


5793302 		
UTILITY SERIAL NUMBER <b>08/747129</b>	PATENT DATE <b>AUG 11 1999</b>	PATENT NUMBER 
SERIAL NUMBER	FILING DATE RULE	CLASS
SUBCLASS		GROUP ART UNIT
EXAMINER		

APPLICANTS

*Bo*

NO

**CERTIFICATE**

MAR 30 1999

**OF CORRECTION**

NOTE-DISCLAIMER  
The term of this patent shall not extend beyond the expiration date of Pat. No. 5,227,344.

Foreign priority claimed 35 USC 119 conditions met	<input type="checkbox"/> yes <input checked="" type="checkbox"/> no	AS FILED	STATE OR COUNTRY	SHEETS OR WGS.	TOTAL CLAIMS	INDER CLAIMS	FILING FEE RECEIVED	ATTORNEY'S DOCKET NO.
Verified and Acknowledged <i>Bo</i>								

ADDRESS

*One Commerce Square*  
*2605 Market Street - 13th Floor*  
*PHILADELPHIA PA 19104*  
*7086*

TITLE

*B7* SECURING INFORMATION RELEVANT TO A TRANSACTION

U.S. DEPT. OF COMM. / PAT. & TM - PTO-436L (Rev. 12-98)

PARTS OF APPLICATION FILED SEPARATELY		CLAIMS ALLOWED Total Claims: <i>91</i> Print Claim: <i>1</i>	
NOTICE OF ALLOWANCE MAILED <i>11/21/98</i>		DRAWING Sheets Drwg. <i>15</i> Figs. Drwg. <i>22</i> Print Fig. <i>1</i>	
ISSUE FEE Amount Due <i>200.00</i> Date Paid <i>11/18/98</i>		PRIMARY EXAMINER <b>BRIAN ZIMMERMAN</b> GROUP 2200 2435	
PREPARED FOR ISSUE		ISSUE BATCH NUMBER <i>V91</i>	

WARNING: The information disclosed herein may be restricted. Unauthorized disclosure may be prohibited by the United States Code Title 35, Sections 122, 361 and 369. Possession outside the U.S. Patent & Trademark Office is restricted to authorized employees and contractors only.

ISSUE FEE IN FILE

*Ne*

# PATENT APPLICATION



08747174

APPROVED FOR LICENSE

INITIALS

## CONTENTS

Date  
Received  
or  
Mailed

1. Application <sup>+15 papers</sup> papers.
2. Letter w/ Drawings 11/12/96
3. PRIOR ART 11/12/96
4. Letter to Draftsman 11/12/96
5. Pre Am't A 11/12/96
6. Pre Am't B 11/12/96
7. ~~Re Am't C~~ March 11/99
- 4/9 8. Restriction (30 days) 4/9/99
9. ~~Restriction~~ 4/9/99
10. Supplemental Spec Art June 16/99
- 8/12 11. Am't C June 16/99
12. 1 Rpt 3 (230) 8-12-97
13. ~~Am't C~~ 11/24/99
14. ~~Am't C~~ Nov. 10/1999
15. ~~Am't C~~ Nov. 10/1999
16. Terminal Disclaimer 11/10/97
- 1/2 17. Notice of Allowability 1/2/98
18. ~~Am't C~~ Dec. 29/99
19. ~~Am't C~~ March 18/99
20. ~~Am't C~~ March 18/99
21. Notice of Entry 4/3/98
22. ~~Am't C~~ 5/4/98 4/24/98
23. PTO GRANT AND IT 1998
24. Extension of Time 4/2/98
25. ~~Am't C~~ 12-23-99
26. Director's Report 2-8-99
27. Pet. 1.28 7-5-97
28. Pet. Granted 8-08-08
- 29.
- 30.
- 31.
- 32.

(FRONT)

SEARCHED			
Class	Sub.	Date	Exmr.
340	825.31 825.34	8/11/97	BZ
380	43 44 45	12/30/97	BZ
update	search		

44

INTERFERENCE SEARCHED			
Class	Sub.	Date	Exmr.
search	Above	12/30/97	BZ

SEARCH NOTES		
	Date	Exmr.
none	12/30/97	BZ

Staple Issue Slip Here

POSITION	ID NO.	DATE
CLASSIFIER	10	12-26-91
EXAMINER	Simms	1-27-92
TYPIST	18	1-31
VERIFIER		
CORPS CORR.		
SPEC. HAND		
FILE MAINT.		
DRAFTING		

# INDEX OF CLAIMS

Claim	Date
Final	Original
1	101
2	102
3	103
4	104
5	105
6	106
7	107
8	108
9	109
10	110
11	111
12	112
13	113
14	114
15	115
16	116
17	117
18	118
19	119
20	120
21	121
22	122
23	123
24	124
25	125
26	126
27	127
28	128
29	129
30	130
31	131
32	132
33	133
34	134
35	135
36	136
37	137
38	138
39	139
40	140
41	141
42	142
43	143
44	144
45	145
46	146
47	147
48	148
49	149
50	150

Claim	Date
Final	Original
51	151
52	152
53	153
54	154
55	155
56	156
57	157
58	158
59	159
60	160
61	161
62	162
63	163
64	164
65	165
66	166
67	167
68	168
69	169
70	170
71	171
72	172
73	173
74	174
75	175
76	176
77	177
78	178
79	179
80	180
81	181
82	182
83	183
84	184
85	185
86	186
87	187
88	188
89	189
90	190
91	191
92	192
93	193
94	194
95	195
96	196
97	197
98	198
99	199
100	200

## SYMBOLS

- ✓ Rejected
- Allowed
- (Through numeral) Canceled
- + Restricted
- N Non-elected
- I Interference
- A Appeal
- O Objected

// EET INSIDE



## File History Report

- ☐ Paper number \_\_\_\_\_ is missing from the United States Patent and Trademark Office's original copy of the file history. No additional information is available.
- ☐ The following page(s) \_\_\_\_\_ of paper number \_\_\_\_\_ is/are missing from the United States Patent and Trademark Office's original copy of the file history. No additional information is available

Additional comments: **The Other Publications contain more than 500 pages; therefore we have not copied the documents due to the cost associated with the high volume of pages. At your request, we will attempt to obtain the missing publication(s) Please note that additional charges will apply to this service.**



US005793302A

## United States Patent [19]

Stambler

[11] Patent Number: 5,793,302

[45] Date of Patent: \*Aug. 11, 1998

[54] METHOD FOR SECURING INFORMATION  
RELEVANT TO A TRANSACTION[76] Inventor: Leon Stambler, 7803 Boulder La.,  
Parkland, Fla. 33067[\*] Notice: The term of this patent shall not extend  
beyond the expiration date of Pat. No.  
5,267,314.

[21] Appl. No.: 747,174

[22] Filed: Nov. 12, 1996

## Related U.S. Application Data

[60] Continuation of Ser. No. 446,369, May 22, 1995, which is a  
division of Ser. No. 122,071, Sep. 14, 1993, Pat. No.  
5,524,073, which is a division of Ser. No. 977,385, Nov. 17,  
1992, Pat. No. 5,267,314.[51] Int. Cl.<sup>6</sup> ..... H04Q 1/00

[52] U.S. Cl. .... 340/825.34; 380/43; 380/45

[58] Field of Search ..... 340/825.31, 825.34;  
380/43, 44, 45

## [56] References Cited

## U.S. PATENT DOCUMENTS

3,609,690 9/1971 Nissman .  
3,611,293 10/1971 Constable .  
3,657,521 4/1972 Constable .  
3,892,948 7/1975 Constable .  
3,938,091 2/1976 Atalla et al .  
4,004,089 1/1977 Richard et al .  
4,016,405 4/1977 McCune et al .  
4,186,871 2/1980 Anderson et al .  
4,198,619 4/1980 Atalla .  
4,200,770 4/1980 Hellman et al . 380/44  
4,208,575 6/1980 Hattot .  
4,208,739 6/1980 Lu .  
4,223,403 9/1980 Konheim et al .  
4,234,932 11/1980 Gorgens .  
4,264,782 4/1981 Konheim .  
4,264,808 4/1981 Owens et al .  
4,268,715 5/1981 Atalla .  
4,281,215 7/1981 Atalla .

(List continued on next page.)

## OTHER PUBLICATIONS

Shipley C., "I threw away my checkbook", PC-Computing,  
vol. 3, No. 11, pp. 112, 114-115, 118-120, Nov. 1990.Iida J., "Electronic Presentment Due for N.Y. Test", American  
Banker, vol. 157, No. 143, p. 3, Jul. 27, 1992.Torrez A., "Banking Industry Looks at Changing Check  
Guarantees", The Business Journal-Phoenix & The Valley  
of the Sun, vol. 9, No. 29, pp. 13-14, May 29, 1989.Sullivan D., "Bank Technology Trick or Treat?", Bankers  
Monthly, vol. 109, No. 11, pp. 10, 12-14, 18, 20, Nov. 1992.Seidenberg, "Bell Companies Now Testing Smart Card  
Offering Increased Feature Functionality", Card News, vol.  
5, No. 10, pp. 5-6, May 21, 1990."General Magnaplate Corporation Issues Three-Month  
Report to Stockholders", PR Newswire, 1 page, Nov. 11,  
1992.Byles T., "More Companies Are Paying Bills Electroni-  
cally", Journal of Commerce, p. 2B, May 5, 1988.Carreker J.D., "Strides in Electronic Checking Transforming  
Payment System", vol. 68, No. 3, pp. 18-19, 22, 24, 26,  
28, 30, Mar. 1992.

Primary Examiner—Brian Zimmerman

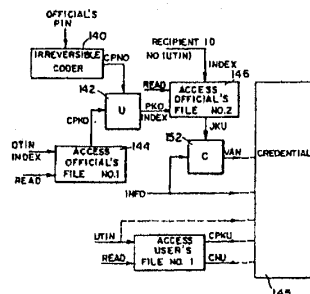
Attorney Agent, or Firm—Panitch Schwarze Jacobs &  
Nadel, P.C.

## [57]

## ABSTRACT

A transaction system wherein, when a transaction, document  
or thing needs to be authenticated, information associated  
with one or more of the parties involved is coded together to  
produce a joint code. This joint code is then utilized to code  
information relevant to the transaction, document or record,  
in order to produce a variable authentication number (VAN)  
at the initiation of the transaction. This VAN is thereafter  
associated with the transaction and is recorded on the  
document or thing, along with the original information that  
was coded. During subsequent stages of the transaction, only  
parties capable of reconstructing the joint code will be able  
to uncode the VAN properly in order to re-derive the  
information. The joint code serves to authenticate the  
parties, and the comparison of the re-derived information  
against the information recorded on the document serves to  
authenticate the accuracy of that information.

91 Claims, 15 Drawing Sheets



U.S. PATENT DOCUMENTS

4,283,599	8/1981	Atalla .	4,992,783	2/1991	Zdunek et al. .	
4,302,810	11/1981	Bonchius et al. .	4,995,082	2/1991	Schnorr .	380/23
4,304,990	12/1981	Atalla .	5,016,274	5/1991	Micali et al. .	
4,317,937	3/1982	Sandrow .	5,023,908	6/1991	Weiss .	
4,319,079	3/1982	Best .	5,054,066	10/1991	Riek .	
4,328,414	5/1982	Atalla .	5,067,155	11/1991	Bianco et al. .	
4,386,266	5/1983	Chesnek .	5,161,244	11/1992	Maurer .	380/43
4,405,829	9/1983	Rivest et al. .	5,163,098	11/1992	Dalbura .	
4,423,287	12/1983	Zeldner .	5,168,520	12/1992	Weiss .	
4,471,163	9/1984	Donald et al. .	5,187,351	2/1993	Clary .	
4,498,000	2/1985	Decavale et al. .	5,191,613	3/1993	Graziano et al. .	
4,590,470	5/1986	Koenig .	5,196,840	3/1993	Leich et al. .	
4,605,820	8/1986	Campbell, Jr. .	5,199,066	3/1993	Logan .	
4,665,396	5/1987	Dieleman .	5,218,637	6/1993	Angebaud et al. .	
4,686,357	8/1987	Duono et al. .	5,224,162	6/1993	Okamoto et al. .	
4,720,859	1/1988	Aaro et al. .	5,233,658	8/1993	Bianco et al. .	
4,734,858	3/1988	Schially .	5,267,314	11/1993	Stambler .	
4,740,890	4/1988	William .	5,283,829	2/1994	Anderson .	
4,747,050	5/1988	Brachfi et al. .	5,297,202	3/1994	Kapp et al. .	
4,755,940	7/1988	Brachfi et al. .	5,321,751	6/1994	Ray et al. .	
4,797,920	1/1989	Stein .	5,326,959	7/1994	Perazza .	
4,799,061	1/1989	Abrams et al. .	5,327,563	7/1994	Singh .	
4,823,264	4/1989	Deming .	5,341,428	8/1994	Schatt .	
4,908,861	3/1990	Brachfi et al. .	5,367,572	11/1994	Weiss .	
4,928,098	5/1990	Dannhaeuser .	5,400,403	3/1995	Fahn et al. .	
4,933,969	6/1990	Marshall et al. .	5,453,601	9/1995	Rosen .	
4,935,962	6/1990	Austin .	5,455,407	10/1995	Rosen .	
4,947,028	8/1990	Goreg .	5,465,299	11/1995	Matsumoto et al. .	
4,965,568	10/1990	Atalla et al. .	5,473,690	12/1995	Grinomez et al. .	
4,977,595	12/1990	Obta et al. .	5,530,755	6/1996	Pallua et al. .	
			5,677,955	10/1997	Doggett et al. .	

FIG. 1

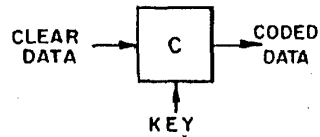


FIG. 2

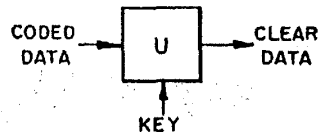


FIG. 3

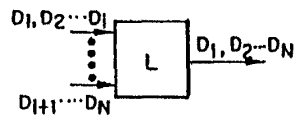


FIG. 4

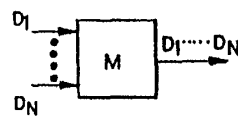


FIG. 5

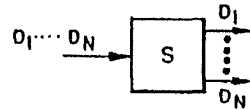
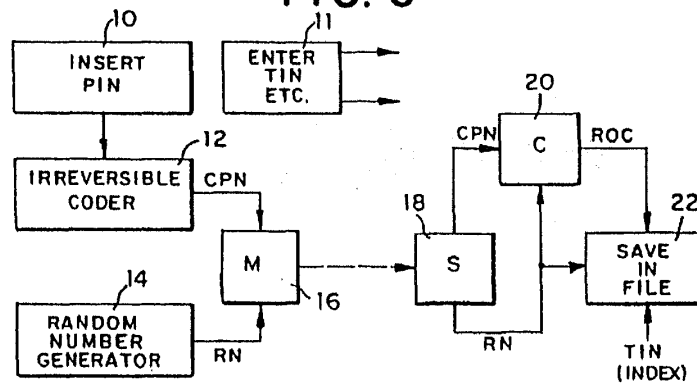
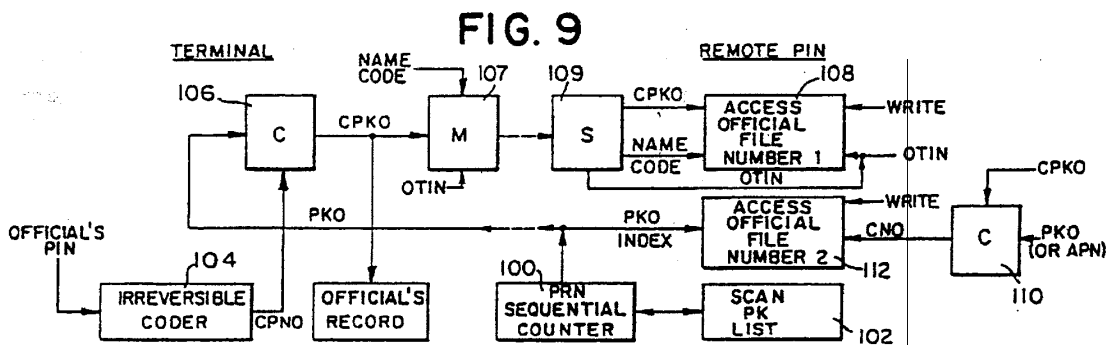
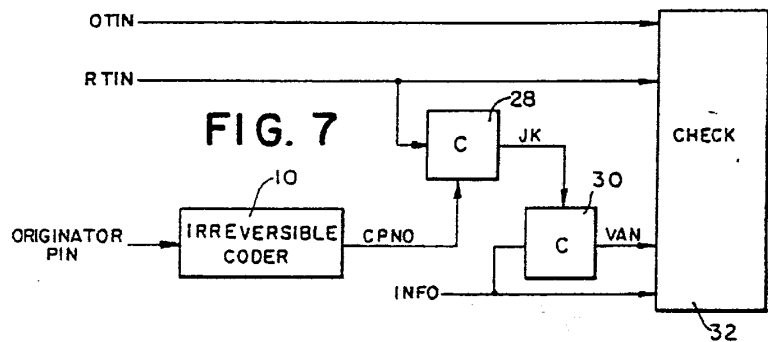
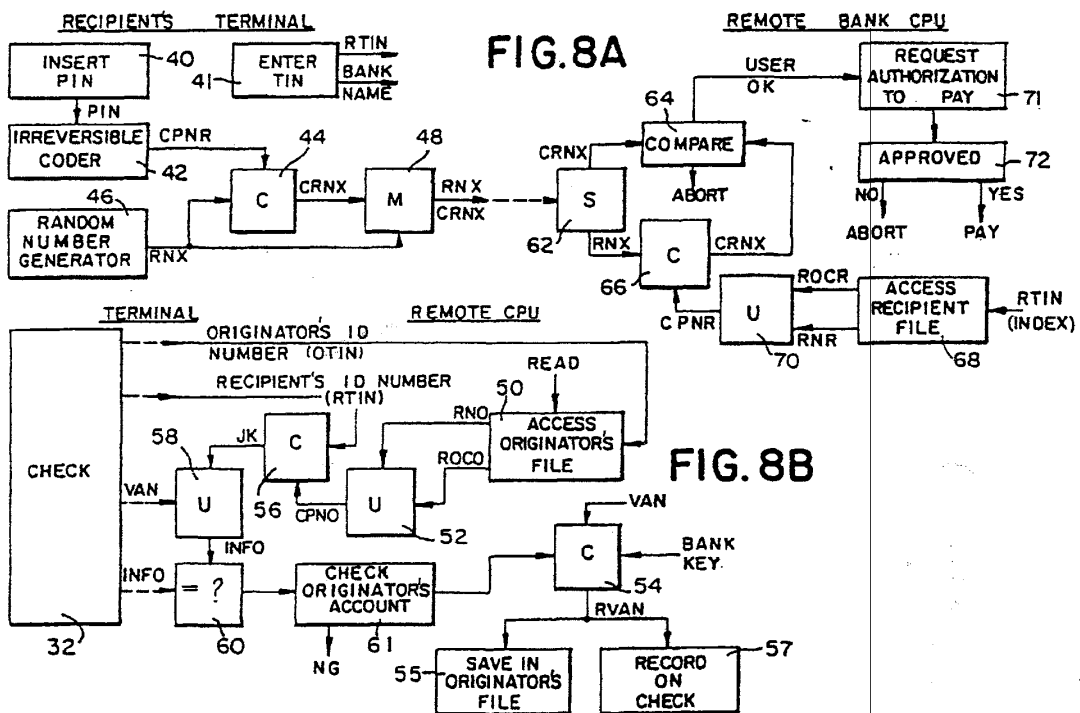


FIG. 6







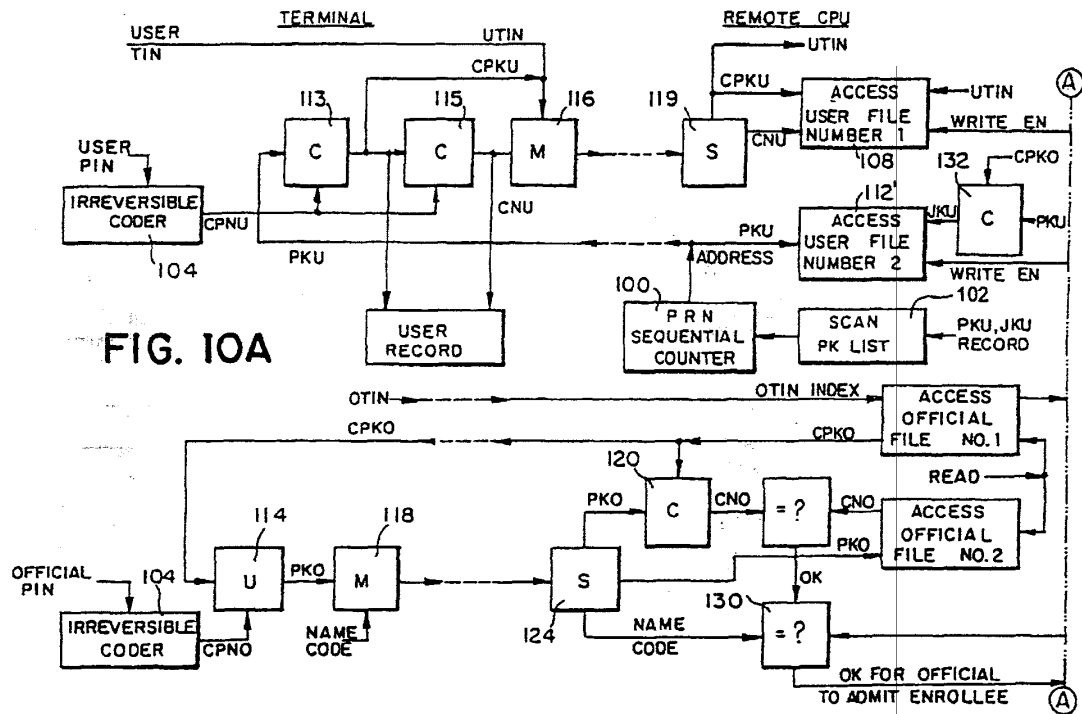


FIG. 10B

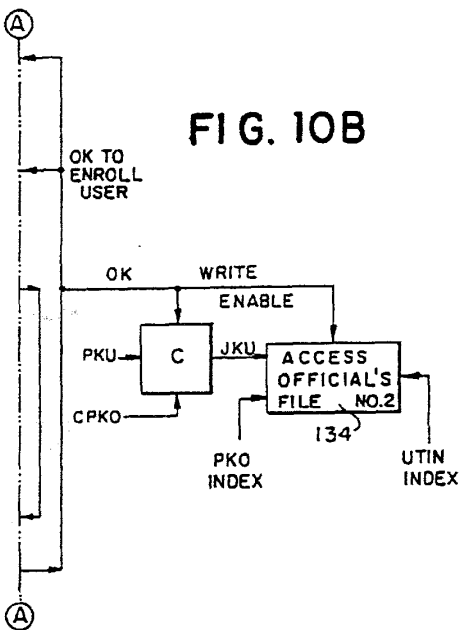
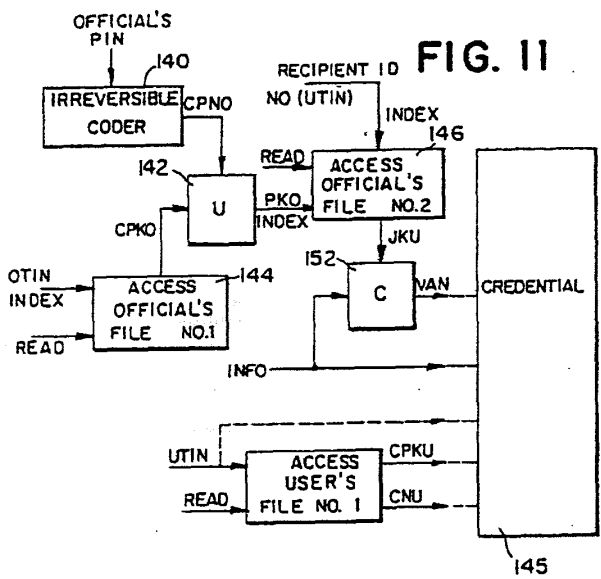


FIG. 11





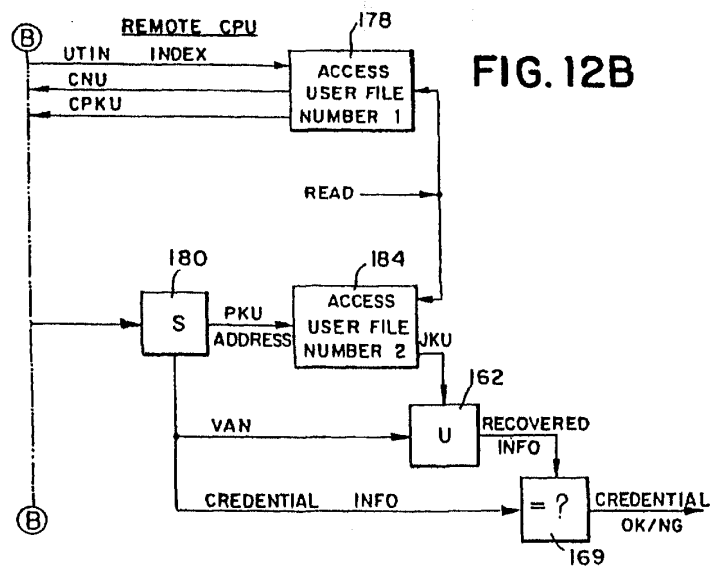
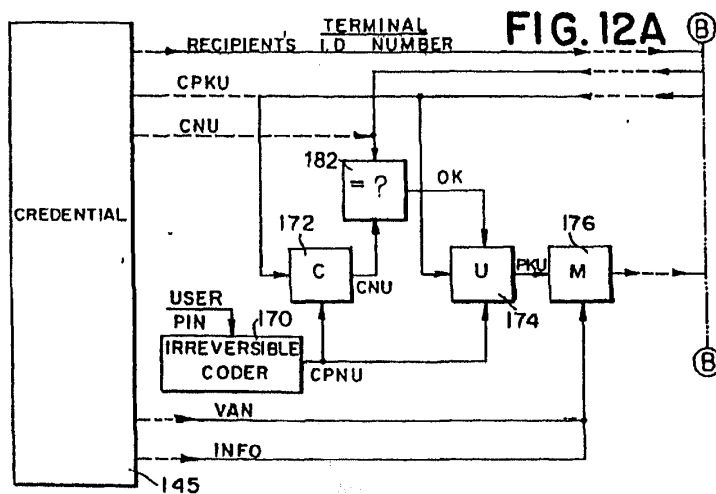
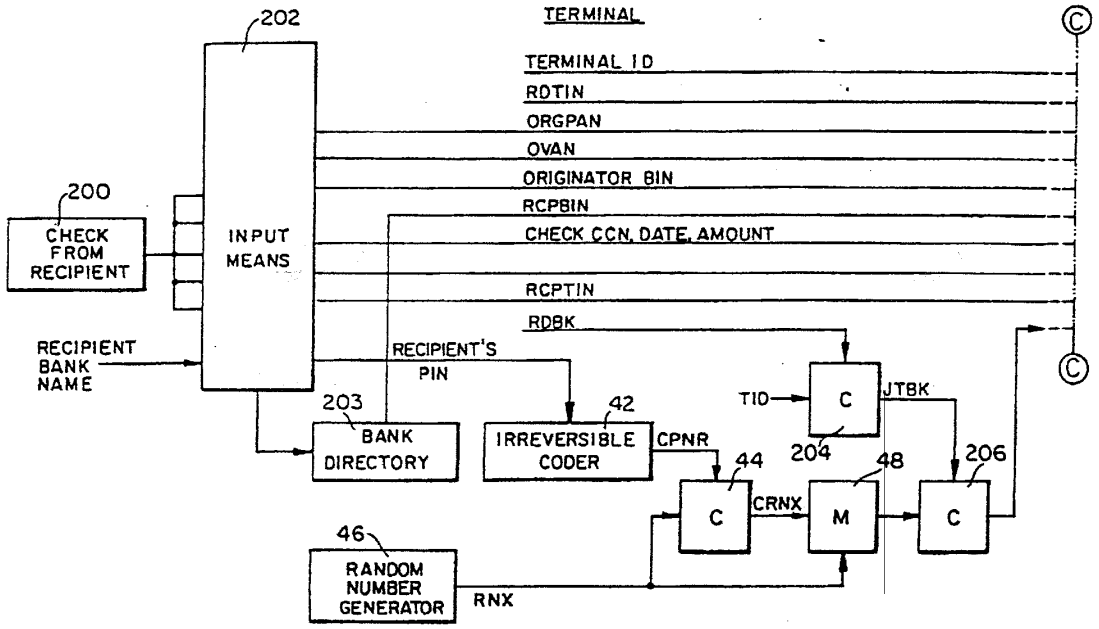
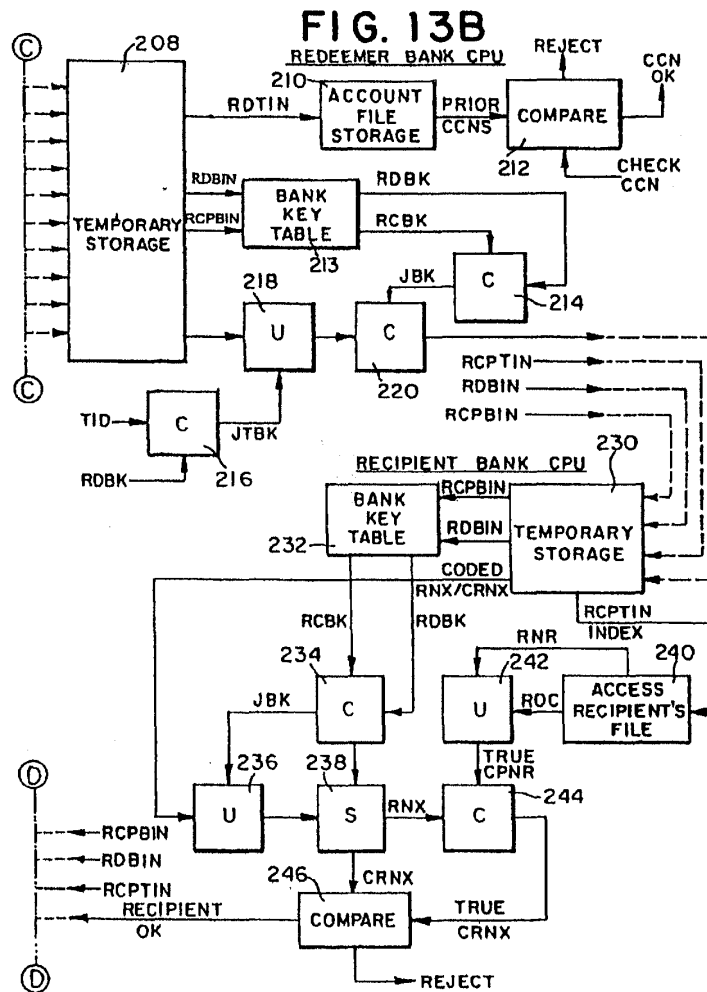


FIG. 13A





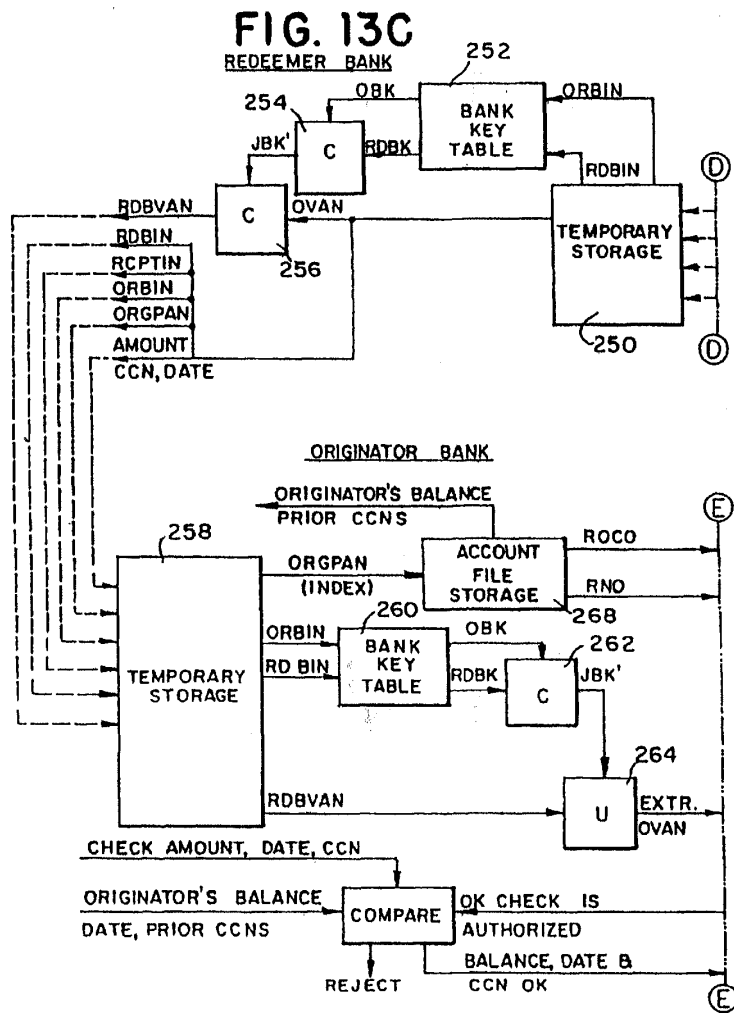
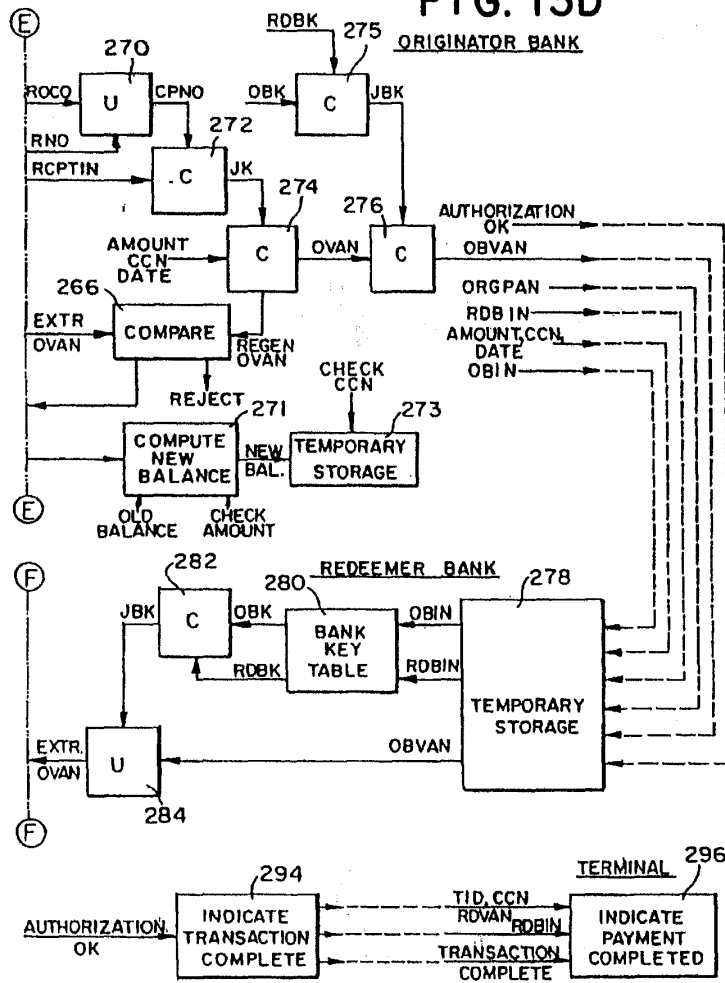
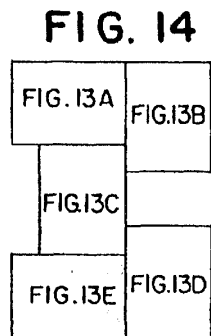
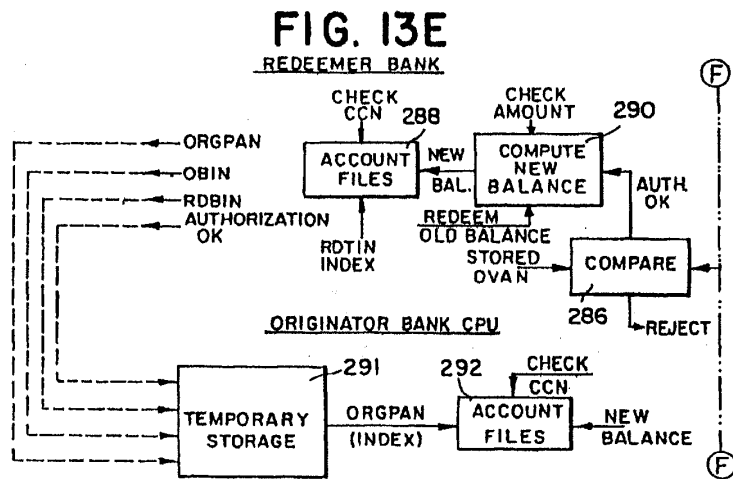
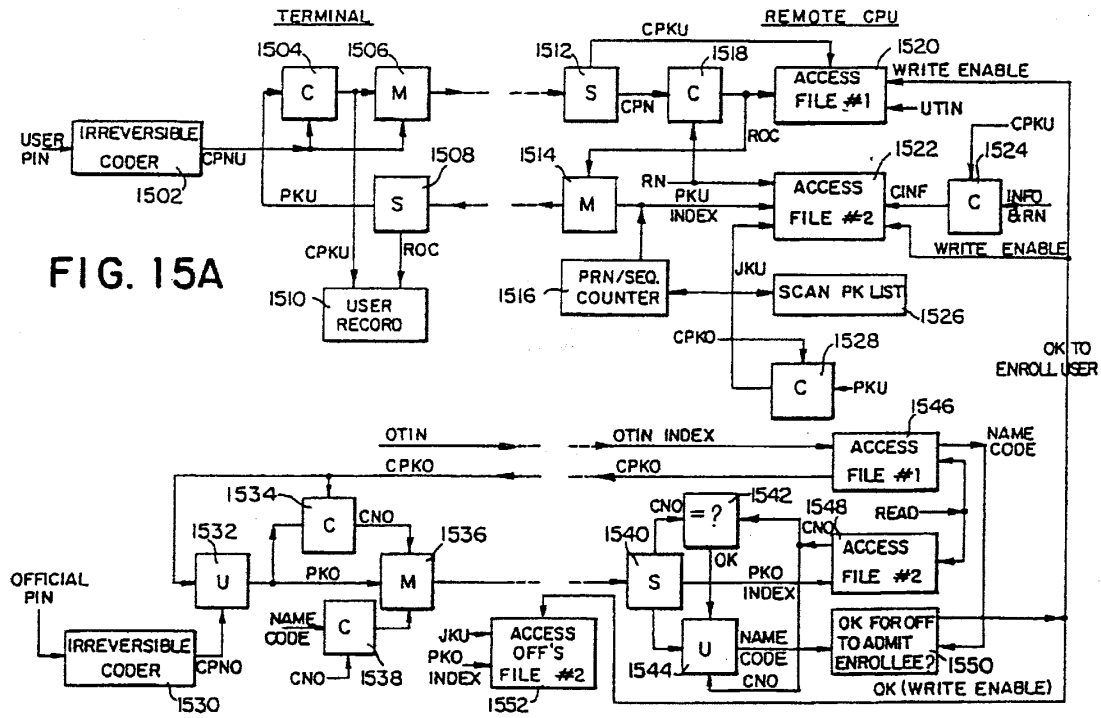


FIG. 13D







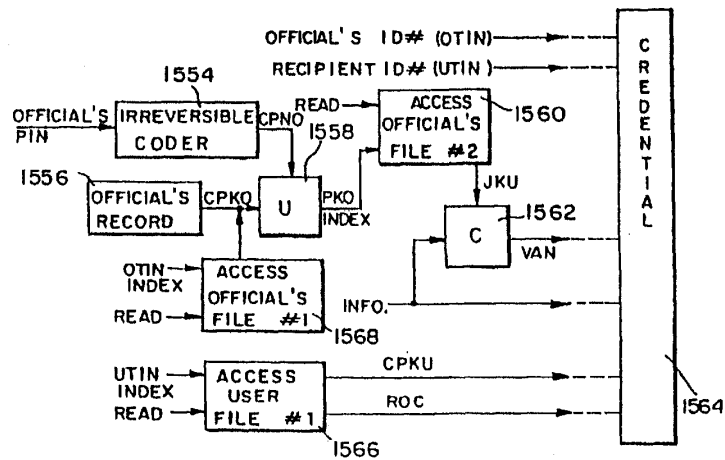
CREDENTIAL ISSUE PROCESSING AGENCY TERMINAL/COMPUTER

FIG. 15B



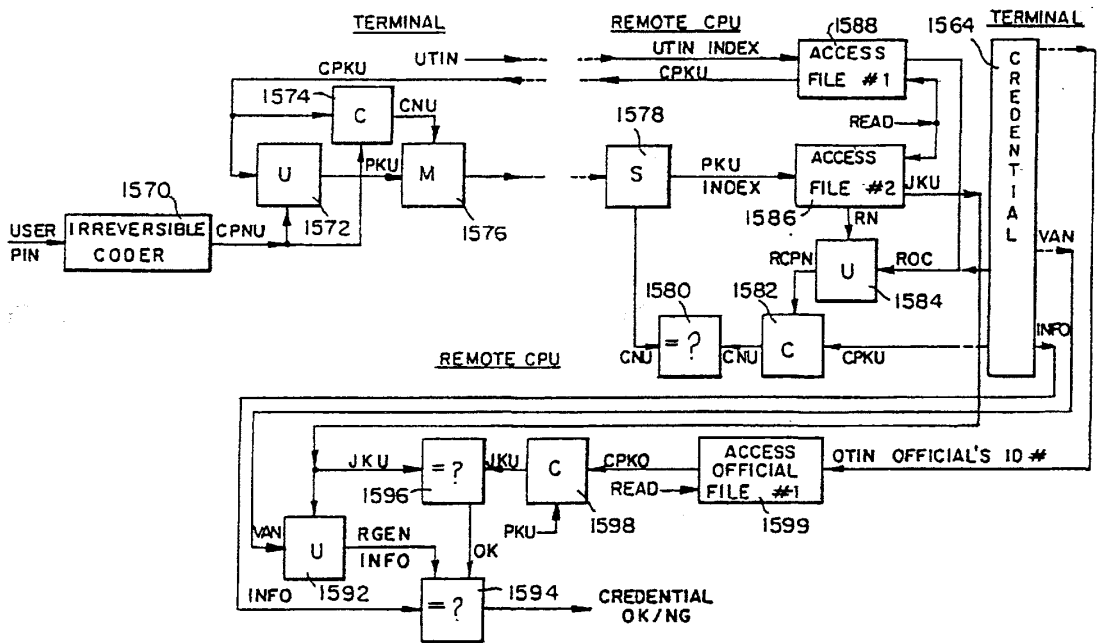


FIG. 15C

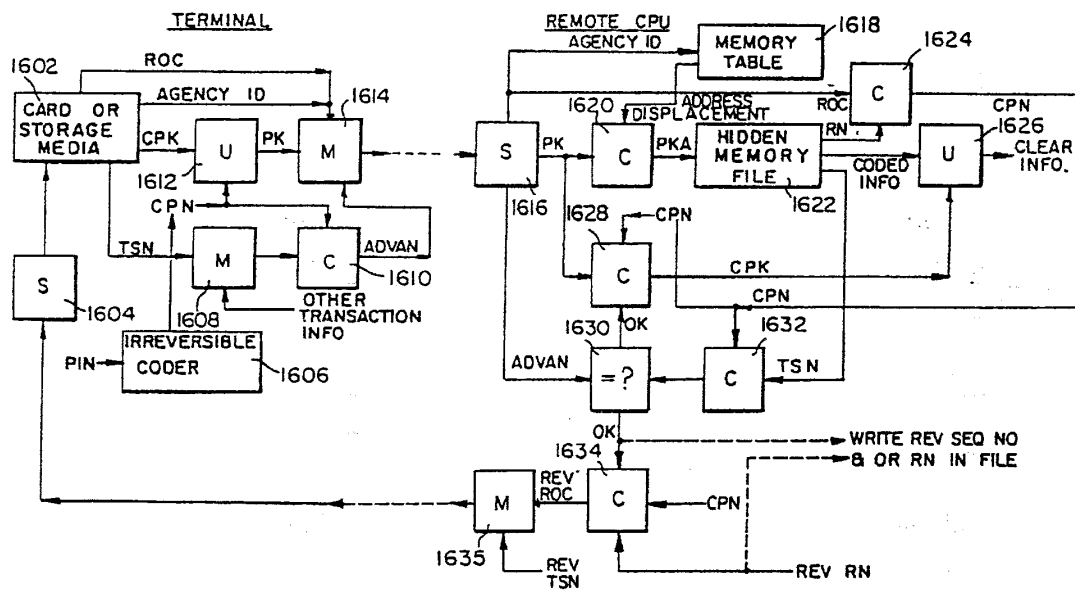


FIG. 16

# 1 **METHOD FOR SECURING INFORMATION RELEVANT TO A TRANSACTION**

This is a continuation of application Ser. No. 08/446,369, filed May 22, 1995, which in turn is a division of application Ser. No. 08/122,071, filed Sep. 14, 1993, now U.S. Pat. No. 5,524,073, which in turn is a division of application Ser. No. 07/977,385, filed Nov. 17, 1992, now U.S. Pat. No. 5,267,314.

This application is related to application Ser. No. 08/445,447, filed May 22, 1995, and application Ser. No. 08/445,612, now U.S. Pat. No. 5,646,998 filed May 22, 1995, now U.S. Pat. No. 5,555,303.

## **FIELD OF THE INVENTION**

The present invention relates generally to secure transaction systems and, more particularly, concerns a method and apparatus for authenticating documents, records and objects as well as the individuals who are involved with them or responsible for them.

## **BACKGROUND OF THE INVENTION**

There are many times in our daily lives when the need arises for highly secure transactions. For example, instruments of commerce, such as checks, stock certificates, and bonds are subject to theft and forgery. From the time a document is issued, the information contained on it, or the name of the recipient could be changed. Similarly, passports, pay checks, motor vehicle registrations, diplomas, food stamps, wage receipts, medical prescriptions, or birth certificates and other official documents are subject to forgery, fraudulent modification or use by an unintended recipient. As a result, special forms, official stamps and seals, and special authentication procedures have been utilized to assure the authenticity of such documents. Medical, legal and personnel records, and all types of information in storage media are also subject to unauthorized access. Passwords and coding of such records have been used to thwart unauthorized access. However, there have always been ingenious individuals who have somehow managed to circumvent or evade all such systems of security.

With the introduction of computers and computer communications into business transactions and document processing, a certain degree of security was gained, in that it is now possible to verify documents and transactions much more quickly, thereby avoiding many frauds which previously went unnoticed until it was too late. However, with the elimination of the human factor, verification of the identity of parties also became more difficult. A pressing need still exists for business transaction, document processing and record access systems which can assure the identity of the parties and the accuracy of the information involved in the transaction. As used herein, the term "record access systems" includes systems which access media which contains data, messages, text, FAX, audio, video, drawings, images, photo, electronic and physical mail, safe boxes, and the like. As used herein the term "business transaction system" will be intended as a generic term to describe all such transaction, document processing and record access systems, including ones not related to business use, such as passport authentication systems.

The security problems described above have been handled with some degree of success in systems involving a single party transaction where the party is present. For example, during the use of an automatic teller machine, the customer is the sole party involved and is present in person. However,

until the present invention, it has not been possible to verify the identity and to secure the interests of all parties to multi-party transactions and, in particular, absent parties to a transaction.

## **SUMMARY OF THE INVENTION**

Briefly, the present invention is directed to a transaction, document processing, or record access system which avoids the shortcomings of known systems of this type. In accordance with an embodiment of the present invention, when a transaction, document or thing needs to be authenticated, information associated with at least one of the parties involved (e.g., an originator and/or a recipient) is coded to produce a joint code. This joint code is then utilized to code information relevant to the transaction, document or record, in order to produce a variable authentication number (VAN) or code at the initiation of the transaction. This VAN is thereafter associated with the transaction and is recorded on the document or thing, along with the original information that was coded. During subsequent stages of the transaction, only parties capable of reconstructing the joint code will be able to uncode the VAN properly in order to re-derive the information. Thus, the joint code serves to authenticate the parties, and the comparison of the re-derived information against the information recorded on the document serves to authenticate the accuracy of that information. Alternatively, the information could be authenticated by regenerating a VAN from the recorded information and comparing the regenerated VAN with the recorded VAN.

