(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(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

(30) Priority: **31.08.2005 US 713528**
16.08.2006 US 464912

(71) Applicant: **Assa Abloy Identification Technology Group AB**
107 23 Stockholm (SE)

(72) Inventors:
- **Davis, Michael L.**
  AMHERT, NY 14228 (US)
- **Hulusi, Tam**
  IRVINE, CA 92618 (US)

(74) Representative: **Grosfillier, Philippe**
Andre Roland S.A.
Intellectual Property Services
Avenue Tissot 15
P.O. Box 1255
1001 Lausanne (CH)

(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.

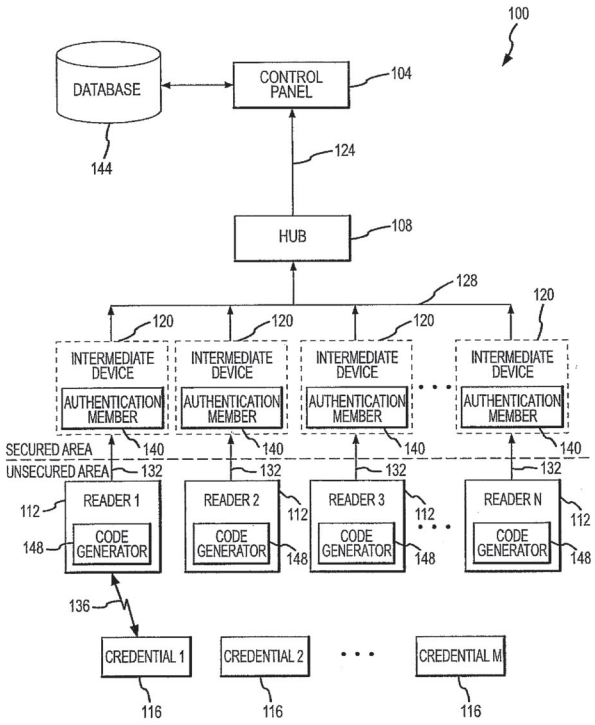


FIG.1

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 aigorithm(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 alternative 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 af 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.

