/2007	Cheng et al.	
	132	7375616	05/20/2008	Rowse et al.	
	133	7378967	05/27/2008	Sullivan et al.	
	134	7407110	08/05/2008	Davis et al.	
	135	7412056	08/12/2008	Farris et al.	
	136	7492898	02/17/2009	Farris et al.	
	137	7492905	02/17/2009	Fitzgibbon	
	138	7551081	06/23/2009	Vrba et al.	
	139	8183980	05/22/2012	Davis et al.	
	140	8358783	01/22/2013	Davis et al.	
Examiner Signature	/Samson Lemma/			Date Considered	12/16/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Receipt date: 03/04/2013

13689088 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	5	of	12	Attorney Docket Number	2943AAAB-178-DIV

	141	2001/0041593	11/15/2001	Asada	
	142	2001/0056534	12/27/2001	Roberts	
	143	2002/0016913	02/07/2002	Wheeler et al.	
	144	2002/0036569	03/28/2002	Martin	
	145	2002/0131595	09/19/2002	Veda et al.	
	146	2002/0184539	12/05/2002	Fukuda et al.	
	147	2003/0007473	01/09/2003	Strong et al.	
	148	2003/0014646	01/16/2003	Buddhikot et al.	
	149	2003/0055667	03/20/2003	Sgambaro et al.	
	150	2003/0074319	04/17/2003	Jaquette	
	151	2003/0081785	05/01/2003	Boneh et al.	
	152	2003/0204541	10/30/2003	Shackleford et al.	
	153	2003/0208697	11/06/2003	Gardner	
	154	2004/0069852	04/15/2004	Seppinen et al.	
	155	2004/0087273	05/06/2004	Pertti1a et al.	
	156	2004/0089707	05/13/2004	Cortina et al.	
	157	2004/0153291	08/05/2004	Kocarev et al.	
	158	2004/0162863	08/19/2004	Barry et al.	
	159	2004/0162864	08/19/2004	Nowshadi et al.	
	160	2004/0176032	09/09/2004	Kotola et al.	
	161	2004/0179684	09/16/2004	Appenzeller et al.	
	162	2004/0212493	10/28/2004	Stilp	
	163	2004/0232220	11/25/2004	Beenau et al.	
	164	2005/0002533	01/06/2005	Langin-Hooper et al.	
	165	2005/0010624	01/13/2005	Stehle	
	166	2005/0010750	01/13/2005	Ward et al.	
	167	2005/0036620	02/17/2005	Casden et al.	
	168	2005/0044119	02/24/2005	Langin-Hooper et al.	
	169	2005/0063004	03/24/2005	Silverbrook et al.	
	170	2005/0110210	05/26/2005	Soltys et al.	
	171	2005/0116813	06/02/2005	Raskar	
	172	2005/0129247	06/16/2005	Gammel et al.	
	173	2005/0127172	06/16/2005	Merkert Sr.	
	174	2005/0166040	07/28/2005	Walmsley	
	175	2005/0182946	08/18/2005	Shatford	
	176	2005/0265546	12/01/2005	Suzuki	
Examiner Signature	/Samson Lemma/			Date Considered	12/16/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Receipt date: 03/04/2013

13689088 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>			Complete if Known		
			Application Number	13/689,088	
			Filing Date	November 29, 2012	
			First Named Inventor	Scott B. Guthery	
			Art Unit	2431	
			Examiner Name		
Sheet	6	of	12	Attorney Docket Number	2943AAAB-178-DIV

	177	2006/0083228	04/20/2006	Ong et al.	
	178	2006/0101274	05/11/2006	Merkert et al.	
	179	2006/0123466	06/08/2006	Davis et al.	
	180	2006/0156027	07/13/2006	Blake	
	181	2006/0174184	08/03/2006	Stroud et al.	
	182	2006/0177056	08/10/2006	Rostin et al.	
	183	2006/0179094	08/10/2006	Onaya et al.	
	184	2006/0181397	08/17/2006	Limbachiya	
	185	2006/0206554	09/14/2006	Lauter et al.	
	186	2006/0210081	09/21/2006	Zhu et al.	
	187	2006/0224901	10/05/2006	Lowe	
	188	2006/0255129	11/16/2006	Griffiths	
	189	2006/0288101	12/21/2006	Mastrodonato et al.	
	190	2006/0294312	12/28/2006	Walmsley	
	191	2007/0016942	01/18/2007	Sakai et al.	
	192	2007/0034691	02/15/2007	Davis et al.	
	193	2007/0043954	02/22/2007	Fox	
	194	2007/0057057	03/15/2007	Andresky et al.	
	195	2007/0076864	04/05/2007	Hwang	
	196	2007/0099597	05/03/2007	Arkko et al.	
	197	2007/0109101	05/17/2007	Colby	
	198	2007/0121943	05/31/2007	Dellow et al.	
	199	2007/0165847	07/19/2007	Langin-Hooper et al.	
	200	2007/0165848	07/19/2007	Reyes	
	201	2007/0178886	08/02/2007	Wang et al.	
	202	2007/0183593	08/09/2007	Yoshida et al.	
	203	2007/0195952	08/23/2007	Singanamala	
	204	2007/0214293	09/13/2007	Gangstoe et al.	
	205	2007/0269048	11/22/2007	Hsu	
	206	2007/0273497	11/29/2007	Kuroda et al.	
	207	2007/0293192	12/20/2007	De Groot	
	208	2007/0294528	12/20/2007	Shoji et al.	
	209	2007/0294531	12/20/2007	Alten	
	210	2007/0294539	12/20/2007	Shulman et al.	
	211	2007/0296817	12/27/2007	Ebrahimi et al.	
	212	2008/0001778	01/03/2008	Challener et al.	
Examiner Signature	/Samson Lemma/			Date Considered	12/16/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Receipt date: 03/04/2013

13689088 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	7	of	12	Attorney Docket Number	2943AAAB-178-DIV

	213	2008/0005532	01/03/2008	Liao et al.	
	214	2008/0010218	01/10/2008	Zank	
	215	2008/0012690	01/17/2008	Friedrich	
	216	2008/0016363	01/17/2008	Lapstun et al.	
	217	2008/0014867	01/17/2008	Finn	
	218	2008/0032626	02/07/2008	Chen	
	219	2008/0037466	02/14/2008	Ngo et al.	
	220	2008/0046493	02/21/2008	Rosenberg	
	221	2008/0061941	03/13/2008	Fischer et al.	
	222	2008/0094171	04/24/2008	Sawhney	
	223	2008/0184349	07/31/2008	Ting	
	224	2008/0229400	09/18/2008	Burke	
	225	2009/0128392	05/21/2009	Hardacker et al.	
	226	2009/0153290	06/18/2009	Bierach	
	227	2009/0315673	12/24/2009	Huang	
	228	2010/0001840	01/17/2010	Kang et al.	

UNPUBLISHED U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-kind Code ² (if known)	Filing Date MM-DD-YYYY	Name of Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	229	13/689108	11/29/2012	Guthery et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document Country Code ³ , Number ⁴ , Kind Code ⁵ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
	230	CN 1307309	08/08/2001	BEIJING KERUIQI TECHNOLOGY DEV		(with English abstract)
	231	EP 0616429	09/21/1994	SIEMENS AG		(with English Abstract)
	232	EP 0697491	02/21/1996	NIPPON DENSO CO		
	233	EP 0843438	05/20/1998	THOMSON MULTIMEDIA SA		

Examiner Signature	/Samson Lemma/	Date Considered	12/16/2013
--------------------	----------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Receipt date: 03/04/2013

13689088 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	8	of	12	Attorney Docket Number	2943AAAB-178-DIV

	234	EP 0872976	10/21/1998	UNITED TECHNOLOGIES AUTOMOTIVE		
	235	EP 0924894	06/23/1999	SIEMENS AG		(with English Abstract)
	236	EP 0949563	10/13/1999	LUCENT TECHNOLOGIES INC		
	237	EP 0956818	11/17/1999	CITICORP DEV CENTER		
	238	EP 0996928	05/03/2000	ASSURE SYSTEMS INC		
	239	EP 1148644	10/24/2001	COMM RES LAB MINISTRY OF PUBLI		
	240	EP 1251448	10/23/2002	TOO MNOGOPROFILNOE PREDPR		
	241	EP 1292882	03/19/2003	ANOTO AB		
	242	EP 1398691	03/17/2004	TOSHIBA KK		
	243	EP 1420542	05/19/2004	ST MICROELECTRONICS SRL		
	244	EP 1460573	09/22/2004	Nokia Corporation		
	245	EP 1643643	04/05/2006	MICRONAS GMBH		(with English translation)
	246	EP 1696360	08/30/2006	SAMSUNG ELECTRONICS CO LTD		
	247	EP 1043687	11/22/2006	CANON KK		
	248	GB 2256170	12/02/1992	BRANDES WILLIAM ROBERT		
	249	GB 2331825	06/02/1999	NEC CORP		
	250	JP 2002-261749	09/13/2002	MATSUSHITA ELECTRIC IND CO LTD		(with English abstract)
	251	KR 2002-0073716	09/28/2002	FIRSTECH INT INC		(with English abstract)

Examiner Signature	/Samson Lemma/	Date Considered	12/16/2013
--------------------	----------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Receipt date: 03/04/2013

13689088 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	9	of	12	Attorney Docket Number	2943AAAB-178-DIV

	252	RU 2158444	10/27/2000	AJ DI SISTEMS INK		(with English abstract)
	253	RU 2195020	12/20/2002	MNOGOPROFIL NOE PRED OOO EHLSI		(with English abstract)
	254	WO 97/17683	05/15/1997	ID SYSTEMS INC		
	255	WO 99/56429	11/04/1999	IDENTIX INC		
	256	WO 01/013218	02/22/2001	Siemens Aktiengesellschaft		(with English Abstract)
	257	WO 01/13218	02/22/2001	SIEMENS AG		(with English Abstract)
	258	WO 01/18331	03/15/2001	Electec System Aktiebolag		
	259	WO 02/082367	10/17/2002	PITTHWAY CORP		
	260	WO 03/027832	04/03/2003	Intel Corporation		
	261	WO 03/042812	05/22/2003	Everbee Networks		(with English Abstract)
	262	WO 2004/010373	01/29/2004	BANQUE TEC INTERNAT PTY LTD		
	263	WO 04/010373	01/29/2004	Banque-Tec International Pty Ltd		
	264	WO 2004/039119	05/06/2004	Anzon Autodoor Limited		
	265	WO 2006/015625	08/09/2004	Telecom Italia S.P.A.		
	266	WO 05/001777	01/06/2005	SCM Microsystems GMBH		
	267	WO 2005/001777	01/06/2005	SCM MICROSYSTEMS GMBH		
	268	WO 2005/018137	02/24/2005	Securicom Pty Ltd		
	269	WO 2005/029315	03/31/2005	Globespanvirata Incorporated		
	270	WO 2005/038729	04/28/2005	SCM Microsystems, Inc.		
	271	WO 2006/032941	03/30/2006	Nokia Corporation		
	272	WO 2006/036521	04/06/2006	Qualcomm Incorporated		

Examiner Signature	/Samson Lemma/	Date Considered	12/16/2013
--------------------	----------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L/

Receipt date: 03/04/2013

13689088 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	10	of	12	Attorney Docket Number	2943AAAB-178-DIV

	273	WO 2006/126688	11/03/2006	NEC Corporation		(with English Abstract)
	274	WO 2006/123316	11/23/2006	KONINKL PHILIPS ELECTRONICS NV		
	275	WO 2007/094868	08/23/2007	MOJIX INC		
	276	WO 2007/103906	09/13/2007	Imagineer Software, Inc.		
	277	WO 2007/117315	10/18/2007	Symbol Technologies, Inc.		
	278	WO 2007/120215	10/25/2007	Imagineer Software, Inc.		
	279	WO 2008/001918	01/03/2008	Yui et al.		
	280	WO 2008/010441	01/24/2008	NEC Corporation		(with English Abstract)
	281	WO 2008/043125	04/17/2008	MICROLATCH PTY LTD		

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	282	"Access Control Standard for the 26-Bit Wiegand Reader Interface," Security Industry Association, October 17, 1996, 15 pages.	
	283	Anashin, V., "Uniformly distributed sequences over p-adic integers," Number Theoretic and Algebraic Methods in Computer Science, Moscow 1993 (A.J. van der Poorten, I.Shparlinski, and H.G. Zimmer eds., 1995), pp. 1-18, available at http://crypto.rsuh.ru/papers/anashin-paper1.pdf .	
	284	Anashin, V., "Pseudorandom number generation by p-adic ergodic transformations" (Jan. 29, 2004), available at http://arxiv.org/abs/cs.CR/0401030 .	
	285	Anashin, V., "Pseudorandom number generation by p-adic ergodic transformations: An addendum" (Feb. 26, 2004), pp. 1-9, available at http://arxiv.org/abs/cs.CR/0402060 .	
	286	ANASHIN "Non-Archimedean Ergodic Theory and Pseudorandom Generators," Oct. 07, 2007, 39 pages, available at http://arxiv.org/abs/0710.1418v1	
	287	Anashin, V., "Uniformly distributed sequences in computer algebra, or how to construct program generators of random numbers," J. Math. Sci., 89(4):1355-1390 (1998), available at http://crypto.rsuh.ru/papers/anashin-paper5.pdf .	
	288	Anashin, V., "Uniformly distributed sequences of p-adic integers," II. Discrete Math. Appl., 12(6):527-590 (2002), available at http://arXiv.org/abs/math.NT/0209407 .	
	289	Anashin, V., "Uniformly distributed sequences of p-adic integers," Mathematical Notes, 55(2):109-133 (1994), available at http://crypto.rsuh.ru/papers/anashin-paper2.pdf .	
Examiner Signature	/Samson Lemma/		Date Considered 12/16/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	11	of	12	Attorney Docket Number	2943AAAB-178-DIV

290	BARKER, Cryptanalysis of Shift-Register Generated Stream Cipher Systems, Cryptographic Series No. 39, Aegean Park Press, 1984, Chapters 1-3, pages 1-38
291	BLUM, M. et al., "How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits," SIAM Journal on Computing, Nov. 1984, Vol. 13, No. 4, pp. 850-864.
292	BRIAN, M., "How Remote Entry Works," Howstuffworks.com, retrieved from http://auto.howstuffworks.com/remote-entry.htm , printed on May 19, 2005, copyright 2005, 8 pages.
293	"Condoplex - The World Leader in Developing Security and Communication Solutions," retrieved from http://web.archive.org/web/20040324112641/http://condoplexinc.com/ , publication date March 24, 2004, 1 page.
294	"Contactless Technology for Secure Physical Access: Technology and Standards Choices," Smart Card Alliance White Paper, October 2002, 36 pages.
295	DAMGARD, I., "On the Randomness of Legendre and Jacobi Sequences," Advances in Cryptology (Proceedings of Crypto '88), Lecture Notes in Computer Science (1990), pp. 163-172.
296	Data Sheet, "26 Bit Weigand Specifications," Essex Electronics Incorporated, April 1, 1998, 1 page.
297	Data Sheet, "Micro RWD EM4001 'Mag swipe' Decimal Output Version," IB Technology, May 3, 2005, pp. 1-8.
298	DAVIS, M., "Reader To Panel Authentication," Cartes 2005, Paris, France, Nov. 1, 2005, 33 pages.
299	GLASS, B., "DMCA Used In Garage Door Battle," Ziff Davis Media, retrieved from http://www.extremetech.com/print_article2/0,2533 on May 19, 2005 (Jan. 23, 2003), 1 page.
300	"Information Technology: Application Profile for Commercial Biometrical Physical Access Control," Project INCITS 1706-D, 2005, 16 pages.
301	KNEBELKAMP et al., "Latest Generation Technology for Immobilizer Systems," Texas Instruments, retrieved from www.ti.com/tiris on May 19, 2005, 11 pages.
302	LEVIN, L., "One Way Functions and Pseudorandom Generators," Combinatorica, Vol. 7(4) (1987), pp. 357-363.
303	Press Release, "Radio Frequency Identification (RFID) based immobilizer systems help to curb auto theft and reduce insurance costs," Texas Instruments, May 7, 1999, 2 pages.
304	"Technology Basics: Understanding Wiegand," HID Corporation, 2004, 5 pages.
305	WEINSTEIN, L., "DMCA: Ma Bell Would Be Proud," Wired News, Jan. 20, 2003, 27 pages.
306	Woodcock, F., et al., "p-Adic Chaos and Random Number Generation," Experimental Mathematics, Vol. 7(4), (1998), pp. 334-342.
307	KOBLITZ, N., p-Adic Number, p-Adic Analysis and Zeta Functions, Chapter 3, Building up Ω , Springer, New York, (1977), pages 52-74.
308	KUIPERS, et al., Uniform Distribution of Sequences, John Wiley & Sons (1974), 400 pages (Submitted in 3 Parts)

Examiner Signature	/Samson Lemma/	Date Considered	12/16/2013
--------------------	----------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./


Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	12	of	12	Attorney Docket Number	2943AAAB-178-DIV

	309	LUBY, M., Pseudorandomness and Cryptographic Applications, Princeton University Press (1996), pages ix-55
	310	Examiner's First Report for Australian Patent Application No. 2006203768, mailed November 20, 2009 (Atty. Ref. No. 2943-114-AU).
	311	Partial European Search Report for European Patent Application No. 06119388 (Atty File No. 2943-114-EP), dated January 10, 2007.
	312	European Search Report for European Patent Application No. 06119388, mailed Apr. 17, 2007 (Attorney Ref. No. 2943-114-PEP), 9 pages
	313	Official Action for European Patent Application No. 06119388, mailed Dec. 14, 2007 (Attorney Ref. No. 2943-114-PEP), 2 pages
	314	Written Opinion of the International Searching Authority for International (PCT) Patent Application No. PCT/US2009/053430 (Atty File No. 2943-178-PCT) mailed November 24, 2009.
	315	International Search Report for International (PCT) Patent Application No. PCT/US2009/053430 (Atty File No. 2943-178-PCT) mailed November 24, 2009.
	316	International Preliminary Report on Patentability for International (PCT) Patent Application No. PCT/US09/53430, mailed Feb. 24, 2011 (Attorney Ref. No. 2943-178-PCT)
	317	European Search Report and Opinion for European Patent Application No. EP09807178, dated Nov. 08, 2011 (Attorney's Ref. No. 2943-178-PEP) 6 pages
	318	Official Action for U.S. Patent Application No. 11/464,912, mailed Jun. 2, 2010 (Attorney Ref. No. 2943-114)
	319	Official Action for U.S. Patent Application No. 11/464,912, mailed Nov. 23, 2010 (Attorney Ref. No. 2943-114)
	320	Notice of Allowance for U.S. Patent Application No. 11/464,912, mailed Jan. 20, 2012 (Attorney's Ref. No. 2943-114) 5 pages
	321	Official Action for U.S. Patent Application No. 12/539,431, mailed Jan. 26, 2012 (Attorney's Ref. No. 2943-178) 7 pages
	322	Official Action for U.S. Patent Application No. 12/539,431, mailed Apr. 13, 2012 (Attorney's Ref. No. 2943-178) 13 pages
	323	Notice of Allowance for U.S. Patent Application No. 12/539,431, mailed Apr. 13, 2012 (Attorney's Ref. No. 2943-178) 13 pages