In accordance with an embodiment of the present invention, at the time of enrolling as a user of the system, each user selects a personal identification number (PIN), which is secret, does not exist in an uncoded form, and cannot be recovered from other information anywhere in the system. During or after enrollment, a non-secret identification code and a secret code are also stored in a user's file at the user associated computer facility. When a user participates in a transaction, the user is required to utilize his or her PIN, which after being coded is used to derive a coded arbitrary number. Subsequently, this arbitrary code is compared to another such code which is generated from a reconstituted version of the coded PIN, in order to authenticate the user's identity. One of the embodiments creates a computer file with a secret address to authenticate a user's identity, and to secure sensitive records. The address is preferably not stored anywhere in the system, but is generated when needed from information supplied by the user. In some embodiments of the present invention, when a joint code is created as described above, one participating user (e.g., the originator) must provide his or her PIN. The other party's non-secret identification code and the PIN are utilized in creating the joint code. In other embodiments, the joint code is created from the coded PIN's of the participants.

## **BRIEF DESCRIPTION OF THE DRAWINGS**

The foregoing brief description as well as further objects, features, and advantages of the present invention will be understood more completely from the following detailed description of the presently preferred, but nonetheless illustrative, embodiments of the invention, with reference being had to the accompanying drawings, in which:

FIGS. 1-5 illustrate the symbols utilized in the present application to represent conventional building blocks used to form the invention, these building blocks being respectively, a coder, an uncoder, a linker, a mixer, and a sorter;

FIGS. 6-8 are functional block diagrams illustrating a check transaction system in accordance with a first embodiment of the present invention, with FIG. 6 illustrating user enrollment, FIG. 7 illustrating how an originator generates a check, and FIGS. 8A and 8B illustrating the authentication process when the check is presented to be cashed;

FIGS. 9-12 are functional block diagrams illustrating a credential issuing and authentication system in accordance with a second embodiment of the present invention, with FIG. 9 illustrating the enrollment of an official, FIG. 10 illustrating the enrollment of a user, FIG. 11 illustrating the issuance of the credential, and FIG. 12 illustrating the authentication of an issued credential;

FIGS. 13A-13E, when arranged as illustrated in FIG. 14, collectively represent a functional block diagram of a check transaction system similar to that of FIGS. 6-8, but including the basic processing necessary to clear and pay a check electronically;

FIGS. 15A-15C are functional block diagrams of a credential issuing and authentication system according to an alternate embodiment of the present invention; and

FIG. 16 is a functional block diagram of a system for authenticating a party and for authorizing access to a secret file associated with the party according to an alternate embodiment of the present invention.

#### DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIGS. 1-5 illustrate the functional building blocks utilized in the preferred embodiments. All of these components are conventional building blocks for computer or communication systems. Moreover, those skilled in the art will appreciate that the blocks can be realized as hardware components, or they can be realized as functional blocks in an overall computer program.

The coder illustrated in FIG. 1 and the uncoder illustrated in FIG. 2 may be any form of such device utilizing a known algorithm, such as the Data Encryption Standard (DES). A coder, as illustrated in FIG. 1, has at least one data input, at which it receives clear data. It also has one or more additional inputs for receiving keys  $K_1$ ,  $K_2$ , which are utilized to code the clear data into a form in which it could not be easily recognized or decoded without the use of the keys. A variable which is used as a key may be padded to obtain the desired security. An uncoder (FIG. 2) reverses the process of the coder. Basically, it receives the coded data and utilizes the same keys to reconstruct the clear data.

A linker (FIG. 3) receives a plurality of data inputs and concatenates them into a longer code word ( $D_1, D_2, \dots, D_n$ ). Similarly, a mixer (FIG. 4) receives a plurality of data inputs ( $D_1$  and  $D_2$  through  $D_n$ ) and mixes their digits or binary bits. A simple example of a mixer would be a conventional time division multiplexer which is used to interleave plural data inputs. However, in many applications, it will be preferable to utilize a more sophisticated mixer, such as one that utilizes arithmetic and logical combinations of digits or bits. A sorter (FIG. 5) reverses the process of a linker or a mixer, that is, it receives a concatenated or mixed code word and reproduces the original component words. A time division demultiplexer could serve as a sorter for a mixed signal originally generated by a multiplexer.

FIGS. 6, 7, 8A and 8B constitute a functional block diagram illustrating the present invention in a check transaction system. The system illustrated in FIGS. 6, 7, 8A and 8B are well suited for use in generating and processing employee paychecks, for example. The system involves

three phases of operation. In the first phase, illustrated in FIG. 6, a user of the system must enroll in order to be recognized by the system. Each user enrolls at his or her bank, or at another convenient location, such as a place of employment, in the presence of an officer, who appropriately verifies the user's identity and obtains the typical information from him, including his taxpayer identification number (TIN) and telephone number. An account is then opened for the user and a file is created for him or her in the bank's computer, and the bank assigns a person account number (PAN) to the user's account. If a bank card is issued to the user, it usually contains the PAN and a bank identification number (BIN).

While operating a terminal, the user is requested to select a personal identification number (PIN) and to enter that PIN into the terminal. The user complies and such entry occurs at block 10 of FIG. 6 with the typical transaction information, including the user's TIN or PAN, being entered at block 11. The PIN is applied directly to an irreversible coder 12, where it is processed to produce a coded PIN (CPN). Coder 12 may be any type of conventional coding device which can process the PIN so that the coding is irreversible (i.e., the PIN cannot be recovered from the CPN). At the same time, a random number generator 14 produces a random number (RN), which is applied to a mixer 16 along with the CPN. Alternately, the user may be permitted to select an arbitrary number for RN.

The signal produced by mixer 16 is then transmitted to the bank's computer, where it is applied to a sorter 18. It is assumed that this transmission preferably occurs over a secure line, such as one protected by a tandem coder and uncoder which can utilize a joint terminal-bank key. The sorter recovers the original CPN and RN, saving RN in the user's file at block 22. It should be noted that in saving RN, the user's file is accessed by using his TIN as an index. The received CPN is applied as the data input to a coder 20, which receives RN as its key input, producing a reversible owner code (ROC) which is saved in the user's file in the same manner as RN. Various additional information is saved in the user's file, such as his personal account number (PAN), name, phone number (PHN), account balance, and other relevant information. The user's TIN, PAN or PHN can be used as an index to access the user's file. CPN represents coded authentication information since it is a coded form of the PIN, and since it is used in other parts of the system to authenticate the user and the transaction. The system preferably maintains RN as a secret number (although in the present embodiment the user file is not secret since it is accessed using a non-secret index) and ROC is maintained as a non-secret number. As explained in detail below, CPN is derivable from ROC and RN.

FIG. 7 illustrates how the originator generates a check in accordance with the present invention. This process preferably takes place at the originator's terminal or computer. It is assumed that the originator would be generating a check in the usual manner and would include on it all of the information usually found on a check, as well as the information normally recorded or imprinted on check forms, such as the recipient's name and TIN (RTIN), and the originator's personal account number and bank identification number. Preferably, the terminal includes a check reader and printer which can read necessary information from the originator's check form and print information on the form, although this could also be done manually by the originator. The originator and the recipient can be the same person, for example, where a person is cashing a personal check originated by the person. In the case of multi-party checks, the check is

5

originated by a present party (i.e., the originator) in favor of an absent party (recipient).

The originator enters his or her PIN at a terminal or computer. Through irreversible coder 10, the originator's PIN is converted to a coded PIN (CPNO), which is applied as the key input to coder 28. The data input to coder 28 is the recipient's TIN (RTIN), which has been read from the check, or accessed from the computer memory, or entered by the originator. The data output of coder 28 is a joint key (JK), which is applied as the key input to a coder 30. Generally, the JK is generated using information associated with at least one of the parties involved in the transaction (in this case, the originator and recipient). As will be shown more fully below, the joint key (or code) is used to protect and authenticate the originator and recipient. The data input to the coder 30 is the information (INFO) to be authenticated (that is, information relevant to the transaction, such as check number, amount, etc.).

The data output of the coder 30 is a variable authentication number (VAN), which codes the information to be authenticated, based upon information related to the recipient and information related to the originator. Note that the VAN is alternatively generated directly from INFO and information associated with at least one of the parties, without the intermediate step of generating the JK. The VAN and at least a portion of the information relevant to the transaction are written or imprinted upon the check 32, thereby becoming a permanent part of it. Alternately, the check may represent an electronic transfer of funds or some other type of electronic transaction. In this case, the VAN and at least a portion of the information relevant to the transaction are included with the electrical signals associated with the electronic transaction.

It is contemplated that in creating the VAN, all information would not necessarily be coded in the same manner. For example, the amount of the check might be considered important enough so as to be recoverable completely, and it would be coded into the VAN in a manner that would permit complete recovery. Other information, such as the date and check control number might be considered less important and would be coded into the VAN in such a manner as to permit detection of changes (e.g., error detection coding), but without complete recovery of the original information.

As noted above, other predetermined information which is known jointly by the originator and recipient, and which does not appear on the check, can also be used to derive the VAN. For example, when a check is drawn to multiple recipients, e.g., husband and wife, each recipient's TIN (which does not appear on the check) may be used to derive the joint code and VAN. This makes it more difficult to fraudulently generate the VAN since the predetermined information not appearing on the check would not be generally known.

FIGS. 8A and 8B illustrate the authentication process at a terminal when the recipient presents the originator's check to be cashed. The terminal communicates via a network of the banks involved in the transaction. Preferably, the terminal includes a device which can read information directly from the check 32. Alternately, the terminal operator can manually key information into the terminal, based upon information appearing on the face of the check 32. At block 40, the recipient inserts his or her PIN, and at block 41, identifies his bank and enters his TIN (RTIN) and all information required by the terminal to initiate the transaction. An irreversible coder 42 processes the PIN to produce the coded PIN, CPNR, which is applied as the key input to

6

a coder 44. A random number generator produces a random number (i.e., an arbitrary number) RNK which is applied as the data input to coder 44. Coder 44 then produces a coded random number (i.e., a coded arbitrary number), CRNK, which is applied to mixer 48 along with RNK. The output of the mixer is, therefore, a signal which contains CRNK and RNK in a converted form, so that neither number nor CPNR may readily be discerned from the signal. CRNK represents coded authentication information because it is a coded representation of CPNR, and because it is used by the system to authenticate the recipient and the transaction.

The mixer signal, along with the information entered in block 41 and the information read from the check are transmitted to the computer at the recipient's bank (i.e., remote bank CPU) over preferably an unsecured line (the use of an unsecured line is possible because CRNK and RNK, not CPNR, are transmitted from the mixer 48 to the sorter 62). The system first authenticates the identity of the check holder at the recipient's bank. Next, the information on the check, as well as the originator and recipient, are authenticated at the originator's bank.

At the recipient's bank, the output of mixer 48 is received in a sorter 62, which separates CRNK and RNK, with CRNK being applied to a comparison block 64 and RNK being applied as the data input to a coder 66. Based upon the recipient's TIN, RTIN, his bank's computer is able to access his file at block 68 and to extract his ROC (a non-secret number) and RN (a secret number), ROCR and RNR therefrom. ROCR and RNR are applied as the data and key inputs, respectively, to an uncoder 70, which generates the recipient's CPN, CPNR, which is applied as the key input to coder 66. Coder 66, therefore, reproduces the recipient's coded random number, CRNK (in the same manner as coder 44), which is applied as the second input to comparison block 64. It should be appreciated that the CPNR output of uncoder 70 is the true CPNR derived from the bank's records. Accordingly, the CRNK produced by coder 66 is the true CRNK. Therefore, should the comparison at block 64 fail, the authentication of the recipient has failed and it is presumed that recipient is not the party presenting the check. The transaction is therefore aborted. On the other hand, if the recipient's identity is authenticated, the transaction can proceed. The recipient's bank then communicates with the originator's bank, conveying all the information about the transaction and requesting authorization to pay (block 71).

As shown in FIG. 8B, at the originator's bank, using OTIN (or the originator's PAN) as an index, the originator's ROCO and random number, RNO, are extracted from the originator's file at block 50. ROCO is applied as the data input to an uncoder 52, and RNO is applied as the key input to uncoder 52. Uncoder 52 therefore reverses the operation performed by coder 20 (FIG. 6) when the originator enrolled, producing the originator's CPN, CPNO. CPNO is then applied as the key input to a coder 56, which receives the recipient's TIN, RTIN, as the data input.

In accordance with the embodiment just described, it is contemplated that security considerations may warrant revising the ROC from time to time independent of any transaction. Toward this end, CPN could be reconstituted from the current ROC and RN as in block 52. Next, a new RN is used with CPN to generate a revised ROC, making use of a coder in the same manner as coder 20 of FIG. 6. The user's new RN and ROC are stored and accessed, and CPN need only be reproduced at the bank where the user maintains an account.

In the same manner as coder 28 of FIG. 7, coder 56 therefore produces the joint key JK. JK is applied as the key

7

input to an uncoder 58, which receives the VAN from check 32 as its data input. Uncoder 58 therefore reverses the coding operation performed by coder 30 of FIG. 7. If the information on the check has been unmodified, the coder 58 should therefore reproduce the information INFO from the check which was sought to be authenticated. In block 60, a comparison is made between the output of uncoder 58 and the information appearing on the check. Failure of this comparison is an indication that the check may have been modified after being issued, and the originator's bank notifies the recipient's bank that the check will not be honored. Alternatively, the joint key JK from the coder 56 can be used to code the information (INFO) from the check to generate a new VAN, which can then be compared with the VAN from the check to authenticate the check.

Should the comparison be favorable, this is an indication that the check is authentic and unmodified, and the originator's bank accesses the originator's account (block 61) to determine if the account is in order and has sufficient funds or credit to pay the check. The date of the check is determined to be acceptable. If the check control number does not appear in the originator's file as a previously cashed check, then the current check control number is saved to prevent fraudulent check reuse. The originator's bank generates a redeemed or redemption VAN (RVAN) in coder 54, using its bank key and the original VAN. RVAN is saved in the originator's file (block 55) and is recorded on the check (block 57). The originator's account is then debited. The originator's bank then authorizes the recipient's bank to pay the check. On the other hand, if originator's bank finds any irregularity in the check or in the originator's account, it will notify the recipient's bank that the check is dishonored.

The RVAN (and other RVAN's from other transactions) can be accessed from originators' files by banks and other financial institutions involved with processing checks to determine the status of checks. Thus, by creating and storing the RVANs in the originators' files, fraudulent reuse of checks is avoided.

At block 72 (FIG. 8A), the recipient's bank receives the originator's bank's instructions. It will then notify the recipient if the check has been dishonored. If the check has been honored, the recipient's account may be credited as in a deposit. Alternately, the recipient can receive payment immediately if he is at an appropriate terminal, such as an automatic teller machine.

Essentially, the check has cleared automatically, on-line, without further check handling or processing.

In a transaction where the user cashes his own personal check, the originator and recipient are one and the same. A VAN is created from a joint code which combines information associated with the user, such as the user's identification number (TIN or PAN) and the user's CPN, which is generated directly from a PIN entered by the user. When the VAN is authenticated, the joint code is derived by combining the user's identification number (TIN or PAN) and the user's true CPN, which is generated from the RN and ROC retrieved from the user's file, with the TIN (or PAN) serving as a file index.

As noted above, in FIG. 8A it is possible to use an unsecured link between the mixer 48 and the sorter 62 because CRNX and RN, not CPNR, are transmitted from the mixer 48 to the sorter 62. However, a security problem still exists in using an unsecured line between the mixer 48 and the sorter 62 because the signal can be recorded and then played back later to attempt to fraudulently authenticate a fraudulent transaction. In an alternate embodiment of the

8

present invention, an anti-duplication variable authentication number (ADVAN) is generated at the recipient's terminal by coding at least a transmission date and time with the CPNR by a coder (not shown). The ADVAN is then mixed with the CRNX and the RN by the mixer 48 and sent to the remote bank CPU over the unsecured line to the sorter 62. At the remote bank CPU, the CPNR which is generated by the uncoder 70 is used to uncode the ADVAN to regenerate the transmission date and time. The signal received over the unsecured line is then authenticated by comparing the regenerated transmission date and time to a reception date and time (that is, the date and time at which the signal was received at the remote bank CPU). In this manner, the recipient and transaction are further authenticated.

According to another embodiment of the present invention, RN is generated at both the recipient terminal and the remote bank CPU. To generate the RN at the remote bank CPU, a random number generator is located at the remote bank CPU, wherein the random number generator at the remote bank CPU is similar to and synchronized with the random number generator 46 located at the recipient's terminal. Instead of transferring the RN and the CRNX, only the CRNX is transferred over the unsecured line from the recipient's terminal to the remote bank CPU.

At the remote bank CPU, the CPNR generated by the uncoder 70 is coded by the coder 66 with the RN generated at the remote bank CPU to generate the CRNX. The generated CRNX is then compared by the comparator 64 with the CRNX transferred from the recipient's terminal to the remote bank CPU to authenticate the recipient and the signal received over the unsecured line. In this manner, the recipient and transaction are further authenticated.

According to another embodiment of the present invention, CRNX is never generated. Instead, the CPNR generated by the irreversible coder 42 is sent to the remote bank CPU over a secured line, rather than over an unsecured line. The CPNR generated by the uncoder 70 is then compared by a comparator (not shown) with the CPNR sent from the recipient's terminal to the remote bank CPU to authenticate the recipient. In this alternate embodiment, the random number generator 46, coder 44, mixer 48, sorter 62, and coder 66 are not required, although a secure line is required.

FIGS. 9-12 constitute a functional block diagram illustrating the present invention in a credential issuing and authentication system. The system involves the same three phases of operation as the check transaction system of FIGS. 6, 7, 8A and 8B. However, all users are enrolled by an authorized official who must be enrolled first. Accordingly, there are two enrollment processes which are somewhat different. The first one is enrollment of the official, and the second one is enrollment of a user prior to or at the time of issuing his credentials. It is contemplated that this system would be useful for all types of credentials and records; for example, motor vehicle registrations, social security cards, passports, birth certificates and all types of identification cards or personal storage media. This system would also be useful in protecting against unauthorized access to all types of records, as previously indicated.

FIG. 9 illustrates enrollment of the official. This can be accomplished at a terminal or computer which is in communication with a remote computer over a link which is assumed to be secure. The remote computer may, for example, be the central computer at the agency issuing the credential. At the remote computer, number generator 100 generates a random number which, at block 102, is com-

pared to a current list of all assigned personal keys. If the random number does not correspond to an assigned personal key, then the random number is assigned as the personal key, PKO, of the official being enrolled. Alternatively, PKO can be selected at random, from a list of unused PKO's, and the list of available PKO's would thereby be diminished. In yet another alternative, PKO could be accessed from a counter, such as a pseudorandom or an ordinary sequential counter the output of which may be coded with a secret key. The size, or length, of PKO can be such as to provide a full size memory address or an offset or an index extension, to limit or enlarge the memory space wherein concealed files are stored. PKO is then transmitted over the secure link to the enrollment terminal.

At the terminal, the official enters his PIN and name and various other information required by the system. The name can be numerically coded by using a telephone type key pad. The PIN is applied to an irreversible coder 104, which produces his coded PIN CPNO. CPNO is applied as the key input to a coder 106, which receives PKO as the data input. The data output of coder 106 is the official's coded personal key, CPKU, which is applied as an input to mixer 107. The official's name code and TIN, OTIN, are also applied as inputs to mixer 107. CPKU represents a coded address since it is a coded representation of PKO.

The output of mixer 107 is transmitted back to the remote computer over the secure link. At the remote computer, sorter 109 separates the received signal into its component parts: CPKU, the official's name code, and OTIN. At block 108, CPKU and the official's name code are then saved (i.e., written) into File No. 1 assigned to the official with the official's TIN, OTIN, serving as a File No. 1 index. It is assumed that during the official's enrollment various other information will be provided by the official over the secure line and may be stored in his File No. 1. It should be noted that OTIN is not secret and, therefore, the location of File No. 1 and the contents of File No. 1 (including CPKU) are not secret.

At block 112, PKO is used as an index for File No. 2, which is also allocated to the enrolling official. The location of File No. 2 (and thus, the contents of File No. 2) is concealed, since PKO is secret and not stored anywhere in the system. The information or records which are stored in File No. 2 can be coded or uncoded. The memory space wherein concealed files are stored may be previously filled (or pre-loaded) with dummy or false information to make the contents and locations of authentic allocated files undistinguishable from the dummy files. The concealed File No. 2 can also be used to store the ROC and RN (or store only RN, since only RN is secret—ROC could be stored in a non-secret file, such as Official's File No. 1), as previously described in FIGS. 6, 7, 8A and 8B, to reconstitute a user's coded PIN, CPN. The concealed File No. 2 can also be used to store other secret information (not shown) associated with the official. An official's coded number, CNO, is generated at the output of coder 110, and is saved in File No. 2 at block 112. The key input to coder 110 is CPKU and the data input to coder 110 is PKO or an arbitrary predetermined number (APN). CNO represents coded authentication information because it is a coded representation of CPKU, and because it is used by the system to authenticate the official.

At coder 110, CPKU and PKO can be interchanged as the key and data inputs. However, the arrangement selected must then be used consistently in each phase of the operation of the system.

Those skilled in the art will appreciate that the present embodiment offers an additional level of security in that, not

only is secret information unavailable to a person who does not know the related PK and PIN, but that person is even unable to determine the location of the file containing the information, and is unable to decode the information contained therein.

FIG. 10 illustrates user enrollment. The user is enrolled by a previously enrolled official, who verifies the user's identity, based on acceptable documentation. Before the user can be enrolled, the official's identity and authority are preferably authenticated. The official operates the terminal, where he enters his PIN, and his TIN, OTIN, and the name code used during his enrollment, which was stored in his "File 1". OTIN is transmitted to the remote computer, where it is used as an index to access CPKU from the official's File No. 1, and CPKU is returned to the terminal. The official's PIN is applied to the irreversible coder 104, which produces CPNO. CPNO is applied as the key input to an uncoder 114, which receives CPKU as a data input over the secure link from the remote computer. It will be appreciated that uncoder 114 simply reverses the process of coder 106 of FIG. 9, therefore producing PKO. PKO is applied to a mixer 118, the other input to which is the official's name code. The output of mixer 118 is then transmitted to the remote computer.

At the remote computer, the signal transmitted from mixer 118 is received in a sorter 124, which separates out PKO, and the name code. The extracted PKO is utilized as an index to address the official's "File 2" whereby CNO is read. The CNO read from File No. 2 is compared against the CNO generated by coder 120, which has as its data input PKO which is extracted by sorter 124 and as its key input is CPKU read from "File 1". Should this comparison fail, the identity of the official is not authenticated and the enrollment of the user is aborted. Assuming that the comparison is successful, comparator 130 is then enabled. At block 130, the name code which is extracted from sorter 124 is compared against the name code read from the official's "File 1" (using OTIN as index). Should this comparison fail, the enrollment of the user is aborted. Should the comparison be successful, the official has been fully authenticated and the user's enrollment may proceed.

At the remote computer, number generator 100 generates a unique random number, which is assigned to the user as a personal address key, PKU. Alternately, PKU can be generated from a counter as previously described. As discussed below, PKU represents a predetermined secret address of a File No. 2 associated with the user. PKU is transmitted over the secure link to the enrollment terminal, where it is applied to the data input of coder 113.

The user operates the terminal and selects a PIN which he enters along with his TIN, UTIN. The user's PIN is applied to the irreversible coder 104, which produces the user's coded PIN, CPNU. CPNU is applied as a key input to coders 113 and 115. The output of coder 113 is the user's coded personal key, CPKU (which represents a coded address of the user's File No. 2), which is applied as a data input to coder 115. The output of coder 115 is the user's coded number, CNU, which is applied to the input of mixer 116. The user's TIN, UTIN and CPKU are also applied as inputs to mixer 116. The output of mixer 116 is transmitted back to the remote computer over the secure link. CNU represents coded authentication information because it is a coded representation of CPKU, and because it is used by the system to authenticate the user.

At the remote computer, sorter 119 separates the received signal into its component parts: CPKU, CNU and UTIN. At

block 108, CPKU and CNU are saved (i.e., written) into File No. 1 assigned to the user, with the user's TIN, UTIN serving as a File No. 1 index. It should be noted that CPKU and CNU may be recorded on the user's credential when they are generated at the terminal. It should also be noted that UTIN is not secret, and therefore, the location and contents of the user's File No. 1 are not secret. It should further be noted that the official's CNO is stored in the official's secret File No. 2 (FIG. 9) while the user's CNU is stored in the user's non-secret File No. 1 (FIG. 10A), even though both CNO and CNU are used to authenticate the official and the user, respectively. These two different ways for storing CNO and CNU (as shown in FIGS. 9 and 10A) illustrate two embodiments of the present invention.

The user's PK, PKU (or an arbitrary predetermined number APN), is applied as the data input to a coder 132, which receives the official's CPKU as a key input. Coder 132 produces a joint key, JKU, which it will be appreciated, is determined by information related to the user and information related to the official. Using PKU as an address, the joint key is written into the user's "File 2" at block 112, and using PKO and UTIN as address indices, the joint key JKU is written into the official's "File 2" at block 134 (FIG. 10B). These writes are enabled as a result of the success of the comparison occurring at block 130. Accordingly, the user's "File 2" will contain a joint key, and the official's "File 2" will contain a joint key for each user the official enrolls. Since the user's file 2 is addressed by PKU (which is secret), the location and contents of the user's file 2 are secret. At coder 132, when the joint key JKU is generated, CPK and PK can be interchanged as key and data inputs, or as to user and official inputs. However, the arrangement selected must then be used consistently.

FIG. 11 illustrates issuance of the credential. This is shown separate from the user enrollment process of FIG. 10. However, in many instances, it would occur at the same time. In the preferred embodiment, this process is shown as occurring at the agency's computer, although it may be performed by the official from a terminal where he may communicate with the computer. It is assumed that the official has a credential printer or recorder which contains credential forms on which information is printed or recorded to produce the actual credential. However, it is also possible to create the credential by inserting information manually or on a typewriter, provided the necessary information derived by the system can be entered. The official enters the usual information (INFO) normally contained on a particular credential 145. The user's TIN may also be recorded on the credential. Alternately, the user's CPKU and CNU may be recorded on the credential, after being extracted from the user's File No. 1, with UTIN serving as a file index. If CPKU and CNU are recorded on the credential, they may be erased from the user's File No. 1. Alternately, only CNU may be recorded on the credential, with CPKU remaining in File No. 1, or vice versa.

The issuing process continues with the official entering his PIN, which is applied to an irreversible coder 140 to produce his CPNO, which is applied as a key input to an uncoder 142. At block 144, the official's TIN, OTIN is utilized as an index to access the official's "File 1", so that CPKO may be read therefrom and applied as the input to uncoder 142. Uncoder 142 therefore performs the same process as uncoder 114 of FIG. 10 to produce PKO. At block 146, PKO and UTIN are utilized as address indices to access the official's "File 2" and JKU is read therefrom. The information INFO on the credential is applied as the data input to a coder 152 and JKU is applied as the key input,

whereby coder 152 codes the INFO to produce a VAN, which is recorded on the credential. After recording the VAN on the credential, the joint key, JKU, may be erased from the official's File 2, where it was stored (or held in escrow or in trust), until the credential was issued. Alternately, the authentic JKU may be replaced with a false or dummy JK for security purposes. This completes the issuance of the credential 145. It should be noted that the joint key JKU stored in the official's File No. 2 can only be used in a transaction if a party exists with knowledge of the official's PIN, since this PIN is required to access the official's File No. 2 (at block 146). Thus, a person who does not have knowledge of the official's PIN (such as an unscrupulous person trying to issue a fraudulent credential) cannot legitimately issue a credential.

The VAN which is generated from information (INFO) recorded on the credential, or from information which is otherwise stored by the system, can include (coded) personal descriptive details to further identify the user (in addition to the user's PIN and TIN) in order to limit the use of the credential to the sole individual to whom it was issued (or sold). Thus, items such as bank cards, tickets, green cards, food stamps, ballots, travel checks, FAX messages, etc., can be protected and used solely by the individuals to whom they were issued. Also, the use of the credential may be enlarged to include a group, such as a family, by coding such information into the VAN.

FIG. 12 illustrates the authentication of an issued credential. This is preferably performed at a terminal provided for that purpose. The terminal includes a reading device for the credential 145 and an input device, such as a keypad for the user. The information could, however, be read from the credential and keyed in by hand. The terminal communicates with the remote processor via a preferably secure link.

As part of the credential authentication process, the identity of the user is authenticated. This requires that the user enter certain information at the terminal, including a PIN and user's TIN, UTIN, which is transmitted to the remote computer, which returns CPKU and CNU (box 178) via a secure data link. Alternately, CPKU and CNU could have been recorded on the credential (or on some other item in the possession of the user, such as a card having a magnetic stripe for storing data) and inputted directly into the terminal. The PIN is applied to the irreversible coder 170 which produces CPNU. CPNU is applied as the key input to coder 172 and uncoder 174. Coder 172 receives CPKU as a data input. It should be noted that coder 172 performs in the same manner as coder 115, which produced CNU at its output during the user's enrollment. The output of coder 172 is applied as an input to the comparator at block 182, which also has as an input the CNU extracted from the user's File No. 1 (or inputted from the user's credential).

Should this comparison fail, the identity of the user is not authenticated, and the credential authentication is aborted. Assuming the comparison is successful, the user is identified, and the credential authentication, with access to the hidden File No. 2, ensues. The favorable output from comparator 182 enables uncoder 174. The data input to uncoder 174 is the user's CPKU. The key input to uncoder 174 is the user's CPNU, as already explained. It will be appreciated that uncoder 174 simply reverses the process of coder 113 of FIG. 10, therefore producing PKU. PKU is applied to a mixer 176 which also receives the VAN and INFO of the credential. The output of mixer 176 is then transmitted to the remote computer over the secure link.

At the remote computer, UTIN is utilized as an index to access the user's "File 1" at block 178. This permits reading



13

of CPKU and CNU from the file, whereby CPKU and CNU were transmitted back to the user's terminal. At the remote computer, the signal transmitted from mixer 176 is received in sorter 180, which separates out PKU, VAN and INFO. The extracted PKU is utilized to address the user's "File No. 2" at block 184 whereby JKU is read. It will be appreciated that the user's File No. 2 has been accessed by an authorized user without reference to, or use of, information stored in the file. The VAN extracted from sorter 180 is applied as a data input to an uncoder 162, which receives the joint key JKU extracted from the user's "File 2" at block 184. It will be appreciated that uncoder 162 therefore reverses the process performed by coder 152 of FIG. 11. Assuming the VAN on the credential is the same one as originally recorded, uncoder 162 will have produced the recovered INFO which should be the same as the actual INFO recorded on the credential.

At block 169, the INFO from the credential is compared to the INFO recovered from uncoder 162. Should the comparison fail, this is an indication that INFO on the credential has been modified, and the credential is indicated as not being authentic. Should the comparison be successful, this is an indication that INFO is accurate, and the authenticity of the credential is confirmed. Alternatively, the credential information from the credential is coded using the JKU from the user's File No. 2 to generate a new VAN, which is compared with the VAN from the credential to authenticate the credential.

In order to enhance the security of this system, it would be desirable to make unassigned areas of memory indistinguishable from those utilized to store information for the "File 1" and "File 2" information. This is accomplished by pre-storing pseudo-information in unused memory allocated as hidden memory space. This pseudo-information constitutes random information arranged in the same format as actual files. This prevents an intruder from searching memory for structures that look like actual information files and using the uncovered information to work backwards to breach security.

FIGS. 13A-13E, when arranged as shown in FIG. 14, constitute a functional block diagram illustrating further aspects of the check transaction system of FIGS. 6, 7, 8A and 8B. Specifically, these figures illustrate a three-party check transaction, with each of the participants and the fidelity of the information on the check being authenticated, the check being automatically cleared, and the funds of the participants being immediately credited or debited, all of these processes being performed on-line. The participating parties in this transaction are the check originator, whose account is to be debited; the check recipient to whom the check is drawn; and the check redeemer, who is cashing the check for the recipient or accepting it in payment for goods or services, and whose account is to be credited. In addition, the banks for each of these participants will also be participating in the transaction, and the messages generated by these banks will be authenticated. It is assumed that any individual or bank participating in the system will have enrolled as illustrated in FIG. 6. In addition, it is assumed that a check used in the system is generated in the manner illustrated in FIG. 7.

Referring first to FIG. 13A, the recipient of the originator's check has presented the check to the redeemer (block 200). The recipient and the redeemer are at a terminal which includes appropriate input means 202. Preferably, the input means includes a check reader and a keypad for each of them. However, in the absence of a check reader, it is also possible to key in information from the face of the check.

14

The check is examined to determine if it contains a redemption VAN from a previous transaction. The presence of a redemption VAN is an indication that the check was used previously, and it will not be honored. If a redemption VAN is not present, then the transaction can proceed. It is assumed that the redeemer's bank identification number (RDBIN), and TIN are stored in the terminal, otherwise the redeemer keys in his bank's name and TIN, and the recipient keys in his TIN, PIN and bank's name. A bank directory is addressed at block 203 to produce the recipient bank's identification number (RCPBIN). The recipient's PIN is applied to an irreversible coder 42, which produces his CPNR. Irreversible coder 42, coder 44, random number generator 46, and mixer 48 are the same components illustrated in FIG. 8A and cooperate in the same manner to produce RNX, CRNX, in a mixed form at the output of mixer 48.

The terminal has available to it the redeemer's bank key (RDBK), which is applied to the key input of a coder 204, the data input to which is the terminal ID (TID), which is generated by the terminal. Coder 204 then produces a joint terminal bank key (JTBK), which is applied as the key input to a coder 206, the data input to which is the output of mixer 48. The mixer output is therefore coded with a joint key JTBK which has been generated on the basis of information related to the redeemer's bank identity and the terminal identity.

The output of coder 206 and the information from input means 202, and the recipient's TIN, RCPBIN, and the redeemer's bank ID number, RCPBIN, are then transmitted to the computer at the redeemer's bank. At the redeemer's bank (FIG. 13B), all of the received information is placed in temporary storage (block 208).

The redeemer's TIN, RDTIN, (originally stored in the terminal, or keyed in by the redeemer), is then utilized as an index to access his account file, at block 210.

The check control number (CCN) of the present check is then compared to the CCN's stored in the redeemer's file during previous transactions (block 212), and the transaction is terminated if the present CCN matches that of a previously processed check. If the CCN of the present check is not a duplicate, processing continues.

RDBIN, and RCPBIN are utilized as indices to access a bank key table (block 213), which produces the redeemer's bank key RDBK, and the recipient's bank key RCBK, which are applied as the data and key inputs, respectively, to a coder 214. The coder 214 then produces a joint bank key JBK, which is derived from information related to the identity of the redeemer's bank and the identity of the recipient's bank.

The terminal identification (TID) is input to a coder 216, which has as a key input RDBK. In the same manner as coder 204, coder 216 therefore produces JTBK, which is applied as a key input to an uncoder 218. The data input to uncoder 218 is the information in temporary storage 208 which was originally received from coder 206. Coder 218 therefore reverses the process performed by coder 206, yielding the output of mixer 48, which is applied as a data input to a coder 220. The key input to coder 220 is JBK, so that the output of mixer 48 is now coded with the joint bank key JBK. The output of coder 220 is then transmitted in a message to the recipient's bank, along with RCPBIN, RDBIN, and RCPBIN.

At the recipient's bank, the received information is saved in temporary storage 230. RCPBIN and RDBIN are then applied to a bank key table (block 232), to yield RCBK and RDBK, which are applied as the key and data inputs.

15

respectively, to a coder 234. In the same manner as coder 214, coder 234 therefore yields the joint bank key JBK, which is applied as a key input to uncoder 236. The data input to this uncoder 236 is the coded combination of RNX and CRNX produced by coder 220. Uncoder 236 therefore reverses the process of coder 220, yielding the mixture of RNX and CRNX as an output. This mixture is applied as an input to a sorter 238, to recover RNX and CRNX.

The recipient's TIN, RCPTIN, is utilized as an index to access the recipient's file at block 240 and read therefrom the random number, RNR, and his ROC, which are applied as the key and data inputs, respectively, to an uncoder 242. In the same manner as uncoder 70 of FIG. 8A, uncoder 242 therefore derives the true CPNR, which is applied as a key input to a coder 244, which receives RNX as a data input. The data output of coder 244 is therefore the true CRNX.

At block 246, this true CRNX is compared to the CRNX derived from sorter 238. If this comparison is favorable, the recipient's identity is confirmed, and processing may proceed. Otherwise, processing is terminated, with the originator's check being dishonored, because the recipient has not been properly authenticated. The recipient's bank then transmits a message to the redeemer's bank, informing it whether or not the recipient has been authenticated. If the recipient has not been authenticated, the redeemer's terminal is notified, and processing will terminate.

Assuming that the recipient has been authenticated, the recipient's bank message includes various information which is temporarily stored by the redeemer's bank (block 250 of FIG. 13C). At block 252, the originator's bank identification number ORBIN, which was read from the check, and the redeemer's bank identification number RDBIN are applied as indices to a bank key table to recover bank keys for these banks, OBK and RDBK, respectively. These keys are applied to a coder 254 to produce a joint bank key JBK', which is therefore dependent upon information related to the originator's bank and the information related to the redeemer's bank. JBK' is applied to the key input of a coder 256, which receives the original VAN, OVAN, (from the check) as a data input. The output of coder 256 is a redeemer's bank RDBVAN, which is transmitted to the originator's bank, along with various transaction information and the information from the check. RDBVAN serves to authenticate the communication between the banks.

At the originator's bank, the received information is temporarily stored at block 258. ORBIN and RDBIN are then utilized to reference a bank key table at block 260, whereby OBK and RDBK are extracted in the same manner as in block 252. The joint key JBK' is then generated by means of a coder 262 in the same manner as coder 254. JBK' is then applied as the key input to an uncoder 264, which receives RDBVAN as a data input. This uncoder 264 therefore reverses the process performed by coder 256 and produces an extracted OVAN, which is applied to a comparator 266 (as shown in FIG. 13D).

The originator's personal account number ORGPAN which originally appeared on the check is utilized as an index to access the originator's account file at block 268 of FIG. 13C. This provides access to various information about the originator's account including the balance and a list of prior check control numbers (CCN's), and in addition, provides access to his revisable owner code ROCO and random number RNO, which are applied as the data and key inputs to an uncoder, to produce the originator's coded pin CPNO. CPNO is then applied as the key input to a coder 272 (FIG. 13D) which receives the recipient's TIN, RCPTIN, as

16

a data input. The output of coder 272 is the joint key JK, which is applied as the key input to a coder 274, which receives the check information as a data input. It will be appreciated that coders 272 and 274 regenerate the original VAN, OVAN, from the check in the same manner as coders 28 and 30 of FIG. 7. This regenerated VAN is then compared to the extracted VAN at block 266. If this comparison fails, it is an indication that the check information may have been tampered with and the originator's bank informs the redeemer's bank that the check will be dishonored. On the other hand, if the comparison succeeds, the process continues.

The originator's bank then performs a series of computations, including determining whether the CCN of the check is proper (i.e., has not been used before) and whether the originator has a sufficient balance in his account (or credit) to cover the check, and whether the date of the check is acceptable. In the case of any defects, the check will be dishonored and the process will terminate. Assuming that everything is in order, modification of the originator's account is approved, and a record of the check created at block 271, with the new information being added to temporary storage at block 273. Coders 275 and 276 are then utilized to encode the original VAN, OVAN, into an originator's bank VAN OBVAN. Various information about the transaction, and authorization to credit the redeemer's account are then transmitted in a message to the redeemer's bank.

At the redeemer's bank, all of the received information is stored in temporary storage at block 278. At block 280, coder 282 and uncoder 284, steps are performed to extract OVAN from OBVAN in a manner which is similar to that which was done in block 260, coder 262 and uncoder 264. This extracted OVAN is then applied to a comparator 286 of FIG. 13E, which receives as an additional input the stored OVAN from the check presented by the recipient. If this comparison fails, the process has not been authenticated, and the originator's bank will be notified. On the other hand, if the comparison succeeds, this is an indication that full authentication of the entire process and all parties has occurred and that the message received from the originator's bank is authentic.

Processing then continues by accessing the redeemer's account at block 288, computing a new balance at block 290 and updating the redeemer's account. The redeemer's bank then transmits a message back to the originator's bank, informing it that the redeemer's account has been credited. This information is saved at the originator's bank in temporary storage at block 291. The originator's bank then accesses the originator's account file using his personal account number ORGPAN as an index, and updates his account with the information that was placed in temporary storage at block 273 (FIG. 13D).

The redeemer's bank also communicates with the terminal at which the check was presented (block 294 of FIG. 13D), and informs it that the transaction has been satisfactorily completed and that the recipient may receive payment in the form of cash, goods or services (block 296). The terminal prints the redemption VAN (RDBVAN) on the check.

Although various embodiments of the present invention have been described herein as useful for particular types of transactions, those skilled in the art will appreciate that they actually have universal utility. For example, the last embodiment (depicted in FIGS. 13A-13E) was described as useful in a check transaction system, but it will be appreciated that it would also be useful in a bill payment system as well as a paperless/cashless system (as further described below).

17

FIGS. 15A, 15B and 15C are functional block diagrams of a credential issuing and authentication system according to an alternate embodiment of the present invention, wherein the alternate embodiment includes many of the features of the embodiments depicted in FIGS. 6-8 and FIGS. 9-12. For example, the alternate embodiment of FIGS. 15A-15C include steps for enrolling an official, enrolling a user, issuing a credential, and authenticating the credential. FIG. 15A illustrates user enrollment, FIG. 15B illustrates issuance of a credential, and FIG. 15C illustrates the authentication of an issued credential. In the alternate embodiment of FIGS. 15A-15C, enrollment of the official is the same as shown in FIG. 9 and, therefore, shall not be discussed further.

Referring to FIG. 15A, a user is enrolled by a previously enrolled official who verifies the user's identity, based on acceptable documentation. Before the user can be enrolled, the official's identity and authority must be authenticated. The official operates a terminal, where he enters his PIN and his TIN, OTIN, and the name code used during his enrollment, which was stored in his File No. 1. OTIN is transmitted to the remote computer, where it is used as an index or address to access the official's File No. 1 and retrieve CPKO (block 1546). CPKO is returned to the terminal.

The official's PIN is applied to irreversible coder 1530, which produces CPNO. CPNO is applied as the key input to an uncoder 1532, which receives CPKO as a data input from the remote computer, and which uncodes CPKO to generate PKO. CPKO is also applied as a key input to a coder 1534, which receives PKO as an input. The coder 1534 codes PKO using CPKO as the key input to generate a coded number for the official (CNO), which represents coded authentication information. Another coder 1538 codes the official's name code using CNO as a key input to generate a coded name code. A mixer 1536 mixes the coded name code, PKO, and CNO and transmits the mixed signal to the sorter 1540 at the remote computer over preferably a secure link.

At the remote computer, the signal transmitted from mixer 1536 is received by the sorter 1548, which separates out PKO, CNO, and the coded name code. PKO is applied as an index (or address) to access the official's File No. 2 and to thereby retrieve CNO, which was previously stored in the official's File No. 2 during the enrollment of the official (see FIG. 9). The CNO transmitted from the terminal and the CNO retrieved from File No. 2 are then compared in a comparator 1542. If the comparison fails, the identity of the official is not authenticated and the enrollment of the user is aborted. Assuming that the comparison is successful, the comparator 1542 is enabled and sends a signal to an uncoder 1544. The uncoder 1544 then uncodes the coded name code using the CNO retrieved from the official's File No. 2 to regenerate the name code. The name code is also accessed from File No. 1 and then compared at 1550. If the comparison fails, the identity of the official is not authenticated and the enrollment of the user is aborted. Assuming that the comparison is successful, the comparator 1550 sends an authentication signal ("okay to enroll user") and user enrollment begins. It should be noted that the "okay to enroll user" signal is applied as a write enabled to the official's File No. 2 at 1552 to save a joint key JKU therein (described below).

At the remote computer, number generator 1516 generates a unique random number (as discussed above), which is assigned to the user as a secret predetermined address or key, PKU. PKU is transmitted over a secured link to the enrollment terminal, where it is applied to the data input of a coder 1504.

The user operates a terminal and selects a PIN which he enters along with his TIN, UTIN. The user's PIN is applied

18

to irreversible coder 1502 which produces the user's coded PIN, CPNU. CPNU is applied as a key input to coder 1504. The output of the coder 1504 is the user's coded predetermined address or key, CPKU. CPKU may be stored in a user record (at block 1510). A mixer 1506 mixes CPNU and CPKU and transmits the mixed signal to the remote CPU.

At the remote computer, sorter 1512 separates the received signal into its component parts CPKU and CPN. At the remote computer, a random number RN is generated (as discussed above) and applied as a key input to coder 1518. The coder 1518 also receives CPN as an input and thereby generates a revisable owner code (ROC). ROC is stored in the user's File No. 1 (at block 1520), wherein the user's File No. 1 is accessed (or addressed) using UTIN. CPKU is also stored in the user's File No. 1 (at block 1520).

PKU is applied as an index or address to the user's File No. 2 in order to store RN (at block 1522). PKU is secret in the system and, therefore, the location and contents of the user's File No. 2 (including RN) is secret. Additional information may be coded in a coder 1524 using CPKU as a key input to generate coded information which is also stored in the user's File No. 2. The information which is coded using CPKU in the coder 1524 may include the secret information RN.

PKU is applied as an input to coder 1528, which also receives CPKO as a key input. The coder 1528 generates a user joint key (JKU) which is stored in the user's File No. 2. JKU is also stored in the official's File No. 2 (at block 1552).

It should be noted that the storage and handling of RN and ROC in the embodiment shown in FIG. 15A is different from the storage and handling of RN and ROC shown in FIG. 6. In FIG. 6, the file in which RN and ROC are stored is generally non-secret because it is indexed (or addressed) by generally non-secret user information (such as the user's TIN). However, in the embodiment shown in FIG. 15A, the non-secret ROC is stored in the user's File No. 1, which is non-secret, and the secret RN is stored in the user's File No. 2, which is secret (since it is accessed or addressed using the secret PKU). Therefore, the embodiment of 15A includes an additional level of security and protection over the embodiment shown in FIG. 6.

FIG. 15B illustrates issuance of a credential according to the alternate embodiment of the present invention. The issuance of credential in the alternate embodiment is essentially the same as the issuance of credentials in the previous embodiment shown in FIG. 11. Note, however, that it is possible to record the ROC retrieved from the user File No. 1 on the credential 1564 since the ROC is public (although the ROC could also have been recorded on the credential in the previous embodiment).

FIG. 15C illustrates the authentication of an issued credential. This is preferably performed at a terminal provided for that purpose. The terminal includes a reading device for the credential 1564 and an input device, such as a keypad, for the user. The information from the credential 1564 could, however, be keyed in by hand. The terminal communicates with the remote processor via a preferably secured link. As part of the credential authentication process, the identity of the user is authenticated. Specifically, the user enters his PIN which is applied as an input to irreversible coder 1570, which generates a coded PIN (CPNU). The user also enters his TIN (UTIN), which is used to access the user File No. 1 (at block 1588) and retrieve CPKU, which is transmitted from the remote CPU to the terminal. CPKU is applied as an input to coder 1574, which also receives CPNU as a key

input. The coder 1574 generates a coded number CNU, which represents coded authentication information. CPKU is also applied as an input to uncoder 1572, which also receives CPNU as a key input. The uncoder 1572 uncodes CPKU to regenerate PKU. Both CNU and PKU are mixed by mixer 1576 and sent to the sorter 1578 at the remote CPU.

At the remote CPU, the sorter 1578 separates the signal into its component parts PKU and CNU. PKU is applied as an index into the user's File No. 2 in order to retrieve the secret information RN. UTIN is applied as an index to the user's File No. 1 to retrieve the non-secret reversible owner code (ROC). ROC is applied as an input to uncoder 1584, and the secret information RN is applied as a key input to uncoder 1584. The uncoder 1584 thereby uncodes ROC using RN in order to regenerate CPNU as RCPN, which is applied as a key input at coder 1582. CPKU, which is read from the credential 1564, is applied as an input to coder 1582. The coder 1582 codes CPKU using RCPN as a key input in order to generate a coded number CNU. The generated coded number CNU is compared at the comparator 1580 to the coded number CNU received from the terminal. If the comparison fails, authentication of the user aborts. However, if the comparison is successful, the user is authenticated and the process continues by authenticating the credential 1564.