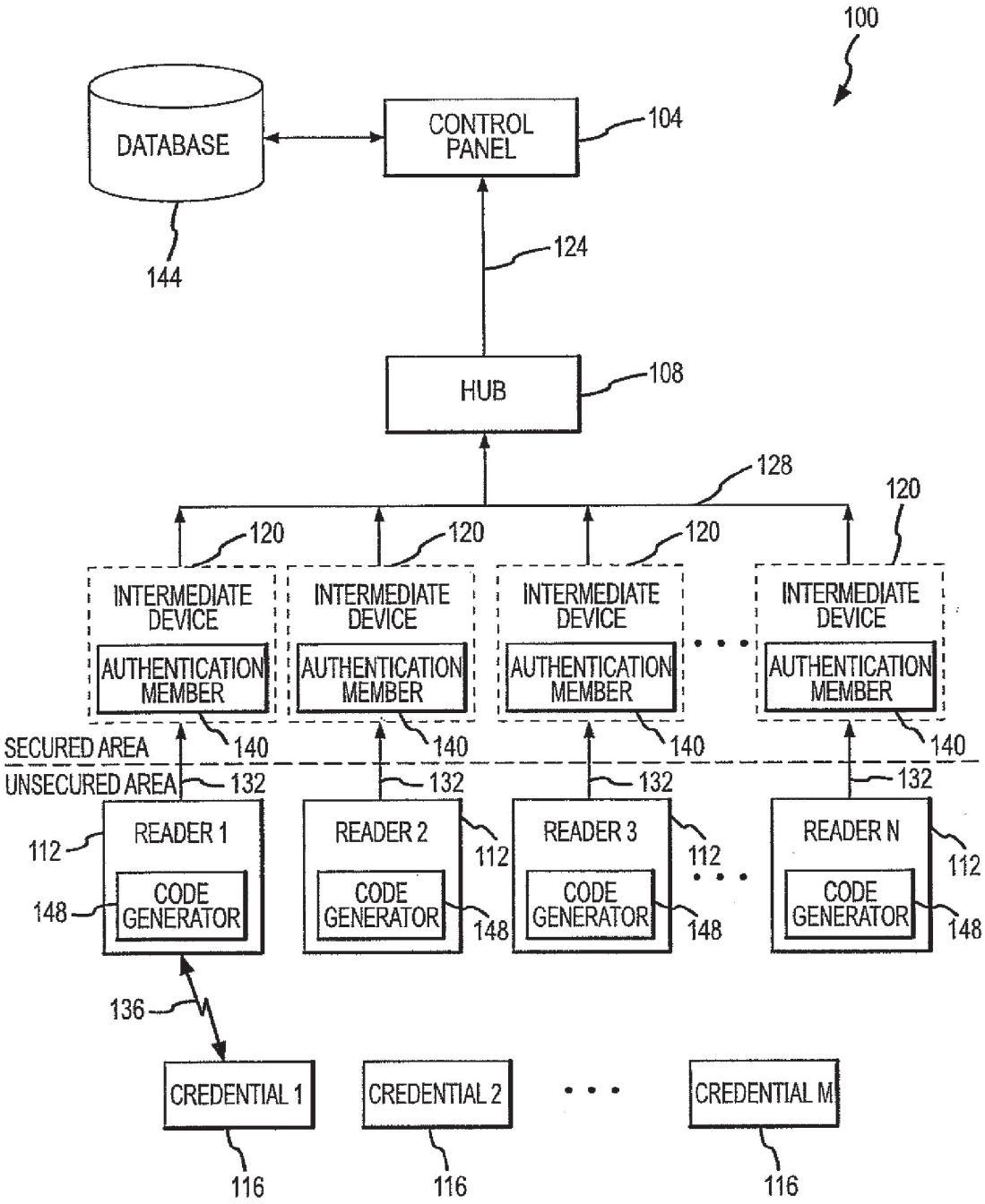


FIG.1

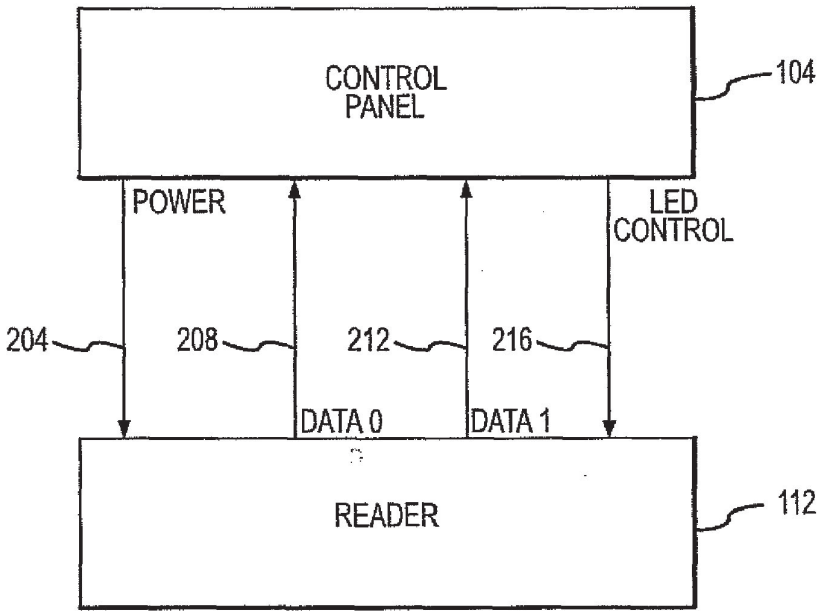


FIG.2