Examiner Signature	/Samson Lemma/	Date Considered	12/16/2013
--------------------	----------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Search Notes 	Application/Control No. 13689088	Applicant(s)/Patent Under Reexamination GUTHERY ET AL.
	Examiner SAMSON LEMMA	Art Unit 2432

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	5, 14	12/14/2013	SL
380	270, 260 and 46	12/14/2013	SL

SEARCH NOTES		
Search Notes	Date	Examiner
713/\$, 726/\$ (With text Search)	12/14/2013	SL
EAST (See at least the attachment)	12/14/2013	SL
NPL (IEEE, ACM DIGITAL LIBRARY, GOOGLE, GOOGLE PATENT, Google Scholar, Scirus....)	12/14/2013	SL
INVENTOR NAME SEARCH	12/14/2013	SL

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

--	--

Receipt date: 05/15/2013

13689088 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	1	of	2	Attorney Docket Number	2943AAAB-178-DIV

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	6084977	07/04/2000	Borza	
	2	6587032	07/01/2003	Armingaud	
	3	7771334	08/10/2010	Bailey et al.	
	4	8138923	03/20/2012	Grunwald et al.	
	5	8312540	11/13/2012	Kahn et al.	
	6	2002/0078381	06/20/2002	Farley et al.	
	7	2005/0216955	09/29/2005	Wilkins et al.	
	8	2008/0072283	03/20/2008	Relyea et al.	
	9	2009/0066509	03/12/2009	Jernstrom et al.	
	10	2010/0039220	02/18/2010	Davis	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document Country Code ³ ; Number ⁴ ; Kind Code ⁵ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
	11	EP 1209551	05/29/2002	IBM		
	12	EP 1418484	05/12/2004	Stonesoft Corp.		
	13	WO 2005/038633	04/28/2005	Vodafone Holding GMBH		(English Abstract)

NON-PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	14	Partial European Search Report for European Patent Application No. 09167708.8, mailed Dec. 4, 2009 (Atty. Ref. No. 2943-184-EP)
	15	Official Communication for European Patent Application No. 09167708.8, dated Jun. 16, 2010 (Attorney Ref. No. 2943-184-EP)
	16	Notice of Allowance for U.S. Patent Application No. 12/539,431, mailed Aug. 31, 2012 (Attorney's Ref. No. 2943-178) 8 pages

Examiner Signature	/Samson Lemma/	Date Considered	12/16/2013
--------------------	----------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if, not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Receipt date: 05/15/2013

13689088 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	2	of	2	Attorney Docket Number	2943AAAB-178-DIV

	17	Official Action for U.S. Patent Application No. 12/541,480, mailed Jun. 14, 2012 (Attorney's Ref. No. 2943AAAB-184) 14 pages
	18	Official Action for U.S. Patent Application No. 12/541,480, mailed Feb. 11, 2013 (Attorney's Ref. No. 2943AAAB-184) 20 pages

Examiner Signature	/Samson Lemma/	Date Considered	12/16/2013
--------------------	----------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2432
				Examiner Name	Samson B. Lemma
Sheet	1	of	1	Attorney Docket Number	2943AAAB-178-DIV

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document Country Code ³ ; Number ⁴ ; Kind Code ⁵ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶

NON-PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	1	Notice of Allowance for European Patent Application No. 09167708.8, dated Nov. 22, 2013 (Attorney's Ref. No. 2943AAAB-184-EP) 5 pages
	2	Official Action for U.S. Patent Application No. 13/689,108, mailed Nov. 22, 2013 (Attorney's Ref. No. 2943AAAB-178-DIV-2) 7 pages
	3	Examiner's Answer to Appeal Brief for U.S. Patent Application No. 12/541,480, mailed Jan. 29, 2014 (Attorney's Ref. No. 2943AAAB-184) 12 pages

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Electronic Patent Application Fee Transmittal				
Application Number:		13689088		
Filing Date:		29-Nov-2012		
Title of Invention:		SECURE WIEGAND COMMUNICATIONS		
First Named Inventor/Applicant Name:		Scott B. Guthery		
Filer:		Matthew Ryan Ellsworth/Theresa Brown		
Attorney Docket Number:		2943AAAB-178-DIV		
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
Total in USD (\$)				180

Electronic Acknowledgement Receipt	
EFS ID:	18306121
Application Number:	13689088
International Application Number:	
Confirmation Number:	9927
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Scott B. Guthery
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Theresa Brown
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943AAAB-178-DIV
Receipt Date:	26-FEB-2014
Filing Date:	29-NOV-2012
Time Stamp:	13:03:02
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 180
RAM confirmation Number	15068
Deposit Account	191970
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		IDS_04.pdf	357914	yes	4
			9c3ae88e134a46793cc3c4f281b2b07b0deae8e5		
	Multipart Description/PDF files in .zip description				
	Document Description		Start		End
	Transmittal Letter		1		3
	Information Disclosure Statement (IDS) Form (SB08)		4		4
Warnings:					
Information:					
2	Non Patent Literature	2943AAAB-184-EP_NOA_11-22-2014.pdf	534129	no	5
			3ae31ea97a319efda8bad3a4dc20532aa4281650		
Warnings:					
Information:					
3	Other Reference-Patent/App/Search documents	2943AAAB-178-DIV-2_OA_11-22-2013.pdf	578360	no	7
			b88398dc8980244d43d0044624275a27a380683d		
Warnings:					
Information:					
4	Other Reference-Patent/App/Search documents	2943AAAB-184_Examiner_Answer_1-29-2014.pdf	419822	no	12
			14be34280a747ccb93e45dff1524e06ca9ec1bd7		
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	30499	no	2
			630821e557fbddea23ff58fe0667afbc34ad1a7		
Warnings:					
Information:					
Total Files Size (in bytes):			1920724		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:)	Group Art Unit: 2432
Scott B. Guthery)	Confirmation No.: 9927
Serial No.: 13/689,088)	Examiner: Samson B. Lemma
Filed: November 29, 2012)	
Atty. File No.: 2943AAAB-178-DIV)	<u>SUPPLEMENTAL</u>
Entitled: "Secure Wiegand Communications")	<u>INFORMATION DISCLOSURE</u>
)	<u>STATEMENT</u>
)	<i>Electronically Submitted</i>

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

The references cited on attached Form PTO/SB08 are being called to the attention of the Examiner.

- ☒ Copies of the cited non-patent and/or foreign references are enclosed herewith.
- ☐ Copies of the cited U.S. patents and/or patent applications are enclosed herewith.
- ☐ Copies of the cited U.S. patents/patent application publications are not enclosed in accordance with 37 C.F.R. § 1.98(a).
- ☐ Copies of the cited references are not enclosed, in accordance with 37 C.F.R. § 1.98(d), because the references were cited by or submitted to the U.S. Patent and Trademark Office in prior application Serial No. _____ filed _____, which is relied upon for an earlier filing date under 35 U.S.C. § 120.
- ☐ To the best of applicants' belief, the pertinence of the foreign-language references is believed to be summarized in the attached English abstracts and/or in the figures, although applicants do not necessarily vouch for the accuracy of the translation.
- ☐ Examiner's attention is drawn to the following related applications:
- Serial No. _____ filed _____ (Attorney Ref. No. _____)
- Serial No. _____ filed _____ (Attorney Ref. No. _____)
- ☐ Other: _____

Submission of the above information is not intended as an admission that any item is citable under the statutes or rules to support a rejection, that any item disclosed represents analogous art, or that those skilled in the art would refer to or recognize the pertinence of any reference without the benefit of hindsight, nor should an inference be drawn as to the pertinence

of the references based on the order in which they are presented. Submission of this statement should not be taken as an indication that a search has been conducted, or that no better art exists.

It is respectfully requested that the cited information be expressly considered during the prosecution of this application and the references made of record therein.

FEES

<input type="checkbox"/>	<p>37 CFR 1.97(b): No fee is believed due in connection with this submission, because the information disclosure statement submitted herewith is satisfied by one of the following conditions ("X" indicates satisfaction):</p> <p><input type="checkbox"/> Within three months of the filing date of a national application other than a continued prosecution application under 37 CFR 1.53(d), or</p> <p><input type="checkbox"/> Within three months of the date of entry of the national stage as set forth in § 1.491 in an international application, or</p> <p><input type="checkbox"/> Before the mailing date of a first Office Action on the merits, or</p> <p><input type="checkbox"/> Before the mailing of a first Office action after the filing of a request for continued examination under 37 CFR 1.114.</p> <p>Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970.</p>
<input checked="" type="checkbox"/>	<p>37 CFR 1.97(c): The information disclosure statement transmitted herewith is being filed after all the above conditions (37 CFR 1.97(b)), but before the mailing date of any one of the following conditions:</p> <p>(1) a final action under 37 C.F.R. 1.113, or</p> <p>(2) a notice of allowance under 37 C.F.R. 1.311, or</p> <p>(3) an action that otherwise closes prosecution in the application.</p> <p>This Information Disclosure Statement is accompanied by:</p> <p><input type="checkbox"/> A Certification (below) as specified by 37 C.F.R. 1.97(e). Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970.</p> <p style="text-align: center;">OR</p> <p><input checked="" type="checkbox"/> Please charge Deposit Account 19-1970 in the amount of \$180.00 for the fee set forth in 37 C.F.R. 1.17(p) for submission of an information disclosure statement. Please credit any overpayment or charge any underpayment to Deposit Account 19-1970.</p>
<input type="checkbox"/>	<p>37 CFR 1.97(d): This Information Disclosure Statement is being submitted after the period specified in 37 CFR 1.97(c).</p> <p><input type="checkbox"/> This information Disclosure Statement includes a Certification (below) as specified by 37 C.F.R. 1.97(e)</p> <p style="text-align: center;">AND</p> <p><input type="checkbox"/> Applicants hereby requests consideration of the reference(s) disclosed herein. Please charge Deposit Account 19-1970 in the amount of \$ under 37 C.F.R. 1.17(p). Please credit any overpayment or charge any underpayment to Deposit Account 19-1970. Election to pay the fee should not be taken as an indication that applicant(s) cannot execute a certification.</p>

Certification (37 C.F.R. 1.97(e))
(Applicable only if checked)

- ☐ The undersigned certifies that:
- ☐ Each item of information contained in the Information Disclosure Statement submitted herewith was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(1).
 - ☐ A copy of the communication from the foreign patent office is enclosed.

OR

- ☐ No item of information contained in the Information Disclosure Statement submitted herewith was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in the Information Disclosure Statement was known to any individual designated in 37 C.F.R. 1.56(c) more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(2).

Respectfully submitted,

SHERIDAN ROSS P.C.

By: /Matthew R. Ellsworth/
Matthew R. Ellsworth
Registration No. 56345
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: February 26, 2014

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:)	Group Art Unit: 2432
)	
GUTHERY et al.)	Examiner: LEMMA, SAMSON B.
)	
Serial No.: 13/689,088)	Confirmation No.: 9927
)	
Filed: November 29, 2012)	
)	
Atty. File No.: 2943AAAB-178-DIV)	
)	
For: "SECURE WIEGAND)	
COMMUNICATIONS")	
)	

AMENDMENT AND RESPONSE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Madam:

Applicant submits this Amendment and Response to address the Office Action having a mailing date of January 17, 2014. Submitted herewith is a Petition for one-month Extension of Time along with the requisite fees. Although no additional fees are believed due in connection with the filing this Response, please charge any additional fees deemed necessary, or credit any overpayment to Deposit Account No. 19-1970.

Please amend the above-identified patent application as follows:

Amendments to the Claims are shown in the listing of claims which begins on page 2 of this paper.

Remarks begin on page 6 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A communication method, comprising:
operating a credential reader in a first mode of operation, the credential reader comprising at least one of a microprocessor and firmware that enable the credential reader to operate in the first mode of operation;
receiving, at a communication interface of the credential reader, a message from an upstream device;
determining, by the credential reader, that the message was transmitted by the upstream device; and
based on determining that the message was transmitted by the upstream device, transitioning the credential reader from the first mode of operation to a second mode of operation, wherein the first mode comprises a non-secure Wiegand mode and wherein the second mode comprises at least one of a secure Wiegand mode and a packet-mode.
2. (Original) The method of claim 1, wherein the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol.
3. (Original) The method of claim 2, wherein the unidirectional communication protocol is the Wiegand protocol.
4. (Original) The method of claim 1, wherein the message transmitted by the upstream device comprises an alteration of a control line signal between the reader and upstream device for a predetermined amount of time.
5. (Currently Amended) The method of claim 4, wherein the predetermined amount of time is less than ~~a human-perceivable amount of time~~ 10ms.

6. (Canceled)

7. (Canceled)

8. (Currently Amended) A non-transitory computer-readable medium comprising processor-executable instructions, the processor-executable instructions comprising:

- instructions configured to cause a credential reader to operated in a first mode of operation;
- instructions configured to receive a message at the reader, the message being received from an upstream device;
- instructions configured to determine that the message was transmitted by the upstream device; and
- instructions configured to transition the credential reader from the first mode of operation to a second mode of operation, wherein the transition from the first mode of operation to the second mode of operation occurs based on determining that the message was transmitted by the upstream device, wherein the first mode comprises a non-secure Wiegand mode and wherein the second mode comprises at least one of a secure Wiegand mode and a packet-mode.

9. (Currently Amended) The non-transitory computer-readable medium of claim 8, wherein the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol.

10. (Currently Amended) The non-transitory computer-readable medium of claim 9, wherein the unidirectional communication protocol is the Wiegand protocol.

11. (Currently Amended) The non-transitory computer-readable medium of claim 8, wherein the message transmitted by the upstream device comprises an alteration

of a control line signal between the reader and upstream device for a predetermined amount of time.

12. (Currently Amended) The non-transitory computer-readable medium of claim 11, wherein the predetermined amount of time is less than ~~a human-perceivable amount of time~~ 10ms.

13. (Canceled)

14. (Canceled)

15. (Currently Amended) A credential reader comprising at least one of a microprocessor and firmware that enable the reader to operate in a first mode of operation, receive a message from an upstream device, determine that the message was transmitted by the upstream device, and, in response thereto transition the credential reader from the first mode of operation to a second mode of operation, wherein the transition from the first mode of operation to the second mode of operation occurs based on determining that the message was transmitted by the upstream device, wherein the first mode comprises a non-secure Wiegand mode and wherein the second mode comprises at least one of a secure Wiegand mode and a packet-mode.

16. (Original) The credential reader of claim 15, wherein the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol, and wherein the unidirectional communication protocol is the Wiegand protocol.

17. (Original) The credential reader of claim 15, wherein the message transmitted by the upstream device comprises an alteration of a control line signal between the reader and upstream device for a predetermined amount of time.

18. (Currently Amended) The credential reader of claim 17, wherein the
predetermined amount of time is less than a human-perceivable amount of time 10ms.

19. (Canceled)

20. (Canceled)

REMARKS

The above-identified patent application has been reviewed in light of the Examiner's Action dated January 17, 2014. Claims 1, 5, 8-12, 15, and 18 have been amended and claims 6-7, 13-14, and 19-20 have been canceled without intending to abandon or to dedicate to the public any patentable subject matter. No claims have been added. Accordingly, Claims 1-5, 8-12, and 15-18 are now pending. As set forth herein, reconsideration and withdrawal of the rejections of the claims are respectfully requested.

Double Patenting

Claims 1-20 have been rejected under the doctrine of obviousness-type double patenting as being unpatentable over claims 1-27 of U.S. Patent 8,358,783. Applicant respectfully requests that the obviousness-type double patenting rejections be held in abeyance until such time as the other rejections of the claims have been overcome and the application is otherwise in condition for allowance.

Rejections under 35 U.S.C. 112

Claims 5, 12, and 18 have been rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. As discussed in the application as-filed, a "human perceivable amount of time" can vary based on a number of factors. However, to expedite prosecution of the instant application, claims 5, 12, and 18 have been amended to replace the term "human perceivable amount of time" with a specific amount of time that is generally agreed to be short enough so as to be subliminal or not perceived at all as described in the originally-filed application at page 30, lines 6-15.

For at least the above reasons, it is respectfully submitted that the rejections of the claims under 35 U.S.C. 112 should be reconsidered and withdrawn.

Rejections under 35 U.S.C. 101

Claims 1-14 have been rejected under 35 U.S.C. 101 as being directed toward non-statutory subject matter. Claim 1 has been amended herein to recite, *inter alia*, the credential reader comprises at least one of a microprocessor and firmware. Claim 1 has

also been amended to recite that the message received at the credential reader is received at a communication interface. The addition of these limitations is believed to place claim 1 and the dependent claims therefrom into compliance with the requirements of 35 U.S.C. 101 due to the clarification that the credential reader is a machine comprising specific hardware components. Thus, the method of claim 1 is executed by a machine. Claim 8 has been amended to recite a non-transitory computer-readable medium. It is believed that the amendments made to claims 1 and 8 now place the claims into compliance with the requirements of 35 U.S.C. 101.

To the extent that claim 1 now recites a credential reader having specific hardware components and claim 8 now recites a non-transitory computer-readable medium, it is respectfully submitted that the rejections of the claims under 35 U.S.C. 101 should be reconsidered and withdrawn.