The credential 1564 is authenticated by reading the official's ID number OTIN from the credential and using OTIN as an index in order to access the official's File No. 1 and read CPKO (block 1599). CPKO is applied as an input to coder 1598 which also receives PKU as a key input. The coder 1598 codes CPKO using PKU in order to regenerate the user joint key JKU. JKU is also read from the user's File No. 2 using PKU as an index and then applied to a comparator 1596. The comparator 1596 compares the JKU which was retrieved from the user's File No. 2 and the JKU which was generated by the coder 1598. If the comparison fails, then authentication of the credential aborts. However, if the comparison is successful, the comparator 1596 is enabled and sends an okay signal to a comparator 1594.

The JKU retrieved from the user's File No. 2 at 1586 is applied to an uncoder 1592, which also receives as an input the VAN which was read from the credential 1564. The uncoder 1592 uncodes the VAN in order to regenerate INPO. The regenerated INPO is applied as an input to the comparator 1594, which also receives the INPO read from the credential 1564. The comparator 1594 compares the regenerated INPO and the INPO from the credential and if the comparison is successful, the credential is authenticated. Otherwise, the credential is not authenticated.

As noted above, in FIG. 15C, the transmission link between the mixer 1576 and the sorter 1578 is preferably secured since using an unsecured link would present a potential security problem. For example, the signal from the mixer 1576 could be recorded and then transmitted to the sorter 1578 at a later date in order to attempt to fraudulently authenticate a user and a credential. In accordance with an alternate embodiment of the present invention, an anti-duplication variable authentication number (ADVAN) is generated at the terminal by coding at least a transmission date and a time with the CPNU. The ADVAN is then mixed with the CNU and the PKU at the mixer 1576 and sent to the sorter 1578 at the remote CPU over an unsecured link. At the remote CPU, the received ADVAN is uncoded using the derived RCPN to regenerate the transmission date and the time. The regenerated transmission date and time are then compared to a reception date and time (that is, the date and time at which the signal was received at the sorter 1578) and

if the comparison is successful, the information transmitted over the transmission medium between the mixer 1576 and the sorter 1578 is authenticated. In this manner, the user and credential are further authenticated.

Alternatively, a semi-random number (not shown) is generated at the terminal using a counter or other random number generator (not shown). The semi-random number is coded using the CPNU to generate a coded semi-random number. The coded semi-random number is then transmitted along with CNU and PKU to the remote CPU over an unsecured medium. At the remote CPU, the coded semi-random number is uncoded using RCPN to regenerate the semi-random number. A second semi-random number is then generated at the remote CPU using another counter or random number generator (not shown) which is generally synchronized with the counter (not shown) at the terminal. The communication medium between the mixer 1576 and the sorter 1578 is then authenticated by comparing at the remote CPU the regenerated semi-random number to the second semi-random number which was generated at the remote CPU. If the comparison is successful, then the information transmitted over the communication medium between the mixer 1576 and the sorter 1578 is authenticated. In this manner, the user and credential are further authenticated.

As described above, the predetermined secret address PKU is coded to generate the coded secret address CPKU. According to an alternate embodiment, PKU comprises one or more components which are combinable to form the predetermined secret address PKU. In this alternative embodiment, only one of the components of the PKU is transmitted from the remote CPU to the terminal. The coder 1544 (FIG. 15A) codes this one component of the PKU to generate CPKU. Therefore, in this alternate embodiment, CPKU represents a coded portion of the PKU. Then, to access the user's File No. 2, the CPKU is uncoded as described above to regenerate the portion of the PKU. This PKU portion is combined with the other portions of the PKU to regenerate the PKU, which is then used to access the user's File No. 2. The other portions of the PKU may be stored throughout the system, such as in the operating system, in the executive program, in files, etc.

FIG. 16 is a functional block diagram of a system for authenticating the identity of a party and for authorizing access to a party's hidden (or secret) file according to an alternate embodiment of the present invention. The party's hidden file (such as hidden memory file 1622) may contain coded or uncoded secret information. In the embodiment of FIG. 16, the party is in possession of a portable storage media, such as a card 1602 having a magnetic stripe for recording information thereon. The card 1602 is issued by an agency, or a bank, during enrollment of the party. Information recorded on the card 1602 includes the party's reversible owner code (ROC), a coded address (CPK) of the hidden file 1622, an agency identification number (AID or Agency ID), and a transaction sequence number (TSN). The party's ROC is generated as described above (see FIG. 6). The coded address CPK of the hidden memory file 1622 may either represent the entire address of the hidden memory file 1622 or only a portion of the address of the hidden memory file 1622, as described above.

The party to be authenticated enters a personal identification number (PIN) at a terminal. The PIN is input to an irreversible coder 1606 to produce a coded personal identification number (CPIN). The information recorded on the party's card 1602 is read from the card 1602 using an appropriate reader (not shown). The CPK read from the card

1602 is applied as an input to an uncoder 1612, which also receives the CPN as a key input. The uncoder 1612 uncodes CPK using CPN as a key input to generate PK, which represents either the total address of the hidden memory file 1622 or a portion of the address of the hidden memory file 1622 (as noted above).

The transaction sequence number (TSN) read from the card 1602 is input to a mixer 1608 and then to a coder 1610. The coder 1610 also receives the CPN as a key input. The coder 1610 codes the TSN using the CPN as a key input to generate an anti-duplication VAN (ADVAN). The ADVAN, PK, ROC, and AID are input to a mixer 1614 and the resulting mixed signal is sent to the remote CPU over a preferably unsecured communication link.

The user's hidden memory file 1622 is part of a memory which is used to store such files at the remote CPU. The sorter 1616 separates the received mixed signal into its component parts ROC, PK, AID, and ADVAN. Where the PK generated by the uncoder 1612 is only a portion of the address to the hidden memory file 1622, the AID is used as an index to a memory table 1618 to retrieve other address components for the hidden memory file 1622. Thus, the address components in the memory table 1618 applicable in any given transaction depends on the particular AID. The PK is combined with the other address components at a combiner 1620 to thereby form the composite address of the hidden memory file 1622. The AID could also identify a predetermined procedure for combining the applicable address components. The composite address is used to access the hidden memory file 1622 to retrieve a secret random number RN (which is generated according to the method described above with respect to FIG. 6). RN is input as a key to a coder 1624. The coder 1624 also receives the ROC from the sorter 1616 and thereby generates CPN.

A transaction sequence number (TSN) is also retrieved from the hidden memory file 1622 and is input to a coder 1632. The coder 1632 also receives CPN as a key input and thereby generates an ADVAN. The ADVAN generated by the coder 1632 is compared with the ADVAN output from the sorter 1616 at a comparator 1630. If a favorable comparison is obtained, then coder 1628 is enabled. If the comparison is not favorable, then the user is not authenticated and does not gain access to the memory file 1622.

Coder 1628 receives PK as an input and CPN as a key and thereby generates CPK. The CPK generated by the coder 1628 is received by an uncoder 1626 as a key input. The uncoder 1626 also receives as input coded information which is retrieved from the hidden memory file 1622. The uncoder 1626 uncodes the coded information from the hidden memory file 1622 using the CPK as a key input to thereby produce clear information. The clear information is then provided to the authenticated user.

As a result of the favorable comparison of the ADVANs at the comparator 1630, a new (or revised) transaction sequence number (TSN) is generated and stored in the hidden memory file 1622. Also, a coder 1634 is enabled. The coder 1634 receives the CPN as an input and also receives a revised RN as a key input. The output of coder 1634 is a new ROC, which is combined with the new TSN in mixer 1635. The mixer 1635 output is sent back to the terminal where the sorter 1604 separates the new TSN and ROC, which are then recorded on the user's card (in order to prepare for the next transaction by the user). Note also that a new CPK may be generated as well by revising a memory address component, such as the address displacement. In this event, the new CPK would also be returned to the terminal to be recorded on the user's card.

It should be noted that an unsecured communication link between the mixer 1614 and the sorter 1616 is utilized if the hidden memory file 1622 is remote from the location where the party's PIN is entered (that is, the terminal). It should also be noted that the transaction sequence number (TSN), in conjunction with the ADVAN, serves to protect the authenticity of the transaction and the user's card against fraudulent duplication of the transaction information (that is, by recording the output of the mixer 1614 and retransmitting it later to the sorter 1616).

A number of additional applications for the present invention will now be described.

The invention could be utilized in a pay telephone system in which calls could be made without the use of money. The call originator uses a telephone in the usual way to enter the telephone number of the party to be called (i.e., to the call recipient). The call originator also enters his own telephone number and PIN. The system then authenticates the identity of the originator as described above (by using, for example, the embodiment depicted in FIGS. 6-8 or in FIGS. 9-12). In the first embodiment (i.e., FIGS. 6, 7, 8A and 8B), the originator's PIN is coded, and used to derive an arbitrary number, which is subsequently compared to another such number which is generated from a reconstituted version of the coded PIN. The reconstituted coded PIN is formed from an RN and ROC which are accessed from the originator's account file, with the originator's telephone number serving as a file index. If the comparison is unfavorable, the call is aborted; otherwise, call processing continues.

In the second embodiment, the originator's telephone number is used as an index to file no. 1 to access an originator's CPKO and true CNO. The originator's coded PIN, CPNO, is then combined with the originator's CPKO to generate a CNO (as in FIG. 12). The originator's identity is then authenticated by comparing the true CNO with the derived CNO. If the comparison is unfavorable, the call is aborted; otherwise, processing continues. The originator can use a machine readable card, or the like which has CPKO and CNO previously recorded thereon. In this event, access to file no. 1 is unnecessary.

In either embodiment, if the identity comparison is favorable, then the originator's credit balance is extracted from the originator's file to determine whether the call should be allowed. If the credit balance is favorable, then the telephone connection is extended to the call recipient, and the recipient's telephone is rung.

At the end of the call, the originator's credit balance is diminished by the cost of the call, and the new balance is computed and rewritten to the originator's file. The originator may then be advised of the cost of the call. When the recipient's telephone rings and the call is answered, the system can require that the identity of the person answering the phone be authenticated, as in a person to person call. In this event, the recipient is asked to enter a PIN, and the recipient's identity is authenticated using either of the two embodiments mentioned above.

Alternatively, a first joint code could be generated when the call is initiated, e.g., from the originator's CPN, and the recipient's reconstituted CPN. When the call is answered, the recipient enters his PIN, which is converted to a CPN and combined with the originator's reconstituted CPN to form a second joint code. A comparison then ensues between the first and second joint codes.

Another application of the invention is a system which uses a bill as the means of (or vehicle for) payment. The bill contains the usual payment information, and a VAN is also

recorded on the bill when the bill is generated. The VAN is derived from the payment information (INFO) and identification information associated with the originator of the bill (e.g., similar to the bank identification line of information which appears at the bottom of an originator's check) or the originator's TIN and BIN. The bill may also contain the recipient's TIN and BIN. Preferably, the above information is coded in a standard format, at a fixed location on the bill itself. The bill is then used in an appropriate document reader to provide the transaction payment information to the system. The party paying the bill (i.e., the payor) enters his PIN and the payor is then authenticated using the PIN. Also, the VAN is authenticated (using one of the methods described above). If the payor and the VAN are authentic, the bill is paid. A redemption VAN is generated (using information associated with the payee party) and printed on the bill, when it has been paid.

Alternatively, the payor could simply key in the information from the face of the bill. When the transaction is completed, a redemption VAN is displayed to the payor, which he records on the bill (or the VAN could be automatically recorded on the bill).

In accordance with a further application of the embodiments of this invention, a medical prescription form which has been originated and issued by a doctor to a patient (a recipient), can be authenticated to permit dispensing of the designated medicine, or drug, in a processing jurisdiction, along with automated payment. Automated payment may include a third party such as an insurance provider. This system is particularly useful for a patient who is in desperate need of medicine, and is in a remote or strange environment, where the prescription cannot be easily authenticated, or an available pharmacy cannot be found.

The prescription form contains identification information associated with the doctor and the patient, and the usual information which appears on a prescription, such as the type of medicine, strength, quantity, application, date, refills, generic, and a control number. The prescription form also contains a VAN, which is the result of coding the medical and identification information. Preferably, the information and the VAN are recorded on the prescription form so that it is readable by an individual, and it also includes coded symbols or characters representing the same information in machine readable form.

When the prescription form is utilized by the recipient to obtain the medicine from a processing entity (such as a drug store), the information on the form is read automatically by a terminal of the system, or it is entered via a keyboard. The recipient also enters his PIN, and the system authenticates the prescription form, the doctor, and the recipient in accordance with the embodiments described previously. An indication of the cost of the prescribed medicine, and the method of payment is provided to the recipient. The recipient may elect to pay by using one of the methods described herein.

Note that the processing entity may also include a centralized clearinghouse in communication with dispensing outlets (i.e., drug stores) for authenticating prescriptions. An RVAN may be generated from the VAN and information associated with the processing entity, and then associated with the transaction, to thereby document the processing entity's involvement in the transaction.

If a patient attempts to use a prescription in a state where the originating physician is not licensed, such as out of state, the original prescription may not be usable. In this situation, a directory system of predetermined licensed "correspondent" physicians may be established, and a correspondent

physician can automatically authorize the prescription of an originating physician (on-line), after the original prescription is authenticated.

The invention also finds utility in a paperless/cashless transaction system, in which "funds transfer" transactions, such as purchases, occur without the use of money, or checks. In this system, the payment originator uses a payment recipient's terminal which stores information to identify the precise location of the recipient's account. Alternatively, an originator PIN, information identifying an originator account and a recipient account, and funds transfer information (INFO) which includes a payment amount are entered directly into a terminal of this system by the payment originator. The system initially generates a VAN. (OVAN), by using the payment information (INFO) in conjunction with the identification information associated with the payment originator and payment recipient. The payment originator is authenticated using the originator PIN using a method described above. The system then approves or disapproves the payment based upon an authentication of the VAN, and the "joint" identification information associated with the participants, and the availability of funds, or credit. Such transactions are carried on entirely electronically, the participant's bank accounts are credited and debited automatically, allowing commercial transactions to be completed "instantaneously". An RVAN may be generated using the INFO and printed on a receipt which is dispensed to the originator.

Although preferred embodiments of the invention have been disclosed for illustrative purposes, those skilled in the art will appreciate that many additions, modifications, and substitutions are possible without departing from the scope or spirit of the invention as defined in the accompanying claims.

I claim:

1. A method for coding and storing information, comprising information associated with a party and other sensitive information, said information associated with a party being subsequently used to authenticate the party and authorize access, the method comprising:

previously receiving a first personal identification number (PIN1) from the party;

previously deriving or accessing first coded authentication information by using the first PIN1;

previously generating at least two numbers using the first coded authentication information, wherein at least one of the at least two numbers is an arbitrary number;

previously storing each of the at least two numbers in one or more storage means;

retrieving each of the at least two numbers previously stored in the one or more storage means;

receiving a second personal identification number (PIN2) from a party to be authenticated;

deriving or accessing second coded authentication information by using the second PIN2;

combining each of the at least two numbers retrieved from the one or more storage means to derive third coded authentication information;

comparing the second coded authentication information with the third coded authentication information; and

authenticating the party and authorizing access if the second coded authentication information and third coded authentication information correspond to each other.

25

2. The method of claim 1 further comprising:  
coding said other sensitive information with said first or second or third coded authentication information to derive coded sensitive information.

3. The method of claim 1 further comprising:  
uncoding said coded sensitive information with said second or third coded authentication information to recover the other sensitive information.

4. The method of claim 1 further comprising:  
revising each of the at least two numbers at an arbitrary time; and  
replacing each of the previous at least two numbers in the one or more storage means with each of the revised at least two numbers.

5. The method of claim 1 wherein at least a first of the one or more storage means is located at a first site, and a second of the one or more storage means is located at a second site.

6. The method of claim 1 wherein at least one of each of the at least two numbers is secret, and at least another of each of the at least two numbers is non-secret.

7. A method for coding first information, the method comprising:  
coding the first information using second information and then coding the result using third information, at least one of the second and third information being associated with at least one entity, the entity comprising a person or a computer program, wherein a credential having non-secret information stored therein is previously issued to at least one entity by a trusted entity, the non-secret information including the second or third information.

8. In a multi-party transaction system, a method for securing information relevant to a transaction, the method comprising:  
coding the information relevant to the transaction using first information associated with a party to generate first coded transaction information;  
coding the first coded transaction information using second information associated with more than one party to generate second coded transaction information, wherein a credential having non-secret information stored therein is previously issued to at least one of the parties by a trusted party, the non-secret information including the first or second information.

9. The method of claim 8 further comprising recovering information relevant to the transaction by:  
uncoding the second coded transaction information using the second information associated with the more than one party to recover the first coded transaction information; and  
uncoding the first coded transaction information using third information associated with the party to recover the information relevant to the transaction.

10. A method for securing in escrow and in trust, a joint key associated with a first party and a second party and stored in a storage means associated with the second party, wherein escrowed or entrusted information was previously used for generating a variable authentication number (VAN), the joint key being derivable from information associated with the first party and information associated with the second party, the VAN being subsequently used in authenticating the first party, the first party being enrolled by the second party and being issued a credential, the VAN being stored in the credential, the method comprising:  
previously receiving information associated with the first party and information associated with the second party;

26

previously generating a joint key using the information associated with the first party, and the information associated with the second party; and  
retaining in the storage means, in trust, at least the joint key.

11. The method of claim 10 wherein the second party is an agent, or an agency, or an official of an agency, or an authority, or an administrator, or an entity entrusted with issuing the credential.

12. A method for enrolling and issuing a credential to a first party by a second party, and subsequently granting the first party access to a first storage means, wherein the first party has a first personal identification number (PIN1), and the second party is previously granted authority to issue a credential to the first party, the first storage means, being accessible only to a party with knowledge of the first PIN1, the method of enrollment and issuing a credential comprising:  
receiving information associated with the first party;  
receiving information associated with the second party;  
storing in escrow and in trust the information associated with the first party and the information associated with the second party in a second storage means, wherein at least a portion of the information retrieved from the second storage means is used in enrolling the first party and issuing the credential; and  
subsequently granting the first party access to the first storage means by using the PIN1 or the credential.

13. The method of claim 12 wherein the second storage means is accessible for storing information therein only by a party with knowledge of a second PIN (PIN2) known to at least the second party, such that if no party exists with knowledge of the second (PIN2), then information cannot be stored in the second storage means.

14. A method for enrolling a first party by a second party, and subsequently granting the first party access to a first storage means, wherein the first party has a first personal identification number (PIN1), and the second party has a second personal identification number (PIN2), the first storage means, being accessible only to a party with knowledge of the first PIN1 or with knowledge of the second PIN2, the method of enrollment comprising:  
receiving information associated with the first party;  
receiving information associated with the second party;  
coding the information associated with the first party and the information associated with the second party to generate a joint code;  
storing the joint code and the information associated with the second party in a second storage means; and  
subsequently receiving and using PIN1 or PIN2, and retrieving and using the joint code and the information associated with the second party in granting the first party access to the first storage means.

15. The method of claim 14 wherein the second storage means is accessible for storing information therein only by a party with knowledge of the second PIN (PIN2), such that if no party exists with knowledge of the second (PIN2) then information cannot be stored in the second storage means.

16. A method for granting a first party access to a first storage means, subsequent to being enrolled by a second party, wherein the first party has a personal identification number (PIN), and wherein information associated with the second party was previously stored during enrollment in a second storage means, and a first joint code was previously generated and stored during enrollment in the second storage

27

means, wherein the joint code was previously generated by using first coded authentication information derived or accessed from the personal identification number (PIN) of the first party and information associated with the second party, the method comprising:

receiving a personal identification number (PIN) from the first party and generating or accessing second coded authentication information using the PIN;  
retrieving from the second storage means the information associated with the second party, and the first joint code;  
coding the second coded authentication information and the information associated with the second party to generate a second joint code;  
comparing the first joint code and the second joint code; and

granting the first party access to the first storage means, if the first joint code corresponds to the second joint code.

17. A method for authenticating a first party at first site by a second party at a second site and granting the first party access to a first storage means at a second site, the second party being a person or a computer program, wherein the first party has a personal identification number (PIN), and wherein first information associated with the second party is generated and stored in a second storage means associated with the second party at the second site, and wherein first coded information previously derived or accessed by using the PIN of the first party was previously stored in the second storage means, the method comprising:

generating the first information, and storing the first information in the second storage means;  
receiving the PIN from the first party and deriving or accessing second coded information by using the PIN;  
retrieving from the second storage means the first information, the first information being previously derived or accessed by using the PIN;  
coding the first coded information previously derived or accessed by using the PIN and the first information associated with the second party to generate a first joint code;

coding the second coded information derived or accessed by using the PIN and the first information associated with the second party to generate a second joint code;  
comparing the first joint code and the second joint code; and

authenticating the first party by the second party, and granting the first party access to the first storage means, if the first joint code corresponds to the second joint code.

18. The method of claim 17 wherein the second party is authenticated by the first party, wherein third information associated with the first party is generated and stored in a third storage means at the first site, and fourth information associated with the second party was previously stored in the third storage means, and fifth information associated with the second party was previously stored in a fourth storage means at a second site, the method further comprising:

generating the third information associated with the first party;  
storing the third information in the third storage means;  
retrieving the third information associated with the first party, and the fifth information associated with the second party;  
coding the fifth information and the third information to generate a third joint code;

28

retrieving the fourth information associated with the second party;

uncoding the third joint code using the fourth information to recover the third information;

comparing the generated third information and the recovered third information; and

authenticating the second party if the generated third information corresponds to the recovered third information.

19. The method of claim 18 wherein a credential previously issued to the second party by a trusted party is used by the first party to verify that the fourth information is secured to the second party.

20. The method of claim 18 wherein the first information associated with the second party, and the third information associated with the first party each comprise a random number.

21. The method of claim 18 wherein the third information associated with the second party, and the fourth information associated with the first party, each comprise a random number.

22. In a computer system comprising a memory containing computer information or a first computer program stored in a controlled memory area to which access is granted only upon proper authentication of an authorized user of the computer system, the user including a person or a second computer program, the memory further including a stored control program for interacting with the user and for making a determination as to whether the user is an authorized user, the memory further including a first area not readily accessible to a user, the first area containing a first revisable code, and a second area containing a second revisable code, a method of authentication of a user comprising:

receiving in the computer system identification information associated with the user;

generating or accessing first coded authentication information using the received identification information associated with the user;

retrieving the first revisable code from the first memory area and the second revisable code from the second memory area and deriving therefrom second coded authentication information;

comparing the first coded authentication information with the second coded authentication information;

authenticating the user, and granting access to the computer information or a first computer program stored in the controlled memory area to the user only if the first and second coded authentication information compare favorably.

23. The method as recited in claim 22 further comprising revising and storing the first and second revisable codes in the original respective memory areas only if the first and second coded authentication information compare favorably.

24. The method as recited in claim 23 wherein computer information stored in the memory of the computer system may be reproduced, the method further comprising:

previously recording the second revisable code with the computer information to be reproduced;

permitting the computer information to be reproduced only if the access has been granted to the user; and

thereafter retrieving the second revisable code retrieved from the reproduced information and using the second revisable code to authenticate the user if the reproduced information is used or accessed.



25. In a computer system comprising a memory containing computer information or a first computer program stored in a controlled memory area to which access is granted only upon proper authentication of an authorized user of the computer system, the user including a person or a second computer program, the memory further including a stored control program for interacting with a user and for making a determination as to whether the user is an authorized user, the memory further including a first area not readily accessible to a user, the first area containing a first revisable code and a second area containing a second revisable code, a method of authentication of a user comprising:

- receiving in the computer system identification information associated with the user;
- generating or accessing first coded authentication information using the received identification information associated with the user;
- retrieving the first revisable code from the first memory area and the second revisable code from the second memory area;
- deriving a third revisable code using the retrieved first revisable code and the first coded authentication information;
- comparing the retrieved second revisable code with the derived third revisable code;
- authenticating the user and granting access to the computer information or first computer program stored in the controlled memory area to the user only if the second and third revisable codes compare favorably.

26. The method as recited in claim 25 further comprising revising and storing the first and second revisable codes in the original respective memory areas only if the second and third revisable codes compare favorably.

27. The method as recited in claim 25 wherein computer information stored in the memory of the computer system may be reproduced, the method further comprising:

- previously recording the second revisable code with the computer information to be reproduced;
- permitting the computer information to be reproduced only if the access has been granted to the user; and
- thereafter retrieving the second revisable code retrieved from the reproduced information and using the second revisable code to authenticate the user if the reproduced information is used or accessed.

28. A method for authenticating a first party by using information stored in a credential, the credential being previously issued to the first party by a second party, wherein information previously stored in the credential comprises at least a non-secret variable authentication number (VAN) and other non-secret credential information, the method comprising:

- previously irreversibly coding at least a portion of the other non-secret credential information to derive an irreversibly coded number, and further coding the irreversibly coded number with first information associated with the second party to derive a variable authentication number (VAN);
- previously storing the VAN and the other non-secret credential information in the credential;
- retrieving the VAN and the other non-secret credential information stored in the credential;
- retrieving second information associated with the second party previously stored in a storage means associated with at least one of the parties;
- uncoding the VAN using the second information associated with the second party to derive the irreversibly coded number; and

authenticating the first party if the irreversibly coded number derived from at least a portion of the other non-secret credential information retrieved from the credential corresponds to the irreversibly coded number uncoded from the VAN.

29. The method of claim 28 wherein the first information associated with the second party comprises a secret key, and the second information associated with the second party comprises a non-secret key.

30. The method of claim 28 wherein the at least a portion of the other non-secret credential information comprises a non-secret key associated with the first party.

31. A method for issuing a credential to a first party by a second party, the method comprising:

- the second party receiving non-secret information associated with the first party;
- the second party authenticating at least a portion of the received non-secret information associated with the first party;
- denying issuance of the credential if at least a portion of the received non-secret information associated with the first party is determined not to be authentic;
- coding at least a portion of the received non-secret information associated with the first party with first information associated with the second party to derive a variable authentication number (VAN);
- storing in the credential the VAN and at least a portion of the received non-secret information associated with the first party, and other information associated with the second party; and
- issuing the credential to the first party.

32. The method of claim 31 wherein at least a portion of the non-secret information associated with the first party comprises a non-secret key associated with the first party.

33. A method for authenticating a first party by using information stored in a credential, the credential being previously issued to the first party by a second party, wherein information previously stored in the credential comprises at least a non-secret variable authentication number (VAN) and other non-secret credential information, the method comprising:

- previously generating a first error detection code (EDC1) by using at least a portion of the other non-secret credential information;
- previously coding the first error detection code (EDC1) with first information associated with the second party to derive a variable authentication number (VAN);
- previously storing the VAN and the other non-secret credential information in the credential;
- retrieving the VAN and the other non-secret credential information stored in the credential;
- deriving a second error detection code (EDC2) by using at least a portion of the retrieved other non-secret credential information;
- retrieving second information associated with the second party previously stored in a storage means associated with at least one of the parties;
- uncoding the VAN using the second information associated with the second party to derive a third error detection code (EDC3); and
- authenticating the first party and at least a portion of the non-secret information stored in the credential if the second error detection code (EDC2) corresponds to the third error detection code (EDC3).

34. The method of claim 33 wherein the first information associated with the second party comprises a secret key, and

31

the second information associated with the second party comprises a non-secret key.

35. The method of claim 33 wherein the at least a portion of the other non-secret credential information comprises a non-secret key associated with the first party.

36. A method for issuing a credential to a first party by a second party, the method comprising:

the second party receiving non-secret information associated with the first party;

the second party authenticating at least a portion of the received non-secret information associated with the first party;

denying issuance of the credential if at least a portion of the received non-secret information associated with the first party is determined not to be authentic;

generating an error detection code (EDC) by using at least a portion the received non-secret information associated with the first party;

storing in the credential the EDC and at least a portion the received non-secret information associated with the first party, and other information associated with the second party; and

issuing the credential to the first party.

37. The method of claim 36 wherein at least a portion of the non-secret information associated with the first party comprises a non-secret key associated with the first party.

38. The method of claim 36 further comprising:

coding the error detection code (EDC) by using first information associated with the second party to derive a variable authentication number (VAN), and storing the VAN in the credential.

39. A method for authenticating a first party at a first site by a second party at a second site, the second party being a person or a computer program, by using a personal identification number (PIN) supplied by the first party at the first site, and further using a first random number (RNI) generated by the second party at the second site, the PIN being previously used to derive or access first coded authentication information, the first coded authentication information being previously stored in a storage means associated with the second party at the second site, the method comprising:

receiving a PIN at the first site from a first party to be authenticated;

generating or accessing second coded authentication information using the received PIN;

generating a first random number (RNI) at a second site by the second party;

storing the first random number (RNI) in the second storage means at the second site;

transmitting the first random number (RNI) from the second site to the first site;

receiving the first random number (RNI) at the first site by the first party;

coding the received first random number (RNI) and the second coded authentication information to derive a first anti-duplication variable authentication number (ADVANI);

transmitting the first anti-duplication variable authentication number (ADVANI) from the first site to the second site;

receiving the first anti-duplication variable authentication number (ADVANI) at the second site by the second party;

retrieving the first coded authentication information from the storage means at the second site;

32

coding the first random number (RNI) and the first coded authentication information to generate a second anti-duplication variable authentication number (ADVAN2);

comparing the first anti-duplication variable authentication number (ADVANI) and the second anti-duplication variable authentication number (ADVAN2); and

authenticating the first party by the second party if the first anti-duplication variable authentication number (ADVANI) and the second anti-duplication variable authentication number (ADVAN2) correspond.

40. The method of claim 39 wherein after authentication occurs, the first party is authorized access to information or programs stored at the second site.

41. A method for authenticating the transfer of funds from a first account associated with a first party to a second account associated with a second party, the first account information being stored in a first storage means, and the second account information being stored in a second storage means, the method comprising:

receiving funds transfer information from the first party, including at least information for identifying the first account of the first party, and information for identifying the second account of the second party, and a transfer amount;

generating a variable authentication number (VAN) using at least a portion of the received funds transfer information;

a third party for determining whether the at least a portion of the received funds transfer information is authentic by using the VAN; and

transferring funds from the first account of the first party to the second account of the second party if the at least a portion of the received funds transfer information and the VAN are determined to be authentic.

42. The method of claim 41 further comprising:

receiving from the first party information for identifying the first party;

determining whether the first party is authentic by using the information for identifying the first party;

determining whether the at least a portion of the received funds transfer information is authentic by using the VAN; and

debiting the first account of the first party and crediting the second account of the second party with the funds transfer amount if the at least a portion of the received funds transfer information is determined to be authentic.

43. The method of claim 41 wherein the funds transfer comprises a payment made by the first party to the second party.

44. The method of claim 43 wherein prior to payment being made to the second party, the first party is presented with the second party's invoice, and after the payment is made to second party, the accounts receivable associated with the second party, and the accounts payable associated with the first party are updated.

45. The method of claim 41 wherein the VAN is used to confirm, substantiate, acknowledge, authorize, reference, validate or verify the transfer of funds.

46. The method of claim 41 wherein the VAN is generated by using an error detection code derived by using at least a portion of the funds transfer information.

47. The method of claim 41 for further securing the transfer of funds, at least one party being previously issued

a credential by a trusted party, the credential information including information associated with the at least one party, and a second variable authentication number (VAN1), the VAN1 being used to secure at least a portion of the credential information to the at least one party, authentication and the transfer of funds being denied to the at least one party if the at least a portion of the credential information cannot be secured to the at least one party by using the VAN1.

48. The method of claim 41 wherein the first party and the second party are the same party.

49. The method of claim 48 wherein the second storage means comprises a credential.

50. The method of claim 41 wherein the first storage means comprises a credential, and the second storage means comprises a credential.

51. A method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party, a credential being previously issued to at least one of the parties by a trusted party, the information stored in the credential being non-secret, the method comprising:

receiving funds transfer information, including at least information for identifying the account of the first party, and information for identifying the account of the second party, and a transfer amount;

generating a variable authentication number (VAN) using at least a portion of the received funds transfer information;

determining whether the at least a portion of the received funds transfer information is authentic by using the VAN and the credential information; and

transferring funds from the account of the first party to the account of the second party if the at least a portion of the received funds transfer information and the VAN are determined to be authentic.

52. The method of claim 51 further comprising:

receiving from the first party information for identifying the first party;

determining whether the first party is authentic by using the information for identifying the first party;

determining whether the at least a portion of the received funds transfer information is authentic by using the VAN; and

debiting the account of the first party, and crediting the account of the second party with the funds transfer amount if the at least a portion of the received funds transfer information is determined to be authentic.

53. The method of claim 51 wherein the funds transfer comprises a payment made by the first party to the second party.

54. The method of claim 51 wherein the VAN is used to confirm, substantiate, acknowledge, authorize, reference, validate or verify the transfer of funds.

55. The method of claim 51 wherein the VAN is generated by using an error detection code derived by using at least a portion of the funds transfer information.

56. The method of claim 51 for further securing the transfer of funds, at least one party being previously issued a credential by a trusted party, the credential information including information associated with the at least one party, and a second variable authentication number (VAN1), the VAN1 being used to secure at least a portion of the credential information to the at least one party, authentication and the transfer of funds being denied to the at least one party if the at least a portion of the credential information cannot be secured to the at least one party by using the VAN1.

57. A method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party, at least a part of the transfer being carried out by a third party, comprising:

receiving funds transfer information, including at least information for identifying the account of the first party, and information for identifying the account of the second party, and information for identifying the account of the third party, and a transfer amount;

generating a first variable authentication number (VAN1) using at least a portion of the received funds transfer information, the VAN1 being associated with the transfer of funds from the account of the third party to the account of the second party;

determining whether the at least a portion of the received funds transfer information is authentic by using VAN1; transferring the funds from the account of the third party to the account of the second party if the at least a portion of the received funds transfer information and the VAN1 are determined to be authentic;

generating a second variable authentication number (VAN2) using at least a portion of the received funds transfer information, the VAN2 being associated with the transfer of funds from the account of the first party to the account of the third party;

determining whether the at least a portion of the received funds transfer information is authentic by using VAN2; and

transferring the funds from the account of the first party to the account of the third party if the at least a portion of the received funds transfer information and the VAN2 are determined to be authentic.

58. The method of claim 57 further comprising:

receiving from the first party information for identifying the first party;

determining whether the first party is authentic by using the information for identifying the first party;

determining whether the at least a portion of the received funds transfer information is authentic by using the VAN2; and

debiting the account of the first party and crediting the account of the third party with the funds transfer amount if the at least a portion of the received funds transfer information and the VAN2 are determined to be authentic.

59. The method of claim 57 wherein the funds transfer comprises a payment made by the first party or the third party to the second party.

60. The method of claim 57 wherein the VAN1 or the VAN2 are used to confirm, substantiate, acknowledge, authorize, reference, validate or verify the transfer of funds.

61. The method of claim 57 wherein the VAN1 or the VAN2 are each generated by using an error detection code derived by using at least a portion of the funds transfer information.

62. The method of claim 57 for further securing the transfer of funds, at least one party being previously issued a credential by a trusted party, the credential information including information associated with the at least one party, and a variable authentication number (VAN3), the VAN3 being used to secure at least a portion of the credential information to the at least one party, authentication and the transfer of funds being denied to the at least one party if the at least a portion of the credential information cannot be secured to the at least one party by using the VAN3.

35

63. A method for authenticating and securing the integrity of relevant information transmitted from a first party at a first site to a second party at a second site by using first information associated with the first party, the first information comprising a secret first key, a non-secret second key, and first credential information, the first information being previously stored in a first storage means at the first site, and the first credential information comprising non-secret information for securing the second key to the first party, the first credential information including a third error detection code (EDC3) being previously stored in the first credential by a third party during prior issuance of the first credential to the first party, and the second key associated with the first party being previously stored in a second storage means at the second site, and the first key being used by the first party to generate a first variable authentication number (VAN1), the VAN1 and the second key being used by the second party to authenticate the first party and the integrity of the relevant information received from the first party, the method comprising:

receiving relevant information from the first party;  
 deriving a first error detection code (EDC1) by using the relevant information;  
 retrieving the first information previously stored in the first storage means;  
 coding the EDC1 with the retrieved first key to generate the first variable authentication number (VAN1);  
 forming a first message including at least the VAN1, the first credential information, and the relevant information;  
 transmitting the first message from the first party at the first site to the second party at the second site, and receiving the first message at the second site;  
 extracting the VAN1, the first credential information, and the relevant information from the first message at the second site;  
 retrieving the second key from the second storage means at the second site;  
 determining if the first party is secured to the second key by using the first credential information and the third error detection code (EDC3);  
 rejecting the first message if the first party is determined not to be secured to the second key;  
 uncoding the VAN1 using the second key to recover the first error detection code (EDC1);  
 deriving a second error detection code (EDC2) by using the relevant information;  
 comparing the first error detection code (EDC1) with the second error detection code (EDC2); and  
 authenticating the first party and the integrity of the relevant information if the first error detection code (EDC1) and the second error detection code (EDC2) correspond.

64. The method of claim 63 wherein second information associated with the second party is previously stored in the second storage means, the second information comprising a secret third key and a non-secret fourth key and second credential information, the second credential information including a fourth error detection code (EDC4) being previously stored in the second credential by a third party during prior issuance of the second credential to the second party, and the non-secret fourth key being previously stored in the first storage means at the first site, the method further comprising:

the second party retrieving the second credential information from the second storage means;

36

the second party transmitting a second message comprising at least the second credential information from the second site to the first site, and the second message being received at the first site;

the first party extracting the second credential information from the received second message;

retrieving the fourth key from the first storage means at the first site;

determining if the second party is secured to the fourth key by using the second credential information and the fourth error detection code (EDC4);

rejecting the second message if the second party is determined not to be secured to the fourth key;

receiving or generating sensitive information;

coding the sensitive information with the fourth key to generate secure coded sensitive information;

transmitting the secure coded sensitive information from the first site to the second site, and receiving the secure coded sensitive information at the second site;

the second party retrieving the third key from the second storage means; and

uncoding the secure coded sensitive information using the third key to recover the sensitive information.

65. The method of claim 63 wherein the first party is granted access to the first key in the first storage means only if the identity of the first party is authenticated by using a personal identification number (PIN) belonging to the first party.

66. The method of claim 63 wherein a second variable authentication number (VAN2) is stored in the first credential during prior issuance of the first credential, the VAN2 being generated by coding the EDC3 with a third secret key associated with the third party, and wherein a fourth non-secret key associated with the third party is previously stored in the second storage means at the second site, the fourth key being used by the second party to authenticate the first credential information, and following the step of retrieving the second key from the second storage means at the second site, the method further comprising:

retrieving the fourth key from the second storage means at the second site;

extracting the EDC3 and the VAN2 from the first credential information in the received first message;

uncoding the VAN2 using the fourth key to recover the third error detection code (EDC3);

determining if the extracted EDC3 and the recovered EDC3 correspond;

rejecting the first message if the extracted EDC3 and the recovered EDC3 do not correspond.

67. The method of claim 64 wherein the sensitive information comprises a session key being subsequently used by the first and second parties to code and uncode information transferred between the first and second sites.

68. The method of claim 64 wherein the first party is granted access to the first key in the first storage means only if the identity of the first party is authenticated by using a personal identification number (PIN) belonging to the first party, and the second party is granted access to the third key in the second storage means only if the identity of the second party is authenticated.

69. The method of claim 64 wherein a third variable authentication number (VAN3) is stored in the second credential during prior issuance of the second credential, the VAN3 being generated by coding the EDC4 with a third secret key associated with the third party, and a fourth

37

non-secret key associated with the third party being previously stored in the first storage means at the first site, the fourth key being used by the first party to authenticate the second credential information, and following the step of retrieving the fourth key from the first storage means at the first site, the method further comprising:

retrieving the fourth key from the first storage means at the first site;  
extracting the EDC4 and the VAN3 from the second credential information in the received second message;  
uncoding the VAN3 using the fourth key to recover the fourth error detection code (EDC4);  
determining if the extracted EDC4 and the recovered EDC4 correspond;  
rejecting the second message if the extracted EDC4 and the recovered EDC4 do not correspond.

70. A method of issuing a credential to a first party at a first site, by a second party at a second site, wherein the first party is authenticated during at least one stage of a subsequent transaction by using the credential, wherein the information stored in the credential comprises at least a first variable authentication number VAN1, information for identifying the first party, a non-secret key associated with the first party, and information for identifying the second party, and first and second storage means at the first site, the first storage means being used to store a secret key associated with the first party, the secret key being accessible to a party with knowledge of a pre-determined personal identification number (PIN), the second storage means being used to store the non-secret key associated with the first party, and third and fourth storage means at the second site, the third storage means being used to store a secret key associated with the second party, the secret key being accessible to an authorized party, the fourth storage means being used to store a non-secret key associated with the second party, the method comprising:

receiving information for identifying the first party, and a pre-determined personal identification number (PIN) from the first party;  
retrieving the secret key associated with the first party from the first storage means, only if the personal identification number (PIN) is determined to be authentic;  
coding at least a portion of the information for identifying the first party to derive a first error detection code (EDC1);  
generating a second variable authentication number VAN2 by coding the EDC1 with the secret key associated with the first party;  
retrieving the non-secret key associated with the first party from the second storage means;  
forming a message including at least the VAN2, the non-secret key associated with the first party, the EDC1, and the information for identifying the first party;  
transmitting the message from the first party at the first site to the second party at the second site, and receiving the message at the second site;  
extracting the VAN2, the non-secret key associated with the first party, the EDC1, and the information for identifying the first party from the message at the second site;  
using at least a portion of the information for identifying the first party to authenticate the identity of the first party;

38

denying issuance of the credential if at least a portion of the information for identifying the first party is determined not to be authentic;

retrieving the secret key associated with the second party from the third storage means at the second site;

generating a first variable authentication number VAN1 by coding the second variable authentication number VAN2 with the secret key associated with the second party;

storing in the credential at least the VAN1, the EDC1, the non-secret key associated with the first party, and information for identifying the second party;

issuing the credential to the first party; wherein the method for authenticating the first party and the credential during at least one stage of a subsequent transaction, comprises:  
retrieving the information previously stored in the credential;

receiving or retrieving the non-secret key associated with the first party and the non-secret key associated with the second party;

uncoding the first variable authentication number VAN1 using the non-secret key associated with the second party to recover the second variable authentication number VAN2;

uncoding the second variable authentication number VAN2 using the non-secret key associated with the first party to recover the EDC1;

authenticating the credential, and the first party who was issued the credential, if the EDC1 retrieved from the credential corresponds to the EDC1 recovered from the second variable authentication number VAN2.

71. The method of claim 70 wherein the non-secret key associated with the second party is retrieved from fourth storage means and stored in the credential, prior to issuing the credential.

72. The method of claim 70 wherein prior to denying issuance of the credential if at least a portion of the information for identifying the first party is determined not to be authentic, the method further comprising:

uncoding the second variable authentication number VAN2 by using the non-secret key associated with the first party to recover the EDC1;

comparing the recovered EDC1 with the EDC1 extracted from the received message; and

denying issuance of the credential if the extracted EDC1 and the recovered EDC1 do not match.

73. A method for determining if an unauthorized duplication or alteration occurred in first transaction information (FXI) and in second transaction information (SXI), the FXI being originated by a second entity at a second site, and being transmitted to a first entity at a first site, the first entity and the second entity being a person, or a computer program, and the SXI being originated at the first site and being combined with the FXI to form first combined transaction information (FCX) at the first site, an anti-duplication variable authentication number (ADVANI) being derived from the FCX and first information (FKI) associated with the first entity, the FKI being previously stored in a first storage means at the first site and being solely accessible to the first entity, the ADVANI, and the SXI being transmitted from the first site to the second the FXI and the SXI being authenticated at the second site, by using the ADVANI, FXI, SXI, and second information (FK2) associated with the first entity, the FK2 being previously stored in a second storage

39

means at the second site, a first transaction record storage means (FXR) being used at the first site, and a second transaction record storage means (SXR) being used at the second site, the FXR and SXR being used to store at least the FXI and the SXI, the method comprising:

generating or receiving first transaction information (FXI) at the second site, and storing the FXI in the second transaction record (SXR) storage means at the second site;

transmitting the FXI from the second site to the first site, and receiving the FXI at the first site;

storing the FXI in the first transaction record (FXR) storage means at the first site;

generating or receiving second transaction information (SXI) at the first site;

storing the SXI in the FXR storage means at the first site; combining the FXI and the SXI to form first combined transaction information (PCX);

retrieving the first information (FK1) associated with the first entity from the first storage means, the FK1 being accessible only to the first entity;

coding the PCX with the retrieved FK1 to derive a first anti-duplication variable authentication number (ADVAN1);

transmitting the first anti-duplication variable authentication number (ADVAN1) and the SXI from the first site to the second site, and receiving the ADVAN1 and the SXI at the second site;

storing the received ADVAN1 and the SXI in the SXR storage means at the second site; and

the second entity subsequently using the ADVAN1, the FXI, the SXI, and second information (FK2) associated with the first entity to determine if an unauthorized duplication or alteration occurred in the first transaction information (FXI) or in the second transaction information (SXI).

74. The method of claim 73 wherein coding the PCX to derive the ADVAN1 further comprises:

irreversibly coding the PCX to derive a first error detection code (EDC1);

storing the EDC1 in the FXR storage means; and coding the EDC1 with the first information (FK1) associated with the first entity to derive the first anti-duplication authentication number (ADVAN1).

75. The method of claim 74 for further authenticating the integrity of the FXI, and for further authenticating the first entity by the second entity, the method further comprising:

retrieving the FXI, the SXI, and the ADVAN1 from the SXR storage means at the second site;

retrieving the second information (FK2) associated with the first entity from the second storage means;

uncoding the ADVAN1 by using the FK2 to recover the first error detection code (EDC1);

combining the retrieved FXI and the retrieved SXI to form a second combined transaction information (SCX);

irreversibly coding the second combined transaction information (SCX) to derive a second error detection code (EDC2);

storing the second error detection code (EDC2) in the SXR storage means at the second site;

comparing the recovered first error detection code (EDC1) and the derived second error detection code (EDC2); and

40

the second entity (1) authenticating the first entity and determining that no unauthorized duplication or alteration occurred in first transaction information (FXI) if the recovered EDC1 and the derived EDC2 correspond; or (2) denying authentication to the first entity or determining that an unauthorized duplication or alteration occurred in first transaction information (FXI) if the recovered EDC1 and the derived EDC2 do not correspond.

76. The method of claim 73 wherein the first entity is authenticated by the second entity, and wherein the FXI comprises a first random number (RN1), and the SXI comprises a second random number (RN2).

77. The method of claim 73 wherein FXI and SXI are both present.

78. The method of claim 73 for further determining if an unauthorized duplication or alteration occurred in the SXI, and for further authenticating the second entity by the first entity, by using a second anti-duplication variable identification number (ADVAN2) derived by the second entity, the ADVAN2 being derived at the second site from the EDC2 and third information (SK3) associated with the second entity, the SK3 being previously stored in a third storage means at the second site, the SXI and the second entity being authenticated by the first entity by using the ADVAN2, the SXI, the FXI, and fourth information (SK4) associated with the second entity, the SK4 being previously stored in a fourth storage means at the first site, the method further comprising:

retrieving the second error detection code (EDC2) from the SXR storage means;

retrieving the third information (SK3) associated with the second entity from the third storage means at the second site;

coding the EDC2 with the SK3 to derive a second anti-duplication variable authentication number (ADVAN2);

transmitting the ADVAN2 from the second site to the first site, and receiving the ADVAN2 at the first site;

storing the ADVAN2 in the FXR storage means;

retrieving fourth information (SK4) associated with the second entity from the fourth storage means at the first site;

retrieving the ADVAN2 from the FXR storage means; uncoding the ADVAN2 by using the SK4 to recover the second error detection code (EDC2);

retrieving the FXI, and the SXI from the FXR storage means;

combining the retrieved FXI and the retrieved SXI to form a third combined transaction information (TCX); irreversibly coding the TCX to derive a third error detection code (EDC3);

storing the third error detection code (EDC3) in FXR storage means;

comparing the derived third error detection code (EDC3) and the recovered second error detection code (EDC2); and

the first entity (1) authenticating the second entity and determining that no unauthorized duplication, or alteration, occurred in the second transaction information (SXI) if the derived EDC3 and the recovered EDC2 correspond, or (2) denying authentication to the second entity or determining that an unauthorized duplication, or alteration, occurred in the second transaction information (SXI) if the derived EDC3 and the recovered EDC2 do not correspond.

41

79. The method of claim 73 for further securing the first and second information associated with the first entity to the first entity by using a credential previously issued to the first entity by a trusted entity, the information stored in the credential including at least the first or second information associated with the first entity, and a first variable authentication number (VAN1), the VAN1 being used to secure the first or second information to the first entity, authentication being denied if the first or second information associated with the first entity cannot be secured to the first entity by using VAN1.

80. The method of claim 73 for further securing the third and fourth information associated with the second entity to the second entity by using a credential previously issued to the second entity by a trusted entity, the information stored in the credential including at least the third or fourth information associated with the second entity, and a second variable authentication number (VAN2), the VAN2 being used to secure the third or fourth information to the second entity, authentication being denied if the third or fourth information associated with the second entity cannot be secured to the second entity by using VAN2.