PRIOR ART

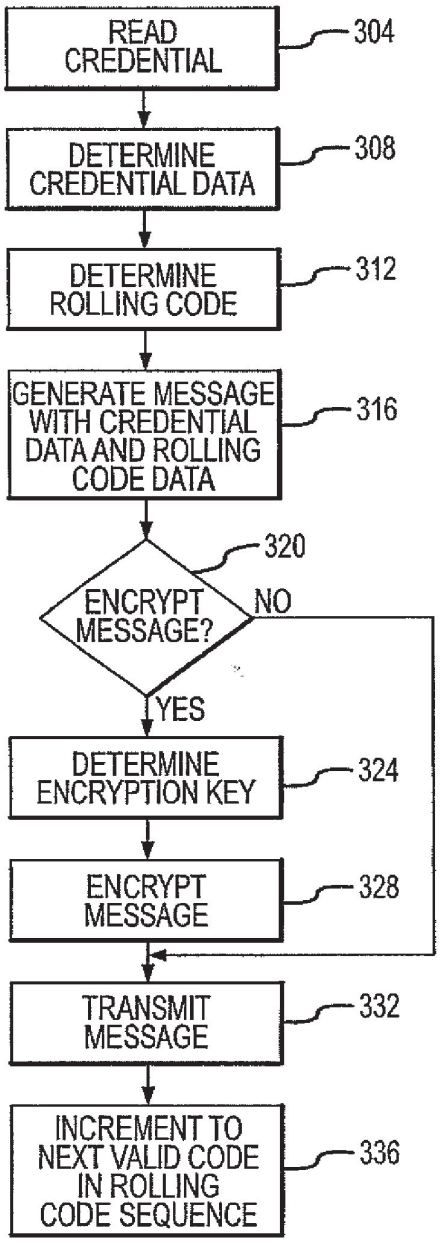


FIG.3

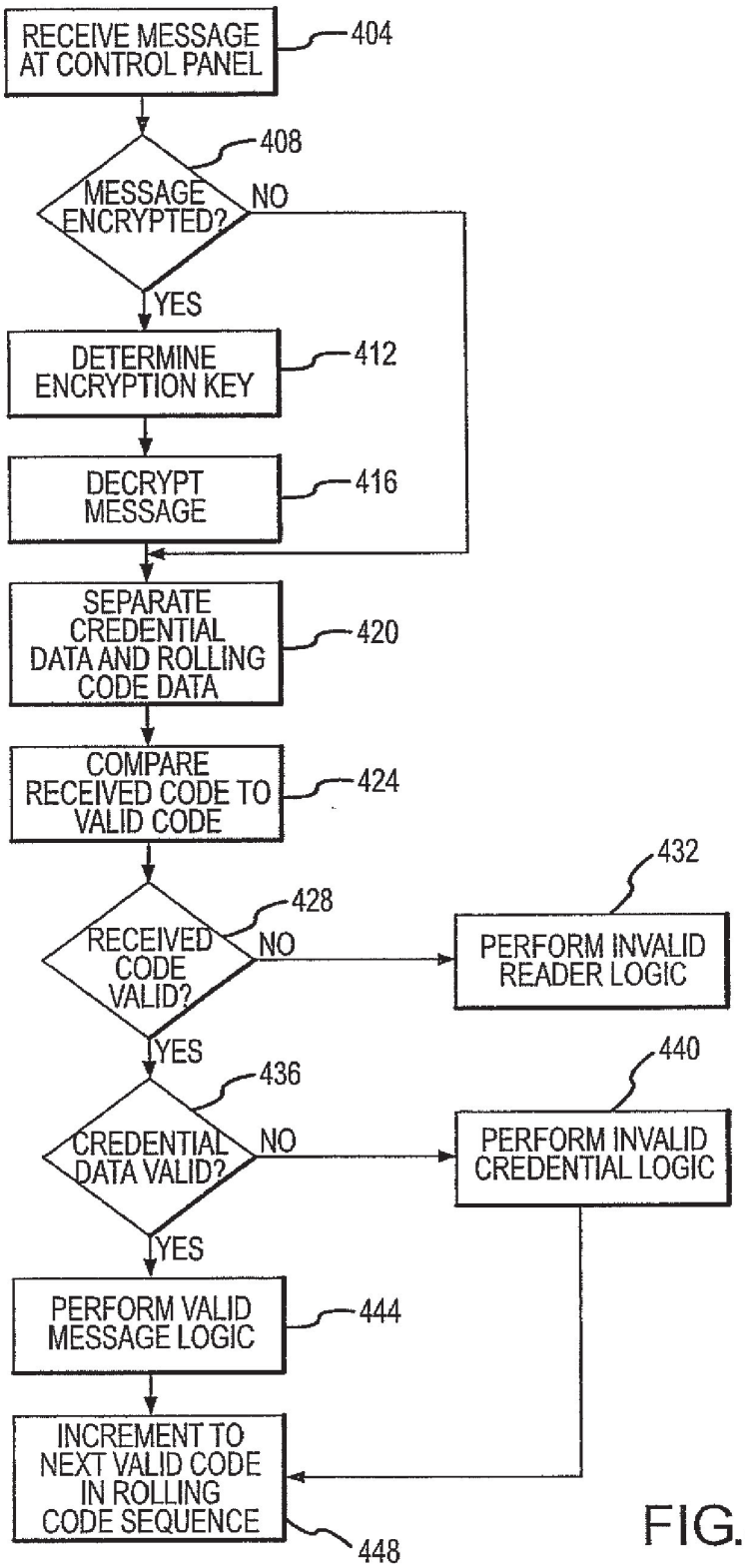