Allowable subject matter

Applicant would like to thank the Examiner for the indication that claims 6-7, 13-14, and 19-20 are allowable but for their dependence from a rejected independent claim. It is respectfully submitted that claims 1, 8, and 15 have been amended to include the allowable subject matter of claims 6-7, 13-14, and 19-20, respectively.

Because claims 1, 8, and 15 have been amended to include the allowable features of claims 6-7, 13-14, and 19-20, it is respectfully submitted that the rejections of claims 1-5, 8-12, and 15-18 as being anticipated by EP1760985 to Davis should be reconsidered and withdrawn.

Based on the foregoing, Applicant believes that all pending claims are in condition for allowance and such disposition is respectfully requested. In the event that a telephone conversation would further prosecution and/or expedite allowance, the Examiner is invited to contact the undersigned.

Respectfully submitted,

SHERIDAN ROSS P.C.

Date: April 21, 2014

By: /Matthew R. Ellsworth/
Matthew R. Ellsworth
Reg. No. 56,345
Telephone: 303-863-2989

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)		Docket Number (Optional) 2943AAAB-178-DIV																																		
Application Number 13/689,088	Filed 2012-11-29																																			
For SECURE WIEGAND COMMUNICATIONS																																				
Art Unit 2432	Examiner LEMMA, SAMSON B.																																			
<p>This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.</p> <p>The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):</p> <table style="width: 100%; border-collapse: collapse;"><thead><tr><th></th><th style="text-align: center;"><u>Fee</u></th><th style="text-align: center;"><u>Small Entity Fee</u></th><th style="text-align: center;"><u>Micro Entity Fee</u></th><th></th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/> One month (37 CFR 1.17(a)(1))</td><td style="text-align: center;">\$200</td><td style="text-align: center;">\$100</td><td style="text-align: center;">\$50</td><td style="text-align: right;">\$ <u>200</u></td></tr><tr><td><input type="checkbox"/> Two months (37 CFR 1.17(a)(2))</td><td style="text-align: center;">\$600</td><td style="text-align: center;">\$300</td><td style="text-align: center;">\$150</td><td style="text-align: right;">\$ _____</td></tr><tr><td><input type="checkbox"/> Three months (37 CFR 1.17(a)(3))</td><td style="text-align: center;">\$1,400</td><td style="text-align: center;">\$700</td><td style="text-align: center;">\$350</td><td style="text-align: right;">\$ _____</td></tr><tr><td><input type="checkbox"/> Four months (37 CFR 1.17(a)(4))</td><td style="text-align: center;">\$2,200</td><td style="text-align: center;">\$1,100</td><td style="text-align: center;">\$550</td><td style="text-align: right;">\$ _____</td></tr><tr><td><input type="checkbox"/> Five months (37 CFR 1.17(a)(5))</td><td style="text-align: center;">\$3,000</td><td style="text-align: center;">\$1,500</td><td style="text-align: center;">\$750</td><td style="text-align: right;">\$ _____</td></tr></tbody></table> <p><input type="checkbox"/> Applicant asserts small entity status. See 37 CFR 1.27.</p> <p><input type="checkbox"/> Applicant certifies micro entity status. See 37 CFR 1.29. Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.</p> <p><input type="checkbox"/> A check in the amount of the fee is enclosed.</p> <p><input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.</p> <p><input type="checkbox"/> The Director has already been authorized to charge fees in this application to a Deposit Account.</p> <p><input checked="" type="checkbox"/> The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number <u>19-1970</u>.</p> <p><input checked="" type="checkbox"/> Payment made via EFS-Web.</p> <p>WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.</p> <p>I am the</p> <p><input type="checkbox"/> applicant.</p> <p><input checked="" type="checkbox"/> attorney or agent of record. Registration number <u>56,345</u>.</p> <p><input type="checkbox"/> attorney or agent acting under 37 CFR 1.34. Registration number _____.</p> <table style="width: 100%; border-collapse: collapse;"><tr><td style="width: 50%; padding: 5px;"><u>/Matthew R. Ellsworth/</u> Signature</td><td style="width: 50%; padding: 5px;"><u>2014-04-21</u> Date</td></tr><tr><td style="padding: 5px;"><u>Matthew R. Ellsworth</u> Typed or printed name</td><td style="padding: 5px;"><u>(303) 863-9700</u> Telephone Number</td></tr></table> <p>NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.</p>				<u>Fee</u>	<u>Small Entity Fee</u>	<u>Micro Entity Fee</u>		<input checked="" type="checkbox"/> One month (37 CFR 1.17(a)(1))	\$200	\$100	\$50	\$ <u>200</u>	<input type="checkbox"/> Two months (37 CFR 1.17(a)(2))	\$600	\$300	\$150	\$ _____	<input type="checkbox"/> Three months (37 CFR 1.17(a)(3))	\$1,400	\$700	\$350	\$ _____	<input type="checkbox"/> Four months (37 CFR 1.17(a)(4))	\$2,200	\$1,100	\$550	\$ _____	<input type="checkbox"/> Five months (37 CFR 1.17(a)(5))	\$3,000	\$1,500	\$750	\$ _____	<u>/Matthew R. Ellsworth/</u> Signature	<u>2014-04-21</u> Date	<u>Matthew R. Ellsworth</u> Typed or printed name	<u>(303) 863-9700</u> Telephone Number
	<u>Fee</u>	<u>Small Entity Fee</u>	<u>Micro Entity Fee</u>																																	
<input checked="" type="checkbox"/> One month (37 CFR 1.17(a)(1))	\$200	\$100	\$50	\$ <u>200</u>																																
<input type="checkbox"/> Two months (37 CFR 1.17(a)(2))	\$600	\$300	\$150	\$ _____																																
<input type="checkbox"/> Three months (37 CFR 1.17(a)(3))	\$1,400	\$700	\$350	\$ _____																																
<input type="checkbox"/> Four months (37 CFR 1.17(a)(4))	\$2,200	\$1,100	\$550	\$ _____																																
<input type="checkbox"/> Five months (37 CFR 1.17(a)(5))	\$3,000	\$1,500	\$750	\$ _____																																
<u>/Matthew R. Ellsworth/</u> Signature	<u>2014-04-21</u> Date																																			
<u>Matthew R. Ellsworth</u> Typed or printed name	<u>(303) 863-9700</u> Telephone Number																																			

☐ * Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal				
Application Number:	13689088			
Filing Date:	29-Nov-2012			
Title of Invention:	SECURE WIEGAND COMMUNICATIONS			
First Named Inventor/Applicant Name:	Scott B. Guthery			
Filer:	Matthew Ryan Ellsworth/Leslie Roberts			
Attorney Docket Number:	2943AAAB-178-DIV			
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with \$0 paid	1251	1	200	200

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				200

Electronic Acknowledgement Receipt	
EFS ID:	18819299
Application Number:	13689088
International Application Number:	
Confirmation Number:	9927
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Scott B. Guthery
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Leslie Roberts
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943AAAB-178-DIV
Receipt Date:	21-APR-2014
Filing Date:	29-NOV-2012
Time Stamp:	18:09:11
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 200
RAM confirmation Number	4761
Deposit Account	191970
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		AMEND_01.pdf	111860 8f40de8fa25089318407c23df34f69c8b9a56f94	yes	8
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment/Req. Reconsideration-After Non-Final Reject		1	1	
	Claims		2	5	
	Applicant Arguments/Remarks Made in an Amendment		6	8	
Warnings:					
Information:					
2	Extension of Time	EXTENSION_OF_TIME.pdf	163162 8f349f4126885f3be1e6d4940ce533630fcafc2	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30757 0cc731d6348a125676ec53d1812ef9e830c99c39	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			305779		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 13/689,088	Filing Date 11/29/2012	<input type="checkbox"/> To be Mailed
ENTITY: <input checked="" type="checkbox"/> LARGE <input type="checkbox"/> SMALL <input type="checkbox"/> MICRO							
APPLICATION AS FILED – PART I							
(Column 1)		(Column 2)					
FOR	NUMBER FILED	NUMBER EXTRA			RATE (\$)	FEE (\$)	
<input type="checkbox"/> BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A			N/A		
<input type="checkbox"/> SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A			N/A		
<input type="checkbox"/> EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A			N/A		
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*			X \$ =		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*			X \$ =		
<input type="checkbox"/> APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.					TOTAL		
APPLICATION AS AMENDED – PART II							
(Column 1)		(Column 2)		(Column 3)			
AMENDMENT	04/21/2014	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(j))	* 14	Minus	** 20	= 0	X \$80 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X \$420 =	0
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))						
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	
					0		
(Column 1)		(Column 2)		(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(j))	*	Minus	**	=	X \$ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$ =	
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))						
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	
<p>* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.</p> <p>** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".</p> <p>*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".</p> <p>The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.</p>							

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/689,088	11/29/2012	Scott B. Guthery	2943AAB-178-DIV	9927
22442	7590	05/22/2014	EXAMINER	
Sheridan Ross PC 1560 Broadway Suite 1200 Denver, CO 80202			LEMMA, SAMSON B	
			ART UNIT	PAPER NUMBER
			2432	
			NOTIFICATION DATE	DELIVERY MODE
			05/22/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

c-docket@sheridanross.com

Office Action Summary	Application No. 13/689,088	Applicant(s) GUTHERY ET AL.	
	Examiner SAMSON LEMMA	Art Unit 2432	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on 04/21/2014.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ____.

2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.

3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.

4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☒ Claim(s) 1-5, 8-12 and 15-18 is/are pending in the application.
5a) Of the above claim(s) ____ is/are withdrawn from consideration.

6) ☐ Claim(s) ____ is/are allowed.

7) ☒ Claim(s) 1-5, 8-12 and 15-18 is/are rejected.

8) ☐ Claim(s) ____ is/are objected to.

9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10) ☐ The specification is objected to by the Examiner.

11) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some** c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. ____.

3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date ____.

3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.

4) ☐ Other: ____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on 04/21/2014. Claims 1-5, 8-12 and 15-18 are pending. Claims 1, 8 and 15 are independent. Each independent claim is amended.
2. The amendment made to each independent overcomes the prior art 102, rejection set forth in the previous office action. Thus, this particular rejection is withdrawn.
3. The amendment made to claims 5, 12 and 18 overcomes the prior art 112, rejection set forth in the previous office action. Thus, this particular rejection is withdrawn.
4. The double patent rejection set forth in the previous office action is maintained.

Response to Arguments

5. Applicant's arguments/remarks filed on 04/21/2014 with respect to claims 1-5, 8-12 and 15-18 have been fully considered and are persuasive. The amendment made to each independent overcomes the prior art 102, rejection set forth in the previous office action. Thus, this particular rejection is withdrawn.

Double Patenting

6. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).
A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).
Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).
7. Claims 1-5, 8-12 and 15-18 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-27 of the U.S. Patent No. 8,358,783 B2 (hereinafter refereed as '783 Patent.) Although the conflicting claims are not identical, they are not patentably distinct from each other.

The following is referring to the independent claims 1, 8 and 15

- As per independent claims 1, 8 and 15,
Independent claim 1, 8 and 15 of the instant application and claim 1, and 18, of the '783 patent recite similar limitation. The above independent claim, namely independent claims 1, 8 and 15 of the instant/present application would have been obvious over independent claims 1 and 18, of

the '783 patent because each and every element of the above independent claims 1, 8 and 15 of the present application is anticipated by the corresponding independent claims 1 and 18 of the '783 patent.

The following is applicable to the dependent claims 2-5, 9-12, and 16-18

- As per dependent claims 2-5, 9-12 and 16-18, Dependent Claims 2-5, 9-12 and 16-18 of the instant application and claims 2-17 and 19-27 of the '783 patent further recite similar/equivalent limitation of the same subject matter. Thus, the above dependent claims, namely dependent claims 2-5, 9-12 and 16-18 of the instant/present application would have been obvious over dependent claims 2-17 and 19-27, of the '783 patent because each and every element of the above dependent claims 2-5, 9-12 and 16-18, of the present application is anticipated by the corresponding dependent claims 2-17 and 19-27 of the '783 patent.

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened

statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.


Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/SAMSON LEMMA/

Primary Examiner, Art Unit 2432

Application/Control Number: 13/689,088
Art Unit: 2432

Page 6

Search Notes 	Application/Control No. 13689088	Applicant(s)/Patent Under Reexamination GUTHERY ET AL.
	Examiner SAMSON LEMMA	Art Unit 2432

CPC- SEARCHED		
Symbol	Date	Examiner


CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	5, 14	5/16/2014	SL
380	270, 260 and 46	5/16/2014	SL

SEARCH NOTES		
Search Notes	Date	Examiner
713/\$, 726/\$ (With text Search)	5/16/2014	SL
EAST (Search is Updated)	5/16/2014	SL
NPL (IEEE, ACM DIGITAL LIBRARY, GOOGLE, GOOGLE PATENT, Google Scholar, Scirus....)	5/16/2014	SL
INVENTOR NAME SEARCH	5/16/2014	SL

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

--	--

<i>Index of Claims</i> 	Application/Control No. 13689088	Applicant(s)/Patent Under Reexamination GUTHERY ET AL.
	Examiner SAMSON LEMMA	Art Unit 2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant				<input type="checkbox"/> CPA		<input type="checkbox"/> T.D.		<input type="checkbox"/> R.1.47	
CLAIM		DATE							
Final	Original	12/14/2013	05/16/2014						
	1	✓	✓						
	2	✓	✓						
	3	✓	✓						
	4	✓	✓						
	5	✓	✓						
	6	O	-						
	7	O	-						
	8	✓	✓						
	9	✓	✓						
	10	✓	✓						
	11	✓	✓						
	12	✓	✓						
	13	O	-						
	14	O	-						
	15	✓	✓						
	16	✓	✓						
	17	✓	✓						
	18	✓	✓						
	19	O	-						
	20	O	-						

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:)	Group Art Unit: 2432
)	
GUTHERY et al.)	Examiner: LEMMA, SAMSON B.
)	
Serial No.: 13/689,088)	Confirmation No.: 9927
)	
Filed: November 29, 2012)	
)	
Atty. File No.: 2943AAAB-178-DIV)	
)	
For: "SECURE WIEGAND)	
COMMUNICATIONS")	
)	

AMENDMENT AND RESPONSE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Madam:

Applicant submits this Amendment and Response to address the final Office Action having a mailing date of May 22, 2014. Although no fees are believed due in connection with the filing this Response, please charge any additional fees deemed necessary, or credit any overpayment to Deposit Account No. 19-1970.

Please amend the above-identified patent application as follows:

Amendments to the Claims are shown in the listing of claims which begins on page 2 of this paper.

Remarks begin on page 6 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) A communication method, comprising:
operating a credential reader in a first mode of operation, the credential reader comprising at least one of a microprocessor and firmware that enable the credential reader to operate in the first mode of operation;
receiving, at a communication interface of the credential reader, a message from an upstream device;
determining, by the credential reader, that the message was transmitted by the upstream device; and
based on determining that the message was transmitted by the upstream device, transitioning the credential reader from the first mode of operation to a second mode of operation, wherein the first mode comprises a non-secure Wiegand mode and wherein the second mode comprises at least one of a secure Wiegand mode and a packet-mode.
2. (Original) The method of claim 1, wherein the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol.
3. (Original) The method of claim 2, wherein the unidirectional communication protocol is the Wiegand protocol.
4. (Original) The method of claim 1, wherein the message transmitted by the upstream device comprises an alteration of a control line signal between the reader and upstream device for a predetermined amount of time.
5. (Previously Presented) The method of claim 4, wherein the predetermined amount of time is less than 10ms.

6. (Canceled)

7. (Canceled)

8. (Previously Presented) A non-transitory computer-readable medium comprising processor-executable instructions, the processor-executable instructions comprising:

instructions configured to cause a credential reader to operated in a first mode of operation;

instructions configured to receive a message at the reader, the message being received from an upstream device;

instructions configured to determine that the message was transmitted by the upstream device; and

instructions configured to transition the credential reader from the first mode of operation to a second mode of operation, wherein the transition from the first mode of operation to the second mode of operation occurs based on determining that the message was transmitted by the upstream device, wherein the first mode comprises a non-secure Wiegand mode and wherein the second mode comprises at least one of a secure Wiegand mode and a packet-mode.

9. (Previously Presented) The non-transitory computer-readable medium of claim 8, wherein the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol.

10. (Previously Presented) The non-transitory computer-readable medium of claim 9, wherein the unidirectional communication protocol is the Wiegand protocol.

11. (Previously Presented) The non-transitory computer-readable medium of claim 8, wherein the message transmitted by the upstream device comprises an alteration

of a control line signal between the reader and upstream device for a predetermined amount of time.

12. (Previously Presented) The non-transitory computer-readable medium of claim 11, wherein the predetermined amount of time is less than 10ms.

13. (Canceled)

14. (Canceled)

15. (Previously Presented) A credential reader comprising at least one of a microprocessor and firmware that enable the reader to operate in a first mode of operation, receive a message from an upstream device, determine that the message was transmitted by the upstream device, and, in response thereto transition the credential reader from the first mode of operation to a second mode of operation, wherein the transition from the first mode of operation to the second mode of operation occurs based on determining that the message was transmitted by the upstream device, wherein the first mode comprises a non-secure Wiegand mode and wherein the second mode comprises at least one of a secure Wiegand mode and a packet-mode.

16. (Original) The credential reader of claim 15, wherein the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol, and wherein the unidirectional communication protocol is the Wiegand protocol.

17. (Original) The credential reader of claim 15, wherein the message transmitted by the upstream device comprises an alteration of a control line signal between the reader and upstream device for a predetermined amount of time.

18. (Previously Presented) The credential reader of claim 17, wherein the predetermined amount of time is less than 10ms.

19. (Canceled)

20. (Canceled)

REMARKS

The above-identified patent application has been reviewed in light of the Examiner's Action dated May 22, 2014. No claims have been amended, canceled, or added. Accordingly, Claims 1-5, 8-12, and 15-18 are now pending. As set forth herein, reconsideration and withdrawal of the rejections of the claims are respectfully requested.