81. The method of claim 73 wherein the first entity has a personal identification number (PIN), the PIN being used to access the FXI information stored in the first storage means. the method further comprising:

receiving a personal identification number (PIN) supplied by the first entity at the first site; and

retrieving the first information associated with the first entity from the first storage means only if the PIN of the first entity is determined to be authentic.

82. The method of claim 73 wherein a transaction number (XN) is used in conjunction with the FXI or the SXI to identify and retrieve transaction information from a storage means associated with an entity participant in a transaction, the method further comprising:

generating an XN at one of the first or second sites, and transmitting the XN to the other of the first or second sites;

storing the XN in the FXR storage means and SXR storage means associated with the transaction;

using the XN to identify the transaction, and as an index in retrieving relevant transaction information.

83. The method of claim 73 wherein one of the first and second information associated with the first entity is secret, and the other of the first and second information associated with the first entity is non-secret.

84. The method of claim 73 wherein one of the third and fourth information associated with the second entity is secret, and the other of the third and fourth information associated with the second entity is non-secret.

85. The method of claim 73 wherein the same key, or either one of RN1 or RN2, is used subsequent to authentication, by each of the first and second entities to code and uncode information transmitted between the sites.

86. The method of claim 73 for further authenticating the participation of the first entity in a transaction by a third entity at a third site, wherein the FXI comprises the XN and fifth information being previously stored in a fifth storage means at the first site and also in a seventh storage means at the third site, and second information associated with the third entity being previously stored in sixth storage means at the first site, and first information associated with the third entity being previously stored in an eighth storage means at the third site, the method further comprising:

42

retrieving the fifth information associated with the first entity from the fifth storage means at the first site;

retrieving the XN from the FXR storage means;

combining the XN and the fifth information to form a first information group (IG1);

irreversibly coding IG1 to derive a fourth error detection code (EDC4);

retrieving the second information associated with the third entity from the sixth storage means at the first site;

coding the EDC4 with the second information associated with the third entity to derive a third anti-duplication authentication number (ADVAN3);

transmitting the ADVAN3 and the XN from the first site to the third site, and receiving the ADVAN3 and the XN at the third site;

retrieving the first information associated with the third entity from the eighth storage means at the third site;

uncoding the ADVAN3 by using the first information associated with the third entity to recover the EDC4;

retrieving the fifth information from the seventh storage means at the third site;

combining the received XN and the fifth information to form a second information group (IG2);

irreversibly coding the IG2 to derive a fifth error detection code (EDC5);

comparing EDC4 and EDC5; and

authenticating the participation of the first entity in the transaction if the EDC4 and EDC5 match, or determining that the entity did not participate in the transaction if the EDC4 and EDC5 do not match.

87. The method of claim 73 wherein the FXI is made secure in transmitting the FXI from the second site to the first site by coding the FXI with third information associated with the first entity to derive coded FXI, the third information associated with the first entity being previously stored in a ninth storage means at the second site, and by uncoding the coded FXI by using fourth information associated with the first entity, the fourth information associated with the first entity being previously stored in a tenth storage means at the first site, the method further comprising:

retrieving the third information associated with the first entity from the ninth storage means at the second site;

coding the FXI with the third information associated with the first entity to derive a coded FXI at the second site;

transmitting the coded FXI from the second site to the first site, and receiving the coded FXI at the first site;

retrieving the fourth information associated with the first entity from the tenth storage means at the first site; and

uncoding the coded FXI by using fourth information associated with the first entity to recover the FXI at the first site.

88. A method for authenticating a first party at a first site by a second party at a second site, the second party being a person or a computer program, by using a personal identification number (PIN) supplied by the first party at the first site, and further using a first random number (RN1) generated by the second party at the second site, the PIN being previously used to derive or access first coded authentication information, the first coded authentication information being previously stored in a storage means associated with the second party at the second site, the method comprising:

receiving a PIN at the first site from a first party to be authenticated;

generating or accessing second coded authentication information using the received PIN;

generating a first random number (RN1) at a second site by the second party;  
 storing the first random number (RN1) in the second storage means at the second site;  
 transmitting the first random number (RN1) from the second site to the first site;  
 receiving the first random number (RN1) at the first site by the first party;  
 coding the received first random number (RN1) and the second coded authentication information to derive a first anti-duplication variable authentication number (ADVANI), the first anti-duplication variable authentication number (ADVANI) further being derived by irreversibly coding the received first random number (RN1) to derive a first error detection code (EDC1), and coding the first error detection code (EDC1) with the second coded authentication information to thereby derive the first anti-duplication variable authentication number (ADVANI);  
 transmitting the first anti-duplication variable authentication number (ADVANI) from the first site to the second site;  
 receiving the first anti-duplication variable authentication number (ADVANI) at the second site by the second party;  
 retrieving the first coded authentication information from the storage means at the second site;  
 uncoding the received first anti-duplication variable authentication number (ADVANI) by using the first coded authentication information to recover the first error detection code (EDC1);  
 retrieving the first random number (RN1) from the storage means at the second site;  
 irreversibly coding the retrieved first random number (RN1) to derive a second error detection code (EDC2);  
 comparing the first error detection code (EDC1) and the second error detection code (EDC2); and  
 authenticating the first party by the second party if the first error detection code (EDC1) and the second error detection code (EDC2) correspond.

89. In a check or payment instrument transaction system, a method for issuing a check or payment instrument by an originator to a recipient, information associated with the check or payment instrument comprising (1) information associated with the originator, (2) information associated with the recipient, and (3) other information which includes at least an amount of the check or payment instrument, the method comprising:

receiving the information associated with the originator and the recipient, and the other information including at least the amount;

deriving a variable authentication number (VAN) using at least a portion of the received information;

associating the received information and the VAN with the check or payment instrument; and

issuing the check or payment instrument.

90. The method of claim 89 wherein the check or payment instrument is authenticated by using at least a portion of the information associated with the check or payment instrument and the VAN.

91. A method for securing in escrow and in trust, a portion of information used to derive a joint key, the joint key being associated with a first party and a second party and being stored in a storage means associated with the second party, wherein escrowed or entrusted information was previously used for generating a variable authentication number (VAN), the joint key being derivable from information associated with the first party and information associated with the second party, the VAN being subsequently used in authenticating the first party, the first party being enrolled by the second party and being issued a credential, the VAN being stored in the credential, the method comprising:

previously receiving information associated with the first party and information associated with the second party;

previously generating a joint key using the information associated with the first party, and the information associated with the second party; and

retaining in the storage means, in trust, at least a portion of information used to derive the joint key.

\* \* \* \* \*



PATENT APPLICATION SERIAL NO. 08/747174

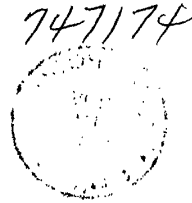
U.S. DEPARTMENT OF COMMERCE  
PATENT AND TRADEMARK OFFICE  
FEE RECORD SHEET

310 CS 16-0235 01/27/97 08747174  
31025 101 1,049.00UR  
31026 201 1,049.00CH



- 71 -

**SECURE TRANSACTION SYSTEM  
AND METHOD UTILIZED THEREIN**



**Abstract of the Disclosure**

B2

A transaction system ~~is disclosed~~ wherein,  
5 when a transaction, document or thing needs to be |  
authenticated, information associated with one or more  
of the parties involved is coded together to produce a  
joint code. This joint code is then utilized to code  
information relevant to the transaction, document or  
10 record, in order to produce a variable authentication  
number (VAN) at the initiation of the transaction. This  
VAN is thereafter associated with the transaction and is  
recorded on the document or thing, along with the  
original information that was coded. During subsequent  
15 stages of the transaction, only parties capable of  
reconstructing the joint code will be able to uncode the  
VAN properly in order to re-derive the information. The  
joint code serves to authenticate the parties, and the  
comparison of the re-derived information against the  
20 information recorded on the document serves to  
authenticate the accuracy of that information.



a17

- 1 -

~~SECURE TRANSACTION SYSTEM~~  
~~AND METHOD UTILIZED THEREIN~~

Field of the Invention

The present invention relates generally to  
5 secure transaction systems and, more particularly,  
concerns a method and apparatus for authenticating  
documents, records and objects as well as the  
individuals who are involved with them or responsible  
for them.

10

Background of the Invention

There are many times in our daily lives when  
the need arises for highly secure transactions. For  
example, instruments of commerce, such as checks, stock  
certificates, and bonds are subject to theft and  
15 forgery. From the time a document is issued, the  
information contained on it, or the name of the  
recipient could be changed. Similarly, passports, pay  
checks, motor vehicle registrations, diplomas, food  
stamps, wager receipts, medical prescriptions, or birth  
20 certificates and other official documents are subject to  
forgery, fraudulent modification or use by an unintended  
recipient. As a result, special forms, official stamps  
and seals, and special authentication procedures have  
been utilized to assure the authenticity of such  
25 documents. Medical, legal and personnel records, and  
all types of information in storage media are also  
subject to unauthorized access. Passwords and coding of  
such records have been used to thwart unauthorized  
access. However, there have always been ingenious  
30 individuals who have somehow managed to circumvent or  
evade all such systems of security.

With the introduction of computers and computer communications into business transactions and document processing, a certain degree of security was gained, in that it is now possible to verify documents and transactions much more quickly, thereby avoiding many frauds which previously went unnoticed until it was too late. However, with the elimination of the human factor, verification of the identify of parties also became more difficult. A pressing need still exists for business transaction, document processing and record access systems which can assure the identity of the parties and the accuracy of the information involved in the transaction. As used herein, the term "record access systems" includes systems which access media which contains data, messages, text, FAX, audio, video, drawings, images, photo, electronic and physical mail, safe boxes, and the like. As used herein the term "business transaction system" will be intended as a generic term to describe all such transaction, document processing and record access systems, including ones not related to business use, such as passport authentication systems.

The security problems described above have been handled with some degree of success in systems involving a single party transaction where the party is present. For example, during the use of an automatic teller machine, the customer is the sole party involved and is present in person. However, until the present invention, it has not been possible to verify the identity and to secure the interests of all parties to multi-party transactions and, in particular, absent parties to a transaction.

Summary of the Invention

Briefly, the present invention is directed to a transaction, document processing, or record access system which avoids the shortcomings of known systems of this type. In accordance with an embodiment of the present invention, when a transaction, document or thing needs to be authenticated, information associated with at least one of the parties involved (e.g., an originator and/or a recipient) is coded to produce a joint code. This joint code is then utilized to code information relevant to the transaction, document or record, in order to produce a variable authentication number (VAN) or code at the initiation of the transaction. This VAN is thereafter associated with the transaction and is recorded on the document or thing, along with the original information that was coded. During subsequent stages of the transaction, only parties capable of reconstructing the joint code will be able to uncode the VAN properly in order to re-derive the information. Thus, the joint code serves to authenticate the parties, and the comparison of the re-derived information against the information recorded on the document serves to authenticate the accuracy of that information. Alternatively, the information could be authenticated by regenerating a VAN from the recorded information and comparing the regenerated VAN with the recorded VAN.

In accordance with an embodiment of the present invention, at the time of enrolling as a user of the system, each user selects a personal identification number (PIN), which is secret, does not exist in an uncoded form, and cannot be recovered from other information anywhere in the system. During or after enrollment, a non-secret identification code and a secret code are also stored in a user's file at the user associated computer facility. When a user participates

in a transaction, the user is required to utilize his or her PIN, which after being coded is used to derive a coded arbitrary number. Subsequently, this arbitrary code is compared to another such code which is generated  
5 from a reconstituted version of the coded PIN, in order to authenticate the user's identity. One of the embodiments creates a computer file with a secret address to authenticate a user's identity, and to secure sensitive records. The address is preferably not stored  
10 anywhere in the system, but is generated when needed from information supplied by the user. In some embodiments of the present invention, when a joint code is created as described above, one participating user (e.g., the originator) must provide his or her PIN. The  
15 other party's non-secret identification code and the PIN are utilized in creating the joint code. In other embodiments, the joint code is created from the coded PIN's of the participants.

#### Brief Description of the Drawings

20 The foregoing brief description as well as further objects, features, and advantages of the present invention will be understood more completely from the following detailed description of the presently preferred, but nonetheless illustrative, embodiments of  
25 the invention, with reference being had to the accompanying drawings, in which:

Figs. 1-5 illustrate the symbols utilized in the present application to represent conventional building blocks used to form the invention, these  
30 building blocks being respectively, a coder, an uncoder, a linker, a mixer, and a sorter;

Figs. 6-8 are functional block diagrams illustrating a check transaction system in accordance with a first embodiment of the present invention, with  
35 Fig. 6 illustrating user enrollment, Fig. 7 illustrating

how an originator generates a check, and Figs. 8A and 8B illustrating the authentication process when the check is presented to be cashed;

5 Figs. 9-12 are functional block diagrams illustrating a credential issuing and authentication system in accordance with a second embodiment of the present invention, with Fig. 9 illustrating the enrollment of an official, Fig. 10 illustrating the enrollment of a user, Fig. 11 illustrating the issuance  
10 of the credential, and Fig. 12 illustrating the authentication of an issued credential;

Figs. 13A-13E, when arranged as illustrated in Fig. 14, collectively represent a functional block diagram of a check transaction system similar to that of  
15 Figs. 6-8, but including the basic processing necessary to clear and pay a check electronically;

Figs. 15A-15C are functional block diagrams of a credential issuing and authentication system according to an alternate embodiment of the present invention; and

20 Fig. 16 is a functional block diagram of a system for authenticating a party and for authorizing access to a secret file associated with the party according to an alternate embodiment of the present invention.

#### 25 Detailed Description of the Preferred Embodiments

Figs. 1-5 illustrate the functional building blocks utilized in the preferred embodiments. All of these components are conventional building blocks for computer or communication systems. Moreover, those  
30 skilled in the art will appreciate that the blocks can be realized as hardware components, or they can be realized as functional blocks in an overall computer program.



The coder illustrated in Fig. 1 and the uncoder illustrated in Fig. 2 may be any form of such device utilizing a known algorithm, such as the Data Encryption Standard (DES). A coder, as illustrated in 5 Fig. 1, has at least one data input, at which it receives clear data. It also has one or more additional inputs for receiving keys  $K_1$ ,  $K_2$ , which are utilized to code the clear data into a form in which it could not be easily recognized or uncoded without the use of the 10 keys. A variable which is used as a key may be padded to obtain the desired security. An uncoder (Fig. 2) reverses the process of the coder. Basically, it receives the coded data and utilizes the same keys to reconstruct the clear data.

15 A linker (Fig. 3) receives a plurality of data inputs and concatenates them into a longer code word ( $D_1, D_2 \dots D_N$ ). Similarly, a mixer (Fig. 4) receives a plurality of data inputs ( $D_1$ , and  $D_2$  through  $D_N$ ) and mixes their digits or binary bits. A simple example of 20 a mixer would be a conventional time division multiplexer which is used to interleave plural data inputs. However, in many applications, it will be preferable to utilize a more sophisticated mixer, such as one that utilizes arithmetic and logical combinations 25 of digits or bits. A sorter (Fig. 5) reverses the process of a linker or a mixer, that is, it receives a concatenated or mixed code word and reproduces the original component words. A time division demultiplexer could serve as a sorter for a mixed signal 30 originally generated by a multiplexer.

Figs. 6, 7, 8A and 8B constitute a functional block diagram illustrating the present invention in a check transaction system. The system illustrated in Figs. 6, 7, 8A and 8B are well suited for use in 35 generating and processing employee paychecks, for example. The system involves three phases of operation.

In the first phase, illustrated in Fig. 6, a user of the system must enroll in order to be recognized by the system. Each user enrolls at his or her bank, or at another convenient location, such as a place of  
5 employment, in the presence of an officer, who appropriately verifies the user's identity and obtains the typical information from him, including his taxpayer identification number (TIN) and telephone number. An account is then opened for the user and a file is  
10 created for him or her in the bank's computer, and the bank assigns a person account number (PAN) to the user's account. If a bank card is issued to the user, it usually contains the PAN and a bank identification number (BIN).

15 While operating a terminal, the user is requested to select a personal identification number (PIN) and to enter that PIN into the terminal. The user complies and such entry occurs at block 10 of Fig. 6 with the typical transaction information, including the  
20 user's TIN or PAN, being entered at block 11. The PIN is applied directly to an irreversible coder 12, where it is processed to produce a coded PIN (CPN). Coder 12 may be any type of conventional coding device which can process the PIN so that the coding is irreversible  
25 (i.e., the PIN cannot be recovered from the CPN). At the same time, a random number generator 14 produces a random number (RN), which is applied to a mixer 16 along with the CPN. Alternately, the user may be permitted to select an arbitrary number for RN.

30 The signal produced by mixer 16 is then transmitted to the bank's computer, where it is applied to a sorter 18. It is assumed that this transmission preferably occurs over a secure line, such as one protected by a tandem coder and uncoder which can  
35 utilize a joint terminal-bank key. The sorter recovers the original CPN and RN, saving RN in the user's file at

block 22. It should be noted that in saving RN, the user's file is accessed by using his TIN as an index. The received CPN is applied as the data input to a coder 20, which receives RN as its key input, producing  
5 a revisable owner code (ROC) which is saved in the user's file in the same manner as RN. Various additional information is saved in the user's file, such as his personal account number (PAN), name, phone number (PHN), account balance, and other relevant information.  
10 The user's TIN, PAN or PHN can be used as an index to access the user's file. CPN represents coded authentication information since it is a coded form of the PIN, and since it is used in other parts of the system to authenticate the user and the transaction.  
15 The system preferably maintains RN as a secret number (although in the present embodiment the user file is not secret since it is accessed using a non-secret index) and ROC is maintained as a non-secret number. As explained in detail below, CPN is derivable from ROC and  
20 RN.

Fig. 7 illustrates how the originator generates a check in accordance with the present invention. This process preferably takes place at the originator's terminal or computer. It is assumed that  
25 the originator would be generating a check in the usual manner and would include on it all of the information usually found on a check, as well as the information normally recorded or imprinted on check forms, such as the recipient's name and TIN (RTIN), and the  
30 originator's personal account number and bank identification number. Preferably, the terminal includes a check reader and printer which can read necessary information from the originator's check form and print information on the form, although this could  
35 also be done manually by the originator. The originator and the recipient can be the same person, for example,

where a person is cashing a personal check originated by the person. In the case of multi-party checks, the check is originated by a present party (i.e., the originator) in favor of an absent party (recipient).

5           The originator enters his or her PIN at a terminal or computer. Through irreversible coder 10, the originator's PIN is converted to a coded PIN (CPNO), which is applied as the key input to coder 28. The data input to coder 28 is the recipient's TIN (RTIN), which  
10 has been read from the check, or accessed from the computer memory, or entered by the originator. The data output of coder 28 is a joint key (JK), which is applied as the key input to a coder 30. Generally, the JK is generated using information associated with at least one  
15 of the parties involved in the transaction (in this case, the originator and recipient). As will be shown more fully below, the joint key (or code) is used to protect and authenticate the originator and recipient. The data input to the coder 30 is the information (INFO)  
20 to be authenticated (that is, information relevant to the transaction, such as check number, amount, etc.).

          The data output of the coder 30 is a variable authentication number (VAN), which codes the information to be authenticated, based upon information related to  
25 the recipient and information related to the originator. Note that the VAN is alternatively generated directly from INFO and information associated with at least one of the parties, without the intermediate step of generating the JK. The VAN and at least a portion of  
30 the information relevant to the transaction are written or imprinted upon the check 32, thereby becoming a permanent part of it. Alternately, the check may represent an electronic transfer of funds or some other type of electronic transaction. In this case, the VAN

and at least a portion of the information relevant to the transaction are included with the electrical signals associated with the electronic transaction.

It is contemplated that in creating the VAN,  
5 all information would not necessarily be coded in the same manner. For example, the amount of the check might be considered important enough so as to be recoverable completely, and it would be coded into the VAN in a manner that would permit complete recovery. Other  
10 information, such as the date and check control number might be considered less important and would be coded into the VAN in such a manner as to permit detection of changes (e.g., error detection coding), but without complete recovery of the original information.

15 As noted above, other predetermined information which is known jointly by the originator and recipient, and which does not appear on the check, can also be used to derive the VAN. For example, when a check is drawn to multiple recipients, e.g., husband and  
20 wife, each recipient's TIN (which does not appear on the check) may be used to derive the joint code and VAN. This makes it more difficult to fraudulently generate the VAN since the predetermined information not appearing on the check would not be generally known.

25 Figs. 8A and 8B illustrate the authentication process at a terminal when the recipient presents the originator's check to be cashed. The terminal communicates via a network of the banks involved in the transaction. Preferably, the terminal includes a device  
30 which can read information directly from the check 32. Alternately, the terminal operator can manually key information into the terminal, based upon information appearing on the face of the check 32. At block 40, the recipient inserts his or her PIN, and at block 41,  
35 identifies his bank and enters his TIN (RTIN) and all information required by the terminal to initiate the

transaction. An irreversible coder 42 processes the PIN to produce the coded PIN, CPNR, which is applied as the key input to a coder 44. A random number generator produces a random number (i.e., an arbitrary number) RNX  
5 which is applied as the data input to coder 44. Coder 44 then produces a coded random number (i.e., a coded arbitrary number), CRNX, which is applied to mixer 48 along with RNX. The output of the mixer is, therefore, a signal which contains CRNX and RNX in a  
10 converted form, so that neither number nor CPNR may readily be discerned from the signal. CRNX represents coded authentication information because it is a coded representation of CPNR, and because it is used by the system to authenticate the recipient and the  
15 transaction.

The mixer signal, along with the information entered in block 41 and the information read from the check are transmitted to the computer at the recipient's bank (i.e., remote bank CPU) over preferably an  
20 unsecured line (the use of an unsecured line is possible because CRNX and RNX, not CPNR, are transmitted from the mixer 48 to the sorter 62). The system first authenticates the identify of the check holder at the recipient's bank. Next, the information on the check,  
25 as well as the originator and recipient, are authenticated at the originator's bank.

At the recipient's bank, the output of mixer 48 is received in a sorter 62, which separates CRNX and RNX, with CRNX being applied to a comparison  
30 block 64 and RNX being applied as the data input to a coder 66. Based upon the recipient's TIN, RTIN, his bank's computer is able to access his file at block 68 and to extract his ROC (a non-secret number) and RN (a secret number), ROCR and RNR therefrom. ROCR and RNR  
35 are applied as the data and key inputs, respectively, to an uncoder 70, which generates the recipient's CPN,

CPNR, which is applied as the key input to coder 66. Coder 66, therefore, reproduces the recipient's coded random number, CRNX (in the same manner as coder 44), which is applied as the second input to comparison  
5 block 64. It should be appreciated that the CPNR output of uncoder 70 is the true CPNR derived from the bank's records. Accordingly, the CRNX produced by coder 66 is the true CRNX. Therefore, should the comparison at  
10 block 64 fail, the authentication of the recipient has failed and it is presumed that recipient is not the party presenting the check. The transaction is therefore aborted. On the other hand, if the recipient's identity is authenticated, the transaction can proceed. The recipient's bank then communicates  
15 with the originator's bank, conveying all the information about the transaction and requesting authorization to pay (block 71).

As shown in Fig. 8B, at the originator's bank, using OTIN (or the originator's PAN) as an index, the  
20 originator's ROCO and random number, RNO, are extracted from the originator's file at block 50. ROCO is applied as the data input to an uncoder 52, and RNO is applied as the key input to uncoder 52. Uncoder 52 therefore reverses the operation performed by coder 20 (Fig. 6)  
25 when the originator enrolled, producing the originator's CPN, CPNO. CPNO is then applied as the key input to a coder 56, which receives the recipient's TIN, RTIN, as the data input.

In accordance with the embodiment just  
30 described, it is contemplated that security considerations may warrant revising the ROC from time to time independent of any transaction. Toward this end, CPN could be reconstituted from the current ROC and RN as in block 52. Next, a new RN is used with CPN to  
35 generate a revised ROC, making use of a coder in the same manner as coder 20 of Fig. 6. The user's new RN

and ROC are stored and accessed, and CPN need only be reproduced at the bank where the user maintains an account.

In the same manner as coder 28 of Fig. 7, coder 56 therefore produces the joint key JK. JK is applied as the key input to an uncoder 58, which receives the VAN from check 32 as its data input. Uncoder 58 therefore reverses the coding operation performed by coder 30 of Fig. 7. If the information on the check has been unmodified, the coder 58 should therefore reproduce the information INFO from the check which was sought to be authenticated. In block 60, a comparison is made between the output of uncoder 58 and the information appearing on the check. Failure of this comparison is an indication that the check may have been modified after being issued, and the originator's bank notifies the recipient's bank that the check will not be honored. Alternatively, the joint key JK from the coder 56 can be used to code the information (INFO) from the check to generate a new VAN, which can then be compared with the VAN from the check to authenticate the check.

Should the comparison be favorable, this is an indication that the check is authentic and unmodified, and the originator's bank accesses the originator's account (block 61) to determine if the account is in order and has sufficient funds or credit to pay the check. The date of the check is determined to be acceptable. If the check control number does not appear in the originator's file as a previously cashed check, then the current check control number is saved to prevent fraudulent check reuse. The originator's bank generates a redeemed or redemption VAN (RVAN) in coder 54, using its bank key and the original VAN. RVAN is saved in the originator's file (block 55) and is recorded on the check (block 57). The originator's



account is then debited. The originator's bank then authorizes the recipient's bank to pay the check. On the other hand, if originator's bank finds any irregularity in the check or in the originator's  
5 account, it will notify the recipient's bank that the check is dishonored.

The RVAN (and other RVAN's from other transactions) can be accessed from originators' files by banks and other financial institutions involved with  
10 processing checks to determine the status of checks. Thus, by creating and storing the RVANs in the originators' files, fraudulent reuse of checks is avoided.

At block 72 (Fig. 8A), the recipient's bank  
15 receives the originator's bank's instructions. It will then notify the recipient if the check has been dishonored. If the check has been honored, the recipient's account may be credited as in a deposit. Alternately, the recipient can receive payment  
20 immediately if he is at an appropriate terminal, such as an automatic teller machine.

Essentially, the check has cleared automatically, on-line, without further check handling or processing.

25 In a transaction where the user cashes his own personal check, the originator and recipient are one and the same. A VAN is created from a joint code which combines information associated with the user, such as the user's identification number (TIN or PAN) and the  
30 user's CPN, which is generated directly from a PIN entered by the user. When the VAN is authenticated, the joint code is derived by combining the user's identification number (TIN or PAN), and the user's true CPN, which is generated from the RN and ROC retrieved  
35 from the user's file, with the TIN (or PAN) serving as a file index.

As noted above, in Fig. 8A it is possible to use an unsecured link between the mixer 48 and the sorter 62 because CRNX and RNX, not CPNR, are transmitted from the mixer 48 to the sorter 62.

5 However, a security problem still exists in using an unsecured line between the mixer 48 and the sorter 62 because the signal can be recorded and then played back later to attempt to fraudulently authenticate a fraudulent transaction. In an alternate embodiment of  
10 the present invention, an anti-duplication variable authentication number (ADVAN) is generated at the recipient's terminal by coding at least a transmission date and time with the CPNR by a coder (not shown). The ADVAN is then mixed with the CRNX and the RNX by the  
15 mixer 48 and sent to the remote bank CPU over the unsecured line to the sorter 62. At the remote bank CPU, the CPNR which is generated by the uncoder 70 is used to uncode the ADVAN to regenerate the transmission date and time. The signal received over the unsecured  
20 line is then authenticated by comparing the regenerated transmission date and time to a reception date and time (that is, the date and time at which the signal was received at the remote bank CPU). In this manner, the recipient and transaction are further authenticated.

25 According to another embodiment of the present invention, RNX is generated at both the recipient terminal and the remote bank CPU. To generate the RNX at the remote bank CPU, a random number generator is located at the remote bank CPU, wherein the random  
30 number generator at the remote bank CPU is similar to and synchronized with the random number generator 46 located at the recipient's terminal. Instead of transferring the RNX and the CRNX, only the CRNX is transferred over the unsecured line from the recipient's  
35 terminal to the remote bank CPU. At the remote bank CPU, the CPNR generated by the uncoder 70 is coded by

Kc

the coder 66 with the RNX generated at the remote bank CPU to generate the CRNX. The generated CRNX is then compared by the comparator 64 with the CRNX transferred from the recipient's terminal to the remote bank CPU to  
5 authenticate the recipient and the signal received over the unsecured line. In this manner, the recipient and transaction are further authenticated.

According to another embodiment of the present invention, CRNX is never generated. Instead, the CPNR  
10 generated by the irreversible coder 42 is sent to the remote bank CPU over a secured line, rather than over an unsecured line. The CPNR generated by the uncoder 70 is then compared by a comparator (not shown) with the CPNR sent from the recipient's terminal to the remote bank  
15 CPU to authenticate the recipient. In this alternate embodiment, the random number generator 46, coder 44, mixer 48, sorter 62, and coder 66 are not required, although a secure line is required.

Figs. 9-12 constitute a functional block  
20 diagram illustrating the present invention in a credential issuing and authentication system. The system involves the same three phases of operation as the check transaction system of Figs. 6, 7, 8A and 8B. However, all users are enrolled by an authorized  
25 official who must be enrolled first. Accordingly, there are two enrollment processes which are somewhat different. The first one is enrollment of the official, and the second one is enrollment of a user prior to or at the time of issuing his credentials. It is  
30 contemplated that this system would be useful for all types of credentials and records; for example, motor vehicle registrations, social security cards, passports, birth certificates and all types of identification cards or personal storage media. This system would also be  
35 useful in protecting against unauthorized access to all types of records, as previously indicated.

Fig. 9 illustrates enrollment of the official. This can be accomplished at a terminal or computer which is in communication with a remote computer over a link which is assumed to be secure. The remote computer may, 5 for example, be the central computer at the agency issuing the credential. At the remote computer, number generator 100 generates a random number which, at block 102, is compared to a current list of all assigned personal keys. If the random number does not correspond 10 to an assigned personal key, then the random number is assigned as the personal key, PKO, of the official being enrolled. Alternatively, PKO can be selected at random, from a list of unused PKO's, and the list of available PKO's would thereby be diminished. In yet another 15 alternative, PKO could be accessed from a counter, such as a pseudorandom or an ordinary sequential counter the output of which may be coded with a secret key. The size, or length, of PKO can be such as to provide a full size memory address or an offset or an index extension, 20 to limit or enlarge the memory space wherein concealed files are stored. PKO is then transmitted over the secure link to the enrollment terminal.

At the terminal, the official enters his PIN and name and various other information required by the 25 system. The name can be numerically coded by using a telephone type key pad. The PIN is applied to an irreversible coder 104, which produces his coded PIN CPNO. CPNO is applied as the key input to a coder 106, which receives PKO as the data input. The data output 30 of coder 106 is the official's coded personal key, CPKO, which is applied as an input to mixer 107. The official's name code and TIN, OTIN, are also applied as inputs to mixer 107. CPKO represents a coded address since it is a coded representation of PKO.

(C)

The output of mixer 107 is transmitted back to the remote computer over the secure link. At the remote computer, sorter 109 separates the received signal into its component parts: CPKO, the official's name code, and OTIN. At block 108, CPKO and the official's name code are then saved (i.e., written) into File No. 1 assigned to the official with the official's TIN, OTIN, serving as a File No. 1 index. It is assumed that during the official's enrollment various other information will be provided by the official over the secure line and may be stored in his File No. 1. It should be noted that OTIN is not secret and, therefore, the location of File No. 1 and the contents of File No. 1 (including CPKO) are not secret.

At block 112, PKO is used as an index for File No. 2, which is also allocated to the enrolling official. The location of File No. 2 (and thus, the contents of File No. 2) is concealed, since PKO is secret and not stored anywhere in the system. The information or records which are stored in File No. 2 can be coded or uncoded. The memory space wherein concealed files are stored may be previously filled (or pre-loaded) with dummy or false information to make the contents and locations of authentic allocated files undistinguishable from the dummy files. The concealed File No. 2 can also be used to store the ROC and RN (or store only RN, since only RN is secret -- ROC could be stored in a non-secret file, such as Official's File No. 1), as previously described in Figs. 6, 7, 8A and 8B, to reconstitute a user's coded PIN, CPN. The concealed File No. 2 can also be used to store other secret information (not shown) associated with the official. An official's coded number, CNO, is generated at the output of coder 110, and is saved in File No. 2 at block 112. The key input to coder 110 is CPKO and the data input to coder 110 is PKO or an arbitrary

predetermined number (APN). CNO represents coded authentication information because it is a coded representation of CPKO, and because it is used by the system to authenticate the official.

5           At coder 110, CPKO and PKO can be interchanged as the key and data inputs. However, the arrangement selected must then be used consistently in each phase of the operation of the system.

          Those skilled in the art will appreciate that  
10 the present embodiment offers an additional level of security in that, not only is secret information unavailable to a person who does not know the related PK and PIN, but that person is even unable to determine the location of the file containing the information, and is  
15 unable to uncode the information contained therein.

          Fig. 10 illustrates user enrollment. The user is enrolled by a previously enrolled official, who verifies the user's identity, based on acceptable documentation. Before the user can be enrolled, the  
20 official's identity and authority are preferably authenticated. The official operates the terminal, where he enters his PIN, and his TIN, OTIN, and the name code used during his enrollment, which was stored in his "File 1". OTIN is transmitted to the remote computer,  
25 where it is used as an index to access CPKO from the official's File No. 1, and CPKO is returned to the terminal. The official's PIN is applied to the irreversible coder 104, which produces CPNO. CPNO is applied as the key input to an uncoder 114, which  
30 receives CPKO as a data input over the secure link from the remote computer. It will be appreciated that uncoder 114 simply reverses the process of coder 106 of Fig. 9, therefore producing PKO. PKO is applied to a mixer 118, the other input to which is the official's  
35 name code. The output of mixer 118 is then transmitted to the remote computer.

At the remote computer, the signal transmitted from mixer 118 is received in a sorter 124, which separates out PKO, and the name code. The extracted PKO is utilized as an index to address the official's "File 2" whereby CNO is read. The CNO read from File No. 2 is compared against the CNO generated by coder 120, which has as its data input PKO which is extracted by sorter 124 and as its key input is CPKO read from "File 1". Should this comparison fail, the identity of the official is not authenticated and the enrollment of the user is aborted. Assuming that the comparison is successful, comparator 130 is then enabled. At block 130, the name code which is extracted from sorter 124 is compared against the name code read from the official's "File 1" (using OTIN as index). Should this comparison fail, the enrollment of the user is aborted. Should the comparison be successful, the official has been fully authenticated and the user's enrollment may proceed.

At the remote computer, number generator 100 generates a unique random number, which is assigned to the user as a personal address key, PKU. Alternately, PKU can be generated from a counter as previously described. As discussed below, PKU represents a predetermined secret address of a File No. 2 associated with the user. PKU is transmitted over the secure link to the enrollment terminal, where it is applied to the data input of coder 113.

The user operates the terminal and selects a PIN which he enters along with his TIN, UTIN. The user's PIN is applied to the irreversible coder 104, which produces the user's coded PIN, CPNU. CPNU is applied as a key input to coders 113 and 115. The output of coder 113 is the user's coded personal key, CPKU (which represents a coded address of the user's File No. 2), which is applied as a data input to

coder 115. The output of coder 115 is the user's coded number, CNU, which is applied to the input of mixer 116. The user's TIN, UTIN and CPKU are also applied as inputs to mixer 116. The output of mixer 116 is transmitted  
5 back to the remote computer over the secure link. CNU represents coded authentication information because it is a coded representation of CPKU, and because it is used by the system to authenticate the user.

At the remote computer, sorter 119 separates  
10 the received signal into its component parts: CPKU, CNU and UTIN. At block 108, CPKU and CNU are saved (i.e., written) into File No. 1 assigned to the user, with the user's TIN, UTIN serving as a File No. 1 index. It should be noted that CPKU and CNU may be recorded on the  
15 user's credential when they are generated at the terminal. It should also be noted that UTIN is not secret, and therefore, the location and contents of the user's File No. 1 are not secret. It should further be noted that the official's CNO is stored in the  
20 official's secret File No. 2 (Fig. 9) while the user's CNU is stored in the user's non-secret File No. 1 (Fig. 10A), even though both CNO and CNU are used to authenticate the official and the user, respectively. These two different ways for storing CNO and CNU (as  
25 shown in Figs. 9 and 10A) illustrate two embodiments of the present invention.

The user's PK, PKU (or an arbitrary predetermined number APN), is applied as the data input to a coder 132, which receives the official's CPKU as a  
30 key input. Coder 132 produces a joint key, JKU, which it will be appreciated, is determined by information related to the user and information related to the official. Using PKU as an address, the joint key is written into the user's "File 2" at block 112', and  
35 using PKO and UTIN as address indices, the joint key JKU is written into the official's "File 2" at block 134



(Fig. 10B). These writes are enabled as a result of the success of the comparison occurring at block 130. Accordingly, the user's "File 2" will contain a joint key, and the official's "File 2" will contain a joint  
5 key for each user the official enrolls. Since the user's file 2 is addressed by PKU (which is secret), the location and contents of the user's file 2 are secret. At coder 132, when the joint key JKU is generated, CPK and PK can be interchanged as key and data inputs, or as  
10 to user and official inputs. However, the arrangement selected must then be used consistently.

Fig. 11 illustrates issuance of the credential. This is shown separate from the user enrollment process of Fig. 10. However, in many  
15 instances, it would occur at the same time. In the preferred embodiment, this process is shown as occurring at the agency's computer, although it may be performed by the official from a terminal where he may communicate with the computer. It is assumed that the official has  
20 a credential printer or recorder which contains credential forms on which information is printed or recorded to produce the actual credential. However, it is also possible to create the credential by inserting information manually or on a typewriter, provided the  
25 necessary information derived by the system can be entered. The official enters the usual information (INFO) normally contained on a particular credential 145. The user's TIN may also be recorded on the credential. Alternately, the user's CPKU and CNU  
30 may be recorded on the credential, after being extracted from the user's File No. 1, with UTIN serving as a file index. If CPKU and CNU are recorded on the credential, they may be erased from the user's File No. 1. Alternatively, only CNU may be recorded on the  
35 credential, with CPKU remaining in File No. 1, or vice versa.

23

The issuing process continues with the official entering his PIN, which is applied to an irreversible coder 140 to produce his CPNO, which is applied as a key input to an uncoder 142. At block 144, 5 the official's TIN, OTIN is utilized as an index to access the official's "File 1", so that CPKO may be read therefrom and applied as the input to uncoder 142. Uncoder 142 therefore performs the same process as uncoder 114 of Fig. 10 to produce PKO. At block 146, 10 PKO and UTIN are utilized as address indices to access the official's "File 2" and JKU is read therefrom. The information INFO on the credential is applied as the data input to a coder 152 and JKU is applied as the key input, whereby coder 152 codes the INFO to produce a 15 VAN, which is recorded on the credential. After recording the VAN on the credential, the joint key, JKU, may be erased from the official's File 2, where it was stored (or held in escrow or in trust), until the credential was issued. Alternately, the authentic JKU 20 may be replaced with a false or dummy JK for security purposes. This completes the issuance of the credential 145. It should be noted that the joint key JKU stored in the official's File No. 2 can only be used in a transaction if a party exists with knowledge of the 25 official's PIN, since this PIN is required to access the official's File No. 2 (at block 146). Thus, a person who does not have knowledge of the official's PIN (such as an unscrupulous person trying to issue a fraudulent credential) cannot legitimately issue a credential. 30 The VAN which is generated from information (INFO) recorded on the credential, or from information which is otherwise stored by the system, can include (coded) personal descriptive details to further identify the user (in addition to the user's PIN and TIN) in 35 order to limit the use of the credential to the sole individual to whom it was issued (or sold). Thus, items

such as bank cards, tickets, green cards, food stamps, ballots, travel checks, FAX messages, etc., can be protected and used solely by the individuals to whom they were issued. Also, the use of the credential may  
5 be enlarged to include a group, such as a family, by coding such information into the VAN.

Fig. 12 illustrates the authentication of an issued credential. This is preferably performed at a terminal provided for that purpose. The terminal  
10 includes a reading device for the credential 145 and an input device, such as a keypad for the user. The information could, however, be read from the credential and keyed in by hand. The terminal communicates with the remote processor via a preferably secure link.

15 As part of the credential authentication process, the identity of the user is authenticated. This requires that the user enter certain information at the terminal, including a PIN and user's TIN, UTIN, which is transmitted to the remote computer, which  
20 returns CPKU and CNU (box 178) via a secure data link. Alternatively, CPKU and CNU could have been recorded on the credential (or on some other item in the possession of the user, such as a card having a magnetic stripe for storing data) and inputted directly into the terminal.  
25 The PIN is applied to the irreversible coder 170 which produces CPNU. CPNU is applied as the key input to coder 172 and uncoder 174. Coder 172 receives CPKU as a data input. It should be noted that coder 172 performs in the same manner as coder 115, which produced CNU at  
30 its output during the user's enrollment. The output of coder 172 is applied as an input to the comparator at block 182, which also has as an input the CNU extracted from the user's File No. 1 (or inputted from the user's credential).

Should this comparison fail, the identity of the user is not authenticated, and the credential authentication is aborted. Assuming the comparison is successful, the user is identified, and the credential authentication, with access to the hidden File No. 2, ensues. The favorable output from comparator 182 enables uncoder 174. The data input to uncoder 174 is the user's CPKU. The key input to uncoder 174 is the user's CPNU, as already explained. It will be appreciated that uncoder 174 simply reverses the process of coder 113 of Fig. 10, therefore producing PKU. PKU is applied to a mixer 176 which also receives the VAN and INFO of the credential. The output of mixer 176 is then transmitted to the remote computer over the secure link.

At the remote computer, UTIN is utilized as an index to access the user's "File 1" at block 178. This permits reading of CPKU and CNU from the file, whereby CPKU and CNU were transmitted back to the user's terminal. At the remote computer, the signal transmitted from mixer 176 is received in sorter 180, which separates out PKU, VAN and INFO. The extracted PKU is utilized to address the user's "File No. 2" at block 184 whereby JKU is read. It will be appreciated that the user's File No. 2 has been accessed by an authorized user without reference to, or use of, information stored in the file. The VAN extracted from sorter 180 is applied as a data input to an uncoder 162, which receives the joint key JKU extracted from the user's "File 2" at block 184. It will be appreciated that uncoder 162 therefore reverses the process performed by coder 152 of Fig. 11. Assuming the VAN on the credential is the same one as originally recorded, uncoder 162 will have produced the recovered INFO which should be the same as the actual INFO recorded on the credential.

26

At block 169, the INFO from the credential is compared to the INFO recovered from uncoder 162. Should the comparison fail, this is an indication that INFO on the credential has been modified, and the credential is indicated as not being authentic. Should the comparison be successful, this is an indication that INFO is accurate, and the authenticity of the credential is confirmed. Alternatively, the credential information from the credential is coded using the JKU from the user's File No. 2 to generate a new VAN, which is compared with the VAN from the credential to authenticate the credential.

In order to enhance the security of this system, it would be desirable to make unassigned areas of memory indistinguishable from those utilized to store information for the "File 1" and "File 2" information. This is accomplished by pre-storing pseudo-information in unused memory allocated as hidden memory space. This pseudo-information constitutes random information arranged in the same format as actual files. This prevents an intruder from searching memory for structures that look like actual information files and using the uncovered information to work backwards to breach security.

Figs. 13A-13E, when arranged as shown in Fig. 14, constitute a functional block diagram illustrating further aspects of the check transaction system of Figs. 6, 7, 8A and 8B. Specifically, these figures illustrate a three-party check transaction, with each of the participants and the fidelity of the information on the check being authenticated, the check being automatically cleared, and the funds of the participants being immediately credited or debited, all of these processes being performed on-line. The participating parties in this transaction are the check originator, whose account is to be debited; the check

recipient to whom the check is drawn; and the check redeemer, who is cashing the check for the recipient or accepting it in payment for goods or services, and whose account is to be credited. In addition, the banks for  
5 each of these participants will also be participating in the transaction, and the messages generated by these banks will be authenticated. It is assumed that any individual or bank participating in the system will have enrolled as illustrated in Fig. 6. In addition, it is  
10 assumed that a check used in the system is generated in the manner illustrated in Fig. 7.

Referring first to Fig. 13A, the recipient of the originator's check has presented the check to the redeemer (block 200). The recipient and the redeemer  
15 are at a terminal which includes appropriate input means 202. Preferably, the input means includes a check reader and a keypad for each of them. However, in the absence of a check reader, it is also possible to key in information from the face of the check. The check is  
20 examined to determine if it contains a redemption VAN from a previous transaction. The presence of a redemption VAN is an indication that the check was used previously, and it will not be honored. If a redemption VAN is not present, then the transaction can proceed.  
25 It is assumed that the redeemer's bank identification number (RDBIN), and TIN are stored in the terminal, otherwise the redeemer keys in his bank's name and TIN, and the recipient keys in his TIN, PIN and bank's name. A bank directory is addressed at block 203 to produce  
30 the recipient bank's identification number (RCPBIN). The recipient's PIN is applied to an irreversible coder 42, which produces his CPNR. Irreversible coder 42, coder 44, random number generator 46, and mixer 48 are the same components illustrated in Fig. 8A  
35 and cooperate in the same manner to produce RNX, CRNX, in a mixed form at the output of mixer 48.

68

The terminal has available to it the redeemer's bank key (RDBK), which is applied to the key input of a coder 204, the data input to which is the terminal ID (TID), which is generated by the terminal.

5 Coder 204 then produces a joint terminal bank key (JTBK), which is applied as the key input to a coder 206, the data input to which is the output of mixer 48. The mixer output is therefore coded with a joint key JTBK which has been generated on the basis of

10 information related to the redeemer's bank identity and the terminal identity.

The output of coder 206 and the information from input means 202, and the recipient's TIN, RCPTIN, and the recipient's bank ID number, RCPBIN, are then

15 transmitted to the computer at the redeemer's bank. At the redeemer's bank (Fig. 13B), all of the received information is placed in temporary storage (block 208).

The redeemer's TIN, RDTIN, (originally stored in the terminal, or keyed in by the redeemer), is then

20 utilized as an index to access his account file, at block 210.

The check control number (CCN) of the present check is then compared to the CCN's stored in the redeemer's file during previous transactions (block

25 212), and the transaction is terminated if the present CCN matches that of a previously processed check. If the CCN of the present check is not a duplicate, processing continues.

RDBIN, and RCPBIN are utilized as indices to

30 access a bank key table (block 213), which produces the redeemer's bank key RDBK, and the recipient's bank key RCBK, which are applied as the data and key inputs, respectively, to a coder 214. The coder 214 then produces a joint bank key JBK, which is derived from

35 information related to the identity of the redeemer's bank and the identity of the recipient's bank.

The terminal identification (TID) is input to a coder 216, which has as a key input RDBK. In the same manner as coder 204, coder 216 therefore produces JTBK, which is applied as a key input to an uncoder 218. The  
5 data input to uncoder 218 is the information in temporary storage 208 which was originally received from coder 206. Coder 218 therefore reverses the process performed by coder 206, yielding the output of mixer 48, which is applied as a data input to a coder 220. The  
10 key input to coder 220 is JBK, so that the output of mixer 48 is now coded with the joint bank key JBK. The output of coder 220 is then transmitted in a message to the recipient's bank, along with RCPTIN, RDBIN, and RCPBIN.

15 At the recipient's bank, the received information is saved in temporary storage 230. RCPBIN and RDBIN are then applied to a bank key table (block 232), to yield RCBK and RDBK, which are applied as the key and data inputs, respectively, to a  
20 coder 234. In the same manner as coder 214, coder 234 therefore yields the joint bank key JBK, which is applied as a key input to uncoder 236. The data input to this uncoder 236 is the coded combination of RNK and CRNK produced by coder 220. Uncoder 236 therefore  
25 reverses the process of coder 220, yielding the mixture of RNK and CRNK as an output. This mixture is applied as an input to a sorter 238, to recover RNK and CRNK.

The recipient's TIN, RCPTIN, is utilized as an index to access the recipient's file at block 240 and  
30 read therefrom the random number, RNR, and his ROC, which are applied as the key and data inputs, respectively, to an uncoder 242. In the same manner as uncoder 70 of Fig. 8A, uncoder 242 therefore derives the true CPNR, which is applied as a key input to a  
35 coder 244, which receives RNK as a data input. The data output of coder 244 is therefore the true CRNK.



At block 246, this true CRNX is compared to the CRNX derived from sorter 238. If this comparison is favorable, the recipient's identity is confirmed, and processing may proceed. Otherwise, processing is terminated, with the originator's check being dishonored, because the recipient has not been properly authenticated. The recipient's bank then transmits a message to the redeemer's bank, informing it whether or not the recipient has been authenticated. If the recipient has not been authenticated, the redeemer's terminal is notified, and processing will terminate.