FIG.4

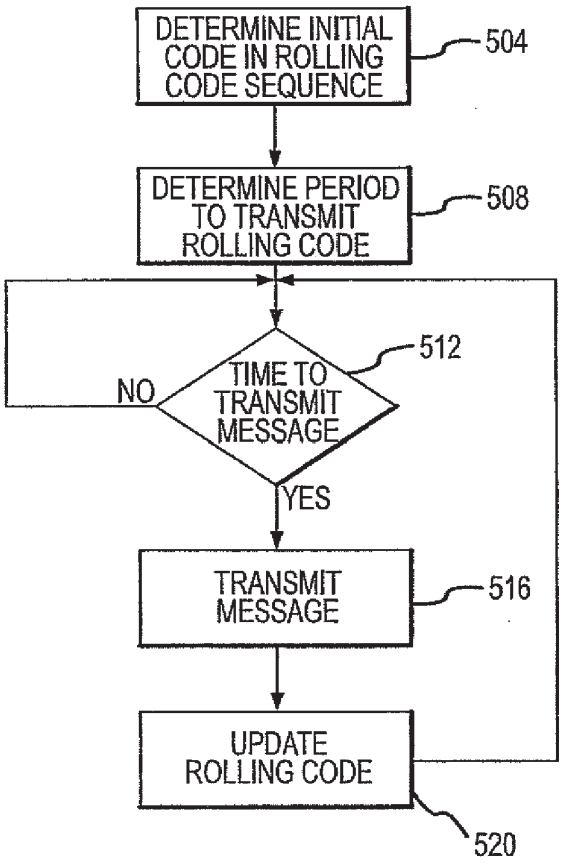


FIG.5

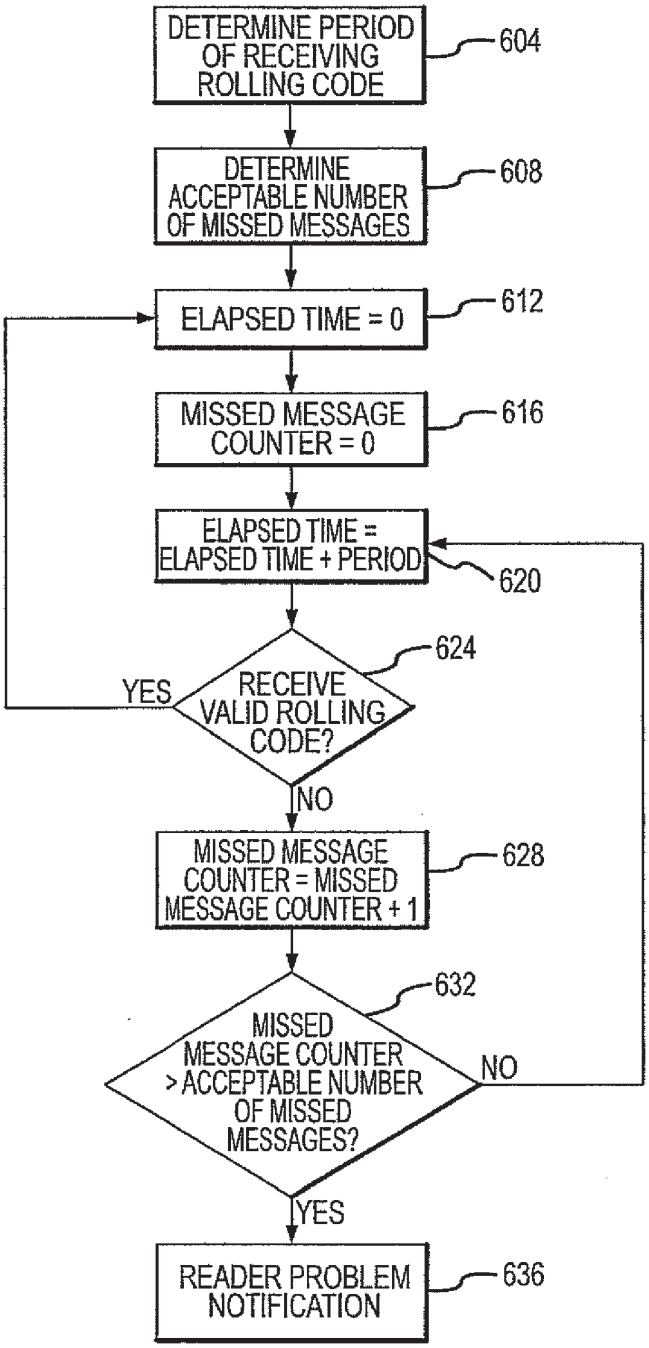