Double Patenting

The Examiner has maintained the double patenting rejections based on U.S. Patent No. 8,358,783. Applicant has filed concurrently herewith a Terminal Disclaimer in compliance with 37 CFR 1.321(c). Accordingly, it is respectfully submitted that the double patenting rejection has been overcome.

Based on the foregoing, Applicant believes that all pending claims are in condition for allowance and such disposition is respectfully requested. In the event that a telephone conversation would further prosecution and/or expedite allowance, the Examiner is invited to contact the undersigned.

Respectfully submitted,

SHERIDAN ROSS P.C.

Date: July 23, 2014

By: /Matthew R. Ellsworth/
Matthew R. Ellsworth
Reg. No. 56,345
Telephone: 303-863-2989

**TERMINAL DISCLAIMER TO OBTAIN A DOUBLE PATENTING
REJECTION OVER A "PRIOR" PATENT**

Docket Number (Optional)
2943AAAB-178-DIV

In re Application of: GUTHERY et al.

Application No.: 13/689,088

Filed: November 29, 2012

For: SECURE WIEGAND COMMUNICATIONS

The applicant, Assa Abloy AB, owner of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 8,358,783 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The applicant hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the applicant does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ The undersigned is the applicant. If the applicant is an assignee, the undersigned is authorized to act on behalf of the assignee.

I hereby acknowledge that any willful false statements made are punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

2. ☒ The undersigned is an attorney or agent of record. Reg. No. 56,345

/Matthew R. Ellsworth/
Signature

2014-07-23
Date

Matthew R. Ellsworth
Typed or printed name

Attorney
Title

(303) 863-9700
Telephone Number

- ☒ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal				
Application Number:		13689088		
Filing Date:		29-Nov-2012		
Title of Invention:		SECURE WIEGAND COMMUNICATIONS		
First Named Inventor/Applicant Name:		Scott B. Guthery		
Filer:		Matthew Ryan Ellsworth/Leslie Roberts		
Attorney Docket Number:		2943AAAB-178-DIV		
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Statutory or Terminal Disclaimer	1814	1	160	160
Total in USD (\$)				160

Electronic Acknowledgement Receipt	
EFS ID:	19663004
Application Number:	13689088
International Application Number:	
Confirmation Number:	9927
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Scott B. Guthery
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Leslie Roberts
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943AAAB-178-DIV
Receipt Date:	23-JUL-2014
Filing Date:	29-NOV-2012
Time Stamp:	16:26:31
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 160
RAM confirmation Number	3011
Deposit Account	191970
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		AMEND_02.pdf	88136	yes	6
			23022c236f3e0fe5d4726d93ec1375be6c7dd5fd		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Response After Final Action		1	1	
	Claims		2	5	
	Applicant Arguments/Remarks Made in an Amendment		6	6	
Warnings:					
Information:					
2	Terminal Disclaimer Filed	TERMINAL_DISCLAIMER.pdf	160301	no	2
			70d42b7cfb87e8d256b0b786ad340b626cd168f3		
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30406	no	2
			5fe444b7fd29629ecce63fa36ee9676d2e049bda		
Warnings:					
Information:					
Total Files Size (in bytes):			278843		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.


New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 13/689,088		Filing Date 11/29/2012		<input type="checkbox"/> To be Mailed	
ENTITY: <input checked="" type="checkbox"/> LARGE <input type="checkbox"/> SMALL <input type="checkbox"/> MICRO										
APPLICATION AS FILED – PART I										
(Column 1)		(Column 2)								
FOR	NUMBER FILED	NUMBER EXTRA		RATE (\$)		FEE (\$)				
<input type="checkbox"/> BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A						
<input type="checkbox"/> SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A						
<input type="checkbox"/> EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A						
TOTAL CLAIMS (37 CFR 1.16(j))	minus 20 =	*		X \$ =						
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		X \$ =						
<input type="checkbox"/> APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).									
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL						
APPLICATION AS AMENDED – PART II										
(Column 1)		(Column 2)		(Column 3)						
AMENDMENT	07/23/2014	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(j))	* 14	Minus	** 20	= 0	X \$80 =		0		
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0	X \$420 =		0		
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))									
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE		0		
(Column 1)		(Column 2)		(Column 3)						
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(j))	*	Minus	**	=	X \$ =				
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$ =				
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))									
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE				
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.										

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Application Number 	Application/Control No.	Applicant(s)/Patent under Reexamination	
	13/689,088	GUTHERY ET AL.	
Document Code - DISQ		Internal Document – DO NOT MAIL	

TERMINAL DISCLAIMER	<input type="checkbox"/> APPROVED	<input checked="" type="checkbox"/> DISAPPROVED
Date Filed : July 23, 2014	This patent is subject to a Terminal Disclaimer	

Approved/Disapproved by:

Henry D Jefferson

[x] The person who signed the terminal disclaimer:

[] failed to state his/her capacity to sign for the business/organization entity. (See FP 14.28.)

[] is not recognized as an officer of the assignee. (See FP 14.29.)

[x] does not have power of attorney, and thus, is not of record. (See FP 14.29.01.)

(Note: Power of Attorney (PoA) can be given to a customer number, wherein all practitioners listed under the customer number have PoA. If PoA is established by a list of practitioners, the list must not comprise more than 10 practitioners. A representative of the assignee, who is not the attorney of record, cannot sign the TD unless it is established that the representative is a party authorized to act on behalf of the assignee.)



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/689,088	11/29/2012	Scott B. Guthery	2943AAB-178-DIV	9927
22442	7590	08/06/2014	EXAMINER	
Sheridan Ross PC 1560 Broadway Suite 1200 Denver, CO 80202			LEMMA, SAMSON B	
			ART UNIT	PAPER NUMBER
			2432	
			NOTIFICATION DATE	DELIVERY MODE
			08/06/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

c-docket@sheridanross.com

Advisory Action Before the Filing of an Appeal Brief	Application No. 13/689,088	Applicant(s) GUTHERY ET AL.	
	Examiner SAMSON LEMMA	Art Unit 2432	AIA (First Inventor to File) Status No

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 23 July 2014 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.
NO NOTICE OF APPEAL FILED

1. ☐ The reply was filed after a final rejection. No Notice of Appeal has been filed. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114 if this is a utility or plant application. Note that RCEs are not permitted in design applications. The reply must be filed within one of the following time periods:

a) ☒ The period for reply expires 6 months from the mailing date of the final rejection.

b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action; or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

c) ☐ A prior Advisory Action was mailed more than 3 months after the mailing date of the final rejection in response to a first after-final reply filed within 2 months of the mailing date of the final rejection. The current period for reply expires _____ months from the mailing date of the prior Advisory Action or SIX MONTHS from the mailing date of the final rejection, whichever is earlier.

Examiner Note: If box 1 is checked, check either box (a), (b) or (c). ONLY CHECK BOX (b) WHEN THIS ADVISORY ACTION IS THE FIRST RESPONSE TO APPLICANT'S FIRST AFTER-FINAL REPLY WHICH WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. ONLY CHECK BOX (c) IN THE LIMITED SITUATION SET FORTH UNDER BOX (c). See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) or (c) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendments filed after a final rejection, but prior to the date of filing a brief, will not be entered because

a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);

b) ☐ They raise the issue of new matter (see NOTE below);

c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or

d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. ☐ Applicant's reply has overcome the following rejection(s): _____.

6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): (a) ☐ will not be entered, or (b) ☒ will be entered, and an explanation of how the new or amended claims would be rejected is provided below or appended.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

9. ☐ The affidavit or other evidence filed after final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

10. ☐ The affidavit or other evidence filed after the date of filing the Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

11. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

12. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:
See Continuation Sheet.

13. ☒ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____

14. ☐ Other: _____.

STATUS OF CLAIMS

15. The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: _____.

Claim(s) objected to: _____.

Claim(s) rejected: 1-5,8-12 and 15-18.

Claim(s) withdrawn from consideration: _____.

	/SAMSON LEMMA/ Primary Examiner, Art Unit 2432
--	---

Continuation of 11. does NOT place the application in condition for allowance because: Examiner asserts that the Terminal Disclaimer filed on 07/23/2014 is disapproved. Enclose herewith is the copy of the reason why it is not approved. Thus the double patent rejection set forth in the previous final office action is maintained.
Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969). A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b). Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-5, 8-12 and 15-18 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-27 of the U.S. Patent No. 8,358,783 B2 (hereinafter referred as '783 Patent.) Although the conflicting claims are not identical, they are not patentably distinct from each other. The following is referring to the independent claims 1, 8 and 15

As per independent claims 1,8 and 15,

Independent claim 1 8 and 15 of the instant application and claim 1, and 18, of the '783 patent recite similar limitation. The above independent claim, namely independent claims 1, 8 and 15 of the instant/present application would have been obvious over independent claims 1 and 18, of the '783 patent because each and every element of the above independent claims 1, 8 and 15 of the present application is anticipated by the corresponding independent claims 1 and 18 of the '783 patent. The following is applicable to the dependent claims 2-5, 9-12, and 16-18

As per dependent claims 2-5, 9-12 and 16-18,

Dependent Claims 2-5, 9-12 and 16-18 of the instant application and claims 2-17 and 19-27 of the '783 patent further recite similar/equivalent limitation of the same subject matter. Thus, the above dependent claims, namely dependent claims 2-5, 9-12 and 16-18 of the instant/present application would have been obvious over dependent claims 2-17 and 19-27, of the '783 patent because each and every element of the above dependent claims 2-5, 9-12 and 16-18, of the present application is anticipated by the corresponding dependent claims 2-17 and 19-27 of the '783 patent.

Receipt date: 02/26/2014

13689088 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2432
				Examiner Name	Samson B. Lemma
Sheet	1	of	1	Attorney Docket Number	2943AAAB-178-DIV

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document Country Code ³ ; Number ⁴ ; Kind Code ⁵ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶

NON-PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	1	Notice of Allowance for European Patent Application No. 09167708.8, dated Nov. 22, 2013 (Attorney's Ref. No. 2943AAAB-184-EP) 5 pages
	2	Official Action for U.S. Patent Application No. 13/689,108, mailed Nov. 22, 2013 (Attorney's Ref. No. 2943AAAB-178-DIV-2) 7 pages
	3	Examiner's Answer to Appeal Brief for U.S. Patent Application No. 12/541,480, mailed Jan. 29, 2014 (Attorney's Ref. No. 2943AAAB-184) 12 pages

Examiner Signature	/Samson Lemma/	Date Considered	07/30/2014
--------------------	----------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:)	Group Art Unit: 2432
)	
GUTHERY et al.)	Examiner: LEMMA, SAMSON B.
)	
Serial No.: 13/689,088)	Confirmation No.: 9927
)	
Filed: November 29, 2012)	
)	
Atty. File No.: 2943AAAB-178-DIV)	
)	
For: "SECURE WIEGAND)	
COMMUNICATIONS")	
)	

AMENDMENT AND RESPONSE

Commissioner for Patents	Please Enter.
P.O. Box 1450	07/30/2014.
Alexandria, VA 22313-1450	


Madam: /S.L./

Applicant submits this Amendment and Response to address the final Office Action having a mailing date of May 22, 2014. Although no fees are believed due in connection with the filing this Response, please charge any additional fees deemed necessary, or credit any overpayment to Deposit Account No. 19-1970.

Please amend the above-identified patent application as follows:

Amendments to the Claims are shown in the listing of claims which begins on page 2 of this paper.

Remarks begin on page 6 of this paper.

Application Number 	Application/Control No.	Applicant(s)/Patent under Reexamination	
	13/689,088	GUTHERY ET AL.	
Document Code - DISQ		Internal Document – DO NOT MAIL	

TERMINAL DISCLAIMER	<input type="checkbox"/> APPROVED	<input checked="" type="checkbox"/> DISAPPROVED
Date Filed : July 23, 2014	This patent is subject to a Terminal Disclaimer	

Approved/Disapproved by:

Henry D Jefferson

[x] The person who signed the terminal disclaimer:

[] failed to state his/her capacity to sign for the business/organization entity. (See FP 14.28.)

[] is not recognized as an officer of the assignee. (See FP 14.29.)

[x] does not have power of attorney, and thus, is not of record. (See FP 14.29.01.)

(Note: Power of Attorney (PoA) can be given to a customer number, wherein all practitioners listed under the customer number have PoA. If PoA is established by a list of practitioners, the list must not comprise more than 10 practitioners. A representative of the assignee, who is not the attorney of record, cannot sign the TD unless it is established that the representative is a party authorized to act on behalf of the assignee.)

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	13/689,088
Filing Date	2012-11-29
First Named Inventor	Scott B. Guthery
Title	SECURE WIEGAND COMMUNICATIONS
Art Unit	2432
Examiner Name	LEMMA, SAMSON B.
Attorney Docket Number	2943AAAB-178-DIV

SIGNATURE of Applicant or Patent Practitioner

Signature	/Matthew R. Ellsworth/	Date (Optional)	2014-08-11
Name	Matthew R. Ellsworth	Registration Number	56,345
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			
<p>NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.</p>			
<input type="checkbox"/> *Total of _____ forms are submitted.			

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

GENERAL POWER OF ATTORNEY

On behalf of Assa Abloy AB, a corporation having a principal place of business at Klarabergsviadukten 90 - P.O. Box 70340, SE-107 23 Stockholm, Sweden, we, Johan Molin as Board Member and Managing Director of Assa Abloy AB, and Tomas Eliasson as authorized signatory and CFO of Assa Abloy AB, hereby appoint:

SHERIDAN ROSS P.C., 1560 Broadway, Suite 1200, Denver, Colorado 80202-5141, telephone number 303/863-9700, Customer No. 22442, as attorneys and agents for ASSA ABLOY AB before the U.S. Patent Office, and all competent International Authorities in connection with any and all U.S. patent applications filed on behalf of ASSA ABLOY AB, with full powers of substitution, association and revocation, and to transact all business in the U.S. Patent and Trademark Office and all international patent offices in connection with any patent application claiming priority to a U.S. patent application.

Date: 29 January 2007

By: J. Molin

Print Name: JOHAN MOLIN

Title: Board Member and Managing Director

Date: 29 January 2007

By: T. Eliasson

Print Name: TOMAS ELIASSON

Title: CFO, Executive Vice President,
authorized signatory

J:\2943\GENPOA.DOC

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Assa Abloy AB

Application No./Patent No.: 13/689,088

Filed/Issue Date: 2012-11-29

Titled: SECURE WIEGAND COMMUNICATIONS

Assa Abloy AB, a Corporation

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☒ The assignee of the entire right, title, and interest.
2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):
- ☐ The extent (by percentage) of its ownership interest is ____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.
- ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

- A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 023275, Frame 0223, or for which a copy thereof is attached.
- B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:
1. From: _____ To: _____
- The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.
2. From: _____ To: _____
- The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

[Page 1 of 2]

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Matthew R. Ellsworth/

2014-08-11

Signature

Date

Matthew R. Ellsworth

56,345

Printed or Typed Name

Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt	
EFS ID:	19832770
Application Number:	13689088
International Application Number:	
Confirmation Number:	9927
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Scott B. Guthery
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Leslie Roberts
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943AAAB-178-DIV
Receipt Date:	11-AUG-2014
Filing Date:	29-NOV-2012
Time Stamp:	16:42:29
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	POA.pdf	223687 8d7f31288151a37d1ae1435c2da5c192b94d8390	no	2

Warnings:

Information:

2	Assignee showing of ownership per 37 CFR 3.73.	STATEMENT.pdf	117743 e0c8ec982077aa2ce42129239937e46162447826	no	3
Warnings:					
Information:					
Total Files Size (in bytes):				341430	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

Doc Code: DIST.E.FILE Document Description: Electronic Terminal Disclaimer - Filed		PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce	
Electronic Petition Request	TERMINAL DISCLAIMER TO OBIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT		
Application Number	13689088		
Filing Date	29-Nov-2012		
First Named Inventor	Scott Guthery		
Attorney Docket Number	2943AAAB-178-DIV		
Title of Invention	SECURE WIEGAND COMMUNICATIONS		
<input checked="" type="checkbox"/> Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action <input checked="" type="checkbox"/> This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.			
Owner		Percent Interest	
ASSA ABLOY AB		100%	
<p>The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)</p> <p>8358783</p> <p>as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.</p> <p>In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:</p> <ul style="list-style-type: none"> - expires for failure to pay a maintenance fee; - is held unenforceable; - is found invalid by a court of competent jurisdiction; - is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321; - has all claims canceled by a reexamination certificate; - is reissued; or - is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer. <p><input type="radio"/> Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.</p>			

<input checked="" type="radio"/> I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.	
<p>THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES</p> <p>I certify, in accordance with 37 CFR 1.4(d)(4) that I am:</p> <p><input checked="" type="radio"/> An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application</p> <p style="margin-left: 40px;">Registration Number <u>56345</u></p> <p><input type="radio"/> A sole inventor</p> <p><input type="radio"/> A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application</p> <p><input type="radio"/> A joint inventor; all of whom are signing this request</p>	
Signature	/Matthew R. Ellsworth/
Name	Matthew R. Ellsworth

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
 Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Doc Code: DISQ.E.FILE

Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 13689088

Filing Date: 29-Nov-2012

Applicant/Patent under Reexamination: Guthery et al.

Electronic Terminal Disclaimer filed on August 14, 2014

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt	
EFS ID:	19867207
Application Number:	13689088
International Application Number:	
Confirmation Number:	9927
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Scott B. Guthery
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Leslie Roberts
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943AAAB-178-DIV
Receipt Date:	14-AUG-2014
Filing Date:	29-NOV-2012
Time Stamp:	14:37:49
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Electronic Terminal Disclaimer-Filed	eTerminal-Disclaimer.pdf	32065 41ec9bf1cb8947989969d3b55a6a52bef175081e	no	2

Warnings:

Information:

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/689,088	11/29/2012	Scott B. Guthery	2943AAAB-178-DIV

CONFIRMATION NO. 9927

POA ACCEPTANCE LETTER



OC000000070196157

22442
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

Date Mailed: 08/19/2014

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 08/11/2014.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/snguyen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:)	Group Art Unit: 2432
)	
GUTHERY et al.)	Examiner: LEMMA, SAMSON B.
)	
Serial No.: 13/689,088)	Confirmation No.: 9927
)	
Filed: November 29, 2012)	
)	
Atty. File No.: 2943AAAB-178-DIV)	
)	
For: "SECURE WIEGAND)	
COMMUNICATIONS")	
)	

RESPONSE TO ADVISORY ACTION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Madam:

Applicant submits this Response to Advisory Action to address the Advisory Action having a mailing date of August 6, 2014.