Assuming that the recipient has been authenticated, the recipient's bank message includes various information which is temporarily stored by the redeemer's bank (block 250 of Fig. 13C). At block 252, the originator's bank identification number ORBIN, which was read from the check, and the redeemer's bank identification number RDBIN are applied as indices to a bank key table to recover bank keys for these banks, OBK and RDBK, respectively. These keys are applied to a coder 254 to produce a joint bank key JBK', which is therefore dependent upon information related to the originator's bank and the information related to the redeemer's bank. JBK' is applied to the key input of a coder 256, which receives the original VAN, OVAN, (from the check) as a data input. The output of coder 256 is a redeemer's bank RDBVAN, which is transmitted to the originator's bank, along with various transaction information and the information from the check. RDBVAN serves to authenticate the communication between the banks.

At the originator's bank, the received information is temporarily stored at block 258. ORBIN and RDBIN are then utilized to reference a bank key table at block 260, whereby OBK and RDBK are extracted in the same manner as in block 252. The joint key JBK'

is then generated by means of a coder 262 in the same manner as coder 254. JBK' is then applied as the key input to an uncoder 264, which receives RDBVAN as a data input. This uncoder 264 therefore reverses the process performed by coder 256 and produces an extracted OVAN, which is applied to a comparator 266 (as shown in Fig. 13D).

The originator's personal account number ORGPAN which originally appeared on the check is utilized as an index to access the originator's account file at block 268 of Fig. 13C. This provides access to various information about the originator's account including the balance and a list of prior check control numbers (CCN's), and in addition, provides access to his revisable owner code ROCO and random number RNO, which are applied as the data and key inputs to an uncoder, to produce the originator's coded pin CPNO. CPNO is then applied as the key input to a coder 272 (Fig. 13D) which receives the recipient's TIN, RCPTIN, as a data input. The output of coder 272 is the joint key JK, which is applied as the key input to a coder 274, which receives the check information as a data input. It will be appreciated that coders 272 and 274 regenerate the original VAN, OVAN, from the check in the same manner as coders 28 and 30 of Fig. 7. This regenerated VAN is then compared to the extracted VAN at block 266. If this comparison fails, it is an indication that the check information may have been tampered with and the originator's bank informs the redeemer's bank that the check will be dishonored. On the other hand, if the comparison succeeds, the process continues.

The originator's bank then performs a series of computations, including determining whether the CCN of the check is proper (i.e., has not been used before) and whether the originator has a sufficient balance in his account (or credit) to cover the check, and whether

the date of the check is acceptable. In the case of any defects, the check will be dishonored and the process will terminate. Assuming that everything is in order, modification of the originator's account is approved, and a record of the check created at block 271, with the new information being added to temporary storage at block 273. Coders 275 and 276 are then utilized to encode the original VAN, OVAN, into an originator's bank VAN OBVAN. Various information about the transaction, and authorization to credit the redeemer's account are then transmitted is a message to the redeemer's bank.

At the redeemer's bank, all of the received information is stored in temporary storage at block 278. At block 280, coder 282 and uncoder 284, steps are performed to extract OVAN from OBVAN in a manner which is similar to that which was done in block 260, coder 262 and uncoder 264. This extracted OVAN is then applied to a comparator 286 of Fig. 13E, which receives as an additional input the stored OVAN from the check presented by the recipient. If this comparison fails, the process has not been authenticated, and the originator's bank will be notified. On the other hand, if the comparison succeeds, this is an indication that full authentication of the entire process and all parties has occurred and that the message received from the originator's bank is authentic.

Processing then continues by accessing the redeemer's account at block 288, computing a new balance at block 290 and updating the redeemer's account. The redeemer's bank then transmits a message back to the originator's bank, informing it that the redeemer's account has been credited. This information is saved at the originator's bank in temporary storage at block 291. The originator's bank then accesses the originator's account file using his personal account number ORGPAN as

an index, and updates his account with the information that was placed in temporary storage at block 273 (Fig. 13D).

The redeemer's bank also communicates with the  
5 terminal at which the check was presented (block 294 of Fig. 13D), and informs it that the transaction has been satisfactorily completed and that the recipient may receive payment in the form of cash, goods or services (block 296). The terminal prints the redemption VAN  
10 (RDBVAN) on the check.

Although various embodiments of the present invention have been described herein as useful for particular types of transactions, those skilled in the art will appreciate that they actually have universal  
15 utility. For example, the last embodiment (depicted in Figs. 13A-13E) was described as useful in a check transaction system, but it will be appreciated that it would also be useful in a bill payment system as well as a paperless/cashless system (as further described  
20 below).

Figs. 15A, 15B and 15C are functional block diagrams of a credential issuing and authentication system according to an alternate embodiment of the present invention, wherein the alternate embodiment  
25 includes many of the features of the embodiments depicted in Figs. 6-8 and Figs. 9-12. For example, the alternate embodiment of Figs. 15A-15C include steps for enrolling an official, enrolling a user, issuing a credential, and authenticating the credential. Fig. 15A  
30 illustrates user enrollment, Fig. 15B illustrates issuance of a credential, and Fig. 15C illustrates the authentication of an issued credential. In the alternate embodiment of Figs. 15A-15C, enrollment of the official is the same as shown in Fig. 9 and, therefore,  
35 shall not be discussed further.

Referring to Fig. 15A, a user is enrolled by a previously enrolled official who verifies the user's identity, based on acceptable documentation. Before the user can be enrolled, the official's identity and  
5 authority must be authenticated. The official operates a terminal, where he enters his PIN and his TIN, OTIN, and the name code used during his enrollment, which was stored in his File No. 1. OTIN is transmitted to the remote computer, where it is used as an index or address  
10 to access the official's File No. 1 and retrieve CPKO (block 1546). CPKO is returned to the terminal.

The official's PIN is applied to irreversible coder 1530, which produces CPNO. CPNO is applied as the key input to an uncoder 1532, which receives CPKO as a  
15 data input from the remote computer, and which uncodes CPKO to generate PKO. CPKO is also applied as a key input to a coder 1534, which receives PKO as an input. The coder 1534 codes PKO using CPKO as the key input to generate a coded number for the official (CNO), which  
20 represents coded authentication information. Another coder 1538 codes the official's name code using CNO as a key input to generate a coded name code. A mixer 1536 mixes the coded name code, PKO, and CNO and transmits the mixed signal to the sorter 1540 at the remote  
25 computer over preferably a secure link.

At the remote computer, the signal transmitted from mixer 1536 is received by the sorter 1540, which separates out PKO, CNO, and the coded name code. PKO is applied as an index (or address) to access the  
30 official's File No. 2 and to thereby retrieve CNO, which was previously stored in the official's File No. 2 during the enrollment of the official (see Fig. 9). The CNO transmitted from the terminal and the CNO retrieved from File No. 2 are then compared in a comparator 1542.  
35 If the comparison fails, the identify of the official is not authenticated and the enrollment of the user is

aborted. Assuming that the comparison is successful, the comparator 1542 is enabled and sends a signal to an uncoder 1544. The uncoder 1544 then uncodes the coded name code using the CNO retrieved from the official's  
5 File No. 2 to regenerate the name code. The name code is also accessed from File No. 1 and then compared at 1550. If the comparison fails, the identify of the official is not authenticated and the enrollment of the user is aborted. Assuming that the comparison is  
10 successful, the comparator 1550 sends an authentication signal ("okay to enroll user") and user enrollment begins. It should be noted that the "okay to enroll user" signal is applied as a write enabled to the official's File No. 2 at 1552 to save a joint key JKU  
15 therein (described below).

At the remote computer, number generator 1516 generates a unique random number (as discussed above), which is assigned to the user as a secret predetermined address or key, PKU. PKU is transmitted over a secured  
20 link to the enrollment terminal, where it is applied to the data input of a coder 1504.

The user operates a terminal and selects a PIN which he enters along with his TIN, UTIN. The user's PIN is applied to irreversible coder 1502 which produces  
25 the user's coded PIN, CPNU. CPNU is applied as a key input to coder 1504. The output of the coder 1504 is the user's coded predetermined address or key, CPKU. CPKU may be stored in a user record (at block 1510). A mixer 1506 mixes CPNU and CPKU and transmits the mixed  
30 signal to the remote CPU.

At the remote computer, sorter 1512 separates the received signal into its component parts CPKU and CPN. At the remote computer, a random number RN is generated (as discussed above) and applied as a key  
35 input to coder 1518. The coder 1518 also receives CPN as an input and thereby generates a revisable owner code

36

(ROC). ROC is stored in the user's File No. 1 (at block 1520), wherein the user's File No. 1 is accessed (or addressed) using UTIN. CPKU is also stored in the user's File No. 1 (at block 1520).

5           PKU is applied as an index or address to the user's File No. 2 in order to store RN (at block 1522). PKU is secret in the system and, therefore, the location and contents of the user's File No. 2 (including RN) is secret. Additional information may be coded in a  
10    coder 1524 using CPKU as a key input to generate coded information which is also stored in the user's File No. 2. The information which is coded using CPKU in the coder 1524 may include the secret information RN.

          PKU is applied as an input to coder 1528,  
15    which also receives CPKO as a key input. The coder 1528 generates a user joint key (JKU) which is stored in the user's File No. 2. JKU is also stored in the official's File No. 2 (at block 1552).

          It should be noted that the storage and  
20    handling of RN and ROC in the embodiment shown in Fig. 15A is different from the storage and handling of RN and ROC shown in Fig. 6. In Fig. 6, the file in which RN and ROC are stored is generally non-secret because it is indexed (or addressed) by generally non-  
25    secret user information (such as the user's TIN). However, in the embodiment shown in Fig. 15A, the non-secret ROC is stored in the user's File No. 1, which is non-secret, and the secret RN is stored in the user's File No. 2, which is secret (since it is accessed or  
30    addressed using the secret PKU). Therefore, the embodiment of 15A includes an additional level of security and protection over the embodiment shown in Fig. 6.

          Fig. 15B illustrates issuance of a credential  
35    according to the alternate embodiment of the present invention. The issuance of credential in the alternate

37

embodiment is essentially the same as the issuance of credentials in the previous embodiment shown in Fig. 11. Note, however, that it is possible to record the ROC retrieved from the user File No. 1 on the  
5 credential 1564 since the ROC is public (although the ROC could also have been recorded on the credential in the previous embodiment).

Fig. 15C illustrates the authentication of an issued credential. This is preferably performed at a  
10 terminal provided for that purpose. The terminal includes a reading device for the credential 1564 and an input device, such as a keypad, for the user. The information from the credential 1564 could, however, be keyed in by hand. The terminal communicates with the  
15 remote processor via a preferably secured link. As part of the credential authentication process, the identity of the user is authenticated. Specifically, the user enters his PIN which is applied as an input to irreversible coder 1570, which generates a coded PIN  
20 (CPNU). The user also enters his TIN (UTIN), which is used to access the user File No. 1 (at block 1588) and retrieve CPKU, which is transmitted from the remote CPU to the terminal. CPKU is applied as an input to coder 1574, which also receives CPNU as a key input.  
25 The coder 1574 generates a coded number CNU, which represents coded authentication information. CPKU is also applied as an input to uncoder 1572, which also receives CPNU as a key input. The uncoder 1572 uncodes CPKU to regenerate PKU. Both CNU and PKU are mixed by  
30 mixer 1576 and sent to the sorter 1578 at the remote CPU.

At the remote CPU, the sorter 1578 separates the signal into its component parts PKU and CNU. PKU is applied as an index into the user's File No. 2 in order  
35 to retrieve the secret information RN. UTIN is applied as an index to the user's File No. 1 to retrieve the



non-secret revisable owner code (ROC). ROC is applied as an input to uncoder 1584, and the secret information RN is applied as a key input to uncoder 1584. The uncoder 1584 thereby uncodes ROC using RN in order to regenerate CPNU as RCPN, which is applied as a key input at coder 1582. CPKU, which is read from the credential 1564, is applied as an input to coder 1582. The coder 1582 codes CPKU using RCPN as a key input in order to generate a coded number CNU. The generated coded number CNU is compared at the comparator 1580 to the coded number CNU received from the terminal. If the comparison fails, authentication of the user aborts. However, if the comparison is successful, the user is authenticated and the process continues by authenticating the credential 1564.

The credential 1564 is authenticated by reading the official's ID number OTIN from the credential and using OTIN as an index in order to access the official's File No. 1 and read CPKO (block 1599). CPKO is applied as an input to coder 1598 which also receives PKU as a key input. The coder 1598 codes CPKO using PKU in order to regenerate the user joint key JKU. JKU is also read from the user's File No. 2 using PKU as an index and then applied to a comparator 1596. The comparator 1596 compares the JKU which was retrieved from the user's File No. 2 and the JKU which was generated by the coder 1598. If the comparison fails, then authentication of the credential aborts. However, if the comparison is successful, the comparator 1596 is enabled and sends an okay signal to a comparator 1594.

The JKU retrieved from the user's File No. 2 at 1586 is applied to an uncoder 1592, which also receives as an input the VAN which was read from the credential 1564. The uncoder 1592 uncodes the VAN in order to regenerate INFO. The regenerated INFO is applied as an input to the comparator 1594, which also

receives the INFO read from the credential 1564. The comparator 1594 compares the regenerated INFO and the INFO from the credential and if the comparison is successful, the credential is authenticated. Otherwise, the credential is not authenticated.

As noted above, in Fig.15C, the transmission link between the mixer 1576 and the sorter 1578 is preferably secured since using an unsecured link would present a potential security problem. For example, the signal from the mixer 1576 could be recorded and then transmitted to the sorter 1578 at a later date in order to attempt to fraudulently authenticate a user and a credential. In accordance with an alternate embodiment of the present invention, an anti-duplication variable authentication number (ADVAN) is generated at the terminal by coding at least a transmission date and a time with the CPNU. The ADVAN is then mixed with the CNU and the PKU at the mixer 1576 and sent to the sorter 1578 at the remote CPU over an unsecured link. At the remote CPU, the received ADVAN is uncoded using the derived RCPN to regenerate the transmission date and the time. The regenerated transmission date and time are then compared to a reception date and time (that is, the date and time at which the signal was received at the sorter 1578) and if the comparison is successful, the information transmitted over the transmission medium between the mixer 1576 and the sorter 1578 is authenticated. In this manner, the user and credential are further authenticated.

Alternatively, a semi-random number (not shown) is generated at the terminal using a counter or other random number generator (not shown). The semi-random number is coded using the CPNU to generate a coded semi-random number. The coded semi-random number is then transmitted along with CNU and PKU to the remote CPU over an unsecured medium. At the remote CPU, the

LHC

coded semi-random number is uncoded using RCPN to regenerate the semi-random number. A second semi-random number is then generated at the remote CPU using another counter or random number generator (not shown) which is  
5 generally synchronized with the counter (not shown) at the terminal. The communication medium between the mixer 1576 and the sorter 1578 is then authenticated by comparing at the remote CPU the regenerated semi-random number to the second semi-random number which was  
10 generated at the remote CPU. If the comparison is successful, then the information transmitted over the communication medium between the mixer 1576 and the sorter 1578 is authenticated. In this manner, the user and credential are further authenticated.

15 As described above, the predetermined secret address PKU is coded to generate the coded secret address CPKU. According to an alternate embodiment, PKU comprises one or more components which are combinable to form the predetermined secret address PKU. In this  
20 alternative embodiment, only one of the components of the PKU is transmitted from the remote CPU to the terminal. The coder 1504 (Fig. 15A) codes this one component of the PKU to generate CPKU. Therefore, in this alternate embodiment, CPKU represents a coded  
25 portion of the PKU. Then, to access the user's File No. 2, the CPKU is uncoded as described above to regenerate the portion of the PKU. This PKU portion is combined with the other portions of the PKU to regenerate the PKU, which is then used to access the  
30 user's File No. 2. The other portions of the PKU may be stored throughout the system, such as in the operating system, in the executive program, in files, etc.

Fig. 16 is a functional block diagram of a system for authenticating the identity of a party and  
35 for authorizing access to a party's hidden (or secret) file according to an alternate embodiment of the present

invention. The party's hidden file (such as hidden memory file 1622) may contain coded or uncoded secret information. In the embodiment of Fig. 16, the party is in possession of a portable storage media, such as, a  
5 card 1602 having a magnetic stripe for recording information thereon. The card 1602 is issued by an agency, or a bank, during enrollment of the party. Information recorded on the card 1602 includes the party's revisable owner code (ROC), a coded address  
10 (CPK) of the hidden file 1622, an agency identification number (AID or Agency ID), and a transaction sequence number (TSN). The party's ROC is generated as described above (see Fig. 6). The coded address CPK of the hidden memory file 1622 may either represent the entire address  
15 of the hidden memory file 1622 or only a portion of the address of the hidden memory file 1622, as described above.

The party to be authenticated enters a personal identification number (PIN) at a terminal. The  
20 PIN is input to an irreversible coder 1606 to produce a coded personal identification number (CPN). The information recorded on the party's card 1602 is read from the card 1602 using an appropriate reader (not shown). The CPK read from the card 1602 is applied as  
25 an input to an uncoder 1612, which also receives the CPN as a key input. The uncoder 1612 uncodes CPK using CPN as a key input to generate PK, which represents either the total address of the hidden memory file 1622 or a portion of the address of the hidden memory file 1622  
30 (as noted above).

The transaction sequence number (TSN) read from the card 1602 is input to a mixer 1608 and then to a coder 1610. The coder 1610 also receives the CPN as a key input. The coder 1610 codes the TSN using the CPN  
35 as a key input to generate an anti-duplication VAN (ADVAN). The ADVAN, PK, ROC, and AID are input to a

*1612*

mixer 1614 and the resulting mixed signal is sent to the remote CPU over a preferably unsecured communication link.

The user's hidden memory file 1622 is part of  
5 a memory which is used to store such files at the remote CPU. The sorter 1616 separates the received mixed signal into its component parts ROC, PK, AID, and ADVAN. Where the PK generated by the uncoder 1612 is only a portion of the address to the hidden memory file 1622,  
10 the AID is used as an index to a memory table 1618 to retrieve other address components for the hidden memory file 1622. Thus, the address components in the memory table 1618 applicable in any given transaction depends on the particular AID. The PK is combined with the  
15 other address components at a combiner 1620 to thereby form the composite address of the hidden memory file 1622. The AID could also identify a predetermined procedure for combining the applicable address components. The composite address is used to access the  
20 hidden memory file 1622 to retrieve a secret random number RN (which is generated according to the method described above with respect to Fig. 6). RN is input as a key to a coder 1624. The coder 1624 also receives the ROC from the sorter 1616 and thereby generates CPN.

25 A transaction sequence number (TSN) is also retrieved from the hidden memory file 1622 and is input to a coder 1632. The coder 1632 also receives CPN as a key input and thereby generates an ADVAN. The ADVAN generated by the coder 1632 is compared with the ADVAN  
30 output from the sorter 1616 at a comparator 1630. If a favorable comparison is obtained, then coder 1628 is enabled. If the comparison is not favorable, then the user is not authenticated and does not gain access to the memory file 1622.

CPN

Coder 1628 receives PK as an input and CPN as a key and thereby generates CPK. The CPK generated by the coder 1628 is received by an uncoder 1626 as a key input. The uncoder 1626 also receives as input coded  
5 information which is retrieved from the hidden memory file 1622. The uncoder 1626 uncodes the coded information from the hidden memory file 1622 using the CPK as a key input to thereby produce clear information. The clear information is then provided to the  
10 authenticated user.

As a result of the favorable comparison of the ADVANs at the comparator 1630, a new (or revised) transaction sequence number (TSN) is generated and stored in the hidden memory file 1622. Also, a  
15 coder 1634 is enabled. The coder 1634 receives the CPN as an input and also receives a revised RN as a key input. The output of coder 1634 is a new ROC, which is combined with the new TSN in mixer 1635. The mixer 1635 output is sent back to the terminal where the  
20 sorter 1604 separates the new TSN and ROC, which are then recorded on the user's card (in order to prepare for the next transaction by the user). Note also that a new CPK may be generated as well by revising a memory address component, such as the address displacement. In  
25 this event, the new CPK would also be returned to the terminal to be recorded on the user's card.

It should be noted that an unsecured communication link between the mixer 1614 and the sorter 1616 is utilized if the hidden memory file 1622  
30 is remote from the location where the party's PIN is entered (that is, the terminal). It should also be noted that the transaction sequence number (TSN), in conjunction with the ADVAN, serves to protect the authenticity of the transaction and the user's card  
35 against fraudulent duplication of the transaction

information (that is, by recording the output of the mixer 1614 and retransmitting it later to the sorter 1616).

A number of additional applications for the present invention will now be described.

The invention could be utilized in a pay telephone system in which calls could be made without the use of money. The call originator uses a telephone in the usual way to enter the telephone number of the party to be called (i.e., to the call recipient). The call originator also enters his own telephone number and PIN. The system then authenticates the identity of the originator as described above (by using, for example, the embodiment depicted in Figs. 6-8 or in Figs. 9-12). In the first embodiment (i.e., Figs. 6, 7, 8A and 8B), the originator's PIN is coded, and used to derive an arbitrary number, which is subsequently compared to another such number which is generated from a reconstituted version of the coded PIN. The reconstituted coded PIN is formed from an RN and ROC which are accessed from the originator's account file, with the originator's telephone number serving as a file index. If the comparison is unfavorable, the call is aborted; otherwise, call processing continues.

In the second embodiment, the originator's telephone number is used as an index to file no. 1 to access an originator's CPKO and true CNO. The originator's coded PIN, CPNO, is then combined with the originator's CPKO to generate a CNO (as in Fig. 12). The originator's identify is then authenticated by comparing the true CNO with the derived CNO. If the comparison is unfavorable, the call is aborted; otherwise, processing continues. The originator can use a machine readable card, or the like which has CPKO and CNO previously recorded thereon. In this event, access to file no. 1 is unnecessary.

In either embodiment, if the identity comparison is favorable, then the originator's credit balance is extracted from the originator's file to determine whether the call should be allowed. If the  
5 credit balance is favorable, then the telephone connection is extended to the call recipient, and the recipient's telephone is rung.

At the end of the call, the originator's credit balance is diminished by the cost of the call,  
10 and the new balance is computed and rewritten to the originator's file. The originator may then be advised of the cost of the call. When the recipient's telephone rings and the call is answered, the system can require that the identity of the person answering the phone be  
15 authenticated, as in a person to person call. In this event, the recipient is asked to enter a PIN, and the recipient's identity is authenticated using either of the two embodiments mentioned above.

Alternatively, a first joint code could be  
20 generated when the call is initiated, e.g., from the originator's CPN, and the recipient's reconstituted CPN. When the call is answered, the recipient enters his PIN, which is converted to a CPN and combined with the originator's reconstituted CPN to form a second joint  
25 code. A comparison then ensues between the first and second joint codes.

Another application of the invention is a system which uses a bill as the means of (or vehicle for) payment. The bill contains the usual payment  
30 information, and a VAN is also recorded on the bill when the bill is generated. The VAN is derived from the payment information (INFO) and identification information associated with the originator of the bill (e.g., similar to the bank identification line of  
35 information which appears at the bottom of an originator's check) or the originator's TIN and BIN.

146



The bill may also contain the recipient's TIN and BIN. Preferably, the above information is coded in a standard format, at a fixed location on the bill itself. The bill is then used in an appropriate document reader to  
5 provide the transaction payment information to the system. The party paying the bill (i.e., the payor) enters his PIN and the payor is then authenticated using the PIN. Also, the VAN is authenticated (using one of the methods described above). If the payor and the VAN  
10 are authentic, the bill is paid. A redemption VAN is generated (using information associated with the payee party) and printed on the bill, when it has been paid.

Alternatively, the payor could simply key in the information from the face of the bill. When the  
15 transaction is completed, a redemption VAN is displayed to the payor, which he records on the bill (or the VAN could be automatically recorded on the bill).

In accordance with a further application of the embodiments of this invention, a medical  
20 prescription form which has been originated and issued by a doctor to a patient (a recipient), can be authenticated to permit dispensing of the designated medicine, or drug, in a processing jurisdiction, along with automated payment. Automated payment may include a  
25 third party such as an insurance provider. This system is particularly useful for a patient who is in desperate need of medicine, and is in a remote or strange environment, where the prescription cannot be easily authenticated, or an available pharmacy cannot be found.

30 The prescription form contains identification information associated with the doctor and the patient, and the usual information which appears on a prescription, such as the type of medicine, strength, quantity, application, date, refills, generic, and a  
35 control number. The prescription form also contains a VAN, which is the result of coding the medical and

47

identification information. Preferably, the information and the VAN are recorded on the prescription form so that it is readable by an individual, and it also includes coded symbols or characters representing the  
5 same information in machine readable form.

When the prescription form is utilized by the recipient to obtain the medicine from a processing entity (such as a drug store), the information on the form is read automatically by a terminal of the system,  
10 or it is entered via a keyboard. The recipient also enters his PIN, and the system authenticates the prescription form, the doctor, and the recipient in accordance with the embodiments described previously. An indication of the cost of the prescribed medicine,  
15 and the method of payment is provided to the recipient. The recipient may elect to pay by using one of the methods described herein.

Note that the processing entity may also include a centralized clearinghouse in communication  
20 with dispensing outlets (i.e., drug stores) for authenticating prescriptions. An RVAN may be generated from the VAN and information associated with the processing entity, and then associated with the transaction, to thereby document the processing entity's  
25 involvement in the transaction.

If a patient attempts to use a prescription in a state where the originating physician is not licensed, such as out of state, the original prescription may not be usable. In this situation, a directory system of  
30 predetermined licensed "correspondent" physicians may be established, and a correspondent physician can automatically authorize the prescription of an originating physician (on-line), after the original prescription is authenticated.

LH

The invention also finds utility in a paperless/cashless transaction system, in which "funds transfer" transactions, such as purchases, occur without the use of money, or checks. In this system, the payment originator uses a payment recipient's terminal which stores information to identify the precise location of the recipient's account. Alternatively, an originator PIN, information identifying an originator account and a recipient account, and funds transfer information (INFO) which includes a payment amount are entered directly into a terminal of this system by the payment originator. The system initially generates a VAN, (OVAN), by using the payment information (INFO) in conjunction with the identification information associated with the payment originator and payment recipient. The payment originator is authenticated using the originator PIN using a method described above. The system then approves or disapproves the payment based upon an authentication of the VAN, and the "joint" identification information associated with the participants, and the availability of funds, or credit. Such transactions are carried on entirely electronically, the participant's bank accounts are credited and debited automatically, allowing commercial transactions to be completed "instantaneously". An RVAN may be generated using the INFO and printed on a receipt which is dispensed to the originator.

Although preferred embodiments of the invention have been disclosed for illustrative purposes, those skilled in the art will appreciate that many additions, modifications, and substitutions are possible without departing from the scope or spirit of the invention as defined in the accompanying claims.

67

I CLAIMS:

1. In a system comprising a storage means addressable using a predetermined address and party information associated with a party and stored in the storage means, the party information comprising first coded authentication information previously generated by using a personal identification number (PIN) associated with the party, a method for authenticating the party comprising the steps of:
  - receiving a PIN from the party to be authenticated;
  - addressing the storage means using the predetermined address to locate the party information and to retrieve the first coded authentication information;
  - generating second coded authentication information using the received PIN;
  - comparing at least part of the retrieved first coded authentication information to at least part of the generated second coded authentication information; and
  - authenticating the party if said at least part of the retrieved first coded authentication information corresponds to said at least part of the generated second coded authentication information.
2. The method of claim 1, wherein the predetermined address comprises non-secret information associated with the party, such that the location of the storage means and the first coded authentication information stored in the storage means are non-secret.
3. The method of claim 1, wherein the first coded authentication information is extracted from a storage means which is in the possession of the party.

4. The method of claim 1, wherein the location of the storage means is secret, and wherein the step of addressing the storage means comprises the steps of:

- 5                   accessing a second storage means using a second predetermined address to locate and to retrieve a coded address previously stored in the second storage means, the coded address having been previously generated by coding the first predetermined address of  
10 the first storage means using the PIN;  
                  uncoding the coded address using the received PIN to generate the first predetermined address; and  
                  accessing the first storage means using  
15 the generated first predetermined address to retrieve the first coded authentication information.

5. The method of claim 4, wherein the first storage means is a part of a memory and wherein, prior to use of the memory, pseudo information is stored in  
20 the memory, thereby making unused portions of the memory indistinguishable from the first storage means.

6. The method of claim 4, wherein the party information also comprises secret information associated with the party.

25               7. In a transaction system, a method for authenticating a transaction and at least one party to the transaction comprising the steps of:

- coding information relevant to a transaction with information associated with at least  
30 one party to generate a variable authentication number (VAN), wherein the information associated with said at least one party comprises coded authentication information derivable from a predetermined secret code and a predetermined non-secret code, and wherein the  
35 coded authentication information was previously

generated by coding a personal identification number (PIN), the PIN being unrecoverable within the transaction system;

5 associating the VAN with the transaction;  
deriving the coded authentication  
information using the predetermined secret and non-secret codes; and  
10 authenticating the VAN associated with the transaction using the derived coded authentication information.

8. The method of claim 7, wherein the information relevant to the transaction comprises at least one information group which is coded so as to enable detection of a change in its content or  
15 structure.

9. The method of claim 7, wherein the transaction involves an electrical signal, the VAN being included in the electrical signal together with at least a portion of the information relevant to the  
20 transaction.

10. The method of claim 7, wherein the transaction includes originating an instrument and wherein the step of associating the VAN with the transaction comprises the step of recording the VAN and  
25 at least a portion of the information relevant to the transaction on the instrument.

11. The method of claim 10, wherein the information relevant to the transaction comprises a combination of predetermined information recorded on the  
30 instrument and predetermined information not recorded on the instrument, such that prevention of fraudulent regeneration of the VAN is enhanced.

12. The method of claim 7, wherein the step of authenticating the VAN comprises the steps of:  
35 uncoding the VAN using at least the derived coded authentication information;

comparing the uncoded VAN to the  
information relevant to the transaction; and  
authenticating the VAN and the  
transaction associated with the VAN if the uncoded VAN  
5 corresponds to the information relevant to the  
transaction.

13. The method of claim 7, wherein the step  
of authenticating the VAN comprises the steps of:  
coding the information relevant to the  
10 transaction using at least the derived coded  
authentication information to generate a second VAN;  
comparing the first VAN associated with  
the transaction to the second VAN; and  
authenticating the first VAN and the  
15 transaction associated with the first VAN if the first  
VAN corresponds to the second VAN.

14. The method of claim 7, wherein the  
transaction comprises originating and processing a  
medical prescription form and said at least one party  
20 comprises an originating physician and a patient  
presenting the medical prescription form for processing  
in a processing jurisdiction, the coded authentication  
information being associated with the originating  
physician and with the patient, and wherein the step of  
25 associating the VAN with the transaction comprises the  
step of recording the VAN on the medical prescription  
form.

15. The method of claim 14, further  
comprising the steps of:  
30 authenticating the patient; and  
dispensing medicine as indicated on the  
medical prescription form to the patient if the VAN and  
the patient are authenticated.

16. The method of claim 15, wherein the VAN is authenticated by a processing entity associated with the processing jurisdiction, further comprising the steps of:

5 if the originating physician is not licensed to practice in the processing jurisdiction, then obtaining authorization for processing the medical prescription form in the processing jurisdiction from a correspondent physician licensed in the processing  
10 jurisdiction;

generating a redemption VAN from the VAN and information associated with the processing entity; and

15 associating the redemption VAN with the medical prescription form, such that the processing entity is accountable for the processing of the medical prescription form.

17. In a multi-party transaction system, a method for authenticating a transaction and parties to  
20 the transaction comprising the steps of:

coding information relevant to a transaction with at least information associated with at least two parties to generate a variable authentication number (VAN); and

25 associating the VAN with the transaction.

18. The method of claim 17, wherein at least one of the parties is present, and wherein at least one of the parties is absent.

19. The method of claim 17, wherein the  
30 coding step comprises the steps of:

coding the information associated with said at least two parties to generate a joint code; and coding the information relevant to the transaction with the joint code to generate the VAN.



20. In a system wherein a party has a personal identification number from which first coded authentication information is generated, the first coded authentication information being derivable from a  
5 predetermined secret number and a predetermined non-secret number which have been previously stored in a storage means, a method for authenticating the party comprising the steps of:  
receiving at a first site a personal  
10 identification number from the party;  
generating second coded authentication information by using the received personal identification number;  
transmitting at least the second coded  
15 authentication information from the first site to a second site;  
retrieving at the second site the secret and non-secret numbers from the storage means;  
generating at the second site third coded  
20 authentication information by using the retrieved secret and non-secret numbers;  
comparing at the second site the second coded authentication information and the third coded authentication information; and  
25 authenticating the party if the second coded authentication information corresponds to the third coded authentication information.

21. The method of claim 20, wherein the transmitting step comprises the step of transmitting the  
30 second coded authentication information from the first site to the second site over a secured communication medium, and wherein the step of generating the third coded authentication information comprises the step of deriving the first coded authentication information from  
35 the retrieved secret and non-secret numbers.

22. The method of claim 20, wherein the step of generating the second coded authentication information comprises the steps of coding the received personal identification number to generate a coded personal identification number and coding an arbitrary number using the coded personal identification number to generate a first coded arbitrary number.

23. The method of claim 22, further comprising the step of generating at the first site an anti-duplication variable authentication number (ADVAN) by coding at least a transmission date and time with the first coded authentication information, wherein the transmitting step comprises the step of transmitting the ADVAN, the first coded arbitrary number and the arbitrary number from the first site to the second site over an unsecured communication medium.

24. The method of claim 23, further comprising the steps of:

deriving at the second site the first coded authentication information from the retrieved secret and non-secret numbers;

uncoding the ADVAN at the second site using the derived first coded authentication information to regenerate the transmission date and time; and

further authenticating the party if the regenerated transmission date and time correspond to a reception date and time.

25. The method of claim 22, wherein the arbitrary number is generated at both the first site and the second site, and wherein the transmitting step comprises the step of transmitting the first coded arbitrary number from the first site to the second site over an unsecured communication medium.

26. The method of claim 25, wherein the step of generating the third coded authentication information comprises the steps of deriving the first coded

authentication information from the retrieved secret and non-secret numbers and coding the arbitrary number generated at the second site using the derived first coded authentication information to generate a second coded arbitrary number.

27. The method of claim 26, wherein the comparing step comprises the step of comparing at the second site the first coded arbitrary number transmitted from the first site to the second site and the second coded arbitrary number, and wherein the authentication step comprises the step of authenticating the party if the first coded arbitrary number corresponds to the second coded arbitrary number.

28. In a transaction system, a method for enrolling a party, wherein the party is authenticated during at least one stage of a subsequent transaction, the method comprising the steps of:

receiving a personal identification number (PIN) from the party;  
coding the PIN to produce a coded PIN (CPN);  
coding the CPN using a predetermined arbitrary number to produce a revisable owner code (ROC); and  
storing the predetermined arbitrary number and the ROC in a storage means at a location associated with the party, wherein the CPN is derivable from the predetermined arbitrary number and the ROC.

29. The method of claim 28, further comprising the step of modifying the predetermined arbitrary number and the ROC such that the CPN remains derivable from the revised arbitrary number and the revised ROC, thereby further preventing unauthorized derivation of the CPN.

30. In a transaction system wherein a party has a first personal identification number (PIN) and an official has a second PIN, a method for enrolling the party comprising the steps of:

5 coding information associated with the party with information associated with the official to generate a joint code, the joint code being subsequently associable with a transaction; and

10 storing the joint code in a first storage means, the first storage means being accessible only to a party with knowledge of the first PIN, such that if no party exists with knowledge of the first PIN, the joint code cannot be accessed from the first storage means and, therefore, cannot be associated with a transaction.

15 31. The method of claim 30, further comprising the steps of:

coding information relevant to the transaction with the joint code to generate a variable authentication number (VAN);

20 recording the VAN on a credential associated with the transaction; and issuing the credential.

32. The method of claim 30, further comprising the steps of:

25 storing the joint code in a second storage means, the second storage means being accessible only to a party having knowledge of the second PIN; receiving the second PIN from the official;

30 using the received second PIN to access the second storage means and to retrieve the joint code;

coding information relevant to the transaction with the joint code to generate a variable authentication number (VAN);

recording the VAN on a credential  
associated with the transaction; and

issuing the credential, wherein a party  
without knowledge of the second PIN cannot access the  
5 second storage means or the joint code stored therein  
and, therefore, cannot legitimately issue the  
credential.

33. In a multi-party transaction system, a  
method for processing transactions comprising the steps  
10 of:

coding information relevant to a  
transaction with information associated with at least  
one party to generate a variable authentication number  
(VAN);

15 associating the VAN with the transaction;  
determining whether a recipient party and  
the transaction are authentic; and  
if the recipient party and the  
transaction are authentic, then authorizing the  
20 transaction.

34. The method of claim 33, further comprising  
the steps of:

coding information associated with at  
least one party with the VAN to generate a redemption  
25 VAN (RVAN);

associating the RVAN with the  
transaction, such that the transaction cannot be  
fraudulently presented for further redemption; and  
storing the RVAN in a storage means  
30 associated with at least one party, such that the  
transaction is cleared in a substantially instantaneous  
manner.

35. The method of claim 34, wherein the  
transaction involves an electrical signal, the RVAN  
35 being included in the electrical signal.

36. A method for enrolling and authenticating a party, comprising the steps of:

receiving a personal identification number (PIN) from the party;

5 generating coded authentication information using the received PIN;

generating first and second numbers such that the coded authentication information is derivable from the first and second numbers, the first number  
10 being secret and the second number being non-secret;

storing information comprising the secret number in a first storage means addressable using a predetermined secret address;

generating a coded secret address using  
15 at least part of the predetermined secret address and the received PIN; and

storing the coded secret address and the non-secret number in a second storage means addressable using a predetermined non-secret address.

20 37. The method of claim 36, wherein the step of storing the information comprising the secret number in the first storage means comprises the steps of:

coding the information comprising the secret number using non-secret information associated  
25 with the party to generate coded information; and  
storing the coded information in the first storage means.

38. The method of claim 37, wherein the non-secret information associated with the party is the  
30 coded secret address.

39. The method of claim 36, further comprising the steps of:

receiving a second PIN from a party to be authenticated;

generating at a first site second coded authentication information using the received second PIN;

5       addressing the second storage means using the predetermined non-secret address to locate and retrieve the coded secret address and the non-secret number;

10       generating at the first site a first coded number using the second coded authentication information and the coded secret address;

      generating the predetermined secret address using at least the received second PIN and the retrieved coded secret address;

15       transmitting at least the first coded number and the predetermined secret address from the first site to a second site;

      addressing the first storage means using the generated predetermined secret address to locate and retrieve the secret number;

20       deriving at the second site the first coded authentication information using the retrieved non-secret number and the retrieved secret number;

      generating at the second site a second coded number using the derived first coded authentication information and the coded secret address;  
25       and

      authenticating the party to be authenticated if the first coded number corresponds to the second coded number.

30       40. The method of claim 39, further comprising the step of generating at the first site an anti-duplication variable authentication number (ADVAN) by coding at least a transmission date and time with the second coded authentication information, the  
35       transmitting step comprising the step of transmitting

the first coded number, the predetermined secret address, and the ADVAN from the first site to the second site via an unsecured communication medium.

41. The method of claim 40, further comprising  
5 the steps of:

uncoding the ADVAN at the second site  
using the derived first coded authentication information  
to regenerate the transmission date and time; and  
further authenticating the party to be  
10 authenticated if the regenerated transmission date and  
time correspond to a reception date and time.

42. The method of claim 39, wherein a first  
semi-random number is generated at the first site using  
a first counter, and further comprising the step of  
15 coding the first semi-random number to generate a coded  
first semi-random number, and wherein the transmitting  
step comprises transmitting the first coded number, the  
predetermined secret address, and the coded first semi-  
random number from the first site to the second site via  
20 an unsecured communication medium.

43. The method of claim 42, further comprising  
the steps of:

uncoding the coded first semi-random  
number at the second site to regenerate the first semi-  
25 random number;

generating at the second site a second  
semi-random number using a second counter which is  
generally synchronized with the first counter; and  
further authenticating the party to be  
30 authenticated if the regenerated first semi-random  
number corresponds to the second semi-random number.

44. The method of claim 39, wherein the  
predetermined secret address comprises one or more  
components combinable to form the predetermined secret  
35 address, the step of generating the coded secret address



comprising the step of coding one of the components of the predetermined secret address using the received first PIN to generate the coded secret address.

45. The method of claim 44, wherein the step  
5 of generating the predetermined secret address comprises the steps of:

uncoding the retrieved coded secret address using the received second PIN to generate said one of the components of the predetermined secret  
10 address; and

generating the predetermined secret address by combining the generated said one of the components with the other components of the predetermined secret address.

46. A method for automatically and  
15 instantaneously transferring funds from an account associated with an originator party to an account associated with a recipient party, the method comprising the steps of:

20 receiving from the originator party a personal identification number (PIN) associated with the originator party, information identifying the originator party account and the recipient party account, and information comprising a payment amount and specifying a  
25 funds transfer;

generating a variable authentication number (VAN) using the originator party PIN, the recipient party account identifying information, and the fund transfer information;

30 determining whether the originator party is authentic by using the PIN;

determining whether the funds transfer is authentic by using the VAN;

if the originator party and the funds transfer are authentic, then transferring authenticated funds to the recipient party account from the originator party account;

- 5           generating a redemption variable authentication number (RVAN) using at least the funds transfer information; and  
            associating the RVAN with the fund transfer, such that the funds transfer is substantiated  
10 by the RVAN.

47. The method of claim 46, wherein the step of associating the RVAN with the funds transfer comprises the step of recording the RVAN on a receipt, the receipt being dispensed to the originator party.

- 15           48. A method for processing an invoice comprising the steps of:  
            generating a variable authentication number (VAN) using at least information associated with an invoice, the information associated with the invoice  
20 including information identifying a payee party account and payment information comprising a payment amount;  
            recording the VAN and the information associated with the invoice on the invoice;  
            receiving the VAN and a personal  
25 identification number (PIN) from a payor party;  
            determining whether the payor party and the VAN are authentic by using the information associated with the invoice and the received PIN;  
            receiving the payee party account  
30 identifying information and the payment information from the invoice; and  
            if the payor party and the VAN are authentic, then crediting the payment amount to the payee party account from funds associated with the payor  
35 party.

49. The method of claim 48, further comprising the steps of:

generating a redemption VAN (RVAN) by coding the VAN with at least information associated with the payee party; and

associating the RVAN with the invoice such that payment of the invoice is substantiated by the RVAN.

50. The method of claim 49, wherein the step of receiving the VAN comprises the steps of:

receiving the invoice from the payor party; and

reading the VAN from the received invoice.

51. A method for authenticating a party and for authorizing access to a storage means associated with the party, the storage means being addressable using a secret predetermined address, the method comprising the steps of:

receiving a personal identification number (PIN) from a party to be authenticated;

generating coded authentication information using the PIN, the coded authentication information being derivable from a secret number

previously stored in the storage means and a non-secret number previously stored in a storage medium in possession of the party;

retrieving from the storage medium, at least a coded address and the non-secret number, the coded address having been previously generated by coding at least a portion of the secret predetermined address using the coded authentication information;

generating said at least a portion of the secret predetermined address by uncoding the coded address using the coded authentication information;

transmitting at least the generated said  
at least a portion of the secret predetermined address  
and the retrieved non-secret number from a first site to  
a second site over a communication link;

5 generating at the second site the secret  
predetermined address using the transmitted said at  
least a portion of the secret predetermined address;  
addressing the storage means using the  
generated secret predetermined address to retrieve the  
10 secret number;

deriving the coded authentication  
information using the retrieved secret number and the  
transmitted non-secret number; and

15 authenticating the party and authorizing  
further access to the storage means by using at least  
the derived coded authentication information.

52. The method of claim 51, further  
comprising the steps of:

20 retrieving from the storage medium a  
first transaction sequence number (TSN) previously  
stored therein;

generating a first anti-duplication  
variable authentication number (ADVAN) by coding the  
first TSN with the coded authentication information;  
25 transmitting the first ADVAN from the  
first site to the second site over the communication  
link;

addressing the storage means using the  
generated secret predetermined address to retrieve a  
30 second TSN previously stored therein;

generating a second ADVAN by coding the  
second TSN with the derived coded authentication  
information; and

35 authenticating the party and authorizing  
further access to the storage means if the second ADVAN  
corresponds to the first ADVAN;

wherein the first and second TSNs are modified after each transaction, such that fraudulent receipt and use of messages over the communication link and fraudulent duplication of the storage medium are prevented.

53. The method of claim 51, further comprising the steps of retrieving agency identification information from the storage medium and transmitting the agency identification information from the first site to the second site over the communication link, wherein the step of generating at the second site the secret predetermined address comprises the steps of using the agency identification information to retrieve other portions of the secret predetermined address and combining the transmitted said at least a portion of the secret predetermined address with the other portions to form the secret predetermined address.

54. The method of claim 51, further comprising the step of revising the TSN, the secret number, and/or the coded address.

55. The method of claim 51, wherein the communication link is unsecured.

56. A multi-party transaction system for authenticating a transaction and parties to the transaction comprising:

means for coding information relevant to a transaction with at least information associated with at least two parties to generate a variable authentication number (VAN); and

means for associating the VAN with the transaction.

57. A transaction system for enrolling a party wherein the enrolled party is authenticated during at least one stage of a subsequent transaction, the system comprising:

means for receiving a personal  
identification number (PIN) from the party;

means for coding the PIN to produce a  
coded PIN (CPN);

5 means for coding the CPN using a  
predetermined arbitrary number to produce a revisable  
owner code (ROC); and

means for storing the predetermined  
arbitrary number and the ROC in a storage means at a  
10 location associated with the party, wherein the CPN is  
derivable from the predetermined arbitrary number and  
the ROC.

58. A transaction system for enrolling a  
party, wherein the party has a first personal  
15 identification number (PIN) and an official has a second  
PIN, the system comprising:

means for coding information associated  
with the party with information associated with the  
official to generate a joint code, the joint code being  
20 subsequently associable with a transaction;

a storage means being accessible only to  
a party with knowledge of the first PIN; and

means for storing the joint code in the  
storage means, such that if no party exists with  
25 knowledge of the first PIN, the joint code cannot be  
accessed from the storage means and, therefore, cannot  
be associated with a transaction.

59. A multi-party transaction system for  
processing transactions comprising:

30 means for coding information relevant to  
a transaction with information associated with at least  
one party to generate a variable authentication number  
(VAN);

means for associating the VAN with the  
35 transaction;

means for determining whether a recipient party and the transaction are authentic; and

means for authorizing redemption of the transaction if the recipient party and the transaction are authentic.

60. A system for authenticating a party comprising:

means for receiving a personal identification number (PIN) from the party;

means for generating coded authentication information using the received PIN;

means for generating first and second numbers such that the coded authentication information is derivable from the first and second numbers, the first number being secret and the second number being non-secret;

means for storing the secret number in a first storage means addressable using a predetermined secret address;

means for generating a coded secret address using at least a part of the predetermined secret address and the received PIN; and

means for storing the coded secret address and the non-secret number in a second storage means addressable using a predetermined non-secret address.

61. The system of claim 60, wherein the second storage means is a storage medium in the possession of the party.

62. In a system comprising a storage means addressable using a secret predetermined address and a first coded number previously stored in the storage means and derivable from the secret predetermined address and a coded address generated by coding the secret predetermined address with first coded.

authentication information associated with a party to be authenticated, a method for authenticating the party comprising the steps of:

- receiving a PIN from the party to be authenticated;
- generating second coded authentication information using the received PIN;
- deriving the secret predetermined address by uncoding the coded address using the second coded authentication information;
- generating a second coded number by coding the derived secret predetermined address with the coded address;
- using the derived secret predetermined address to access the storage means and retrieve the first coded number; and
- authenticating the party if the retrieved first coded number corresponds to the generated second coded number.

63. In a system comprising a credential and party information associated with a party and recorded on the credential, the party information comprising first coded authentication information previously generated by using a personal identification number (PIN) associated with the party, a method for authenticating the party comprising the steps of:
- receiving a PIN from the party to be authenticated;
  - retrieving the first coded authentication information from the credential;
  - generating second coded authentication information using the received PIN;
  - comparing at least part of the retrieved first coded authentication information to at least part of the generated second coded authentication information; and



~~authenticating the party if said at least part of the retrieved first coded authentication information corresponds to said at least part of the generated second coded authentication information.~~

old  
B27

Attorney Docket No. 6074-1

**DECLARATION AND POWER OF ATTORNEY**  
(Original Application)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled  
SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN

the specification of which (check one)

☒ is attached hereto.

☐ was filed on \_\_\_\_\_  
as Application Serial No. \_\_\_\_\_

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to herein.

I acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119, of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

FOREIGN PRIORITY APPLICATION(S)

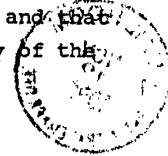
			<u>Priority Claimed</u>
<u>N/A</u>			[ ] Yes [ ] No
(Number)	(Country)	(Day/month/ year filed)	
			[ ] Yes [ ] No
(Number)	(Country)	(Day/month year filed)	

And I hereby appoint Ronald L. Panitch, Registration No. 22,825; William W. Schwarze, Registration No. 25,918; Alan S. Nadal, Registration No. 27,363; Leslie L. Kasten, Jr., Registration No. 28,959; Joel S. Goldhammer, Registration No. 22,130; Wallace D. Newcomb, Registration No. 14,823; John Jamieson, Jr., Registration No. 29,546; Martin G. Belisario, Registration No. 32,886; Kirk Baumeister, Registration No. 33,833; Michele L. Simons, Registration No. 34,962, a Patent Agent; and Michael Q. Lee, Registration No. 35,239, a Patent Agent; as my attorneys or agents with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Address all correspondence to PANITCH SCHWARZE JACOBS & NADEL, 1601 Market Street, 36th Floor, Philadelphia, Pennsylvania 19103. Please direct all communications and telephone calls to Michael Q. Lee at 215-567-2020.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made 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 so made are punishable by fine or imprisonment, or both,

under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.



Full name of sole or first inventor 1-00 Leon Stambler  
Inventor's Signature Leon Stambler  
Date 11/16/92  
Residence Parkland, Florida JS 11/16/92  
Citizenship U.S.A.  
Post Office Address 7803 Boulder Lane  
Parkland, Florida 33067 JS 11/16/92

Full name of second joint inventor, if any \_\_\_\_\_  
Inventor's Signature \_\_\_\_\_  
Date \_\_\_\_\_  
Residence \_\_\_\_\_  
Citizenship \_\_\_\_\_  
Post Office Address \_\_\_\_\_

Full name of third joint inventor, if any \_\_\_\_\_  
Inventor's Signature \_\_\_\_\_  
Date \_\_\_\_\_  
Residence \_\_\_\_\_  
Citizenship \_\_\_\_\_  
Post Office Address \_\_\_\_\_

08/747,174

FIG. 1

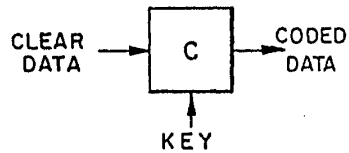


FIG. 2

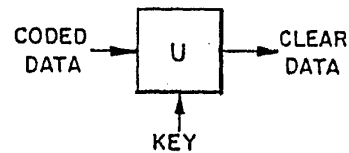


FIG. 3

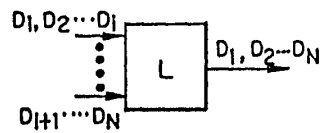


FIG. 4

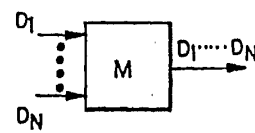


FIG. 5

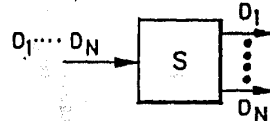
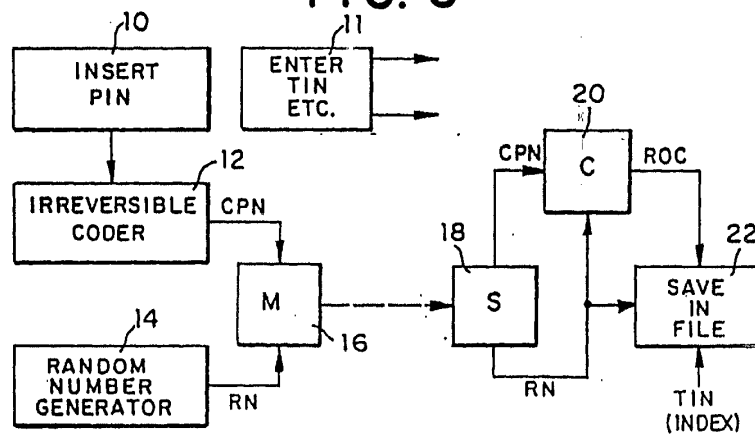
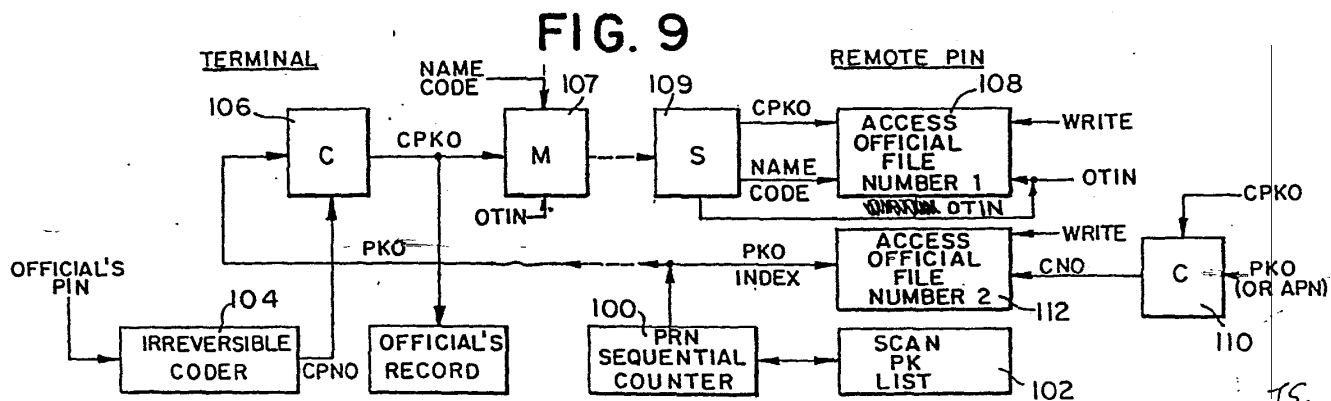
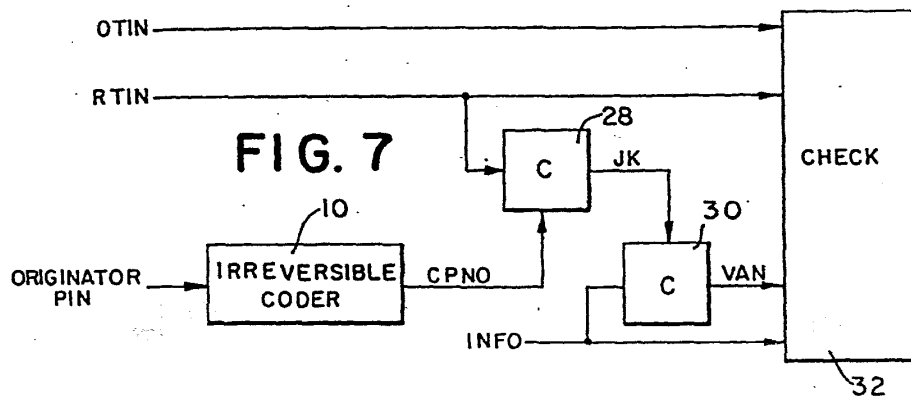


FIG. 6





JS.  
11/1/62

FIG. 8A

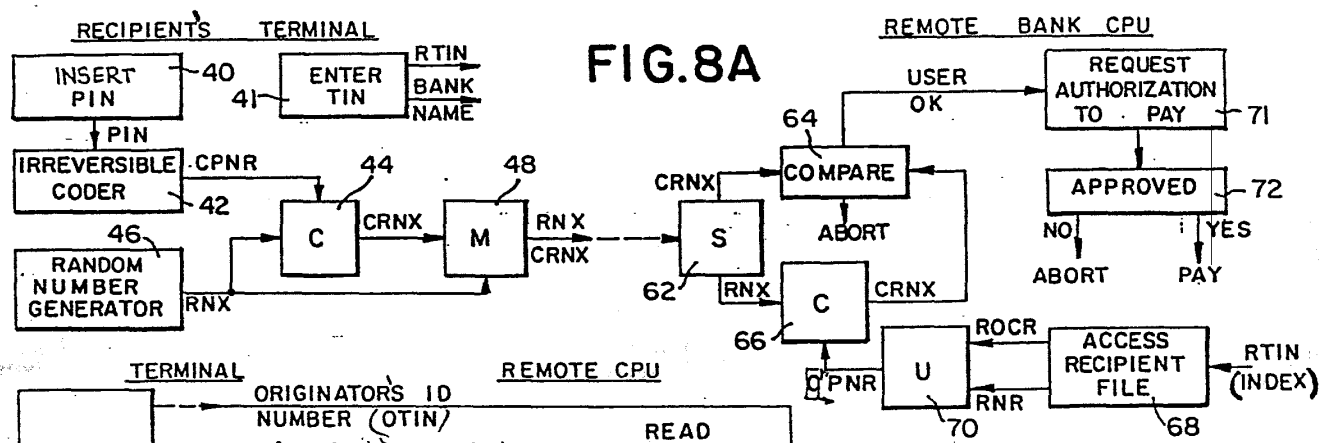
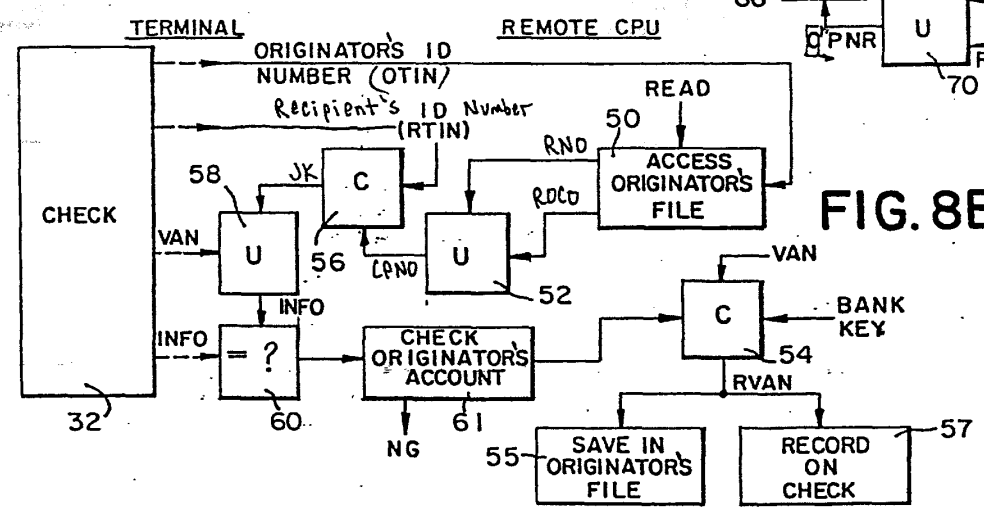


FIG. 8B



*Handwritten initials*

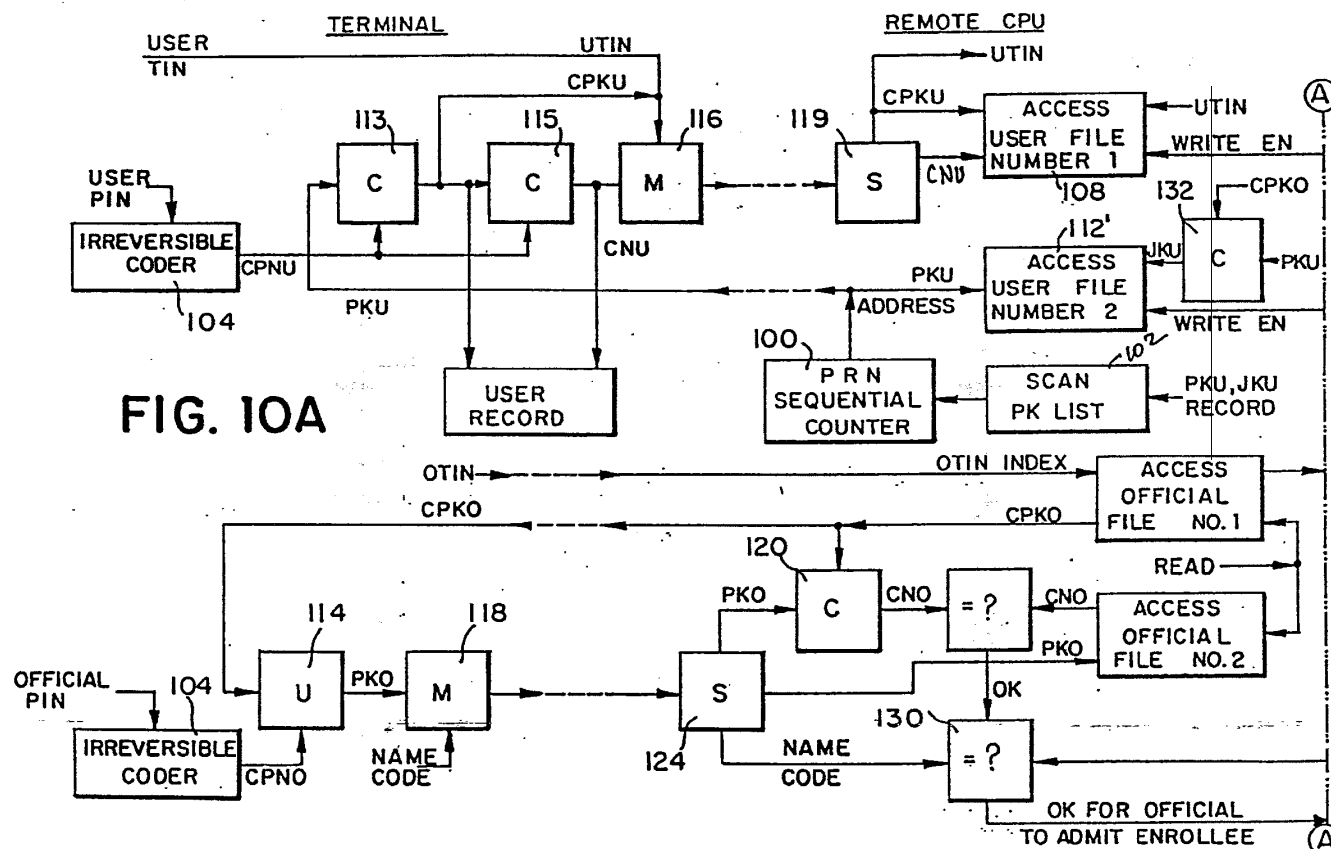
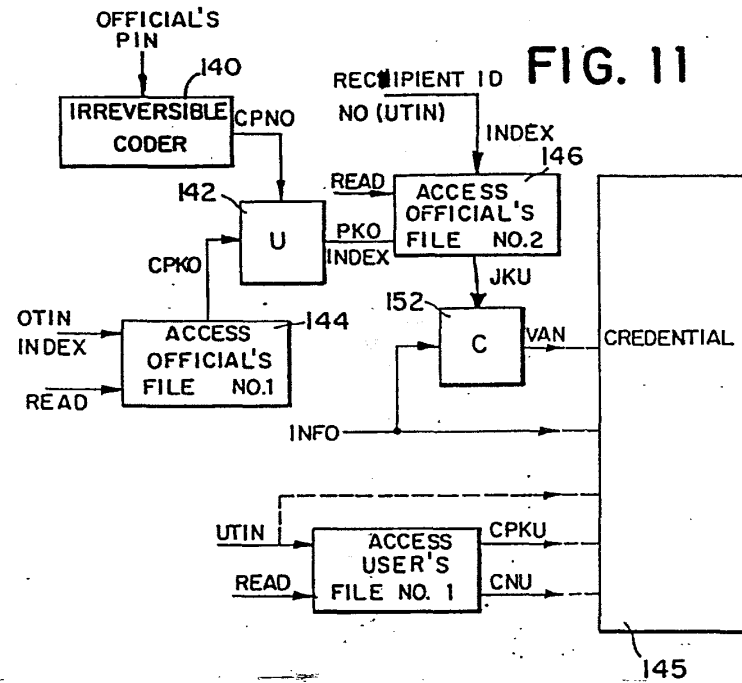
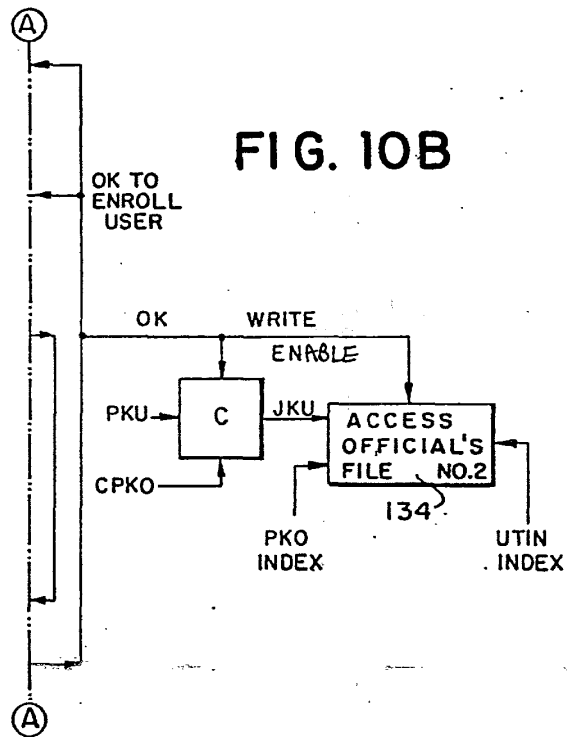


FIG. 10A

JS.  
11/16/82





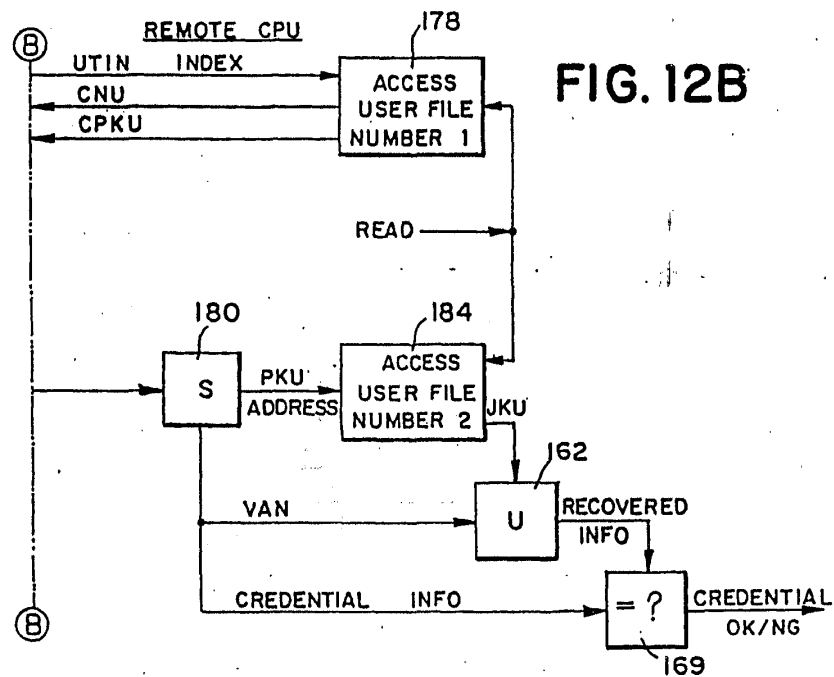
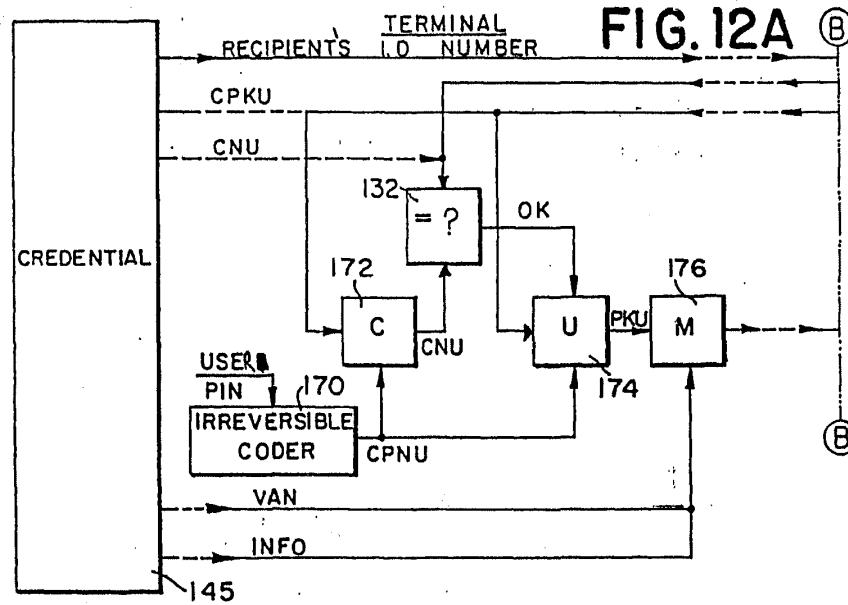
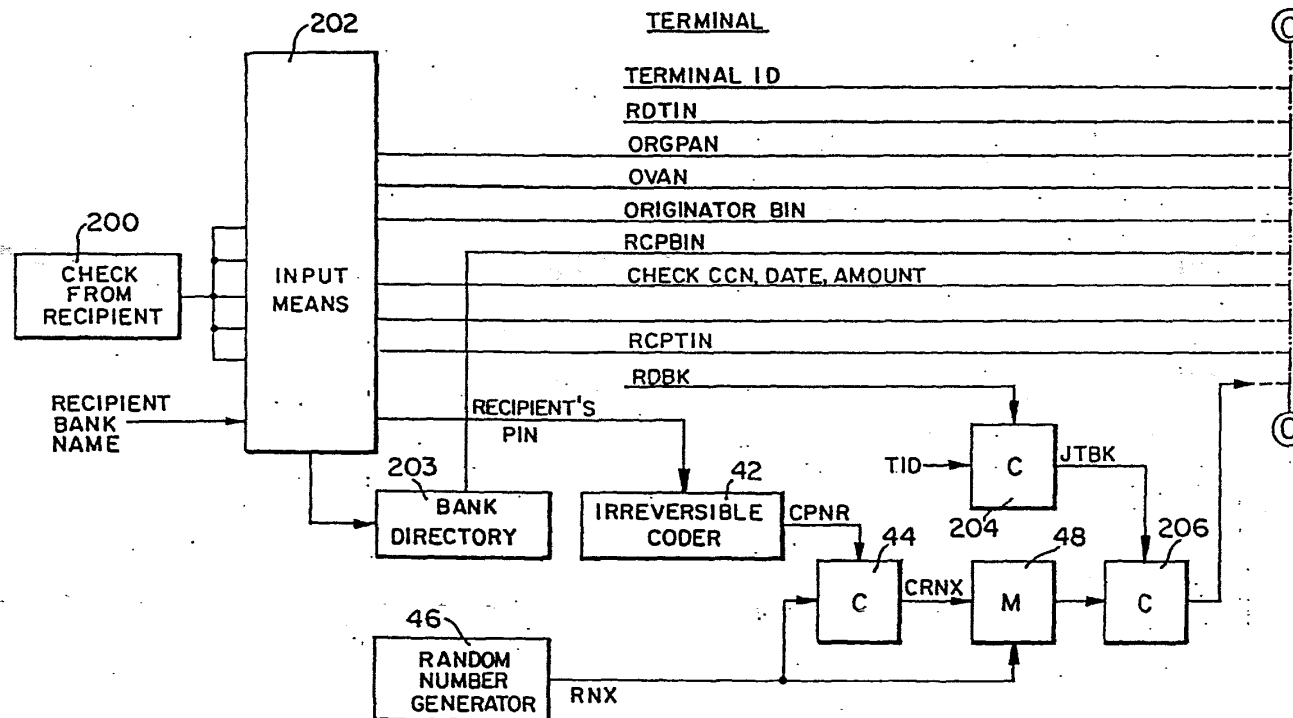


FIG. 13A



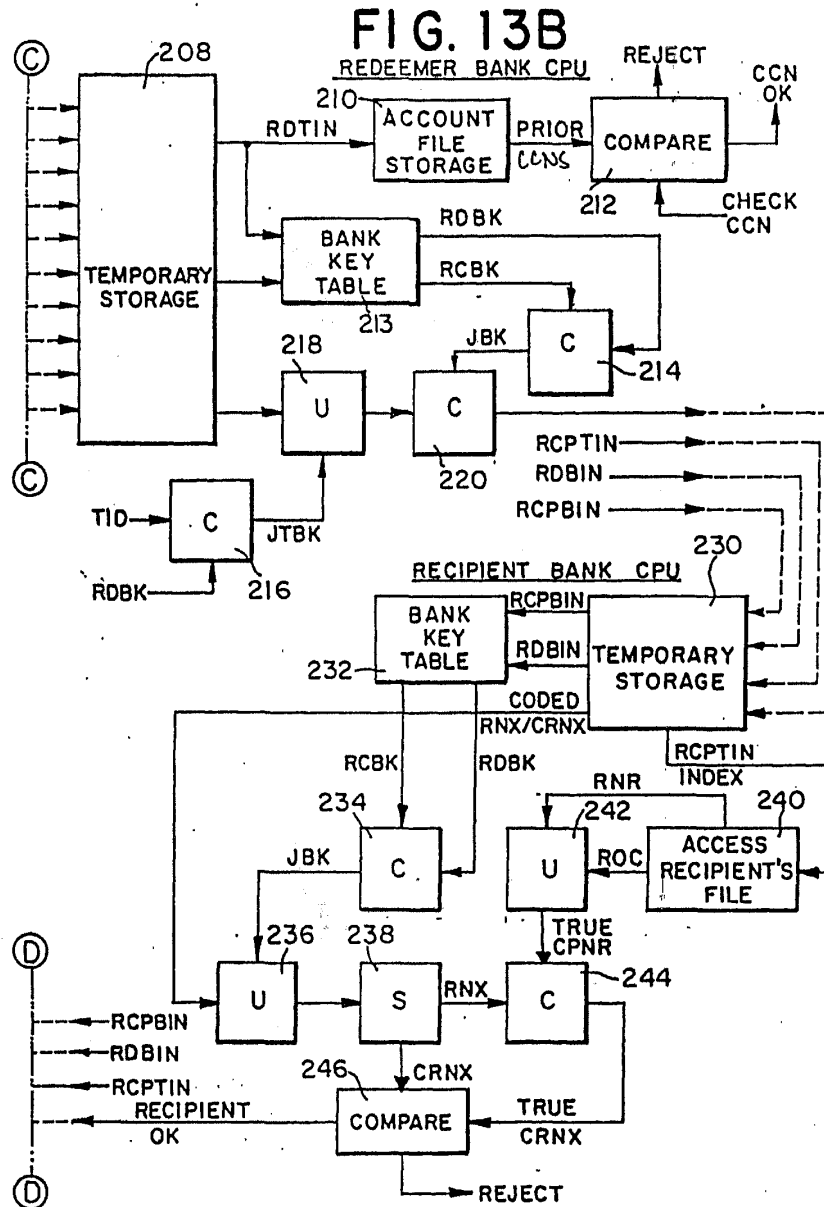


FIG. 13C

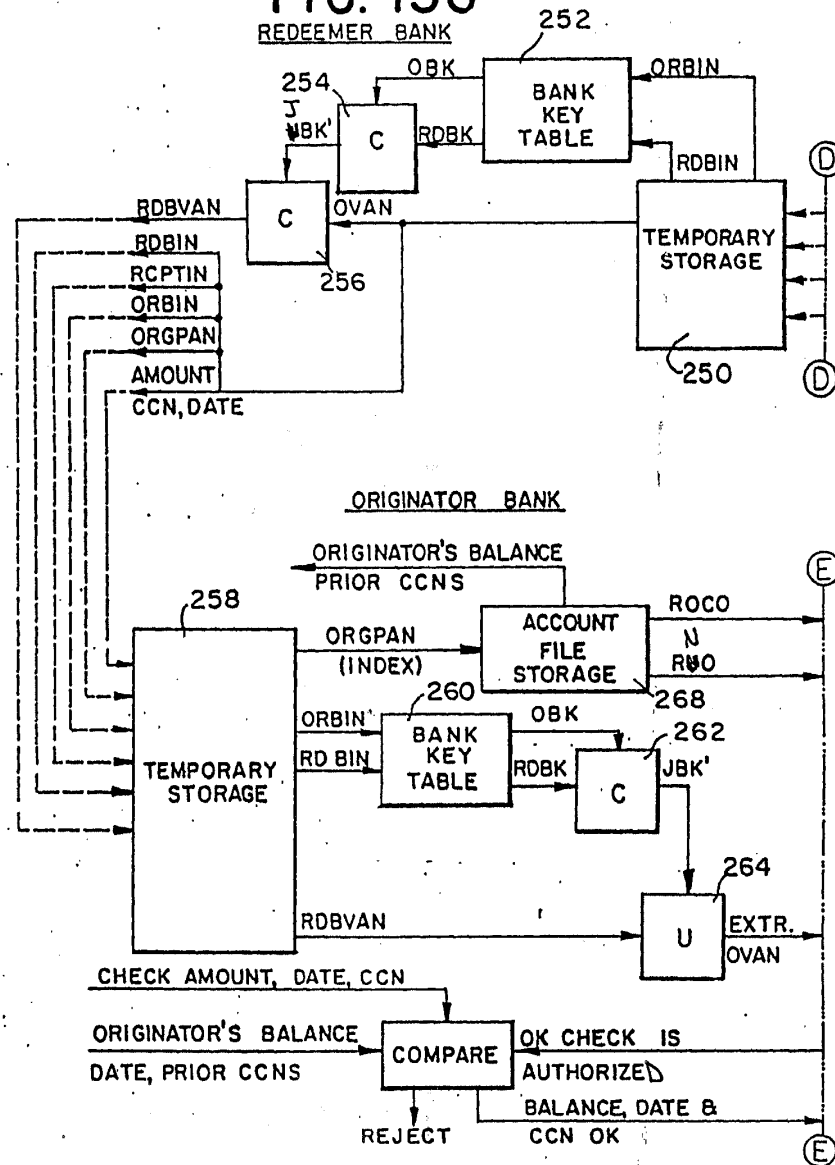
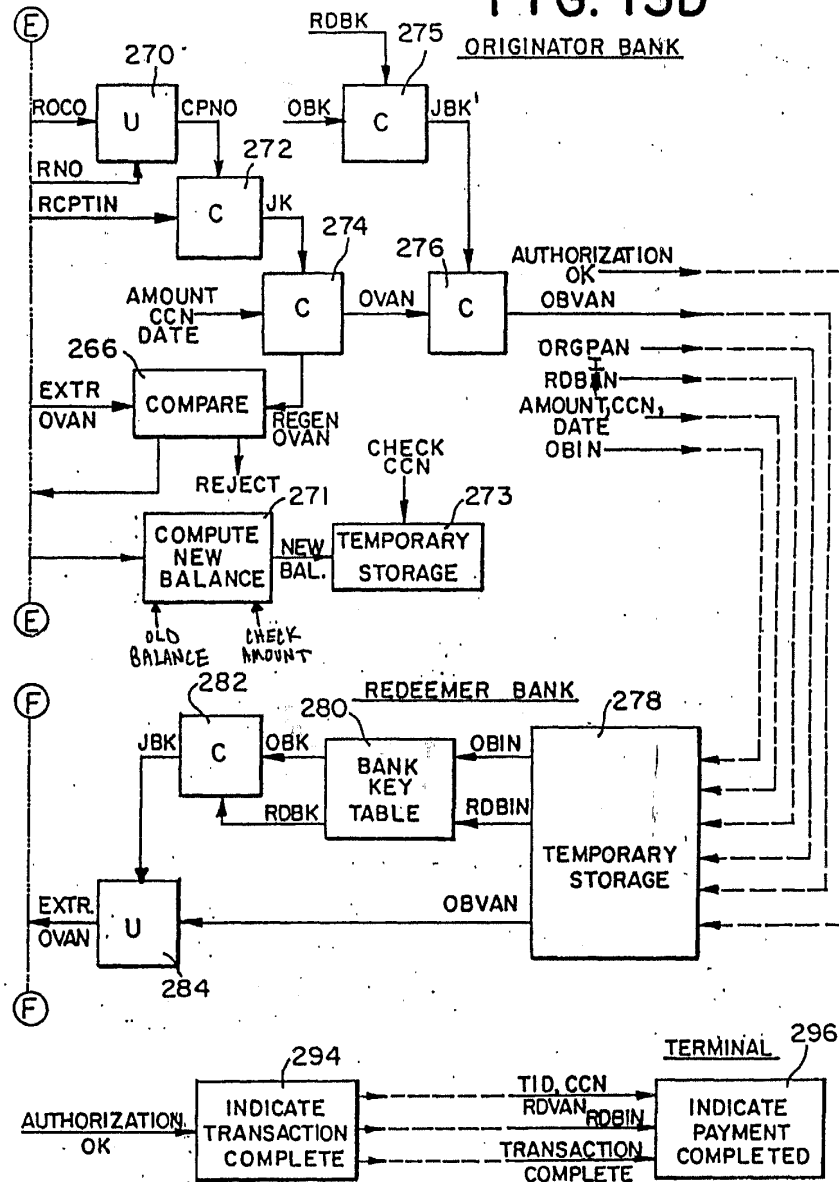
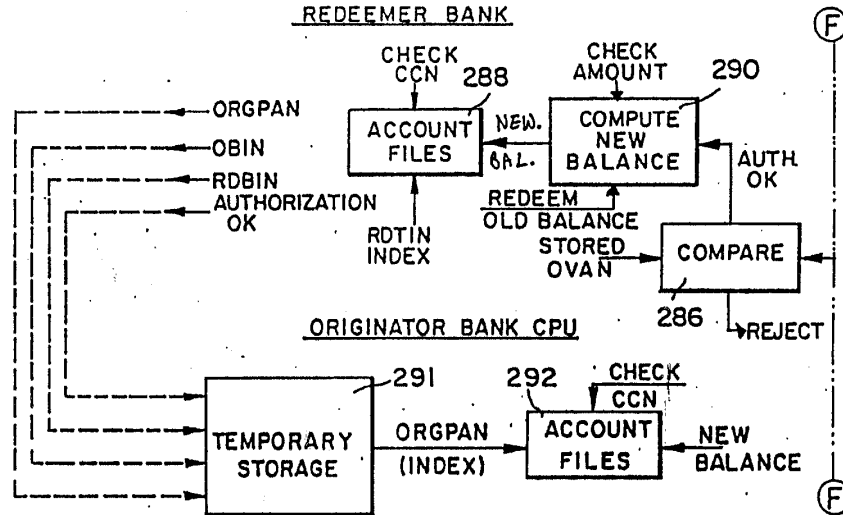


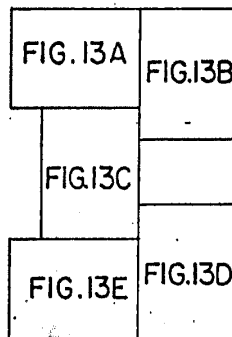
FIG. 13D

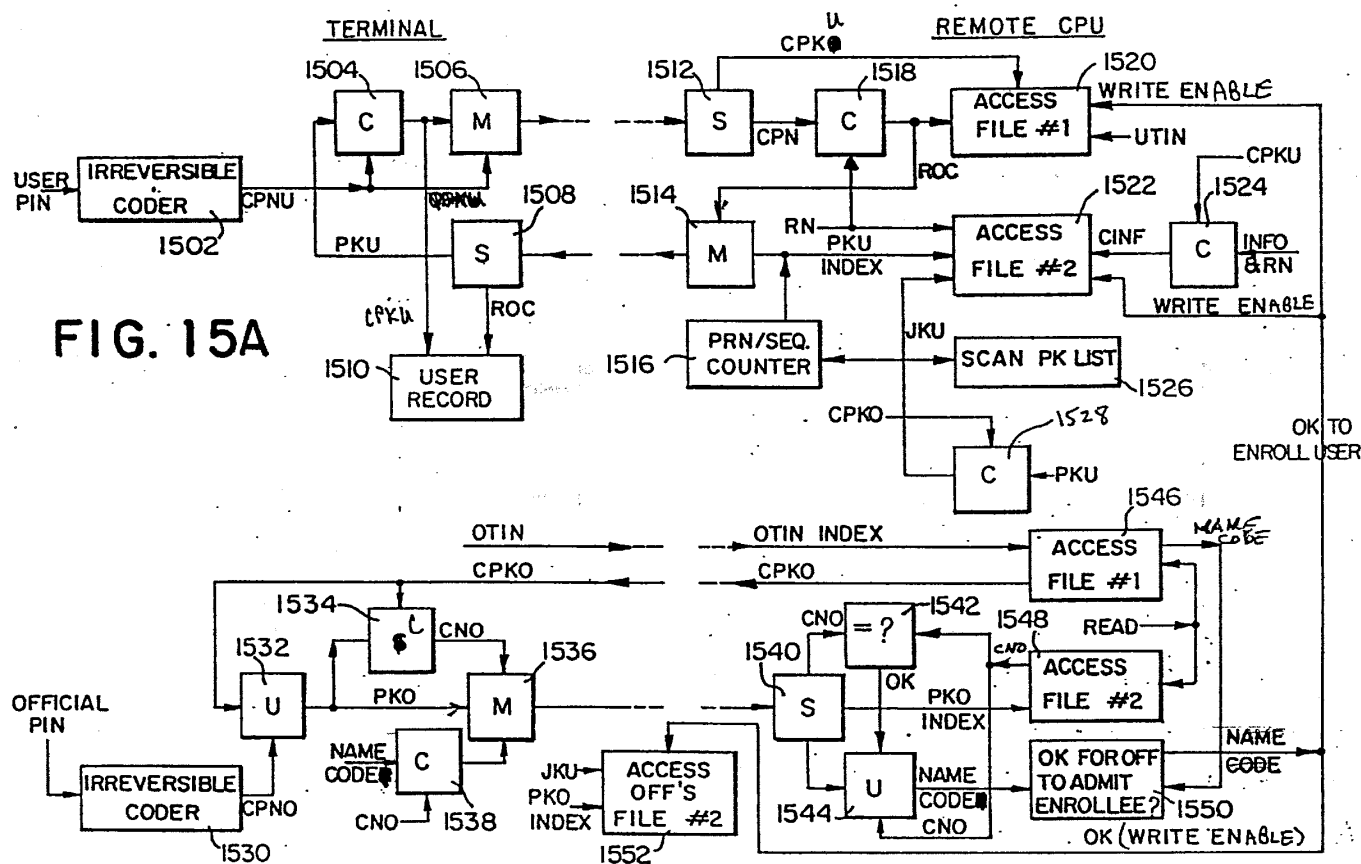


**FIG. 13E**



**FIG. 14**





JS  
11/16/82



CREDENTIAL ISSUE PROCESSING AGENCY TERMINAL / COMPUTER

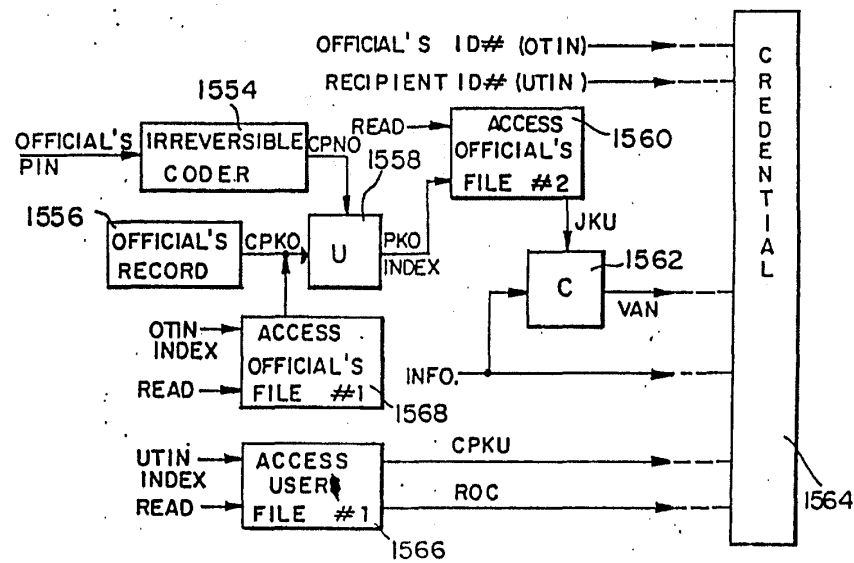


FIG. 15B

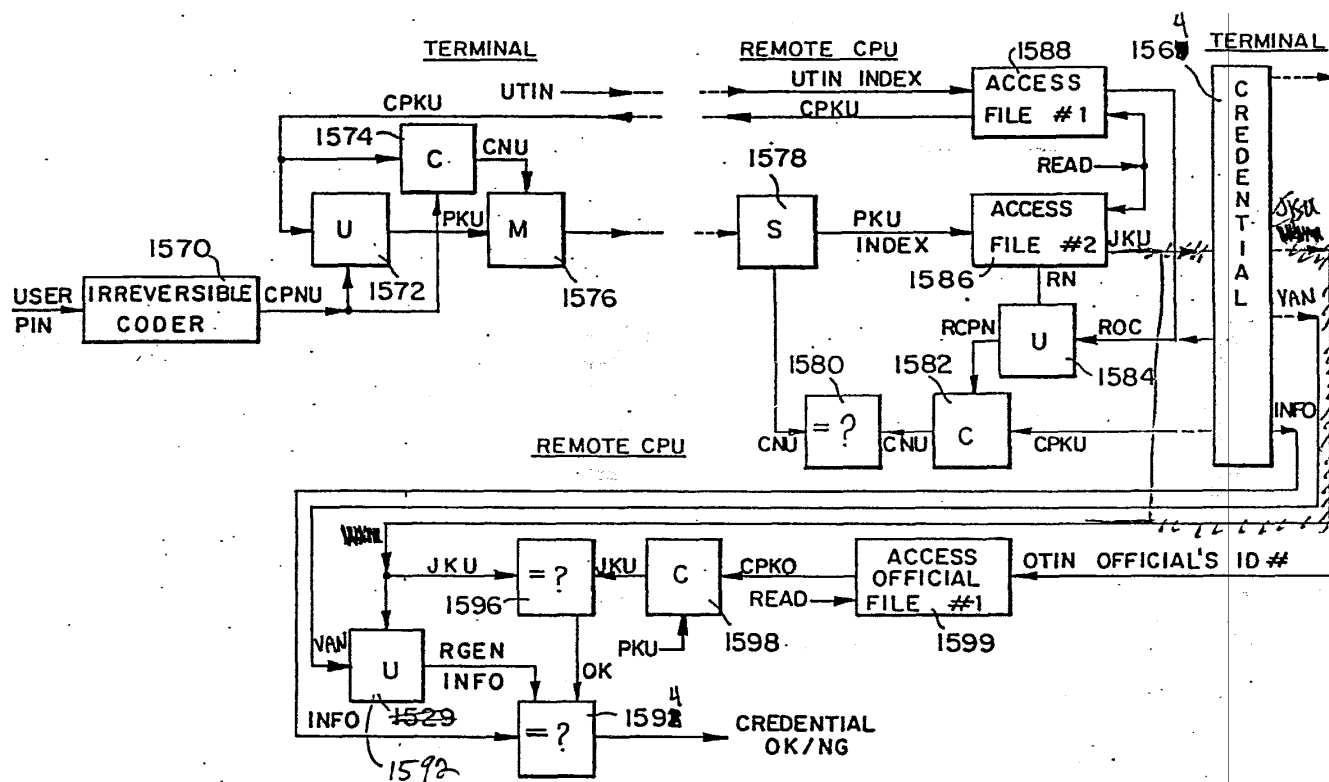


FIG. 15C

18  
11/15/92

PRINT OF DRAWINGS  
AS ORIGINALLY FILED

08/ 7174

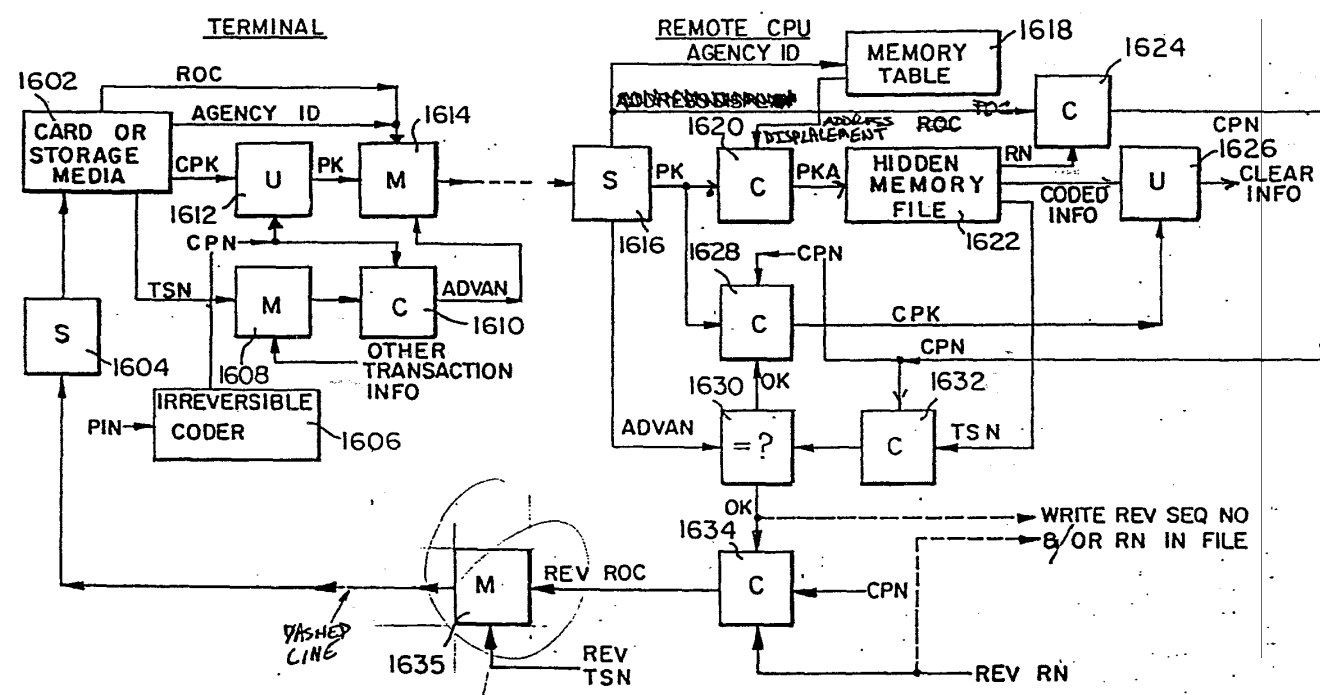


FIG. 16

03/747174

"EXPRESS MAIL" Mailing Label No. **EM131838914US**



*#2*  
*Letter w/ B.N.*  
*Re H201*  
PATENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re: Patent Application of : Group Art Unit:  
Leon Stambler :  
Applic. No.: : Examiner:  
Filed: Herewith :  
For: SECURE TRANSACTION : Attorney Docket  
SYSTEM AND METHOD : No. 6074-1U5  
UTILIZED THEREIN :

**TRANSMITTAL OF FORMAL DRAWINGS**  
**PRIOR TO NOTICE OF ALLOWANCE**

Attached please find the formal drawings for this application. The formal drawings incorporate the changes in the "SUBMISSION OF PROPOSED DRAWING AMENDMENT FOR APPROVAL BY EXAMINER" filed herewith. Approval of the formal drawings is respectfully requested.