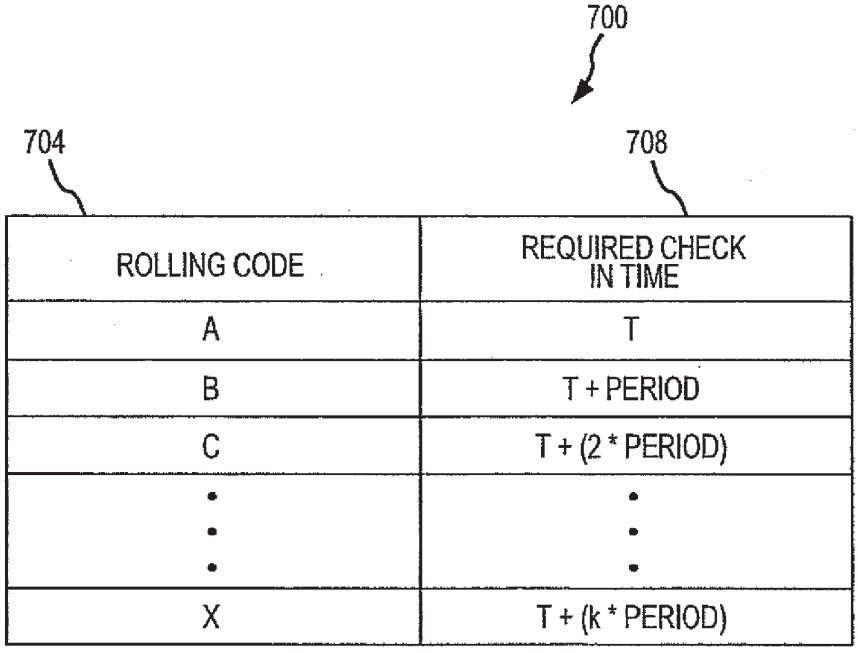


FIG.6



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]**