A Terminal Disclaimer was filed on August 14, 2014, in connection with the double patenting rejection based on U.S. Patent No. 8,358,783. Accordingly, it is respectfully submitted that the double patenting rejection has been overcome. Although no fees are believed due in connection with the filing this Response, please charge any additional fees deemed necessary, or credit any overpayment to Deposit Account No. 19-1970.

Based on the foregoing, Applicant believes that all pending claims are in condition for allowance and such disposition is respectfully requested. In the event that a telephone conversation would further prosecution and/or expedite allowance, the Examiner is invited to contact the undersigned.

Respectfully submitted,

SHERIDAN ROSS P.C.

Date: August 22, 2014

By: /Matthew R. Ellsworth/
Matthew R. Ellsworth
Reg. No. 56,345
Telephone: 303-863-2989

Electronic Acknowledgement Receipt	
EFS ID:	19945578
Application Number:	13689088
International Application Number:	
Confirmation Number:	9927
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Scott B. Guthery
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Leslie Roberts
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943AAAB-178-DIV
Receipt Date:	22-AUG-2014
Filing Date:	29-NOV-2012
Time Stamp:	17:42:20
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Response After Final Action	RESPONSE_ADVISORY_ACTION.pdf	72721 b7641d25880107d583fee7d0ab2e34f5c95771af	no	1

Warnings:

Information:

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 13/689,088		Filing Date 11/29/2012		<input type="checkbox"/> To be Mailed	
ENTITY: <input checked="" type="checkbox"/> LARGE <input type="checkbox"/> SMALL <input type="checkbox"/> MICRO										
APPLICATION AS FILED – PART I										
(Column 1)		(Column 2)								
FOR		NUMBER FILED		NUMBER EXTRA		RATE (\$)		FEE (\$)		
<input type="checkbox"/> BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A		N/A		N/A				
<input type="checkbox"/> SEARCH FEE (37 CFR 1.16(k), (i), or (m))		N/A		N/A		N/A				
<input type="checkbox"/> EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A		N/A		N/A				
TOTAL CLAIMS (37 CFR 1.16(j))		minus 20 =		*		X \$ =				
INDEPENDENT CLAIMS (37 CFR 1.16(h))		minus 3 =		*		X \$ =				
<input type="checkbox"/> APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).								
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
* If the difference in column 1 is less than zero, enter "0" in column 2.						TOTAL				
APPLICATION AS AMENDED – PART II										
(Column 1)		(Column 2)		(Column 3)						
AMENDMENT	08/22/2014	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(j))	* 14	Minus	** 20	= 0	X \$80 =		0		
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0	X \$420 =		0		
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))									
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE		0		
(Column 1)		(Column 2)		(Column 3)						
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(j))	*	Minus	**	=	X \$ =				
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$ =				
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))									
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE				
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.										

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

22442 7590 09/16/2014
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

EXAMINER

LEMMA, SAMSON B

ART UNIT

PAPER NUMBER

2432

DATE MAILED: 09/16/2014

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/689,088	11/29/2012	Scott B. Guthery	2943AAAB-178-DIV	9927

TITLE OF INVENTION: SECURE WIEGAND COMMUNICATIONS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$960	\$0	\$0	\$960	12/16/2014

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

22442 7590 09/16/2014
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/689,088	11/29/2012	Scott B. Guthery	2943AAAB-178-DIV	9927

TITLE OF INVENTION: SECURE WIEGAND COMMUNICATIONS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$960	\$0	\$0	\$960	12/16/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
LEMMA, SAMSON B	2432	726-005000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a **Customer Number is required.**

2. For printing on the patent front page, list

- (1) The names of up to 3 registered patent attorneys or agents OR, alternatively, 1 _____
- (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____
- 3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☐ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
- ☐ Applicant asserting small entity status. See 37 CFR 1.27
- ☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/689,088	11/29/2012	Scott B. Guthery	2943AAAB-178-DIV	9927
22442	7590	09/16/2014	EXAMINER	
Sheridan Ross PC 1560 Broadway Suite 1200 Denver, CO 80202			LEMMA, SAMSON B	
			ART UNIT	PAPER NUMBER
			2432	

DATE MAILED: 09/16/2014

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 13/689,088	Applicant(s) GUTHERY ET AL.	
	Examiner SAMSON LEMMA	Art Unit 2432	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to after final amendment filed on 08/22/2014.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are 1-5, 8-12 and 15-18. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
Certified copies:
a) ☐ All b) ☐ Some *c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
* Certified copies not received: _____.


Applicant has **THREE MONTHS FROM THE "MAILING DATE"** of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)


1. <input type="checkbox"/> Notice of References Cited (PTO-892)	5. <input type="checkbox"/> Examiner's Amendment/Comment
2. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____	6. <input type="checkbox"/> Examiner's Statement of Reasons for Allowance
3. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit of Biological Material	7. <input type="checkbox"/> Other _____
4. <input type="checkbox"/> Interview Summary (PTO-413), Paper No./Mail Date _____	

/SAMSON LEMMA/ Primary Examiner, Art Unit 2432	
---	--

<p align="center">Index of Claims</p> 	<p>Application/Control No.</p> <p>13689088</p>	<p>Applicant(s)/Patent Under Reexamination</p> <p>GUTHERY ET AL.</p>
	<p>Examiner</p> <p>SAMSON LEMMA</p>	<p>Art Unit</p> <p>2432</p>

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected


<input type="checkbox"/> Claims renumbered in the same order as presented by applicant					<input type="checkbox"/> CPA <input checked="" type="checkbox"/> T.D. <input type="checkbox"/> R.1.47				
CLAIM		DATE							
Final	Original	12/14/2013	05/16/2014	09/01/2014					
1	1	✓	✓	=					
2	2	✓	✓	=					
3	3	✓	✓	=					
4	4	✓	✓	=					
5	5	✓	✓	=					
	6	O	-	-					
	7	O	-	-					
6	8	✓	✓	=					
7	9	✓	✓	=					
8	10	✓	✓	=					
9	11	✓	✓	=					
10	12	✓	✓	=					
	13	O	-	-					
	14	O	-	-					
11	15	✓	✓	=					
12	16	✓	✓	=					
13	17	✓	✓	=					
14	18	✓	✓	=					
	19	O	-	-					
	20	O	-	-					

Issue Classification 	Application/Control No. 13689088	Applicant(s)/Patent Under Reexamination GUTHERY ET AL.	
	Examiner SAMSON LEMMA	Art Unit 2432	

CPC					
Symbol				Type	Version
H04L	63	/	08	F	2013-01-01
G06F	21	/	606	I	2013-01-01
H04L	9	/	12	I	2013-01-01
H04L	63	/	0428	I	2013-01-01
H04L	63	/	04	I	2013-01-01
H04L	9	/	0662	I	2013-01-01
H04L	9	/	0637	I	2013-01-01
H04L	9	/	16	I	2013-01-01
H04L	9	/	3226	I	2013-01-01
H04L	2209	/	805	A	2013-01-01
		/			
		/			
		/			
		/			
		/			


CPC Combination Sets						
Symbol			Type	Set	Ranking	Version
		/				
		/				

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	14	
/SAMSON LEMMA/ Primary Examiner.Art Unit 2432	09/01/2014	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification 	Application/Control No. 13689088	Applicant(s)/Patent Under Reexamination GUTHERY ET AL.
	Examiner SAMSON LEMMA	Art Unit 2432

US ORIGINAL CLASSIFICATION						INTERNATIONAL CLASSIFICATION													
CLASS		SUBCLASS				CLAIMED					NON-CLAIMED								
726		5				G	0	6	F	7 / 04 (2006.01.01)									
CROSS REFERENCE(S)																			
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)																		
726	14																		

NONE		Total Claims Allowed:	
		14	
(Assistant Examiner)	(Date)		
/SAMSON LEMMA/ Primary Examiner.Art Unit 2432	09/01/2014	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification 	Application/Control No. 13689088	Applicant(s)/Patent Under Reexamination GUTHERY ET AL.
	Examiner SAMSON LEMMA	Art Unit 2432

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant <input type="checkbox"/> CPA <input checked="" type="checkbox"/> T.D. <input type="checkbox"/> R.1.47															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	13	17												
2	2	14	18												
3	3		19												
4	4		20												
5	5														
	6														
	7														
6	8														
7	9														
8	10														
9	11														
10	12														
	13														
	14														
11	15														
12	16														

NONE		Total Claims Allowed:	
		14	
(Assistant Examiner)	(Date)		
/SAMSON LEMMA/ Primary Examiner.Art Unit 2432	09/01/2014	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

wiegand protocol credential

Sign In

[View](#)
[Images](#)
[Shopping](#)
[News](#)
[More](#)
[Search tools](#)

About 1,880 results (0.28 seconds)

Secure **wiegand communications**
www.google.com/patents/US20130117827

App. - Filed Nov 29, 2012 - Published May 9, 2013 - Scott B. Guthery - Assa Abloy Ab

operating a credential reader in a first mode of operation; ... The Wiegand protocol is the predominant method by which physical access control ...

[Overview](#) · [Related](#) · [Discuss](#)**Event driven second factor **credential** authentication**
www.google.com/patents/WO201300301A1?cl=en

App. - Filed Jul 12, 2011 - Published Jan 17, 2013 - Michael L. Davis - Assa Abloy Ab

The reader is configured to analyze credential data as well as ... As one example, the reader 104 may utilize the Wiegand protocol to ...

[Overview](#) · [Related](#) · [Discuss](#)**Event driven second factor **credential** authentication**
www.google.com/patents/EP2732579A1?cl=en

App. - Filed Jul 12, 2011 - Published May 21, 2014 - Michael L. Davis - Assa Abloy Ab

The reader is configured to analyze credential data as well as ... As one example, the reader 104 may utilize the Wiegand protocol to ...

[Overview](#) · [Related](#) · [Discuss](#)**Device authentication using a unidirectional **protocol****
www.google.com/patents/CA2556843A1?cl=en

App. - Filed Aug 22, 2006 - Published Feb 28, 2007 - Michael L. Davis - Assa Abloy Identification Technology Group Ab

The method of claim 1, wherein said credential is machine readable and ... Due to its popularity, the Wiegand protocol has become a de-facto ...

[Overview](#) · [Related](#) · [Discuss](#)**Rfid reader with embedded attack detection heuristics**
www.google.com/patents/US20100039220

App. - Filed Aug 14, 2009 - Published Feb 18, 2010 - Michael L. Davis - Assa Abloy Ab

(v) a credential presented to the reader is attempting to utilize a ... For reader utilizing the Wiegand protocol, this is a real possibility and has ...

[Overview](#) · [Related](#) · [Discuss](#)**Unified reference id mechanism in a multi-application ...**
www.google.com/patents/US20070039041

App. - Filed Aug 14, 2006 - Published Feb 15, 2007 - Michael Davis - Davis Michael L

The single credential is loaded with a unified reference ID that is accessible and ... communication protocol, for example, the Wiegand protocol.

[Overview](#) · [Related](#) · [Discuss](#)**Secure **wiegand** communications**
www.google.com/patents/US8358783

Grant - Filed Aug 11, 2009 - Issued Jan 22, 2013 - Michael Davis - Assa Abloy Ab

The Wiegand protocol is the predominant method by which physical ... format and reader status data read from an access control credential ...

[Overview](#) · [Related](#) · [Discuss](#)**RFID reader with embedded attack detection heuristics**
www.google.com/patents/EP2157526B1?cl=en

Grant - Filed Aug 12, 2009 - Issued Apr 30, 2014 - Michael Davis - Assa



Abloy Ab

As an example, the credential 120 may comprise a magstripe or the like
... For reader utilizing the Wiegand protocol, this is a real possibility ...
[Overview](#) · [Related](#) · [Discuss](#)

Method of migrating rfid transponders in situwww.google.com/patents/US20070174907

App. - Filed Nov 21, 2006 - Published Jul 26, 2007 - Michael Davis - Assa
Abloy Identification Technology Group Ab

The RFID transponder on the credential that has new data written thereon
does ... communication protocol, for example, the Wiegand protocol.
[Overview](#) · [Related](#) · [Discuss](#)

Method of migrating RFID transponders in situwww.google.com/patents/EP1788530A2?cl=en

App. - Filed Nov 21, 2006 - Published May 23, 2007 - Michael L. Davis -
Assa Abloy Identification Technology Group AB

The RFID transponder on the credential that has new data written thereon
does ... communication protocol, for example, the Wiegand protocol.
[Overview](#) · [Related](#) · [Discuss](#)

1 2 3 4 5 6 7 8 9 10 **Next**

[Help](#)[Send feedback](#)[Privacy & Terms](#)

Access control subsystem and method for distributed computer system using locally cached authentication credentials

M Abadi, A Birrell, B Lampson, E Wobber - US Patent 5,235,642, 1993 - Google Patents

... For example the Internet Transmission Control **Protocol** provides a bi-directional connection between two ... with a time limit (eg, a datum indicating that the corresponding **credential** is valid ... for the requester, plus the required **credentials**, using digital signing **protocols** well known ...

Cited by 367 Related articles All 2 versions Cite Save

Systems and methods for multi-factor authentication

D Ting, O Hussain, G LaRoche - US Patent App. 11/698,271, 2007 - Google Patents

... The connections can be established using a variety of communication **protocols** (eg, HTTP(S) ... card is detected and transmitted to the control panel 220 using, for example, the **Wiegand protocol**. ... **credentials** are relatively difficult to imitate, a valid biometric **credential** may contribute ...

Cited by 47 Related articles All 2 versions Cite Save

Legacy access control security system modernization apparatus

CW Fox - US Patent 7,669,054, 2010 - Google Patents

... Because there are no universal standards for how these switches are wired or for the communications **protocols** used to operate and ... panel interface 610 to the legacy control panel 110 in accordance with SIA's access control standard **protocol** for **Wiegand** reader interfaces. ...

Cited by 3 Related articles All 4 versions Cite Save

Method of migrating rfid transponders in situ

M Davis - US Patent App. 11/562,314, 2006 - Google Patents

... unidirectional interfaces that use a unidirectional communication **protocol**, for example, the **Wiegand protocol**. ... from a common manufacturer either having the same communication **protocol** but different access codes or even having different communication **protocols**. ...

Cited by 6 Related articles All 3 versions Cite Save

Portable identity card reader system for physical and logical access

D Finn - US Patent 7,748,636, 2010 - Google Patents

... The **Wiegand protocol** consists of three wires, one of which is a common ground, and ... Wireless and contactless use different communications **protocols** with different capabilities and are typically ... for example, that 100 cm (ISO 15693, an RFID contactless **protocol**) is considered to ...

Cited by 14 Related articles All 5 versions Cite Save

Contactless technology for secure physical access: Technology and standards choices

SC Alliance - Smart Card Alliance Research Report, 2002 - chasesecurity.com.au

... Manufacturers have therefore had greater latitude to develop different products and **protocols**. ...

Wiegand-compliance typically refers to the communication **protocol** and interface used between readers and the other non-card components of a physical access system. ...

Cited by 15 Related articles All 16 versions Cite Save More

Rfid reader with embedded attack detection heuristics

ML Davis - US Patent App. 12/541,480, 2009 - Google Patents

... For readers communicating with its upstream device using the **Wiegand protocol**, the upstream device ... back to the upstream device using whatever communication interface and **protocol** is available ... The systems, methods and **protocols** of this invention can be implemented on a ...

Cited by 2 Related articles All 2 versions Cite Save

Use of snmp for management of small footprint devices

SB Guthery - US Patent App. 12/480,505, 2009 - Google Patents

... The **protocols** used by the communication network 104 to manager 116/managed device 108 communications may include, but is not limited to, the TCP/IP **protocol**, Power-Over-Ethernet (POE), Wi-Fi, **Wiegand Protocol**, RS 232, RS 485, RS422, Current ...

Cited by 2 Related articles All 2 versions Cite Save

Contactless smart cards: Dumb (and dangerous) ways to use them

ML Davis - Card Technology Today, 2007 - Elsevier

... CSN readers are readers that use the CSN of a contactless smart card instead of the **credential** data stored in the secure area of ... Most readers used for access control applications transmit their data using the **Wiegand protocol** 3 . This **protocol** is both an electrical interface and a ...

Cited by 2 Related articles All 2 versions Cite Save

Device authentication using a unidirectional protocol

ML Davis, T Hulusi - US Patent 8,183,980, 2012 - Google Patents

... Although well suited for use in an access system utilizing the **Wiegand protocol**, embodiments of the present invention may be ... The **protocols** used to communicate between the control panel 104 and the readers 112 may include one or more of the TCP/IP **protocol**, RS 232 ...

Cited by 1 Related articles All 5 versions Cite Save

wiegand protocol credential

Sign In

Web

Images

On your device


News

Videos


Maps

Search Tools


About 528,000 results (0.42 seconds)

Wiegand interface - Wikipedia, the free encyclopediaen.wikipedia.org/wiki/Wiegand_interface 


The Wiegand Interface is a de facto wiring standard which arose from the popularity of Wiegand effect card readers in the 1980s. It is commonly used to connect ...

[PDF] EK6 A&E Specs - ECKeyeckey.com/wp-content/uploads/AE-Specification-EK6_June2014_FINAL.pdf 


A. The product specified is a proximity reader providing Wiegand protocol interface ... with a Bluetooth 2.1 or earlier actuating device (CREDENTIAL) such as a ...

[PDF] 206A West James Street•Lancaster•PA•17603 +1 ... - EC...eckey.com/wp-content/uploads/AE_Specification_EK6_03.08.13.pdf 


A. The product specified is a proximity reader providing Wiegand protocol ... with an actuating device (credential) such as a mobile phones, computers and ...

[PDF] Pyramid Series Wiegand Data Format - Keri Systemswww.kerisys.com/Pyramid_Series_Wiegand_Data_Format_Reference... 


Protocol for the 26-Bit Wiegand Reader Interface document. ... credentials), it is possible to have duplicate card coding (i.e. identical format, facility code, and ID.