Respectfully submitted,

LEON STAMBLER

Nov 11, 1996 BY: *Leslie L. Kasten, Jr.*  
(Date)  
Leslie L. Kasten, Jr.  
Registration No. 28,959  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
1601 Market Street, 36th Floor  
Philadelphia, PA 19103  
Telephone: (215) 567-2020  
Facsimile: (215) 567-2991

Enclosures

15 747174

FIG. 1

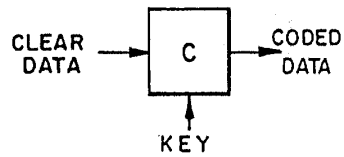


FIG. 2

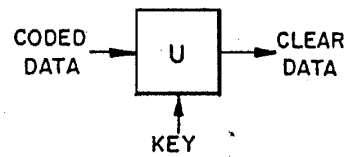


FIG. 3

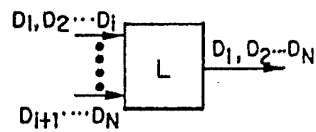


FIG. 4

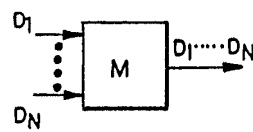


FIG. 5

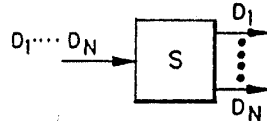
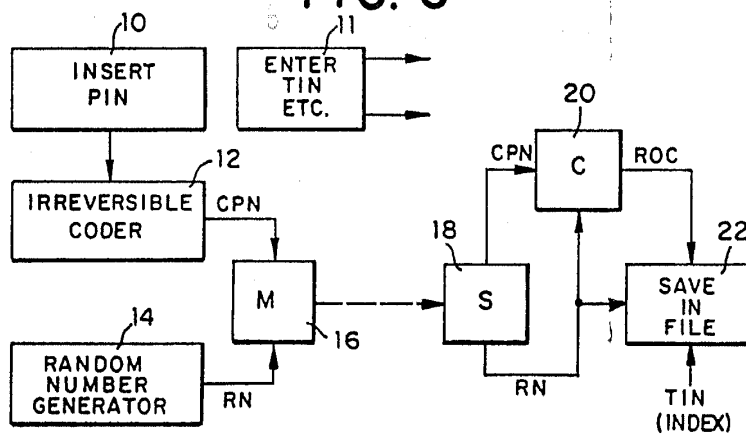
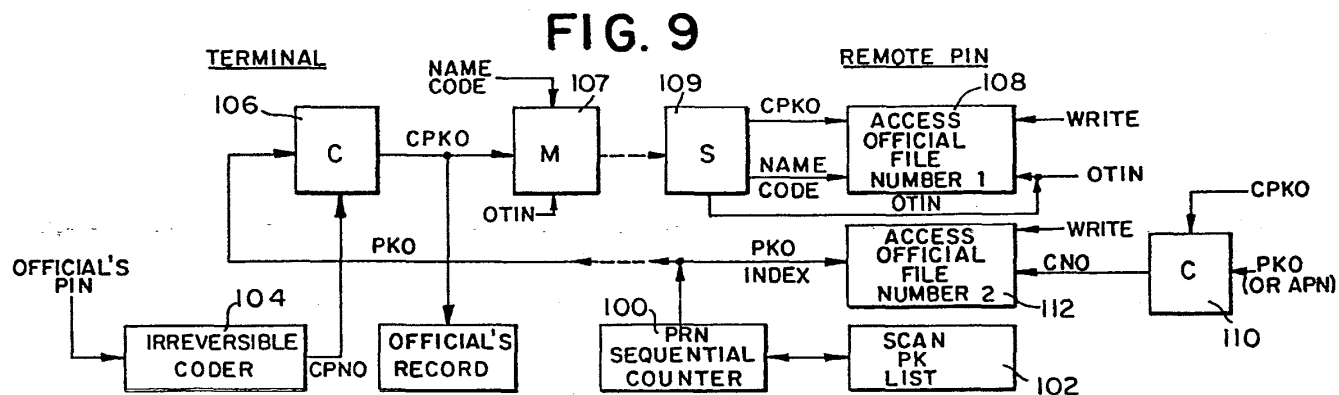
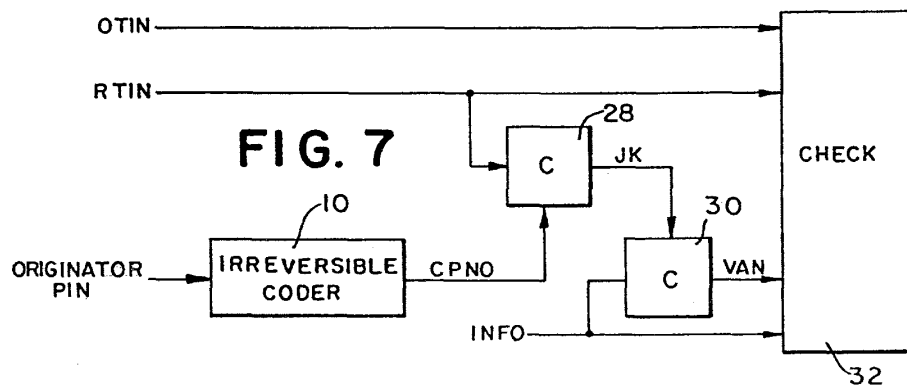


FIG. 6





08/24/74

FIG. 8A

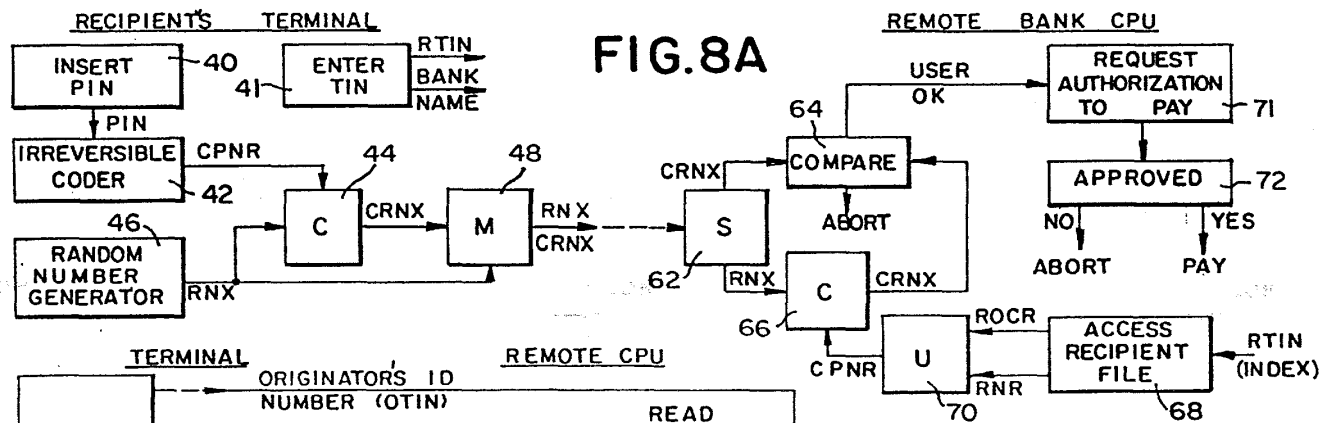
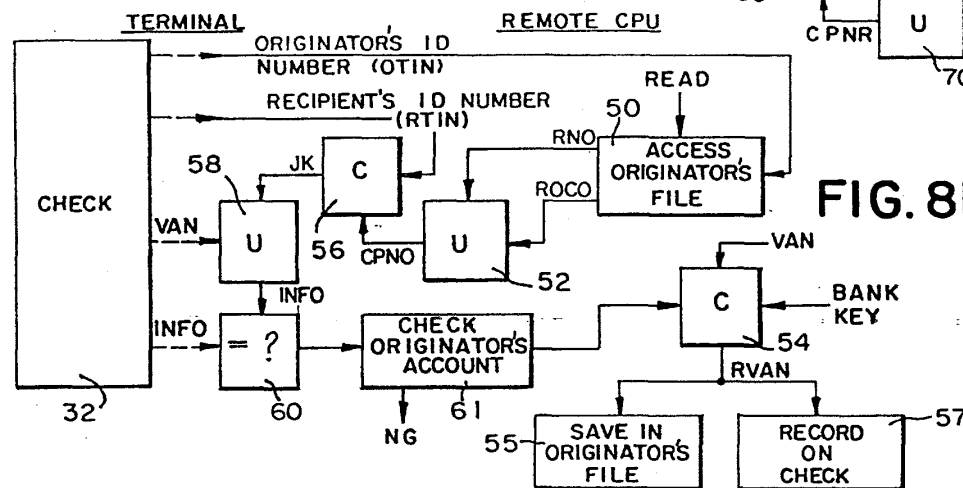


FIG. 8B



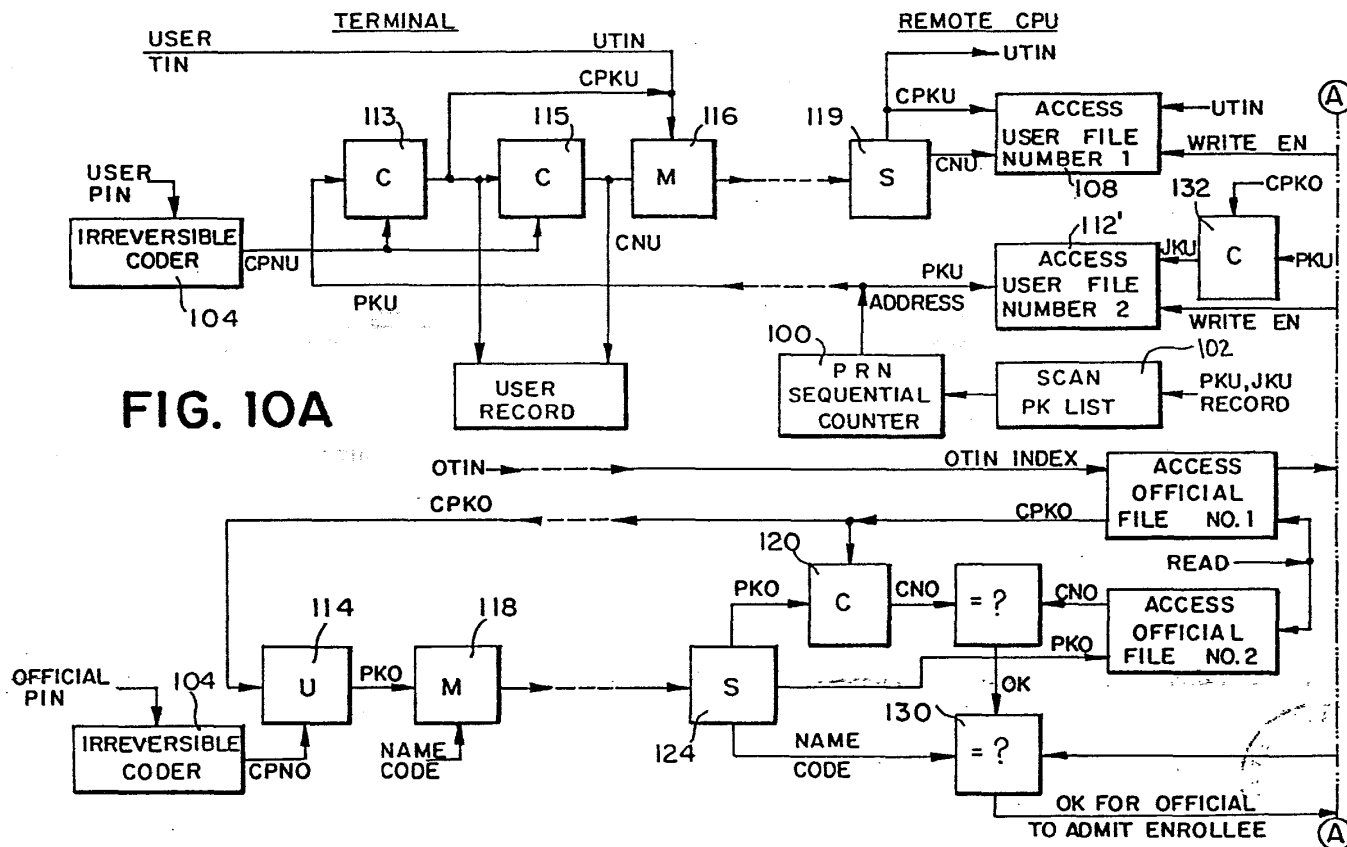




FIG. 10B

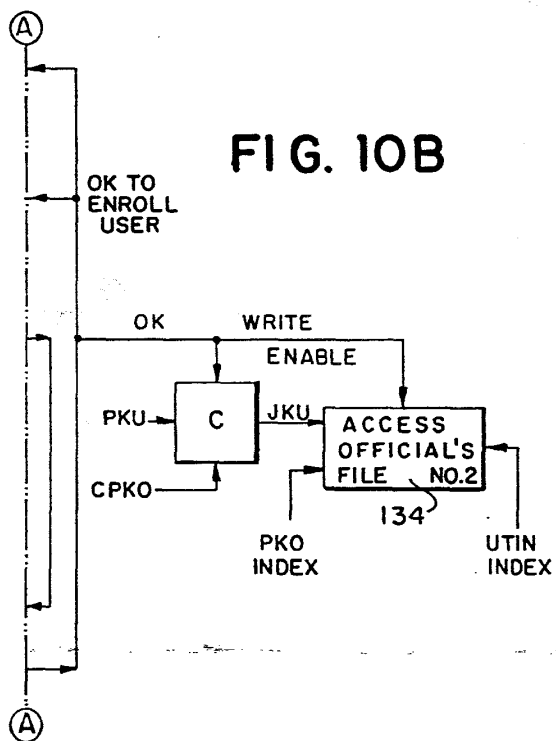
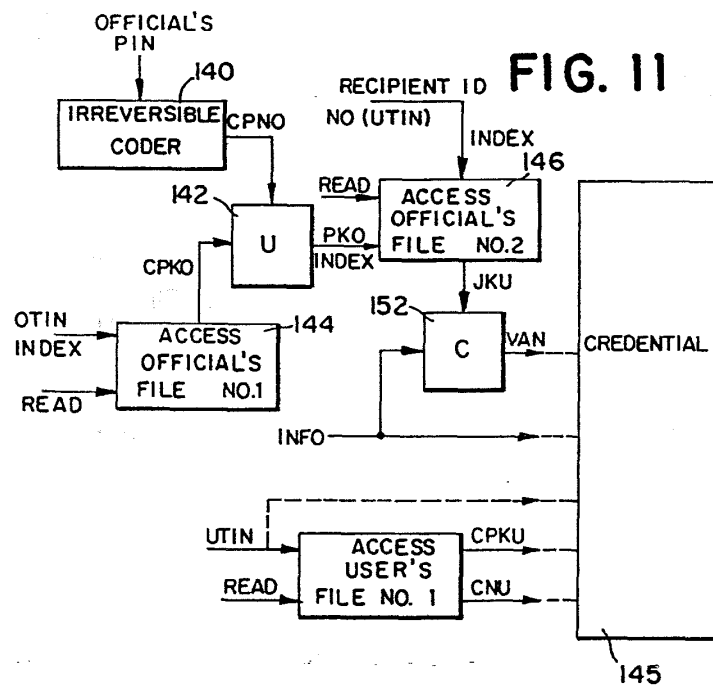
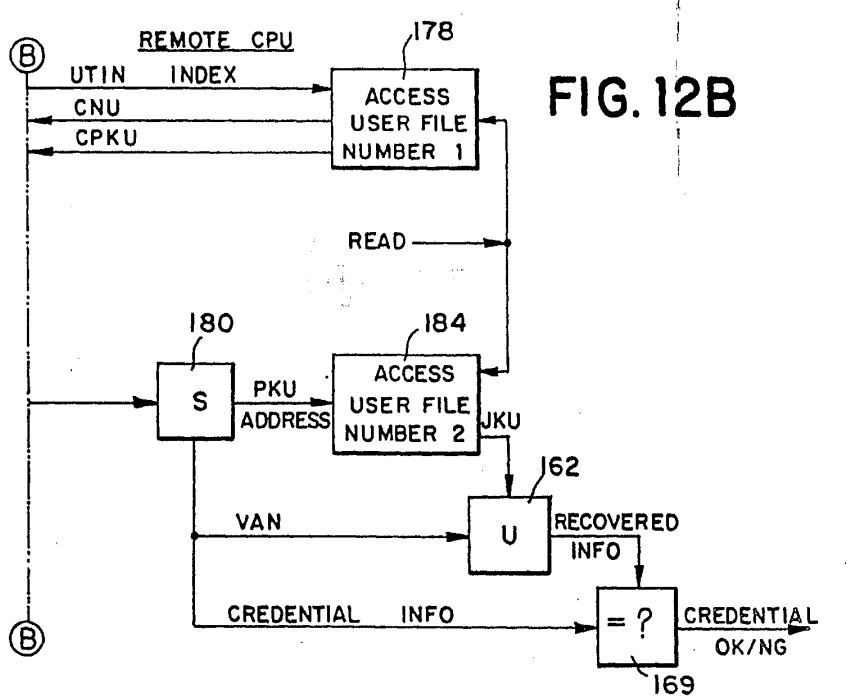
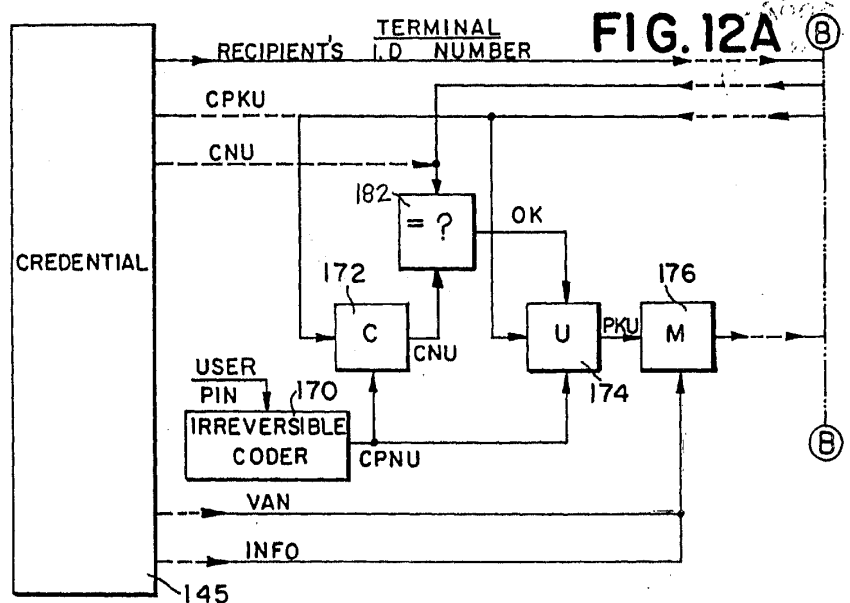


FIG. 11

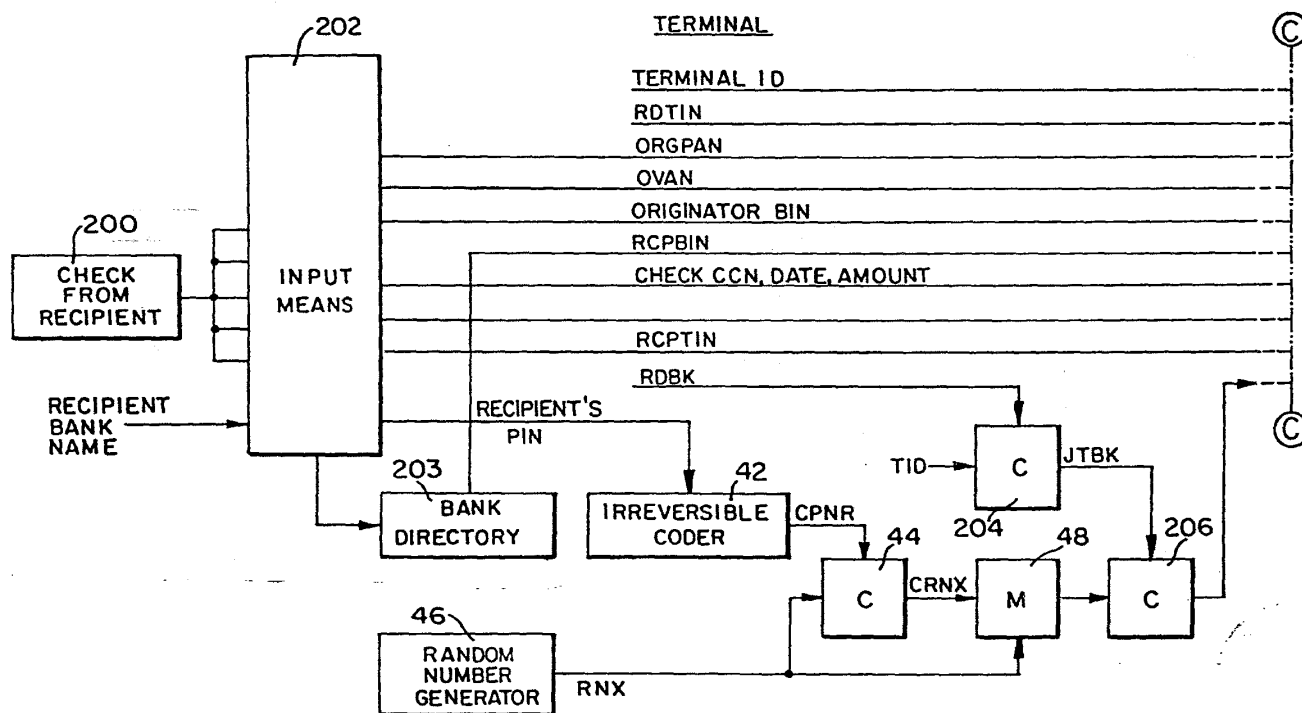


18/747174

FIG. 12A (B)



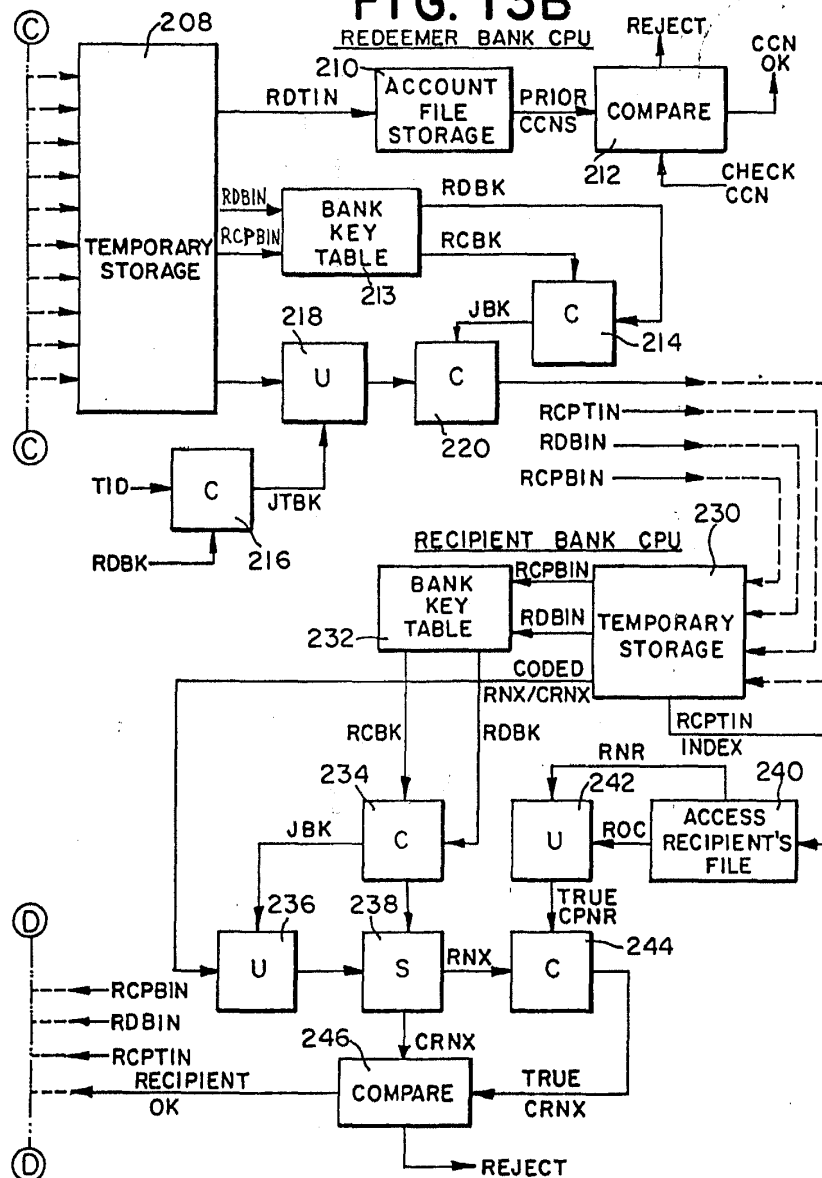
TERMINAL

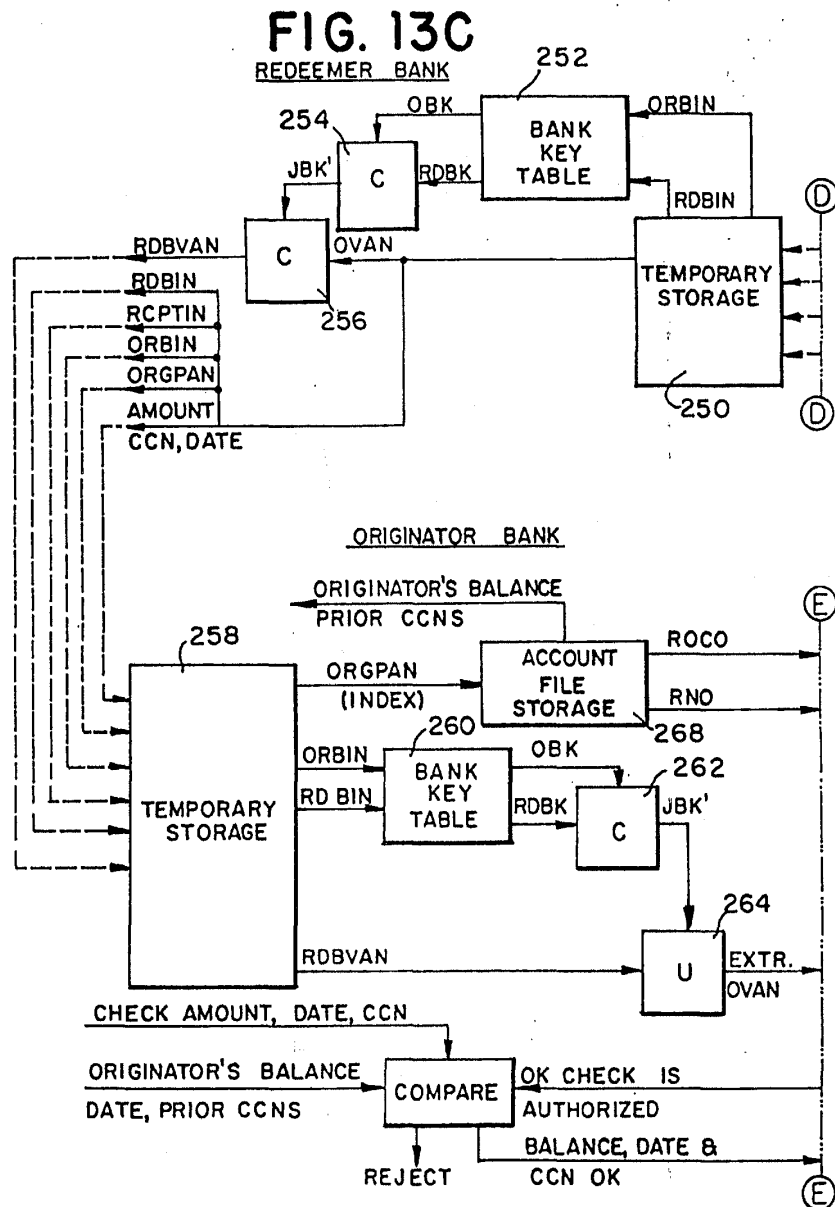


817471

63/747174

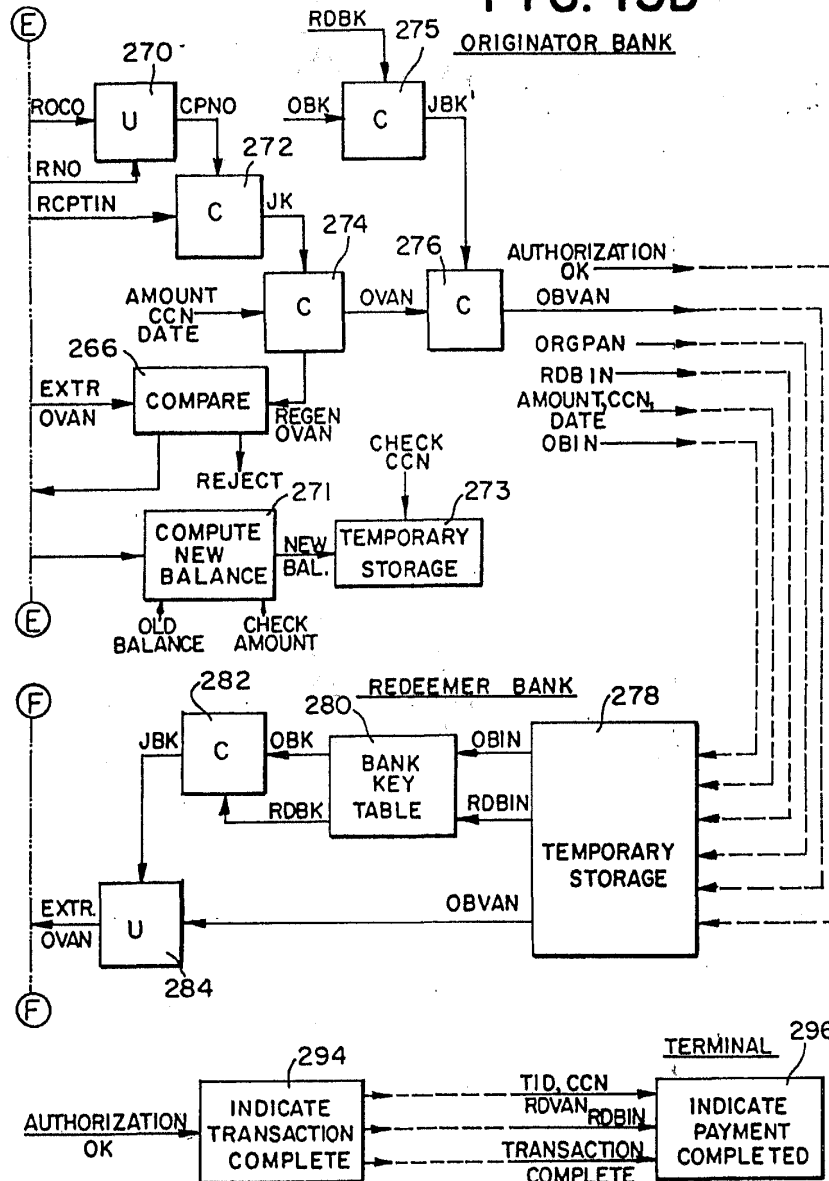
FIG. 13B





08/747174

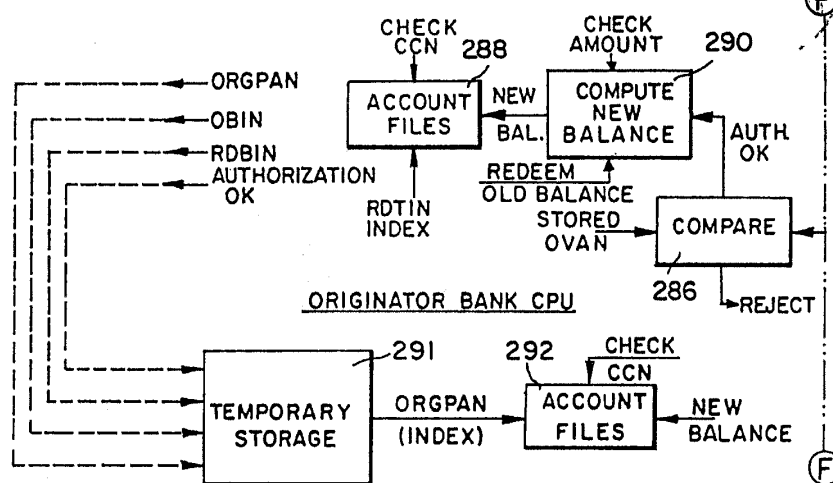
FIG. 13D



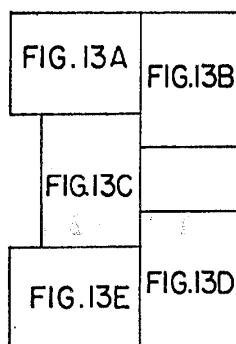
13/747174

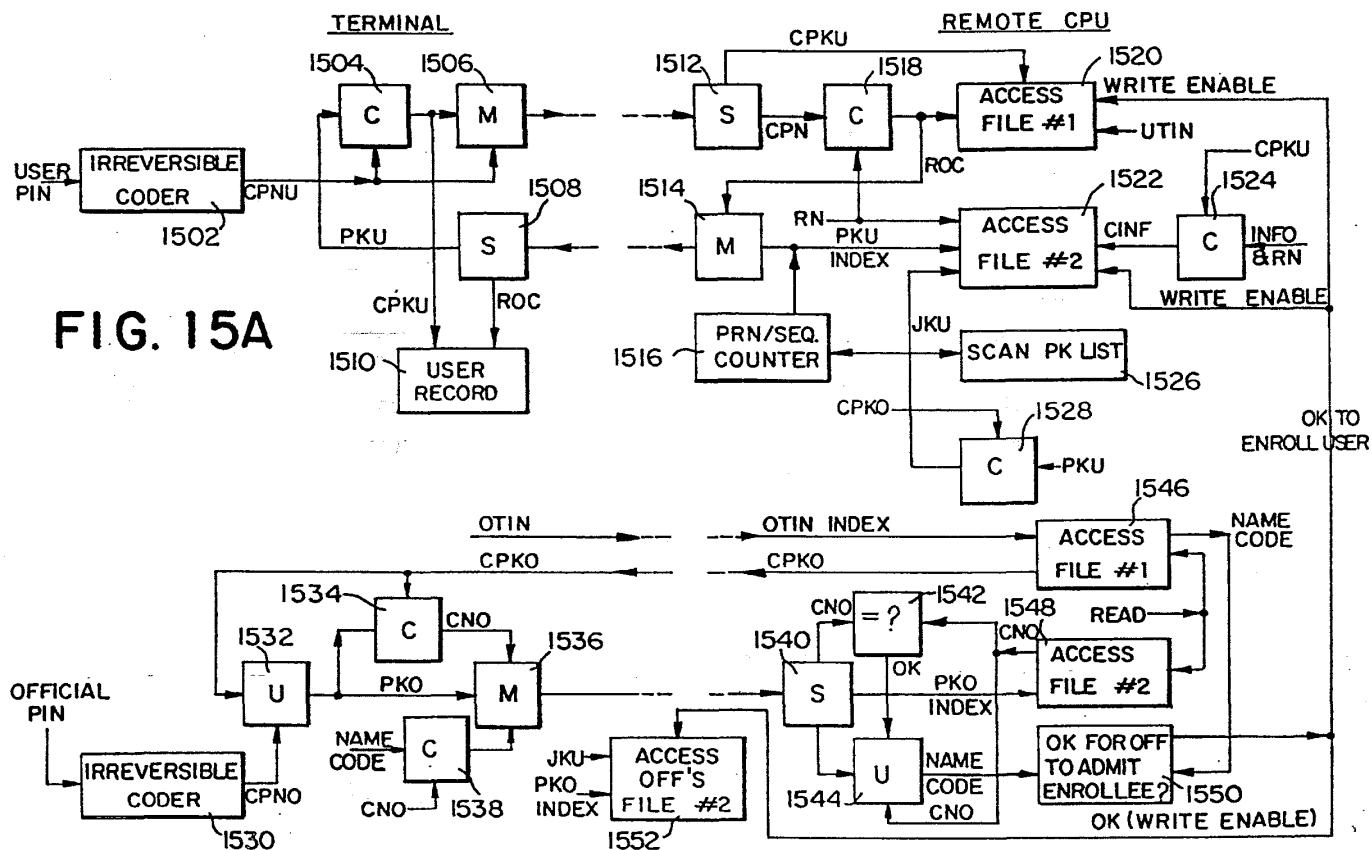
**FIG. 13E**

REDEEMER BANK



**FIG. 14**







8/747174

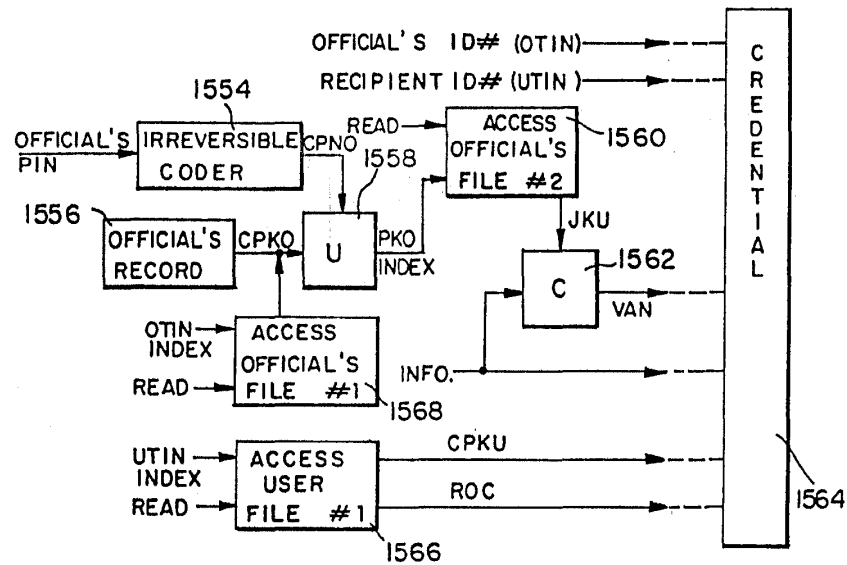
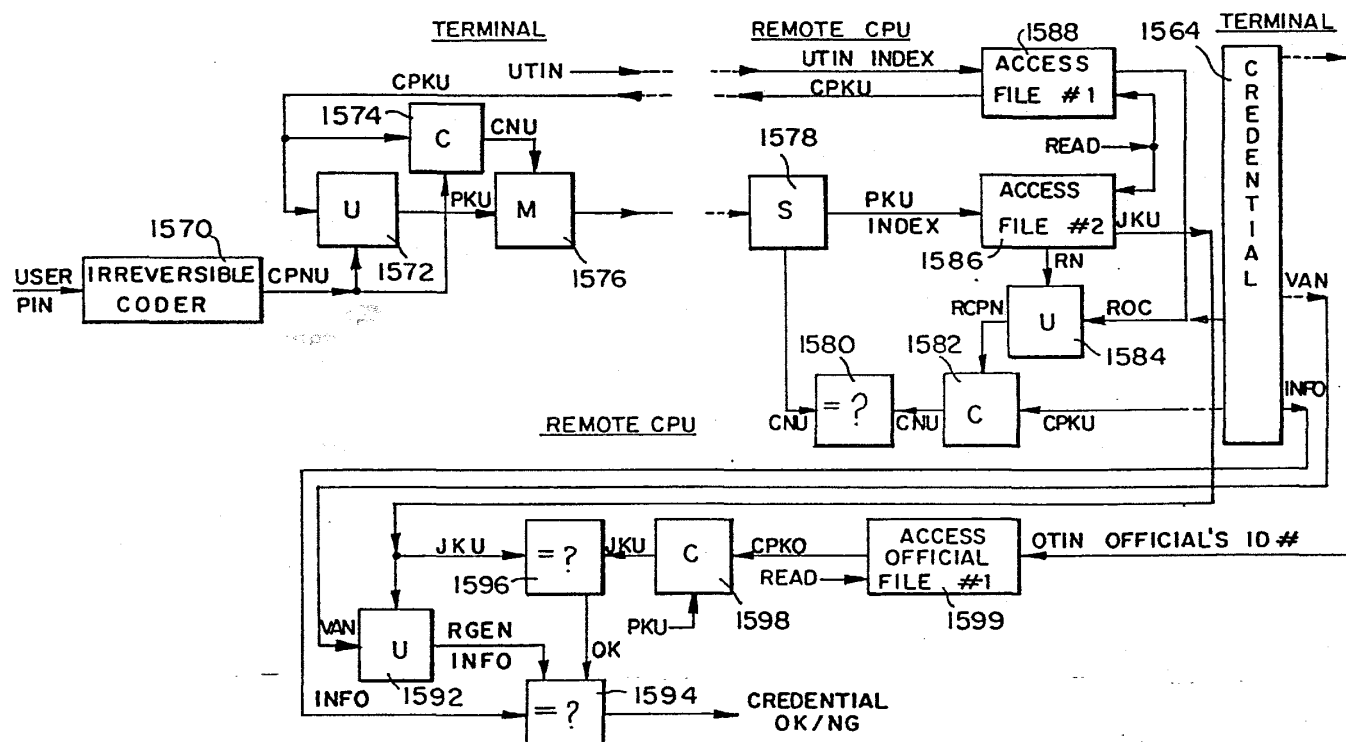


FIG. 15B



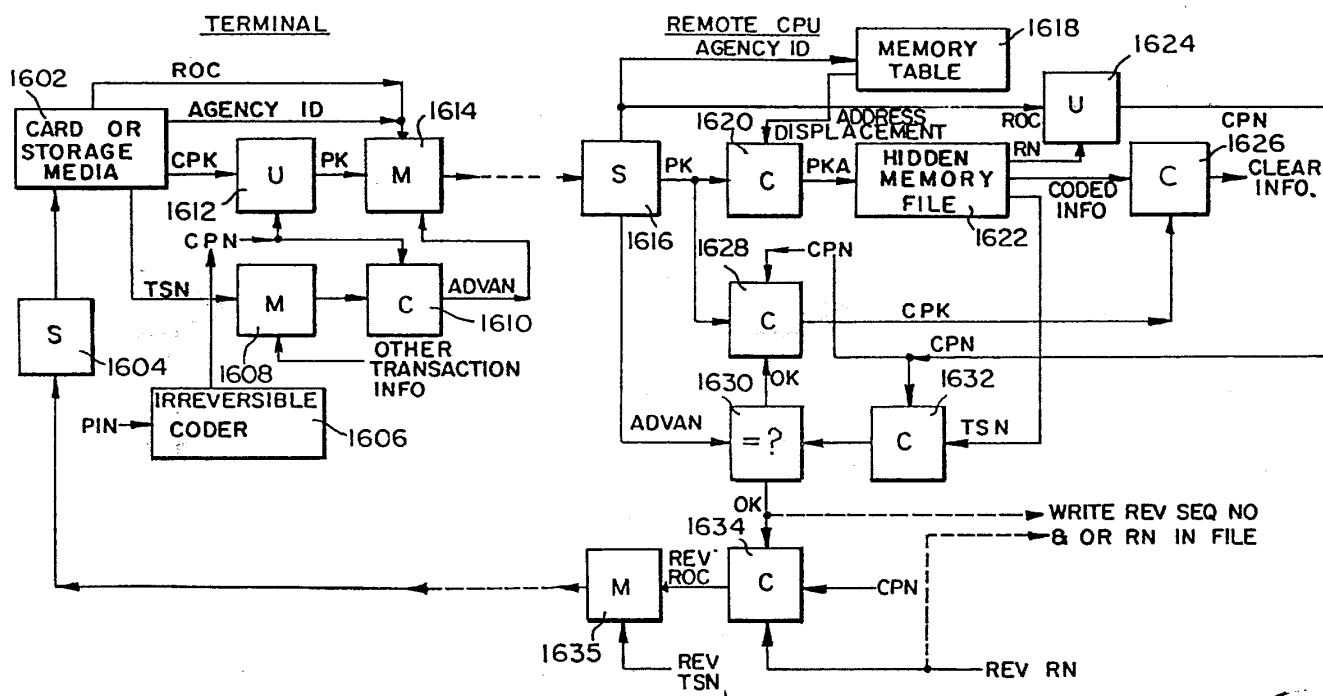


FIG. 16

08/747174 #3

"EXPRESS MAIL" Mailing Label No. **EM131838914US**



PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit: 2735  
Leon Stambler :  
Applic. No.: : Examiner:  
Filed: Herewith :  
For: SECURE TRANSACTION : Attorney Docket No. 6074-1U5  
SYSTEM AND METHOD :  
UTILIZED THEREIN :

MAR 12 1999

Group 2700

INFORMATION DISCLOSURE STATEMENT

It is requested that the references listed on the attached Information Disclosure Citation Form PTO-1449 be considered by the Patent Examiner in connection with the above-identified application and be made of record therein.

All of the references cited herein were previously cited and either submitted by Applicant or made of record by the Examiner in related Application Nos. 08/446,369 filed May 22, 1995 (pending); 08/445,612 filed May 22, 1995 (now U.S. Patent No. 5,555,303); 08/445,477 filed May 22, 1995 (allowed); 08/122,071 filed September 14, 1993 (now U.S. Patent No. 5,524,073); or 07/977,385 filed November 17, 1992 (now U.S. Patent No. 5,267,314), and thus are not enclosed.

The present application is a continuation of Application No. 08/446,369, filed May 22, 1995, which in turn is a division of Application No. 08/122,071, filed September 14, 1993, now U.S. Patent No. 5,524,073, which in turn is a division

PSJN2/62466.1

of Application No. 07/977,385, filed November 17, 1992, now U.S.  
Patent No. 5,267,314.

Independent consideration and acknowledgment of the  
listed references are respectfully requested.

Respectfully submitted,

LEON STAMBLER

Nov 8, 1996 BY: Leslie L. Kasten, Jr.  
(Date)  
Registration No. 28,959  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
1601 Market Street, 36th Floor  
Philadelphia, PA 19103  
Telephone: (215) 567-2020  
Facsimile: (215) 567-2991

Enclosure (PTO-1449 - three sheets)

Form PTO-1449 (REV. 8-83)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY DOCKET NO.: 6074-1 U5		APPLICATION NO.: Not yet assigned	
<b>INFORMATION DISCLOSURE CITATION</b> <small>(Form PTO-1449 Modified 8/95)</small> (Use several sheets if necessary)				APPLICANT: Leon Stambler		GROUP ART UNIT: Not yet assigned	
				FILING DATE: Filed herewith			
U.S. PATENT DOCUMENTS							
EX. INIT	DOCUMENT	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE
B2		3,609,690	09/1971	Nissman			
B2		3,611,293	10/1971	Constable			
B2		3,657,521	04/1972	Constable			
B2		3,892,948	07/1975	Constable			
B2		3,938,091	02/1976	Atalla <i>et al.</i>			
B2		4,004,089	01/1977	Richard <i>et al.</i>			
B2		4,016,405	04/1977	McCune <i>et al.</i>			
B2		4,186,871	02/1980	Anderson <i>et al.</i>			
B2		4,198,619	04/1980	Atalla			
B2		4,200,770	04/1980	Hellman <i>et al.</i>	380	44	
B2		4,208,575	06/1980	Haltof			
B2		4,208,739	06/1980	Lu			
B2		4,223,403	09/1980	Konheim <i>et al.</i>			
B2		4,234,932	11/1980	Gorgens			
B2		4,264,782	04/1981	Konheim			
B2		4,268,715	05/1981	Atalla			
B2		4,281,215	07/1981	Atalla			
B2		4,283,599	08/1981	Atalla			
B2		4,302,810	11/1981	Bouricius <i>et al.</i>			
B2		4,304,990	12/1981	Atalla			
B2		4,317,957	03/1981	Sendrow			
B2		4,319,079	03/1982	Best			
B2		4,328,414	05/1982	Atalla			
B2		4,386,266	05/1983	Chesarek			
B2		4,405,829	09/1983	Rivest <i>et al.</i>			
EXAMINER <i>B. Zimmerman</i>				DATE CONSIDERED <i>8/11/97</i>			
<small>*EXAMINER: Initial if citation 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.</small>							

Form PTO-1449 (REV. 8-83)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY DOCKET NO.: 6074-1 U5		APPLICATION NO.: Not yet assigned	
INFORMATION DISCLOSURE CITATION  <small>(Form PTO-1449 Modified 5/98) (Use several sheets if necessary)</small>				APPLICANT: Leon Stambler		GROUP ART UNIT: Not yet assigned	
				FILING DATE: Filed herewith			
U.S. PATENT DOCUMENTS							
EX. INIT	DOCUMENT	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE
66		4,471,163	09/1984	Donald <i>et al.</i>			
		4,498,000	02/1985	Decavele <i>et al.</i>			
		4,590,470	05/1986	Koenig			
		4,605,820	08/1986	Campbell, Jr.			
		4,665,396	05/1987	Dieleman			
		4,686,357	08/1987	Duono <i>et al.</i>			
		4,720,859	01/1988	Aaro <i>et al.</i>			
		4,734,858	03/1988	Schlaflly			
		4,740,890	04/1988	William			
		4,747,050	05/1988	Brachtl <i>et al.</i>			
		4,755,940	07/1988	Brachtl <i>et al.</i>			
		4,797,920	01/1989	Stein			
		4,799,061	01/1989	Abraham <i>et al.</i>			
		4,908,861	03/1990	Brachtl <i>et al.</i>			
		4,928,098	05/1990	Dannhaeuser			
		4,933,969	06/1990	Marshall <i>et al.</i>			
		4,935,962	06/1990	Austin			
		4,947,028	08/1990	Gorog			
		4,965,568	10/1990	Atalla <i>et al.</i>			
		4,977,595	12/1990	Ohta <i>et al.</i>			
		4,992,783	02/1991	Zdunek <i>et al.</i>			
		5,016,274	05/1991	Micali <i>et al.</i>			
		5,023,908	06/1991	Weiss			
		5,054,066	10/1991	Riek			
		5,067,155	11/1991	Bianco <i>et al.</i>			
66		5,161,244	11/1992	Maurer	380	43	
EXAMINER <i>B. Zimmerman</i>				DATE CONSIDERED			
*EXAMINER: Initial if citation 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.							