Understanding 26-bit Wiegand - SecurityInfoWatch.comwww.securityinfowatch.com/article/.../understanding-26-bit-wiegand 

Oct 27, 2008 - The "26-bit" referred to the protocol of the data on the card. Proximity credentials and readers typically use the Wiegand interface and 26-bit ...


GE Interlogix Two-State Wiegand Interface Card Supports ...securednws.com/.../ge-interlogix-two-state-wiegand-interface-card-sup... 

Aug 13, 2003 - Home; GE Interlogix Two-State Wiegand Interface Card Supports Multi-Credential Formats. GE Interlogix Two-State Wiegand Interface Card ...


SECURE WIEGAND COMMUNICATIONS - Patent applicationwww.fqqs.org/patents/app/20130117827 

May 9, 2013 - Class name: Access control or authentication network credential ...


[0003] The Wiegand protocol is the predominant method by which physical ...

[PDF] Understanding Card Data Formats - HID Globalwww.hidglobal.com/.../hid-understanding_card_data_format... 

Wiegand™ Format. The term Wiegand is applied to several characteristics related to access control readers and cards. ... A specific binary reader-to-controller interface. 3. An electronic ... panel. All HID credentials (card, fobs, tags, etc.) can be ...

[PDF] K-SECURE - Keyscanwww.keyscan.ca/PDFs/Credentials/K-SECURE.pdf 

K-SECURE 13.56MHz contactless smartcard credentials provide the highest level of ... credential anti-counterfeiting protection. K-SECURE ... Wiegand protocol

Wiegand Protocol Interfaces - Smart R Distributionwww.smartdistribution.com/cgi-bin/sitewise.pl?act=sect&s=1481 

Integrates any card reader using the Wiegand interface standard with any computing platform that supports USB Human Interface Device keyboard input.

Searches related to wiegand protocol credential

wiegand protocol arduino

wiegand protocol access control systems

wiegand protocol example

wiegand protocol specification

1 2 3 4 5 6 7 8 9 10 **Next**

○ Alexandria, VA - From your internet address - Use precise location - Learn more

[Help](#) [Send feedback](#) [Privacy & Terms](#)

EAST Search History**EAST Search History (Prior Art)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	("8358783").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 22:22
L2	3	"20130117827"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 22:34
L3	2	("6988203").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 22:41
L7	2228	(713/185).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:15
L8	4378	(713/182).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:15
L9	2860	(713/186).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:15
L10	6346	(726/2).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:15
L11	5835	(726/5).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:16
L12	1814	(726/14).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:16
L13	3469	(380/270).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:16
L14	452	(380/260).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:16
L15	1623	(380/46).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:16

L16	31704	(H04L63/08).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:16
L17	3582	(H04L63/04).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:16
L18	27609	(H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:16
L19	4878	(G06F21/606).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:17
L20	5545	(H04L2209/805).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:17
L21	1845	(H04L9/0637).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:17
L22	3146	(H04L9/0662).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:17
L23	3262	(H04L9/12).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:17
L25	958	(H04L9/06).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:18
L26	5012	(H04L9/3226).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:18
L27	12	(Wiegand with protocol).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:20
L28	10	(Wiegand adj protocol).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:20
L29	1621170	(Wiegand adj protocol)".ti"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:20
L30	14	(Wiegand adj protocol).ti.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:20
L31	39	(Wiegand adj protocol).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	OFF	2014/09/04 23:21

			IBM_TDB			
L32	3	(Wiegand adj protocol).clm. and (mode with operation).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:21
L33	3	(Wiegand adj protocol).clm. and (mode with operation).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:22
L34	2	(Wiegand adj protocol).clm. and (mode with operation).clm. and (credential with reader).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:25
L35	5	(Wiegand adj protocol) and (mode with operation) and (credential with reader)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:26
L36	7	(Wiegand adj protocol) and (mode with operation\$) and (credential with reader)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:27
L37	7	(Wiegand adj protocol) and (mode with operation\$) and (credential with reader\$)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:27
L38	2	(Wiegand adj protocol).clm. and (mode with operation\$).clm. and (credential with reader\$).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 23:36

9/ 4/ 2014 11:36:42 PM

C:\Users\slemma\Documents\EAST\Workspaces\13181890.wsp

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:) Group Art Unit: 2432
)
GUTHERY et al.) Examiner: LEMMA, SAMSON B.
)
Serial No.: 13/689,088) Confirmation No.: 9927
)
Filed: November 29, 2012)
)
Atty. File No.: 2943AAAB-178-DIV)
)
For: "SECURE WIEGAND)
COMMUNICATIONS")
)

RESPONSE TO ADVISORY ACTION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Please Enter.
09/01/2014.
/S.L./

Madam:

Applicant submits this Response to Advisory Action to address the Advisory Action having a mailing date of August 6, 2014.

A Terminal Disclaimer was filed on August 14, 2014, in connection with the double patenting rejection based on U.S. Patent No. 8,358,783. Accordingly, it is respectfully submitted that the double patenting rejection has been overcome. Although no fees are believed due in connection with the filing this Response, please charge any additional fees deemed necessary, or credit any overpayment to Deposit Account No. 19-1970.


Based on the foregoing, Applicant believes that all pending claims are in condition for allowance and such disposition is respectfully requested. In the event that a telephone conversation would further prosecution and/or expedite allowance, the Examiner is invited to contact the undersigned.

Respectfully submitted,

SHERIDAN ROSS P.C.

Date: August 22, 2014

By: /Matthew R. Ellsworth/
Matthew R. Ellsworth
Reg. No. 56,345
Telephone: 303-863-2989

Search Notes 	Application/Control No. 13689088	Applicant(s)/Patent Under Reexamination GUTHERY ET AL.
	Examiner SAMSON LEMMA	Art Unit 2432

CPC- SEARCHED		
Symbol	Date	Examiner
H04L63/08	9/1/2014	SL
H04L63/04	9/1/2014	SL
H04L63/0428	9/1/2014	SL
H04L9/0637	9/1/2014	SL
H04L9/0662	9/1/2014	SL
H04L9/12	9/1/2014	SL
H04L9/6	9/1/2014	SL
H04L9/3226	9/1/2014	SL
H04L2209/805	9/1/2014	SL

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	2, 5 and 14	9/1/2014	SL
380	270, 260 and 46	9/1/2014	SL
713	182, 185-186		

SEARCH NOTES		
Search Notes	Date	Examiner
713/\$, 380/\$, 726/\$, H04L63/\$, G06F21/\$, H04L2209/\$, H04L9/\$ (With text Search)(Search is Updated)	9/1/2014	SL
EAST and Interference Search (Search is Updated)	9/1/2014	SL
NPL (IEEE, ACM DIGITAL LIBRARY, GOOGLE, GOOGLE PATENT, Google Scholar....)	9/1/2014	SL
INVENTOR NAME SEARCH	9/1/2014	SL

--	--

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
Interference Search History Printout	Interference Search History Printout	9/1/2014	SL

--	--

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known			
				Application Number		13/689,088	
				Filing Date		November 29, 2012	
				First Named Inventor		Scott B. Guthery	
				Art Unit		2432	
				Examiner Name		Samson B. Lemma	
Sheet	1	of	1	Attorney Docket Number		2943AAAB-178-DIV	

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document Country Code ³ ; Number ⁴ ; Kind Code ⁵ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶

NON-PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	1	Notice of Allowance for U.S. Patent Application No. 13/689,108, mailed Aug. 22, 2014 (Attorney's Ref. No. 2943AAAB-178-DIV-2) 9 pages

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Electronic Patent Application Fee Transmittal				
Application Number:		13689088		
Filing Date:		29-Nov-2012		
Title of Invention:		SECURE WIEGAND COMMUNICATIONS		
First Named Inventor/Applicant Name:		Scott B. Guthery		
Filer:		Matthew Ryan Ellsworth/Robert Roe-Pachirat		
Attorney Docket Number:		2943AAAB-178-DIV		
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
Total in USD (\$)				180

Electronic Acknowledgement Receipt	
EFS ID:	20396773
Application Number:	13689088
International Application Number:	
Confirmation Number:	9927
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Scott B. Guthery
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Robert Roe-Pachirat
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943AAAB-178-DIV
Receipt Date:	13-OCT-2014
Filing Date:	29-NOV-2012
Time Stamp:	13:44:13
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 180
RAM confirmation Number	8874
Deposit Account	191970
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		2943AAAB-178-DIV_IDS_05.pdf	149207 2d06186ac890b35d8a7d303b7a57505af843cb42	yes	4
	Multipart Description/PDF files in .zip description				
	Document Description		Start		End
	Transmittal Letter		1		3
	Information Disclosure Statement (IDS) Form (SB08)		4		4
Warnings:					
Information:					
2	Non Patent Literature	2943AAAB-178-DIV-2_NOA_08-22-2014.pdf	490901 59a77fd064ce0aba32b8ad4436e07c4c3b9a2932	no	9
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30589 4cb6fc8963090dc0ca04bfc37b6fcee6b0de1dd	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			670697		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:)	Group Art Unit: 2432
Scott B. Guthery)	Confirmation No.: 9927
Serial No.: 13/689,088)	Examiner: Samson B. Lemma
Filed: November 29, 2012)	
Atty. File No.: 2943AAAB-178-DIV)	<u>SUPPLEMENTAL</u>
Entitled: "Secure Wiegand Communications")	<u>INFORMATION DISCLOSURE</u>
)	<u>STATEMENT</u>
)	<i>Electronically Submitted</i>

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

The references cited on attached Form PTO/SB08 are being called to the attention of the Examiner.

- ☒ Copies of the cited non-patent and/or foreign references are enclosed herewith.
- ☐ Copies of the cited U.S. patents and/or patent applications are enclosed herewith.
- ☐ Copies of the cited U.S. patents/patent application publications are not enclosed in accordance with 37 C.F.R. § 1.98(a).
- ☐ Copies of the cited references are not enclosed, in accordance with 37 C.F.R. § 1.98(d), because the references were cited by or submitted to the U.S. Patent and Trademark Office in prior application Serial No. _____ filed _____, which is relied upon for an earlier filing date under 35 U.S.C. § 120.
- ☐ To the best of applicants' belief, the pertinence of the foreign-language references is believed to be summarized in the attached English abstracts and/or in the figures, although applicants do not necessarily vouch for the accuracy of the translation.
- ☐ Examiner's attention is drawn to the following related applications:
Serial No. _____ filed _____ (Attorney Ref. No. _____)
Serial No. _____ filed _____ (Attorney Ref. No. _____)
- ☐ Other: _____

Submission of the above information is not intended as an admission that any item is citable under the statutes or rules to support a rejection, that any item disclosed represents analogous art, or that those skilled in the art would refer to or recognize the pertinence of any reference without the benefit of hindsight, nor should an inference be drawn as to the pertinence

of the references based on the order in which they are presented. Submission of this statement should not be taken as an indication that a search has been conducted, or that no better art exists.

It is respectfully requested that the cited information be expressly considered during the prosecution of this application and the references made of record therein.

FEES

<input type="checkbox"/>	<p>37 CFR 1.97(b): No fee is believed due in connection with this submission, because the information disclosure statement submitted herewith is satisfied by one of the following conditions ("X" indicates satisfaction):</p> <div style="margin-left: 20px;"> <input type="checkbox"/> Within three months of the filing date of a national application other than a continued prosecution application under 37 CFR 1.53(d), or <input type="checkbox"/> Within three months of the date of entry of the national stage as set forth in § 1.491 in an international application, or <input type="checkbox"/> Before the mailing date of a first Office Action on the merits, or <input type="checkbox"/> Before the mailing of a first Office action after the filing of a request for continued examination under 37 CFR 1.114. </div> <p>Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970.</p>
<input type="checkbox"/>	<p>37 CFR 1.97(c): The information disclosure statement transmitted herewith is being filed after all the above conditions (37 CFR 1.97(b)), but before the mailing date of any one of the following conditions:</p> <div style="margin-left: 40px;"> (1) a final action under 37 C.F.R. 1.113, or (2) a notice of allowance under 37 C.F.R. 1.311, or (3) an action that otherwise closes prosecution in the application. </div> <p>This Information Disclosure Statement is accompanied by:</p> <div style="margin-left: 20px;"> <input type="checkbox"/> A Certification (below) as specified by 37 C.F.R. 1.97(e). Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970. <div style="text-align: center; margin: 5px 0;">OR</div> <input type="checkbox"/> Please charge Deposit Account 19-1970 in the amount of \$180.00 for the fee set forth in 37 C.F.R. 1.17(p) for submission of an information disclosure statement. Please credit any overpayment or charge any underpayment to Deposit Account 19-1970. </div>
<input checked="" type="checkbox"/>	<p>37 CFR 1.97(d): This Information Disclosure Statement is being submitted after the period specified in 37 CFR 1.97(c).</p> <div style="margin-left: 20px;"> <input checked="" type="checkbox"/> This information Disclosure Statement includes a Certification (below) as specified by 37 C.F.R. 1.97(e) <div style="text-align: center; margin: 5px 0;">AND</div> <input checked="" type="checkbox"/> Applicants hereby requests consideration of the reference(s) disclosed herein. Please charge Deposit Account 19-1970 in the amount of \$180.00 under 37 C.F.R. 1.17(p). Please credit any overpayment or charge any underpayment to Deposit Account 19-1970. Election to pay the fee should not be taken as an indication that applicant(s) cannot execute a certification. </div>

Certification (37 C.F.R. 1.97(e))
(Applicable only if checked)

- ☒ The undersigned certifies that:
- ☐ Each item of information contained in the Information Disclosure Statement submitted herewith was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(1).
 - ☐ A copy of the communication from the foreign patent office is enclosed.

OR

- ☒ No item of information contained in the Information Disclosure Statement submitted herewith was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in the Information Disclosure Statement was known to any individual designated in 37 C.F.R. 1.56(c) more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(2).

Respectfully submitted,

SHERIDAN ROSS P.C.

By: /Matthew R. Ellsworth/
Matthew R. Ellsworth
Registration No. 56345
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: October 13, 2014

Receipt date: 10/13/2014

13689088 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known			
				Application Number		13/689,088	
				Filing Date		November 29, 2012	
				First Named Inventor		Scott B. Guthery	
				Art Unit		2432	
				Examiner Name		Samson B. Lemma	
Sheet	1	of	1	Attorney Docket Number		2943AAAB-178-DIV	

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document Country Code ³ ; Number ⁴ ; Kind Code ⁵ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶

NON-PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	1	Notice of Allowance for U.S. Patent Application No. 13/689,108, mailed Aug. 22, 2014 (Attorney's Ref. No. 2943AAAB-178-DIV-2) 9 pages

Examiner Signature	/Samson Lemma/	Date Considered	10/20/2014
--------------------	----------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2432
				Examiner Name	Samson B. Lemma
Sheet	1	of	1	Attorney Docket Number	2943AAAB-178-DIV

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document Country Code ³ ; Number ⁴ ; Kind Code ⁵ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
	1	AU 2004100358	06/03/2004	BQT SOLUTIONS PTY LTD		

NON-PATENT LITERATURE DOCUMENTS	
Examiner Initials*	Cite No. ¹
Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

(12) INNOVATION PATENT
(19) AUSTRALIAN PATENT OFFICE

(11) Application No. **AU 2004100358 A4**

(54) Title
Dual Wiegand Reader

(51)⁷ International Patent Classification(s)
G06K 009/62 G06K 009/40

(21) Application No: **2004100358** (22) Date of Filing: **2004.05.13**

(30) Priority Data

(31) Number **2003902317** (32) Date **2003.05.14** (33) Country **AU**

(45) Publication Date: **2004.06.03**

(45) Publication Journal Date: **2004.06.03**

(45) Granted Journal Date: **2004.06.03**

(71) Applicant(s)
BQT Solutions Pty Ltd

(72) Inventor(s)
Blake, Christopher Ian

(74) Agent / Attorney
Spruson & Ferguson, Level 35 St Martins Tower 31 Market Street, Sydney, NSW, 2000

Dual Wiegand Reader

ABSTRACT

- 5 A dual Wiegand reader is disclosed. The reader comprises a processing unit producing both Standard Wiegand output and Single Wiegand output. The processing unit is preferably a microcontroller. The dual Wiegand reader may also comprise buffers coupled to the microcontroller for buffering the output of the microcontroller to provide the Standard Wiegand output. A network of electrical and/or electronic
- 10 components may be coupled to the buffers to produce the Single Wiegand output. The reader comprises an interface adapted for coupling to a controller having Standard Wiegand inputs, Single Wiegand inputs, or both. The dual Wiegand reader is implemented as unitary device in a housing, and is implemented using a single printed circuit board.

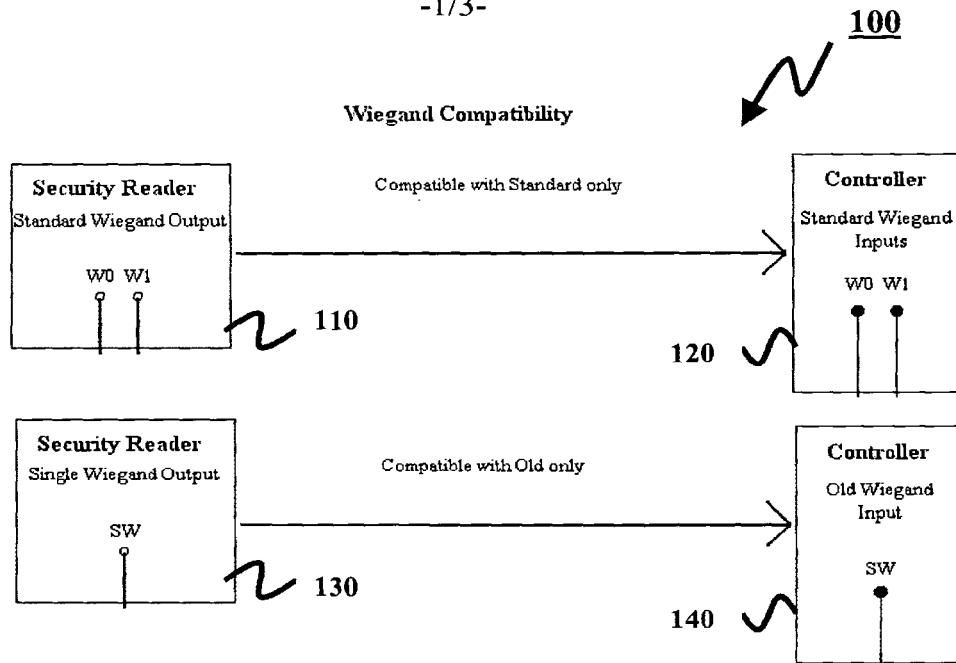


FIG. 1

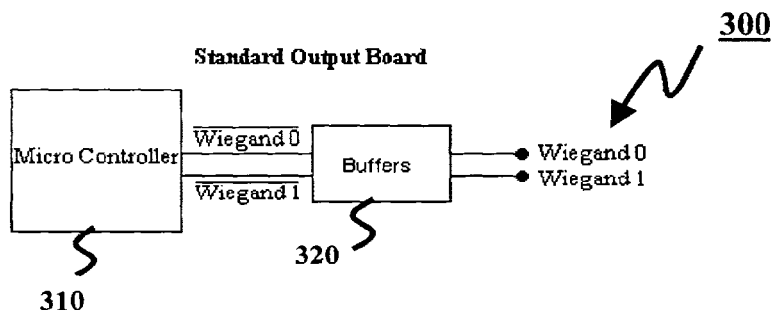


FIG. 3

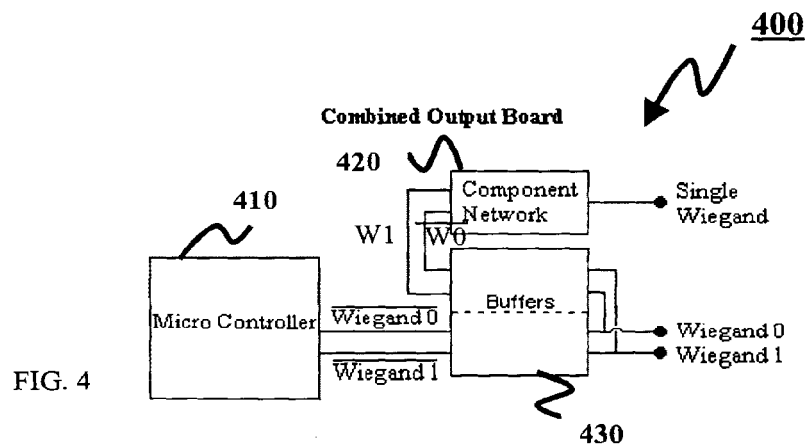


FIG. 4

AUSTRALIA

PATENTS ACT 1990

INNOVATION PATENT SPECIFICATION

Name and Address of Applicant :	BQT Solutions Pty Ltd, an Australian company, ACN 072 066 641, of Unit 5, 12-18 Victoria Street East, Lidcombe, New South Wales, 2141, Australia
------------------------------------	---

Actual Inventor(s):	Christopher Ian Blake
---------------------	-----------------------

Address for Service:	Spruson & Ferguson St Martins Tower Level 35 31 Market Street Sydney NSW 2000 (CCN 3710000177)
----------------------	--

Invention Title:	Dual Wiegand Reader
------------------	---------------------

The following statement is a full description of this invention, including the best method of performing it known to me/us:-

Dual Wiegand Reader

5 FIELD OF THE INVENTION

The present invention relates generally to security readers, and in particular to such readers that utilise Wiegand outputs.

BACKGROUND

10 Smartcard readers, proximity readers, and Wiegand readers are all examples of security readers used for controlling access points. Such devices are used to read badges, smartcards, and other like types of security identification mechanisms. Further, biometric data is increasingly used as a mechanism of security identification, with the security reader having a biometrics sensing device. Biometrics sensor
15 systems recognize a person based on the person's physical or behavioural characteristics. A number of different encoded signals are produced as outputs of such security readers. The output formats produced by security readers include Standard Wiegand Output, and Single Wiegand Output, amongst others.

20 Security readers that utilise either Standard Wiegand Output or the older Single Wiegand Output can be readily integrated with many existing access control systems. Accordingly, many biometrics-based security systems have been developed utilising either one of these protocols.

25 Fig. 1 is a block diagram illustrating conventional security readers and controllers and their compatibility in terms of Wiegand Outputs. A security reader 130 provides Single Wiegand Output (SW) to a compatible controller 140 that only accepts this old Wiegand input (SW). Further, a security reader 110 providing Standard Wiegand Output (W0, W1) is compatible with a controller 120 that has
30 Standard Wiegand Inputs (W0, W1).

Fig. 2 contains three timing diagrams. The top-most, middle, and bottom timing diagrams shows the Standard Wiegand 0 (W0) output, Standard Wiegand 1 (W1) output, and Single Wiegand Output signals, respectively.

5 The Standard Wiegand format is described as follows:

- It has 2 lines: Wiegand 0 and Wiegand 1.
- The existing format requirements are:
 - Pulse width = 50us to 100us,
 - Period = 1ms to 1.2ms, and
 - 10 - +5V is the steady state, going to 0V as active.

The Single Wiegand protocol is described as follows:

- There is only a single line for Wiegand information (SW).
- The existing format requirements are:
 - 15 - Pulse width = 50us to 100us,
 - Period = 1ms to 1.2ms, and
 - +2.5V is the steady state, going high to +4.8V for a data 0 and low to +0.2V for a data 1.

20 A significant disadvantage of these security readers 110, 130 is that they are not interchangeable, and require separate installations, since the controllers 120, 140 are incompatible with the security readers 130, 110, respectively. In large security systems for large organisations, there may be a number of older security readers with Single Wiegand Output for corresponding controllers, as well as a number of security
25 readers with Standard Wiegand Output for corresponding controllers. This results in a proliferation of security readers and associated installation and maintenance costs.

 Currently, security readers are produced using Standard Wiegand (W0, W1).
Fig. 3 is a block diagram illustrating a Standard Wiegand output board 300. A
30 microcontroller 310 produces negated Wiegand 0 and Wiegand 1 at its output, which

is coupled to a buffer 320. The buffer 320 produces Wiegand 0 and Wiegand 1 at its output. This is implemented as a single unit.

Single Wiegand readers are not regularly produced any longer, but Single
5 Wiegand controllers are still common. Instead, the newer format "Standard" Wiegand readers are produced. A separate converter may be used to convert the current Standard Wiegand to Single Wiegand format to install new readers with the older controllers.

10 Fig. 5 is a block diagram of a converter 500 used to convert the Standard Wiegand to Single Wiegand format. This separate device would be connected to the Standard Wiegand output board 300 of Fig. 3. The W0 and W1 outputs of the reader 310 are provided as input to a filter 520. The Wiegand lines coming from the Standard Wiegand reader may be over a length of line. That length of line picks up
15 interference and harmonics. Therefore, filtering circuitry 520 is used to 'clean' up the Wiegand output. The output of the filter 520 is buffered by buffers 530, before being converted to Single Wiegand (SW) output by component network 540. The buffers 530 and the component network 540 change the 2.5V steady state W0 and W1 signals to a single signal that is steady state at 2.5V and goes high or low with W0 or W1. As
20 indicated in Fig. 5, a regulator 510 regulates power to the elements of the converter 500. This is the method by which a party or organisation attempts to overcome installing newer Standard Wiegand readers with older Single Wiegand controllers.

Disadvantageously, if a converter is used, a power supply is required to supply
25 the converter 500. If the same power supply is not used, grounding issues exist if the installers are not previously briefed on the grounding issues.

Thus, a need clearly exists for an improved security reader capable of
providing both Single and Standard Wiegand Outputs.

30

SUMMARY

In accordance with an aspect of the invention, a dual Wiegand reader, comprises a processing unit producing both Standard Wiegand output (W0, W1) and a mechanism for producing Single Wiegand output (SW). The processing unit is preferably a microcontroller. The dual Wiegand reader also comprises buffers coupled to the microcontroller for buffering the output of the microcontroller to provide the Standard Wiegand output. A network of electrical and/or electronic components may be coupled to the buffers to produce the Single Wiegand output. The reader comprises an interface adapted for coupling to a controller having Standard Wiegand inputs, Single Wiegand inputs, or both. The dual Wiegand reader is implemented as unitary device in a housing, and is implemented using a single printed circuit board (PCB).

BRIEF DESCRIPTION OF THE DRAWINGS

A small number of embodiments are described hereinafter with reference to the drawings, in which:

Fig. 1 is a block diagram illustrating conventional security readers and controllers and their compatibility in terms of Wiegand Outputs;

20

Fig. 2 is a timing diagram illustrating the Standard Wiegand 0, Standard Wiegand 1, and Single Wiegand Output signals;

Fig. 3 is a block diagram of a Standard Wiegand Output board;

25

Fig. 4 is block diagram of a dual Wiegand reader in accordance with an embodiment of the invention;

Fig. 5 is a block diagram of a converter;

30

Fig. 6 is a block diagram of security reader having dual Wiegand Output in accordance with the embodiment of the invention; and

Fig. 7 is a schematic diagram of the buffers and the component network.

5

DETAILED DESCRIPTION

A dual Wiegand reader is described hereinafter. In the following description, numerous specific details are set forth. However, from this disclosure, it will be apparent to those skilled in the art that modifications and/or substitutions may be made without departing from the scope and spirit of the invention. In other
10 circumstances, specific details may be omitted so as not to obscure the invention.

The dual Wiegand reader in accordance with an embodiment of the invention is designed to output both the current standard Wiegand (W0 and W1) and the single
15 Wiegand (SW) protocols, within the same security reader. This dual Wiegand reader is applicable to all security readers, including contact, contactless, proximity, and smartcard readers. The only requirement is that the security reader provide Wiegand output. For example, the dual Wiegand reader may be used with contactless Mifare Smartcard technology.

20

Fig. 4 is a block diagram of a dual Wiegand reader in accordance with the embodiment of the invention. A processing unit produces Standard Wiegand output (W0, W1). Preferably, the processing unit includes a microcontroller 410 that produces negated W0 and W1 output. In the preferred exemplary embodiment, the
25 microcontroller is implement using an 8052 series microcontroller. However, any of a large number of microcontrollers may be used. There is not much restriction on the range of microcontrollers that may be practiced. Buffers 430 are connected to the W0 and W1 outputs of the microcontroller 410. The dashed line in block 430 indicates that some of the buffers on a buffers chip are used for the initial output, which is W0 and W1. The buffers are inverters. They change a 0V to a 5V or visa versa, so initially
30 the buffers change the inverted Wiegand 0 (0V) to Wiegand 0 (5V). To obtain the

desired levels for the single Wiegand, the buffers are used to obtain a buffered Wiegand 1 (5V steady state, 2 inverters negate each other, but ensure the signal is isolated from the outputs) and an inverted Wiegand 0 (0V steady state, 3 inverters are used here. The buffers 430 buffer the output of the microcontroller 410 to provide the
5 Standard Wiegand output (W0, W1).

The network of electrical and/or electronic components 420 is connected to an output of the buffers 430 as a mechanism to produce the Single Wiegand output. W1 and an inverted W0 are produced by the buffers and provided as input to the network
10 420.

Fig. 7 is a schematic diagram illustrating a configuration 700 of the buffers 430 and the component network 420. In Fig. 7, the relevant buffers 430 of Fig. 4 are surrounded by a dashed line, with inputs W1 and W0. The W1 input passes through
15 two buffers to produce W1 and the W0 input passes through three buffers to produce the inverted W0. W1 and inverted W0 are provided to resistances Ry and Rw, respectively. The other terminals of resistances Ry and Rw are coupled together to form a node. A resistance Rx is coupled between the node and a voltage supply (5V). Another resistor Rz is coupled to the node and the other terminal of the resistance Rz
20 provides the Single Wiegand output (SW), which has a steady state value of 2.5V. The resistances may be implemented using conventional resistors with appropriate values.

The dual Wiegand reader 400 comprises an interface adapted for connecting
25 the reader to a controller having Standard Wiegand inputs, Single Wiegand inputs, or both. The dual Wiegand reader 400 is implemented as unitary device in a housing, and using a single printed circuit board (PCB). This reader 400 is described further in relation to Fig. 6, which shows an application of the reader 400.

30 Fig. 6 is a block diagram of a configuration 600 of a security reader 610 having a dual Wiegand reader 400 of Fig. 4. The security reader 610 provides dual Wiegand output (SW, and W0 and W1) as a single unit. The reader 610 is fully

compatible with both Standard Wiegand and Single Wiegand controllers 620 and 630. Thus, the reader 610 can be connected to the Standard Wiegand controller 620 with W0 and W1 inputs, and to the Single Wiegand controller 630 with SW input ("old Wiegand input").

5

The dual Wiegand reader may be used by businesses and organisations, amongst others, that have installed old technology controllers such as the Cardax Controller. The "old" controllers only accept Single Wiegand information. The dual Wiegand reader in accordance with the embodiment of the invention provides this
10 output. The reader however also provides Standard Wiegand output from the same unit.

Previously, a person or organisation would need to buy a new Wiegand format reader and also buy a "Standard Wiegand to Single Wiegand converter". The dual
15 Wiegand reader in accordance with the embodiments of the invention eliminates the need to purchase such a converter, and also assists in installation as there is only one piece of hardware to be installed rather than two.

A benefit of having both Wiegand formats available on the one reader is for
20 logistic purposes. A party need purchase only one dual Wiegand reader and be assured when upgrades are occurring, that the readers are suitable.

In the embodiment of the invention, the Dual Wiegand Reader has both Standard and Single Wiegand outputs, W0 W1 and SW, on the same printed circuit
25 board (PCB), which has benefits as there are no or significantly reduced interference problems. When using a converter that takes W0 W1 and sends SW, there is a distance where interference can be induced on the wires.

Further, if a converter is used, a power supply is required to supply the
30 converter. If the same power supply is not used, grounding issues exist if the installers are not previously briefed on the grounding issues.

Advantageously, the embodiment of the invention does not require additional filtering circuitry when both Wiegand outputs are provided on the same reader. In contrast the conventional separate converter needs the filtering due to interference
5 picked up on the Wiegand lines that must be cleaned up before manipulating the signals.

In the foregoing manner, a dual Wiegand reader has been disclosed. While only a small number of embodiments are described, it will be apparent to those skilled
10 in the art in view of this disclosure that numerous changes and/or substitutions can be made without departing from the scope and spirit of the invention.

The claims defining the invention are as follows:

1. A dual Wiegand reader, comprising:
a processing unit producing Standard Wiegand output (W0, W1); and
5 means for producing Single Wiegand output (SW) coupled to said processing unit.
2. The dual Wiegand reader according to claim 1, wherein said
10 processing unit is a microcontroller.
3. The dual Wiegand reader according to claim 2, further comprising
buffers coupled to said microcontroller for buffering the output of said
microcontroller to provide said Standard Wiegand output.
- 15 4. The dual Wiegand reader according to claim 3, further comprising a
network of electrical and/or electronic components coupled to said buffers to produce
said Single Wiegand output.
- 20 5. The dual Wiegand reader according to claim 4, further comprising an
interface adapted for coupling to a controller having Standard Wiegand inputs, Single
Wiegand inputs, or both.

DATED this 13th Day of May, 2004

25

BQT Solutions Pty Ltd
Patent Attorneys for the Applicant
SPRUSON & FERGUSON

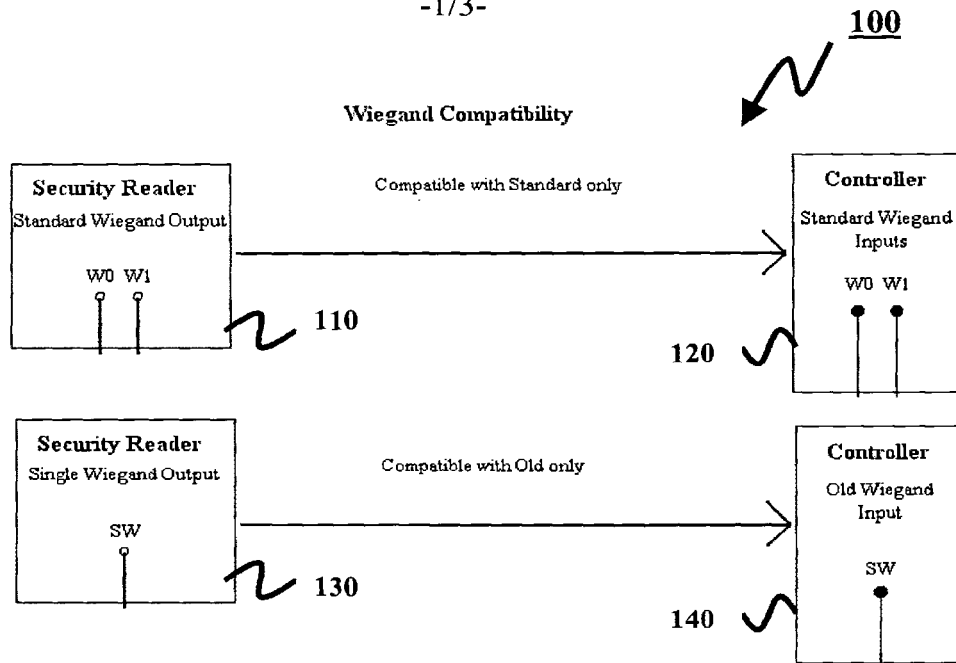


FIG. 1

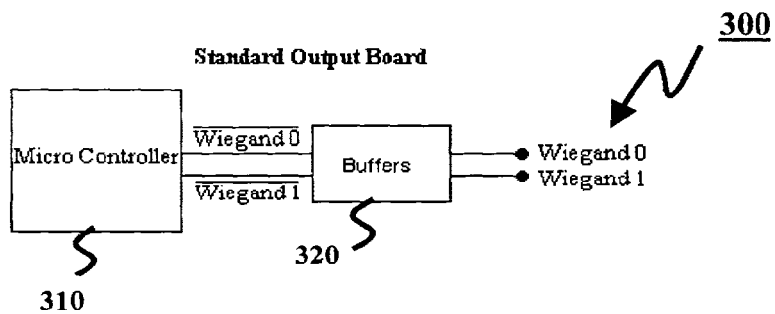


FIG. 3

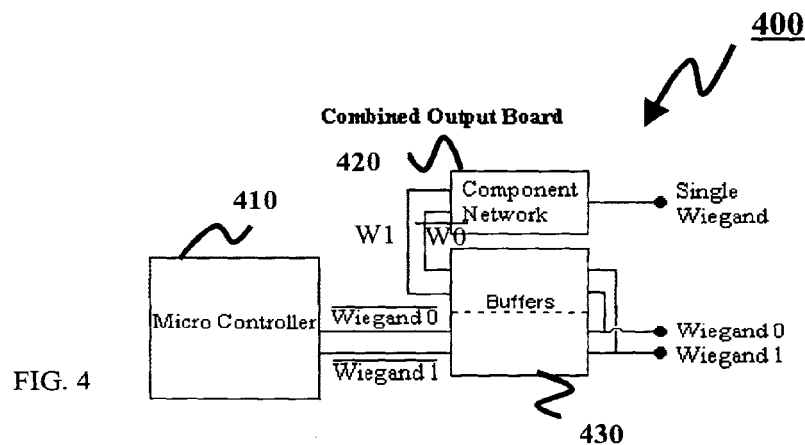


FIG. 4

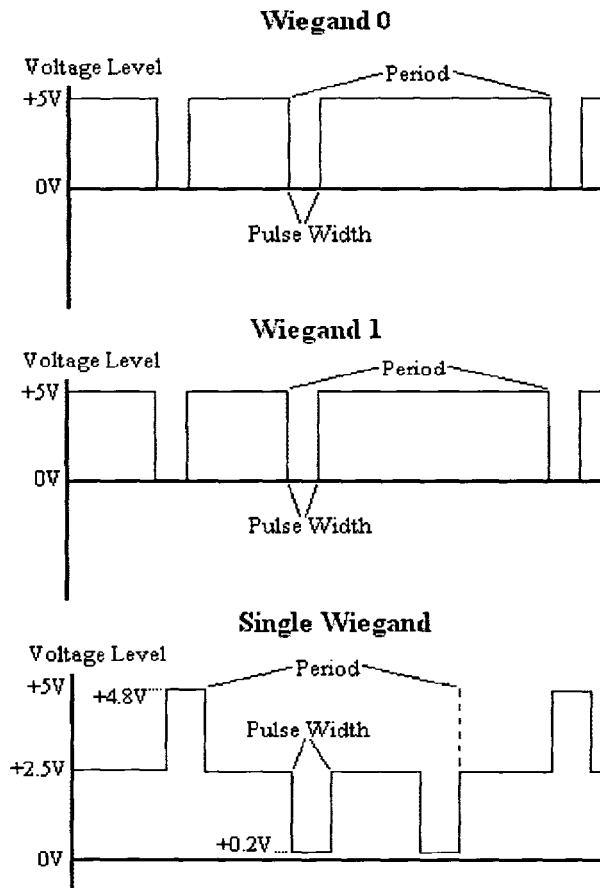


FIG. 2

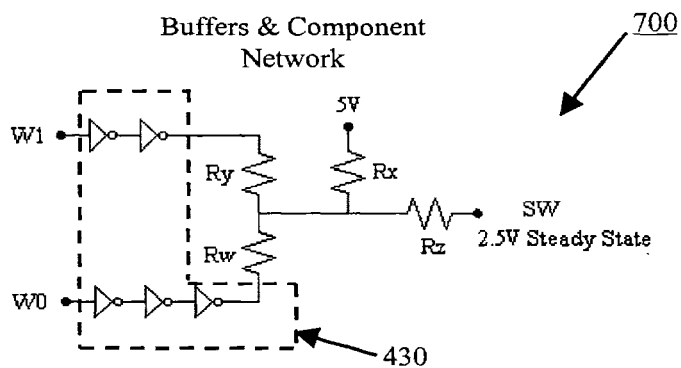


FIG. 7

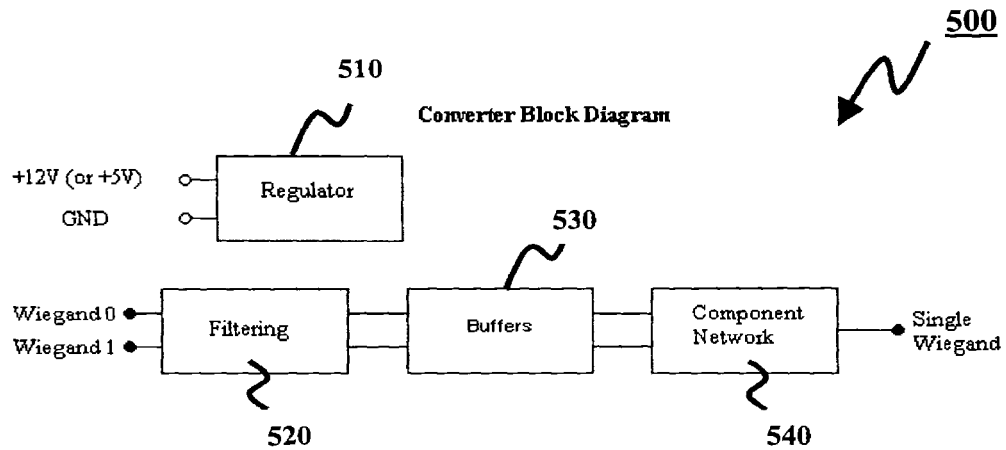


FIG. 5

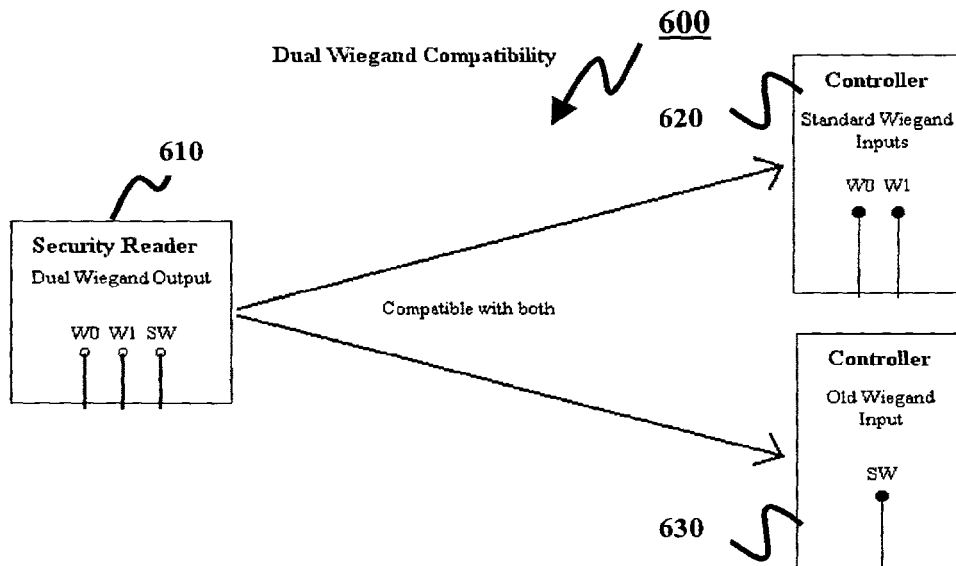


FIG. 6

Electronic Acknowledgement Receipt	
EFS ID:	20952254
Application Number:	13689088
International Application Number:	
Confirmation Number:	9927
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Scott B. Guthery
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Theresa Brown
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943AAAB-178-DIV
Receipt Date:	12-DEC-2014
Filing Date:	29-NOV-2012
Time Stamp:	17:39:32
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		IDS_06.pdf	89500	yes	3
			ecd0056da8b71cf17451c51a63923156332c086f		

Multipart Description/PDF files in .zip description							
Document Description			Start	End			
Transmittal Letter			1	2			
Information Disclosure Statement (IDS) Form (SB08)			3	3			
Warnings:							
Information:							
2	Foreign Reference	AU2004-100358.pdf	464357	no	16		
			5c18c1a9a160410675fc2b291c2850617465185b				
Warnings:							
Information:							
Total Files Size (in bytes):			553857				
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>							

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:)	Group Art Unit: 2432
Scott B. Guthery)	Confirmation No.: 9927
Serial No.: 13/689,088)	Examiner: Samson B. Lemma
Filed: November 29, 2012)	
Atty. File No.: 2943AAAB-178-DIV)	<u>SUPPLEMENTAL</u>
Entitled: "Secure Wiegand Communications")	<u>INFORMATION DISCLOSURE</u>
)	<u>STATEMENT</u>
)	<i>Electronically Submitted</i>

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

The references cited on attached Form PTO/SB08 are being called to the attention of the Examiner.

- ☒ Copies of the cited non-patent and/or foreign references are enclosed herewith.
- ☐ Copies of the cited U.S. patents and/or patent applications are enclosed herewith.
- ☐ Copies of the cited U.S. patents/patent application publications are not enclosed in accordance with 37 C.F.R. § 1.98(a).
- ☐ Copies of the cited references are not enclosed, in accordance with 37 C.F.R. § 1.98(d), because the references were cited by or submitted to the U.S. Patent and Trademark Office in prior application Serial No. _____ filed _____, which is relied upon for an earlier filing date under 35 U.S.C. § 120.
- ☐ To the best of applicants' belief, the pertinence of the foreign-language references is believed to be summarized in the attached English abstracts and/or in the figures, although applicants do not necessarily vouch for the accuracy of the translation.
- ☐ Examiner's attention is drawn to the following related applications:
Serial No. _____ filed _____ (Attorney Ref. No. _____)
Serial No. _____ filed _____ (Attorney Ref. No. _____)
- ☐ Other: _____

Submission of the above information is not intended as an admission that any item is citable under the statutes or rules to support a rejection, that any item disclosed represents analogous art, or that those skilled in the art would refer to or recognize the pertinence of any reference without the benefit of hindsight, nor should an inference be drawn as to the pertinence

of the references based on the order in which they are presented. Submission of this statement should not be taken as an indication that a search has been conducted, or that no better art exists.

Respectfully submitted,

SHERIDAN ROSS P.C.

By: /Matthew R. Ellsworth/
Matthew R. Ellsworth
Registration No. 56345
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: December 12, 2014

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

22442 7596 09/16/2014
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Leslie M. Roberts	(Depositor's name)
/Leslie M. Roberts/	(Signature)
December 12, 2014	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/689,088	11/29/2012	Scott B. Guthery	2943AAAB-178-DIV	9927

TITLE OF INVENTION: SECURE WIEGAND COMMUNICATIONS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$960	\$0	\$0	\$960	12/16/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
LEMMA, SAMSON B	2432	726-005000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.563).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a **Customer Number is required.**

2. For printing on the patent front page, list

- (1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
- (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Sheridan Ross P.C.

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

ASSA ABLOY AB

SWEDEN

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☒ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 19-1970 (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
- ☐ Applicant asserting small entity status. See 37 CFR 1.27
- ☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Matthew R. Ellsworth/

Date December 12, 2014

Typed or printed name Matthew R. Ellsworth

Registration No. 56,345

Electronic Patent Application Fee Transmittal				
Application Number:		13689088		
Filing Date:		29-Nov-2012		
Title of Invention:		SECURE WIEGAND COMMUNICATIONS		
First Named Inventor/Applicant Name:		Scott B. Guthery		
Filer:		Matthew Ryan Ellsworth/Leslie Roberts		
Attorney Docket Number:		2943AAAB-178-DIV		
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	1501	1	960	960

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				960

Electronic Acknowledgement Receipt	
EFS ID:	20953156
Application Number:	13689088
International Application Number:	
Confirmation Number:	9927
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Scott B. Guthery
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Leslie Roberts
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943AAAB-178-DIV
Receipt Date:	12-DEC-2014
Filing Date:	29-NOV-2012
Time Stamp:	18:38:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 960
RAM confirmation Number	4938
Deposit Account	191970
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	ISSUE_FEE.pdf	1553704 <small>72519064b8f5469cca93cd72704f1f6570efe3fe</small>	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30863 <small>aa16230a129fae48491f77ed0d002c92562f3d</small>	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			1584567		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/689,088	11/29/2012	Scott B. Guthery	2943AAAB-178-DIV	9927
EXAMINER				
LEMMA, SAMSON B				
ART UNIT		PAPER NUMBER		
2432				
NOTIFICATION DATE		DELIVERY MODE		
12/17/2014		ELECTRONIC		

7590
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

NOTICE OF NON-COMPLIANT INFORMATION DISCLOSURE STATEMENT

An Information Disclosure Statement (IDS) filed 12-12-14 in the above-identified application fails to meet the requirements of 37 CFR 1.97(d) for the reason(s) specified below. Accordingly, the IDS will be placed in the file, but the information referred to therein has not been considered.

The IDS is not compliant with 37 CFR 1.97(d) because:

- ☒ The IDS lacks a statement as specified in 37 CFR 1.97(e).
- ☐ The IDS lacks the fee set forth in 37 CFR 1.17(p).
- ☐ The IDS was filed after the issue fee was paid. Applicant may wish to consider filing a petition to withdraw the application from issue under 37 CFR 1.313(c) to have the IDS considered. See MPEP 1308.

571-272-4200 or 1-888-786-0101
Application Assistance Unit
Office of Data Management

Receipt date: 03/04/2013

13689088 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	9	of	12	Attorney Docket Number	2943AAAB-178-DIV

	252	RU 2158444	10/27/2000	AJ DI SISTEMS INK		(with English abstract)
	253	RU 2195020	12/20/2002	MNOGOPROFIL NOE PRED OOO EHLSI		(with English abstract)
	254	WO 97/17683	05/15/1997	ID SYSTEMS INC		
	255	WO 99/56429	11/04/1999	IDENTIX INC		
	256	WO 01/013218	02/22/2001	Siemens Aktiengesellschaft		(with English Abstract)
	257	WO 01/13218	02/22/2001	SIEMENS AG		(with English Abstract)
	258	WO 01/18331	03/15/2001	Electec System Aktiebolag		
	259	WO 02/082367	10/17/2002	PITTHWAY CORP		
	260	WO 03/027832	04/03/2003	Intel Corporation		
	261	WO 03/042812	05/22/2003	Everbee Networks		(with English Abstract)
	262	WO 2004/010373	01/29/2004	BANQUE TEC INTERNAT PTY LTD		
	263	WO 04/010373	01/29/2004	Banque-Tec International Pty Ltd		
	264	WO 2004/039119	05/06/2004	Anzon Autodoor Limited		
	265	WO 2006/015625	08/09/2004	Telecom Italia S.P.A.	2006-02-16	
	266	WO 05/001777	01/06/2005	SCM Microsystems GMBH		
	267	WO 2005/001777	01/06/2005	SCM MICROSYSTEMS GMBH		
	268	WO 2005/018137	02/24/2005	Securicom Pty Ltd		
	269	WO 2005/029315	03/31/2005	Globespanvirata Incorporated		
	270	WO 2005/038729	04/28/2005	SCM Microsystems, Inc.		
	271	WO 2006/032941	03/30/2006	Nokia Corporation		
	272	WO 2006/036521	04/06/2006	Qualcomm Incorporated		

Change(s) applied
to document,
/M.H.E./
10/21/2014

Examiner Signature	/Samson Lemma/	Date Considered	12/16/2013
-----------------------	----------------	--------------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Receipt date: 03/04/2013

13689088 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/689,088
				Filing Date	November 29, 2012
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	
Sheet	5	of	12	Attorney Docket Number	2943AAAB-178-DIV

	141	2001/0041593	11/15/2001	Asada	
	142	2001/0056534	12/27/2001	Roberts	
	143	2002/0016913	02/07/2002	Wheeler et al.	
	144	2002/0036569	03/28/2002	Martin	
	145	2002/0131595	09/19/2002	Veda et al.	
	146	2002/0184539	12/05/2002	Fukuda et al.	
	147	2003/0007473	01/09/2003	Strong et al.	
	148	2003/0014646	01/16/2003	Buddhikot et al.	
	149	2003/0055667	03/20/2003	Sgambaro et al.	
	150	2003/0074319	04/17/2003	Jaquette	
	151	2003/0081785	05/01/2003	Boneh et al.	
	152	2003/0204541	10/30/2003	Shackleford et al.	
	153	2003/0208697	11/06/2003	Gardner	
	154	2004/0069852	04/15/2004	Seppinen et al.	
	155	2004/0087273	05/06/2004	Perttinen et al.	Perttinen
	156	2004/0089707	05/13/2004	Cortina et al.	
	157	2004/0153291	08/05/2004	Kocarev et al.	
	158	2004/0162863	08/19/2004	Barry et al.	
	159	2004/0162864	08/19/2004	Nowshadi et al.	
	160	2004/0176032	09/09/2004	Kotola et al.	
	161	2004/0179684	09/16/2004	Appenzeller et al.	
	162	2004/0212493	10/28/2004	Stilp	
	163	2004/0232220	11/25/2004	Beenau et al.	
	164	2005/0002533	01/06/2005	Langin-Hooper et al.	
	165	2005/0010624	01/13/2005	Stehle	
	166	2005/0010750	01/13/2005	Ward et al.	
	167	2005/0036620	02/17/2005	Casden et al.	
	168	2005/0044119	02/24/2005	Langin-Hooper et al.	
	169	2005/0063004	03/24/2005	Silverbrook et al.	
	170	2005/0110210	05/26/2005	Soltys et al.	
	171	2005/0116813	06/02/2005	Raskar	
	172	2005/0129247	06/16/2005	Gammel et al.	
	173	2005/0127172	06/16/2005	Merkert Sr.	
	174	2005/0166040	07/28/2005	Walmsley	
	175	2005/0182946	08/18/2005	Shatford	
	176	2005/0265546	12/01/2005	Suzuki	
Examiner Signature	/Samson Lemma/			Date Considered	12/16/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

WAVELYNX EX. 1002, Pg. 440

WaveLynx Technologies v. ASSA Abloy, IPR2023-01018



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/689,088	01/27/2015	8943562	2943AAAB-178-DIV	9927

22442 7590 01/07/2015
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Scott B. Guthery, Chestnut Hill, MA;
Mark Robinton, Somerville, MA;
Michael Lawrence Davis, Amherst, NY;
David Andresky, Lafayette, CO;
ASSA ABLOY AB, Stockholm, SWEDEN

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.