Form PTO-1449 (REV. 8-83)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY DOCKET NO.: 6074-1 U5	APPLICATION NO.: Not yet assigned				
<b>INFORMATION DISCLOSURE CITATION</b> <small>(Form PTO-1449 Modified 5/90)</small> (Use several sheets if necessary)		APPLICANT: Leon Stambler					
		FILING DATE: Filed herewith	GROUP ART UNIT: Not yet assigned				
<b>U.S. PATENT DOCUMENTS</b>							
EX. INIT	DOCU-MENT	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE
Dr		5,163,098	11/1992	Dahbura			
		5,168,520	12/1992	Weiss			
		5,196,840	03/1993	Leich <i>et al.</i>			
		5,199,066	03/1993	Logan			
		5,233,658	08/1993	Bianco <i>et al.</i>			
		5,267,314	11/1993	Stambler			
		5,327,563	07/1994	Singh			
		5,341,428	08/1994	Schatz			
		5,367,572	11/1994	Weiss			
BZ		5,400,403	03/1995	Fahn <i>et al.</i>			
<b>FOREIGN PATENT DOCUMENTS</b>							
EX. INIT	DOCU-MENT	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB-CLASS	TRANSLATION
							YES NO
<b>OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)</b>							
EXAMINER		B. Zimmerman					
		DATE CONSIDERED 8/11/97					
<small>*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 809; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.</small>							





EXPRESS MAIL" Mailing Label No. **EM131838914US**

08/747174 #4  
LETTER TO  
DRAFTSMAN  
PATENT # 269

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

re:	Patent Application of Leon Stambler	: Group Art Unit: :
Applic. No.:		: Examiner: :
Filed:	Herewith	: Attorney Docket :
For:	SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN	: No. 6074-1U5 :

SUBMISSION OF PROPOSED DRAWING AMENDMENT  
FOR APPROVAL BY EXAMINER (37 CFR 1.123)

Attached please find a copy of the original informal sheets of drawings with red ink markings, showing the proposed changes to the drawings in this application, for which the approval of the Examiner is requested. The proposed drawing changes are as follows:

1. Fig. 11: In the line connecting the block labeled "142" to the block labeled as "146", add an arrow pointing to the block labeled "146".
2. Fig. 12A: The block labeled as "132" should be changed to read "182".
3. Fig. 13B:
  - a. The signal line from the output of block 208 to the input of block 213 should be relabeled as "RCPBIN".
  - b. An additional signal line should be added from the output of block 208 to the input of block 213, and should be labeled as "RDBIN".

PSJN2/62417.1

c. The RDTIN signal line output from block 208 to the input of block 213 should be deleted.

A detailed explanation of the corrections is provided immediately below:

1. Correction to Fig. 11: The PKO INDEX signal should be shown as being output from the uncoder 142 and received by the second Access Official's File 146 to be consistent with page 23, lines 1-11 of the specification.

2. Correction to Fig. 12A: The block labeled as "132" should have read "182" to be consistent with page 24, line 32 of the specification.

3. Correction to Fig. 13B: The signal line from the output of block 208 to the input of block 213 should have been labeled as "RCPBIN". An additional signal line should have been included from the output of block 208 to the input of block 213, and should have been labeled as "RDBIN". The RDTIN signal line output from block 208 to the input of block 213 should be deleted. These corrections conform the figure to the corresponding text on page 28, lines 12-21 and 29-36 of the specification.

The above-identified corrections are fully supported by the original specification and thus do not constitute new matter. Correction is thus believed to be permitted.

Respectfully submitted,

LEON STAMBLER

Nov 8, 1996 BY: Leslie L. Kasten, Jr.  
(Date)  
Registration No. 28,959  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
1601 Market Street, 36th Floor  
Philadelphia, PA 19103  
Telephone: (215) 567-2020  
Facsimile: (215) 567-2991

Enclosures

FIG. 10B

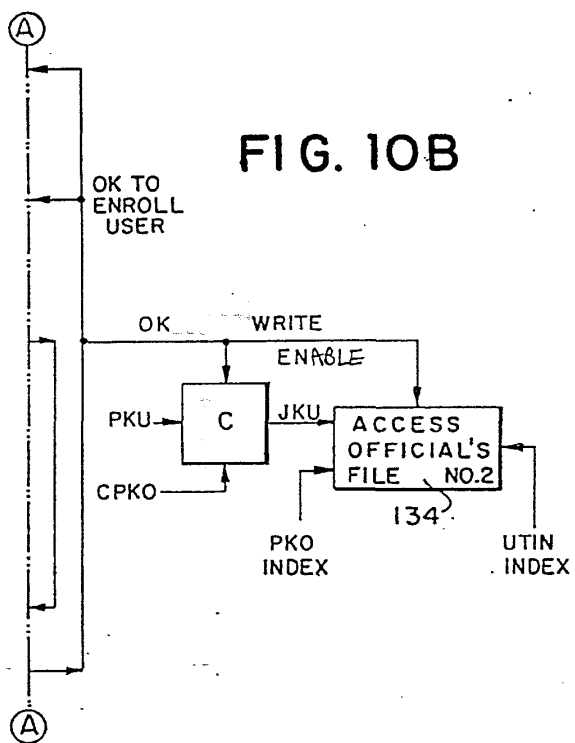
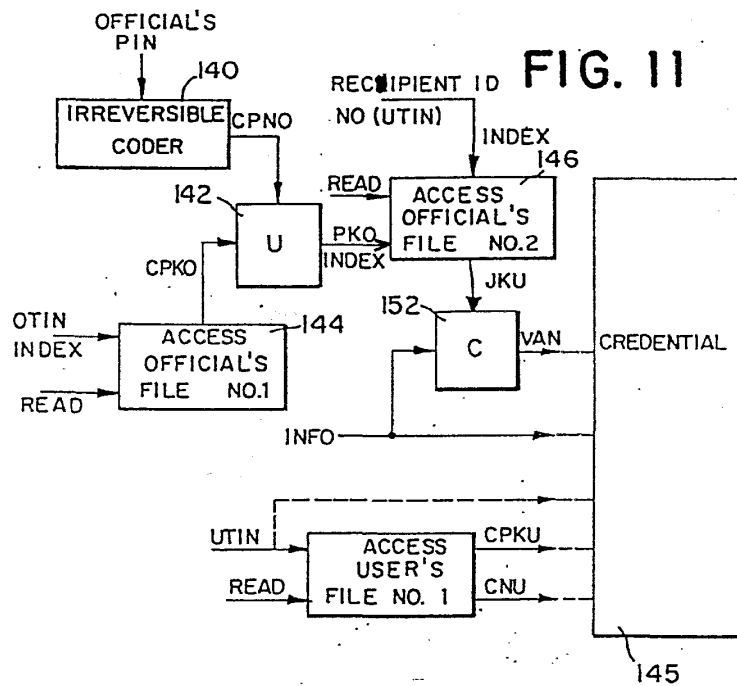
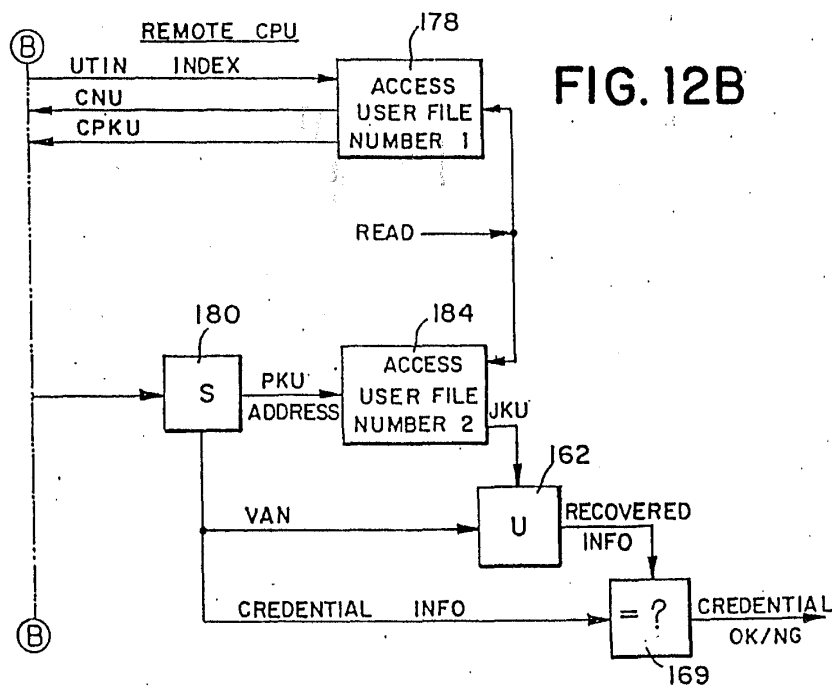
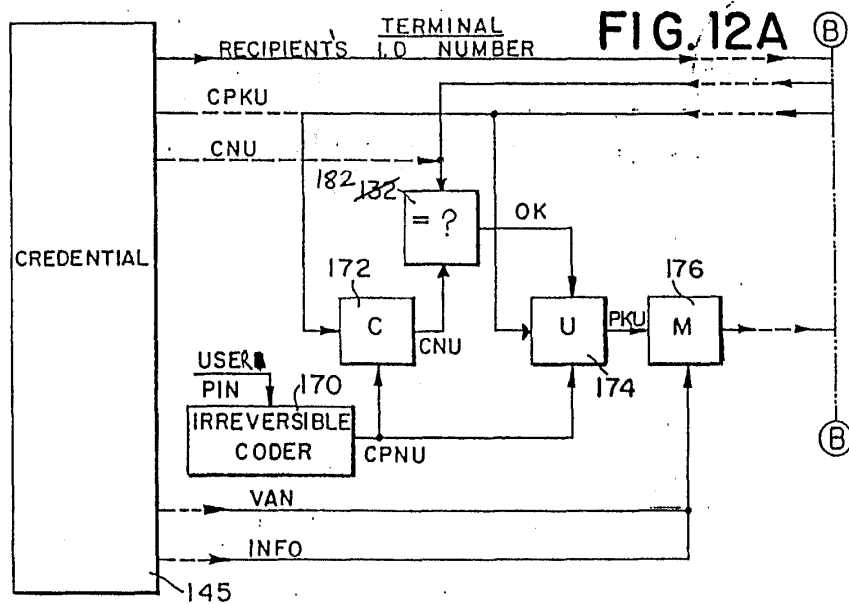
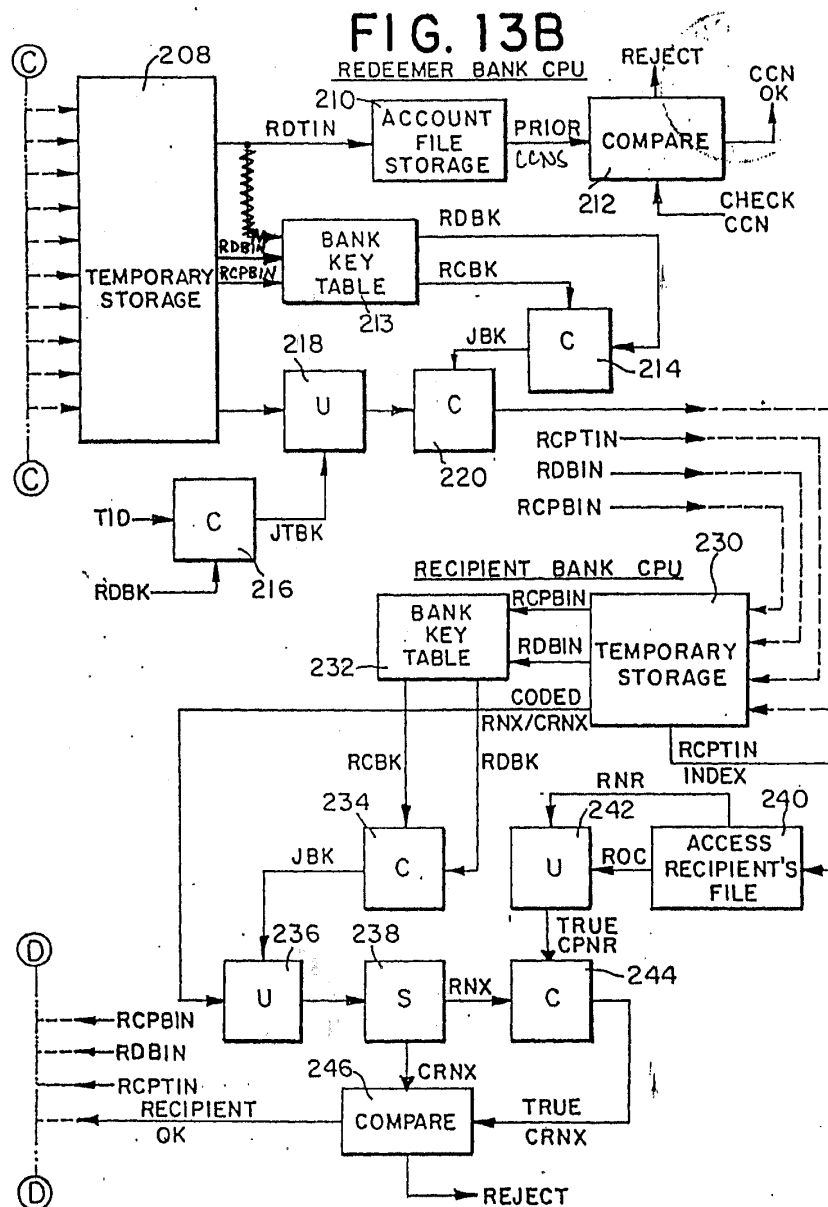


FIG. 11









"Express Mail Mailing Label"

Number EM131838914US

of Deposit November 12, 1996

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231

Name: Mike Grove

Signed: [Signature]

PATENT  
Attorney Docket No. 6074-1 U5  
BOX PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

This is a request under 37 C.F.R. §1.60 for filing a

☒ Continuation application (Group Art Unit 2202)

☐ Divisional application. Anticipated classification  
Class \_\_\_\_\_, Subclass \_\_\_\_\_,

of pending prior Application No. 08/446,369, filed

on May 22, 1995 of Leon Stambler  
inventor(s)

for SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN

(title of invention)

☒ Enclosed is a copy of the prior application as originally filed including:

☒ 15 sheets of drawings (informal)

☒ a properly executed Declaration and Power of Attorney.

☒ I hereby verify that the attached papers are a true copy of the prior application identified above as originally filed.

- ☐ Applicant(s) hereby claim the right of foreign priority under 35 U.S.C. §119(a)-(d) based on the following application(s):

Country:	Application No.:	Filing Date:
_____	_____	_____
_____	_____	_____

- ☐ A certified copy of the priority document(s) is of record in the prior application or application S.N. \_\_\_\_\_, filed \_\_\_\_\_.

- ☒ Applicant(s) hereby claim the right of priority under 35 U.S.C. §120 based on the following U.S. application:

Appln. No.:	Filing Date:	Status:
08/446,369	May 22, 1995	pending
08/122,071	September 14, 1993	issued
07/977,385	November 17, 1992	issued

- ☒ Cancel claims 1-63

- ☒ Amend the specification by inserting before the first line:

--This is a continuation of Application No. 08/446,369, filed May 22, 1995, which in turn is a division of Application No. 08/122,071, filed September 14, 1993, now U.S. Patent No. 5,524,073, which in turn is a division of Application No. 07/977,385, filed November 17, 1992, now U.S. Patent No. 5,267,314.

*now U.S. Patent 5,644,994*  
This application is related to Application No. 08/445,477, filed May 22, 1995, and Application No. 08/445,612, filed May 22, 1995, now U.S. Patent No. 5,555,303.--

- ☒ A preliminary amendment is enclosed.
- ☒ An Information Disclosure Statement is enclosed.
- ☒ A proposed drawing amendment is enclosed.
- ☒ New formal drawings are enclosed for replacing the informal drawings filed in the prior application. The new formal drawings incorporate the changes requested in the proposed drawing amendment.
- ☒ The power of attorney in the present application is to the attorneys and agents in the firm of Panitch Schwarze Jacobs & Nadel as listed in:
- ☐ A new Declaration and Power of Attorney is enclosed.
- ☒ The power appears in the prior application, as filed.



[ ] The prior application is assigned to \_\_\_\_\_

[X] Address all future communications to the undersigned at the address and telephone number set forth below.

[X] A Verified Statement Claiming Small Entity Status:

[X] was filed with the original application No. 07/977,385, and such status is still proper and desired (37 C.F.R. §1.28(a)).

[ ] is enclosed herewith.

The filing fee is calculated below:

			SMALL ENTITY		OR	LARGE ENTITY	
CLAIMS	NO. FILED	NO. EXTRA	BASIC FEE	\$385		BASIC FEE	\$770
TOTAL	44-20=	24	x11=	\$264	OR	x22=	\$
INDEPENDENT	13-3 =	10	x40=	\$400	OR	x80=	\$
MULTIPLE DEPENDENT CLAIMS PRESENT			x130=	\$	OR	x260=	\$
			TOTAL	\$1,049	OR TOTAL	\$	

[X] The Commissioner is hereby authorized to charge any of the following fees which may be required, or credit any overpayment, to Deposit Account No. 16-0235. One additional copy of this request is enclosed for accounting purposes.

[X] The above calculated filing fee \$ 1,049.00.

[X] Any additional fees required under 37 C.F.R. §1.16 or §1.17.

[X] If the filing of any paper during the prosecution of this application requires an extension of time in order for the paper to be timely filed, applicant(s) hereby petition(s) for the appropriate extension of time pursuant to 37 C.F.R. §1.136(a).

Respectfully submitted,

Nov 8, 1996  
(Date)

By:

Leslie L. Kasten, Jr.  
Registration No. 28,959  
PANITCH SCHWARZE JACOBS & NADEL  
1601 Market Street - 36th Floor  
Philadelphia, PA 19103-2398  
Telephone: 215-567-2020  
Telecopier: 215-567-2991

LLK:amh  
Enclosures



"EXPRESS MAIL" Mailing Label No. **EM131838914US**

0. '747174 <sup>#6</sup> Pre Amended  
ltg 1/24/1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit:  
Leon Stambler :  
:   
Appln. No.: : Examiner:  
:   
Filed: Herewith :   
:   
For: METHOD FOR SECURING :   
INFORMATION RELEVANT TO A : Attorney Docket  
TRANSACTION (as amended) : No. 6074-1U5

PRELIMINARY AMENDMENT

This preliminary amendment is being filed before receipt of a first Office Action. Please enter this preliminary amendment before examination of the application.

Charge any fee associated with this response and credit any overcharge to Deposit Account No. 16-0235.

Please amend the above-identified application as follows, without prejudice:

In the Title:

✓ Delete the original title and replace it with the following new title: --METHOD FOR SECURING INFORMATION RELEVANT TO A TRANSACTION--.

In the Claims:

✓ Add new claims 64-107 as follows:

PSJN2/62457.1

~~Sub 7~~  
--64. A method for coding and storing information, comprising information associated with a party and other sensitive information, said information associated with a party being subsequently used to authenticate the party and authorize access, the method comprising the steps of:

B27  
previously receiving a first personal identification number (PIN) from the party;  
previously deriving first coded authentication information by using the first PIN;  
previously generating at least two numbers using the first coded authentication information, wherein at least one of the at least two numbers is an arbitrary number;  
previously storing each of the at least two numbers in one or more first storage means;  
previously storing each of the at least two numbers in one or more second storage means;  
retrieving each of the at least two numbers previously stored in the first one or more storage means;  
retrieving each of the at least two numbers previously stored in the second one or more storage means;  
comparing each of the at least two numbers retrieved from the first one or more storage means with each of the at least two numbers retrieved from the second one or more storage means; and  
authorizing access if each of the at least two numbers retrieved from the first one or more storage means and

each of the at least two numbers retrieved from the second one or more storage means correspond to each other.

65. The method of claim 64 further comprising the steps of:

receiving a second personal identification number (PIN) from a party to be authenticated;

deriving second coded authentication information by using the second PIN;

combining each of the at least two numbers retrieved from the first or second one or more storage means to derive third coded authentication information;

comparing the second coded authentication information with the third coded authentication information; and

authorizing access if the second coded authentication information and third coded authentication information correspond to each other.

66. The method of claim 65 further comprising the step of:

coding said other sensitive information with said first or second or third coded authentication information to derive coded sensitive information.

67. The method of claim 65 further comprising the step of:

uncoding said coded sensitive information with  
said second or third coded authentication information to recover  
the other sensitive information.

68. The method of claim 64 further comprising the  
steps of:

combining each of the at least two numbers  
retrieved from the first one or more storage means to derive  
second coded authentication information;

combining each of the at least two numbers  
retrieved from the second one or more storage means to derive  
third coded authentication information;

comparing the second coded authentication  
information with the third coded authentication information; and

authorizing access if the second coded  
authentication information and third coded authentication  
information correspond to each other.

69. The method of claim 64 further comprising the  
steps of:

revising each of the at least two numbers at an  
arbitrary time; and

replacing each of the previous at least two  
numbers in the first and second one or more storage means with  
each of the revised at least two numbers.

70. The method of claim 64 wherein at least one of each of the at least two numbers is stored in the first one or more storage means and at least another of each of the at least two numbers is stored in the second one or more storage means, wherein the first and second one or more storage means are located at first and second respective sites.

<sup>6</sup>  
~~71.~~ The method of claim ~~64~~ wherein at least one of each of the at least two numbers is secret, and at least another of each of the at least two numbers is non-secret.

B2  
with ~~Sub E~~  
72. A method for coding first information, the method comprising the step of:

coding the first information using second information and then coding the result using third information, wherein the second or third information was previously generated and stored during an enrollment process, and wherein the second or third information are not derivable from each other.

~~Sub E~~  
73. In a multi-party transaction system, a method for securing information relevant to a transaction, the method comprising the steps of:

coding the information relevant to the transaction using first information associated with a party to generate first coded transaction information;

## File History Report

☐ Paper number \_\_\_\_\_ is missing from the United States Patent and Trademark Office's original copy of the file history. No additional information is available.

☐ The following page(s) 6 of paper number 6 is/are missing from the United States Patent and Trademark Office's original copy of the file history. No additional information is available

Additional comments: \_\_\_\_\_

associated with each of a group of one or more parties, or each of the other of the at least two information groups is previously stored in one or more storage means;

previously storing the arbitrary number in a storage medium;

coding the sensitive information by using the predetermined first key to derive the coded sensitive information;

subsequently retrieving the arbitrary number from the storage medium;

receiving the other of the at least two information groups from each of the group of one or more parties, or retrieving the other of the at least two information groups from the one or more storage means;

deriving the predetermined joint key by combining the predetermined arbitrary number with the other of the at least two information groups;

uncoding the coded sensitive information by using the predetermined joint key to recover the sensitive information.

76. The method of claim 75 wherein the predetermined arbitrary number is derived by combining the predetermined joint key with the other of the at least two information groups, such that the combination of the predetermined arbitrary number and the other of the at least two information group results in the predetermined joint key.



77. The method of claim 75 wherein at least one information group associated with at least one of the parties is derived from a personal identification number (PIN).

78. The method of claim 75 wherein the predetermined joint key is unrecoverable within the system.

32  
cont  
7  
79. The method of claim 75 wherein the location for retrieving the other of the at least two information groups from the one or more storage means is derived from identification information of a party associated with the predetermined first key.

80. A method for securing the integrity of first transaction information, and the integrity of second information associated with an originator party, by using an anti duplication variable authentication number (ADVAN), the first transaction information comprising a transaction sequence number and other transaction information, the transaction sequence number being previously stored in a storage means and being revised for each transaction, the method comprising the steps of:

coding the first transaction information using the second information to derive a first ADVAN1;

coding the second information using the transaction sequence number to derive third information;

appending the third information to the first  
ADVANI to derive integrated information;  
retrieving the transaction sequence number from  
the storage means;  
extracting the third information from the  
integrated information;  
uncoding the third information using the retrieved  
transaction sequence number to recover the second information;  
extracting the first ADVANI from the integrated  
information;  
uncoding the first ADVANI using the recovered  
second information to recover the first transaction information;  
extracting the transaction sequence number from  
the recovered first transaction information;  
comparing the extracted transaction sequence  
number with the retrieved transaction sequence number; and  
authenticating the integrity of the first  
transaction information and the second information if the  
extracted transaction sequence number compares favorably with the  
retrieved transaction sequence number.

81. The method of claim 80 further comprising the  
steps of:  
retrieving fourth information from the storage  
means, the fourth information being associated with the  
originator party;

deriving an ADVAN3 by coding the revised transaction sequence number with the fourth information;  
transmitting the ADVAN3 from the second site to the first site; and  
receiving the ADVAN3 at the first site, and uncoding the ADVAN3 by using fifth information to recover the revised transaction sequence number, the fifth information being associated with the originator party.

82  
cite 7

82. The method of claim 81 wherein the revised transaction sequence number is used as a key to code information during the current or during a subsequent transaction.

83. The method of claim 81 wherein the fourth and fifth information are derivable by using the PIN of the originator party.

84. The method of claim 80 further comprising the steps of:

extracting the other transaction information from the recovered first transaction information;

combining the other transaction information with the retrieved transaction sequence number to derive second transaction information;

coding the second transaction information using the recovered second information to derive a second ADVAN2;

comparing the ADVAN1 and the ADVAN2 to further authenticate the integrity of the other transaction information if the ADVAN1 and the ADVAN2 compare favorably.

85. The method of claim 80 further comprising the steps of:

revising the transaction sequence number and storing the revised transaction sequence number in the storage means for use during a subsequent transaction.

B2  
win 7

86. The method of claim 80 wherein the ADVAN1 and third information are derived at a first site and are transmitted to a second site, the integrity of the first transaction information and the second information being authenticated at the second site after retrieving the transaction sequence number from the storage means at the second site.

87. The method of claim 80 wherein more than one algorithm is used to code and uncode said information.

88. The method of claim 80 wherein at least selected portions of the first transaction information are coded to derive a compact error detection code, and wherein the compact error detection code is further coded with at least the second information to derive a compact ADVAN which is used to detect

*C* changes in at least the ~~first~~ <sup>first</sup> transaction information and at least the second information.

89. The method of claim 80 wherein the first transaction information comprises solely the transaction sequence number.

*B2*  
*with* 90. A method for authenticating a credential and a first party who was issued the credential, and a second party associated with issuing the credential, the method comprising the steps of:

retrieving information previously stored in the credential;

using at least a portion of the retrieved information previously stored in the credential to further retrieve information previously stored in a storage means associated with at least one of the parties, wherein the information retrieved from said storage means includes a first joint key;

*1* receiving ~~secret~~ <sup>non-secret</sup> information associated with one of the parties, and secret information associated with the other party;

*2* coding the ~~secret~~ <sup>non-secret</sup> information associated with one of the parties, and the secret information associated with the other party to generate a second joint key;

extracting the previously stored first joint key  
from the information retrieved from the storage means; and  
authenticating the credential, and the first party  
who was issued the credential, and the second party associated  
with issuing the credential, if the retrieved first joint key  
corresponds to the generated second joint key.

B2  
info 7 91. The method of claim 90 wherein the secret  
information associated with the one of the parties comprises  
information derived in conjunction with a PIN of that party.

92. The method of claim 90 wherein the second party is  
an agent, or an agency, or an official of an agency, or an  
authority, or an administrator, or an entity entrusted with  
issuing a credential.

93. A method for securing in escrow, and in trust,  
information associated with a first party in a storage means  
associated with a second party, wherein at least a portion of the  
escrowed information may be used for generating a joint key,  
wherein the joint key is derivable from information associated  
with the first party and information associated with a second  
party, the first party being enrolled by the second party and  
issued a credential, the method comprising the steps of:

previously receiving information associated with  
the first party and information associated with the second party;

previously generating a joint key using the  
information associated with the first party, and the information  
associated with the second party; and  
retaining in the storage means, in trust, at least  
the information associated with the first party and the  
information associated with the second party which was previously  
used to generate the joint key.

B2  
unit 7

94. The method of claim 93 wherein the escrowed  
information comprises at least the joint key.

Section 7

95. The method of claim 93 wherein the second party is  
an agent, or an agency, or an official of an agency, or an  
authority, or an administrator, or an entity entrusted with  
issuing a credential.

96. A method for enrolling a first party by a second  
party, and subsequently granting the first party access to a  
first storage means, or other thing, wherein the first party has  
a first personal identification number (PIN1), and the second  
party has a second personal identification number (PIN2), the  
first storage means, or other thing, being accessible only to a  
party with knowledge of the first PIN1 or with knowledge of the  
second PIN2, the method of enrollment comprising the steps of:  
receiving information associated with the first  
party;

receiving information associated with the second party; and

storing the information associated with the first party and the information associated with the second party in a second storage means, wherein the information retrieved subsequently from the second storage means is used in granting access to the first storage means, or other thing.

B2  
cont 7

97. The method of claim 96 wherein the second storage means is accessible for storing information therein only by a party with knowledge of the second PIN (PIN2), such that if no party exists with knowledge of the second (PIN2) then information cannot be stored in the second storage means.

98. A method for enrolling a first party by a second party, and subsequently granting the first party access to a first storage means, or other thing, wherein the first party has a first personal identification number (PIN1), and the second party has a second personal identification number (PIN2), the first storage means, or other thing, being accessible only to a party with knowledge of the first PIN1 or with knowledge of the second PIN2, the method of enrollment comprising the steps of:

receiving information associated with the first party;

receiving information associated with the second party;



coding the information associated with the first party and the information associated with the second party to generate a joint code; and

storing the code and the information associated with the second party in a second storage means, wherein the joint code and the information associated with the second party retrieved subsequently from the second storage means are used in granting access to the first storage means, or other thing.

B2  
with 7

<sup>15</sup> 99. The method of claim ~~98~~<sup>14</sup> wherein the second storage means is accessible for storing information therein only by a party with knowledge of the second PIN (PIN2), such that if no party exists with knowledge of the second (PIN2) then information cannot be stored in the second storage means.

~~Sub 18~~ 100. A method for granting a first party access to a first storage means, or other thing, subsequent to being enrolled by a second party, wherein the first party has a personal identification number (PIN), and wherein information associated with the second party was previously stored during enrollment in a second storage means, and a first joint code was previously generated and stored during enrollment in the second storage means, wherein the joint code was previously generated by using first coded authentication information derived from the personal identification number (PIN) of the first party and information

associated with the second party, the method comprising the steps of:

receiving a personal identification number (PIN) from the first party and generating second coded authentication information using the PIN;

retrieving from the second storage means the information associated with the second party, and the first joint code;

B2  
into 7 coding the second coded authentication information and the information associated with the second party to generate a second joint code;

comparing the first joint code and the second joint code; and

granting the first party access to the first storage means, or other thing, if the first joint code corresponds to the second joint code.

101. A method for granting a first party access to a first storage means, or other thing, subsequent to being enrolled by a second party, wherein the first party has a personal identification number (PIN), and wherein information associated with the second party was previously stored during enrollment in a second storage means, and wherein first information previously derived by using the PIN of the first party was previously stored during enrollment in the second storage means, the method comprising the steps of:

receiving the PIN from the first party and  
deriving second information by using the PIN;

retrieving from the second storage means the  
information associated with the second party, and the first  
information previously derived by using the PIN;

coding the first information previously derived by  
using the PIN and the information associated with the second  
party to generate a first joint code;

coding the second information derived by using the  
PIN and the information associated with the second party to  
generate a second joint code;

comparing the first joint code and the second  
joint code; and

granting the first party access to the first  
storage means, or other thing, if the first joint code  
corresponds to the second joint code.

102. In a computer system comprising a memory  
containing computer information stored in a controlled memory  
area to which access is granted only upon proper authentication  
of an authorized user of the computer system, the memory further  
including a stored control program for interacting with a user  
and for making a determination as to whether the user is an  
authorized user, the memory further including a first area, not  
readily accessible to a user, the first memory area containing a  
first revisable code and a second area containing a second

revisable code, a method of authentication of a user comprising the steps of:

receiving in the computer system identification information associated with the user;

generating first coded authentication information using the received identification information associated with the user;

B2  
wire? retrieving the first revisable code from the first memory area and the second revisable code from the second memory area and deriving therefrom second coded authentication information;

comparing the first coded authentication information with the second coded authentication information;

granting access to the computer information stored in the controlled memory area to the user only if the first and second coded authentication information compare favorably.

103. The method as recited in claim 102 further comprising the step of revising and storing the first and second revisable codes in the original respective memory areas only if the first and second coded authentication information compare favorably.

104. The method as recited in claim 103 wherein computer information stored in the memory of the computer system may be reproduced, the method further comprising the steps of:

previously recording the second revisable code  
with the computer information to be reproduced;

permitting the computer information to be  
reproduced only if the access has been granted to the user; and

thereafter retrieving the second revisable code  
retrieved from the reproduced information and using the second  
revisable code to authenticate the user if the reproduced  
information is used or accessed.

B2 - full 2  
with full 2  
105. In a computer system comprising a memory  
containing computer information stored in a controlled memory  
area to which access is granted only upon proper authentication  
of an authorized user of the computer system, the memory further  
including a stored control program for interacting with a user  
and for making a determination as to whether the user is an  
authorized user, the memory further including a first area, not  
readily accessible to a user, the first memory area containing a  
first revisable code and a second area containing a second  
revisable code, a method of authentication of a <sup>user</sup> comprising  
the steps of:

receiving in the computer system identification  
information associated with the user;

generating first coded authentication information  
using the received identification information associated with the  
user;

retrieving the first revisable code from the first memory area and the second revisable code from the second memory area;

1/ deriving a third revisable <sup>code</sup> using the retrieved  
2/ first revisable codes and the first coded authentication information;

comparing the retrieved second revisable code with the derived third revisable code;

B2  
unw granting access to the computer information stored in the controlled memory area to the user only if the second and third revisable codes compare favorably.

~~106. The method as recited in claim 105 further comprising the step of revising and storing the first and second revisable codes in the original respective memory areas only if the second and third revisable codes compare favorably.~~

107. The method as recited in claim 105 wherein computer information stored in the memory of the computer system may be reproduced, the method further comprising the steps of:

previously recording the second revisable code with the computer information to be reproduced;

permitting the computer information to be reproduced only if the access has been granted to the user; and

thereafter retrieving the second revisable code retrieved from the reproduced information and using the second

B2  
un'y

revisable code to authenticate the user if the reproduced  
information is used or accessed.--

REMARKS

Claims 64-107 are pending in this application. Claims  
1-63 were canceled because they are directed to the subject  
matter in parent applications related hereto. Prompt examination  
of the present application is requested.

Respectfully submitted,

LEON STAMBLER

NOV 8, 1996  
(Date)

BY:

*Leslie L. Kasten, Jr.*  
Leslie L. Kasten, Jr.  
Registration No. 28,959  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
1601 Market Street, 36th Floor  
Philadelphia, PA 19103  
Telephone: (215) 567-2020  
Facsimile: (215) 567-2991

LLK:rdm

#7

PANITCH SCHWARZE JACOBS & NADEL, P.C.  
INTELLECTUAL PROPERTY ATTORNEYS  
1601 Market Street - 36th Floor - Philadelphia, PA 19103-2398  
TELEPHONE: (215) 567-2020 - FACSIMILE: (215) 567-2991 - E-MAIL: psjn@psjn.com

**CERTIFICATION OF FACSIMILE TRANSMISSION**

I hereby certify that this paper is being facsimile transmitted  
to the U.S. Patent and Trademark Office on the date shown below

LOUISA DRAIN

Type or print name of person signing certification

*Louisa Drain*

Signature

March 14, 1997

Date

**FACSIMILE COVER SHEET**

Examiner: B. Zimmerman

FAX No.: 1 (703) 308-7382

Group Art Unit: 2211

Date: March 14, 1997

From: Leslie L. Kasten, Jr.

FAX Operator: Louisa Drain

Re: U.S. Patent Application No. 08/747,174 Filed 11/12/96 for "METHOD FOR SECURING  
INFORMATION RELEVANT TO A TRANSACTION"

Title of Paper sent via Facsimile: SUPPLEMENTAL PRELIMINARY AMENDMENT

4:20  
Time: 4:13 PM

PSJ&N File No: 6074-1U5 Page 1 of \_\_\_ pages

IF YOU DO NOT RECEIVE ALL THE PAGES, PLEASE CONTACT  
LOUISA DRAIN AT 215-567-2020

THIS FACSIMILE MESSAGE IS CONFIDENTIAL AND MAY CONTAIN ATTORNEY PRIVILEGED  
INFORMATION INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR COMPANY NAMED ABOVE.

If you are not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, any dissemination, distribution or copying of this  
communication is strictly prohibited. If you have received this communication in error, please immediately call us so that we may arrange for the return of the  
original message to us. Thank you!



Handwritten signature and date 3/19

#7

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit: 2211  
Leon Stambler :  
:   
Appln. No.: 08/747,174 : Examiner: B. Zimmerman  
:   
Filed: November 12, 1996 :  
:   
For: METHOD FOR SECURING :  
INFORMATION RELEVANT TO A : Attorney Docket  
TRANSACTION (as amended) : No. 6074-LU5

RECEIVED  
MAR 14 1997  
GROUP 2200

SUPPLEMENTAL PRELIMINARY AMENDMENT

This supplemental preliminary amendment is being filed  
before receipt of a first Office Action. Please enter this  
preliminary amendment before examination of the application.

Charge any fee associated with this response and credit  
any overcharge to Deposit Account No. 16-0235.

Please amend the above-identified application as  
follows, without prejudice:

In the Claims:

Claim 88, line 6: delete "firs" and replace it with  
--first--.

Claim 90, lines 13 and 16: delete "secret" and replace  
both occurrences with --non-secret--.

PSJN2/90720.1

RECEIVED

1997 MAR 14 10:22

18:22 03/14/97

Claim 105, line 10: delete "suer" and replace it with

--user--.

line 20: after "revisable", insert --code--.

line 21: delete "codes" and replace it with

--code--.

REMARKS

Claims 64-107 are pending in this application. Claims 88, 90 and 105 are amended to correct errors in the original set of claims. Prompt examination of the present application is requested.

Respectfully submitted,

LEON STAMBLER

3/14/97

(Date)

BY: 

Leslie L. Kasten, Jr.  
Registration No. 28,959  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
1601 Market Street, 36th Floor  
Philadelphia, PA 19103  
Telephone: (215) 567-2020  
Facsimile: (215) 567-2991

LLK:lcd

0000

PANITCH

03/14/97 16:22 215 567 2991



UNITED STATES DEPARTMENT OF COMMERCE  
Patent and Trademark Office

Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231

SERIAL NUMBER	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
---------------	-------------	----------------------	---------------------

107-107 11/ 1/ 1 1 1 1 1

EXAMINER

ART UNIT

PAPER NUMBER

8

DATE MAILED: 11/ 1/ 1

This is a communication from the examiner in charge of your application.  
COMMISSIONER OF PATENTS AND TRADEMARKS

☐ This application has been examined ☐ Responsive to communication filed on ☐ This action is made final.

A shortened statutory period for response to this action is set to expire 30 month(s), 30 days from the date of this letter.  
Failure to respond within the period for response will cause the application to become abandoned. 35 U.S.C. 133

Part I THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

- |   |   |
|---|---|
| 1. <input type="checkbox"/> Notice of References Cited by Examiner, PTO-892.        | 2. <input type="checkbox"/> Notice of Draftsman's Patent Drawing Review, PTO-948. |
| 3. <input type="checkbox"/> Notice of Art Cited by Applicant, PTO-1449.             | 4. <input type="checkbox"/> Notice of Informal Patent Application, PTO-152.       |
| 5. <input type="checkbox"/> Information on How to Effect Drawing Changes, PTO-1474. | 6. <input type="checkbox"/>   |

Part II SUMMARY OF ACTION

1. ☒ Claims 64-107 are pending in the application.  
Of the above, claims 64-107 are withdrawn from consideration.
2. ☐ Claims 64-107 have been cancelled.
3. ☐ Claims 64-107 are allowed.
4. ☐ Claims 64-107 are rejected.
5. ☐ Claims 64-107 are objected to.
6. ☒ Claims 64-107 are subject to restriction or election requirement.
7. ☐ This application has been filed with Informal drawings under 37 C.F.R. 1.85 which are acceptable for examination purposes.
8. ☐ Formal drawings are required in response to this Office action.
9. ☐ The corrected or substitute drawings have been received on 11/ 1/ 1. Under 37 C.F.R. 1.84 these drawings are ☐ acceptable; ☐ not acceptable (see explanation or Notice of Draftsman's Patent Drawing Review, PTO-948).
10. ☐ The proposed additional or substitute sheet(s) of drawings, filed on 11/ 1/ 1, has (have) been ☐ approved by the examiner; ☐ disapproved by the examiner (see explanation).
11. ☐ The proposed drawing correction, filed 11/ 1/ 1, has been ☐ approved; ☐ disapproved (see explanation).
12. ☐ Acknowledgement is made of the claim for priority under 35 U.S.C. 119. The certified copy has ☐ been received ☐ not been received ☐ been filed in parent application, serial no. 107-107; filed on 11/ 1/ 1.
13. ☐ Since this application appears to be 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.
14. ☐ Other

EXAMINER'S ACTION

PTOL-326 (Rev. 2/93)

Serial Number: 08/717714

-2-

Art Unit: 2211

Restriction to one of the following inventions is required under 35 U.S.C. 121:

Group I. Claims 64-74, 90-107, drawn to an authorization system, classified in Class 340, subclass 825.34.

Group II. Claims 75-89, drawn to an encryption system, classified in Class 380, subclass 20.

The inventions are distinct, each from the other because of the following reasons:

1. Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention II has separate utility such as for use in exchanging computer programs. See M.P.E.P. § 806.05(d).
2. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.
3. Because these inventions are distinct for the reasons given above and the search required for Group I is not required for

Serial Number: 08/717714

-3-

Art Unit: 2211

Group II, restriction for examination purposes as indicated is proper.

4. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art because of their recognized divergent subject matter, restriction for examination purposes as indicated is proper.

Applicant is advised that the response to this requirement to be complete must include an election of the invention to be examined even though the requirement be traversed.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brian Zimmerman whose telephone number is (703) 305-4796.



BRIAN ZIMMERMAN  
PRIMARY EXAMINER  
GROUP 2200

BZ  
April 8, 1997

2211  
3/28  
I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.

BY Elizabeth A. v. Glend DATE 5/7/97

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit: 2211  
Leon Stambler :  
:   
Appln. No.: 08/747,174 : Examiner: B. Zimmerman  
:   
Filed: November 12, 1996 :   
:   
For: METHOD FOR SECURING :   
INFORMATION RELEVANT TO A : Attorney Docket  
TRANSACTION (as amended) : No. 6074-105

SECOND SUPPLEMENTAL PRELIMINARY AMENDMENT  
AND RESPONSE TO RESTRICTION REQUIREMENT

This correspondence is in response to an Office Action setting forth a written restriction requirement, mailed April 9, 1997 (Paper no. 8), and is being timely filed within the shortened statutory period set for response in the Office Action.

Charge any fee associated with this response and credit any overcharge to Deposit Account No. 16-0235.

Applicant elects Group I, claims 64-74 and 90-107 for examination. The election is without traverse.

Please amend the above-identified application as follows, without prejudice:

In the Claims:

Cancel claims 75-89 without prejudice to filing a divisional application on such claims.

Add new claims 108-143 as follows:

*Sub E3*  
--108. A method for authenticating a first party by using information stored in a credential, the credential being previously issued to the first party by a second party, wherein information previously stored in the credential comprises at least a variable authentication number (VAN) and other credential information, the method comprising the steps of:

previously coding at least a portion of the other credential information with first information associated with the second party to derive a variable authentication number (VAN);

previously storing the VAN and the other credential information in the credential;

retrieving the VAN and the other credential information stored in the credential;

retrieving second information associated with the  
second party previously stored in a storage means associated with  
at least one of the parties;

uncoding the VAN using the second information  
associated with the second party to derive the at least a portion  
of the other credential information; and

authenticating the first party if the at least a  
portion of the other credential information retrieved from the  
credential corresponds to the at least a portion of the other  
credential information uncoded from the VAN.

29. The method of claim 108 wherein the first  
information associated with the second party comprises a secret  
key, and the second information associated with the second party  
comprises a non-secret key.

110. The method of claim 108 wherein the at least  
a portion of the other credential information comprises a name  
and a non-secret key associated with the first party.

111. A method for issuing a credential to a first  
party by a second party, the method comprising the steps of:



the second party receiving information associated with  
the first party;

the second party authenticating at least a portion of  
the received information associated with the first party;

denying issuance of the credential if at least a  
portion of the received information associated with the first  
party is determined not to be authentic;

coding at least a portion of the received information  
associated with the first party with first information associated  
with the second party to derive a variable authentication number  
(VAN);

storing the VAN and at least a portion the received  
information associated with the first party, and other  
information associated with the second party, in the credential;  
and

issuing the credential to the first party.

112. The method of claim 111 wherein at least a  
portion of the information associated with the first party  
comprises the name and a non-secret key associated with the first  
party.

113. A method for authenticating a first party by using information stored in a credential, the credential being previously issued to the first party by a second party, wherein information previously stored in the credential comprises at least a variable authentication number (VAN) and other credential information, the method comprising the steps of:

previously generating a first error detection code (EDC1) by using at least a portion the other credential information:

previously coding the first error detection code (EDC1) with first information associated with the second party to derive a variable authentication number (VAN):

previously storing the VAN and the other credential information in the credential;

retrieving the VAN and the other credential information stored in the credential;

deriving a second error detection code (EDC2) by using at least a portion of the retrieved other credential information;

retrieving second information associated with the second party previously stored in a storage means associated with at least one of the parties;

uncoding the VAN using the second information associated with the second party to derive a third error detection code (EDC3); and

authenticating the first party and at least a portion of the information stored in the credential if the second error detection code (EDC2) corresponds to the third error detection code (EDC3).

*114.34* 114. The method of claim *33* 113 wherein the first information associated with the second party comprises a secret key, and the second information associated with the second party comprises a non-secret key.

*Sub 6* 115. The method of claim 113 wherein the at least a portion of the other credential information comprises a name and a non-secret key associated with the first party.

116. A method for issuing a credential to a first party by a second party, the method comprising the steps of:

the second party receiving information associated with the first party;

the second party authenticating at least a portion of the received information associated with the first party;

denying issuance of the credential if at least a portion of the received information associated with the first party is determined not to be authentic;

generating an error detection code (EDC) by using at least a portion the received information associated with the first party;

coding the error detection code (EDC) by using information associated with the second party to derive a variable authentication number (VAN);

storing the VAN and at least a portion the received information associated with the first party, and other information associated with the second party, in the credential; and

issuing the credential to the first party.

117. The method of claim 116 wherein at least a portion of the information associated with the first party comprises the name and a non-secret key associated with the first party.

*118* 118. A method for authenticating a first party at a first site by a second party at a second site by using a personal identification number (PIN) or a password (PW) supplied by the first party at the first site, and further using a first random number (RN1) generated by the second party at the second site, the PIN or password (PW) being previously used to derive first coded authentication information, the first coded authentication information being previously stored in a storage means associated with the second party at the second site, the method comprising the steps of:

- receiving a PIN or a password (PW) at the first site from a first party to be authenticated;
- generating second coded authentication information using the received PIN or password (PW);
- generating a first random number (RN1) at a second site by the second party;
- transmitting the first random number (RN1) from the second site to the first site;
- receiving the first random number (RN1) at the first site by the first party;

coding the received first random number (RN1) and the second coded authentication information to derive a first anti-duplication variable authentication number (ADVAN1);

transmitting the first anti-duplication variable authentication number (ADVAN1) from the first site to the second site;

receiving the first anti-duplication variable authentication number (ADVAN1) at the second site by the second party;

retrieving the first coded authentication information from the storage means at the second site;

coding the first random number (RN1) and the first coded authentication information to generate a second anti-duplication variable authentication number (ADVAN2);

comparing the first anti-duplication variable authentication number (ADVAN1) and the second anti-duplication variable authentication number (ADVAN2); and

authenticating the first party by the second party if the first anti-duplication variable authentication number (ADVAN1) and the second anti-duplication variable authentication number (ADVAN2) correspond.

*Sub 119*  
119. The method of claim 118 wherein after authentication occurs, the first party is authorized access to information stored at the second site.

*Sub 120*  
120. A method for authenticating a first party at a first site by a second party at a second site, wherein first information associated with the first party is previously stored in a first storage means at the first site, second information associated with the second party is previously stored in a second storage means at the first site, third information associated with the second party is previously stored in a third storage means at the second site, and fourth information associated with the first party is previously stored in a fourth storage means at the second site, the method comprising the steps of;

generating a first random number (RN1) at the second site;

retrieving the fourth information associated with the first party from the fourth storage means at the second site;

generating a first anti-duplication variable authentication number (ADVAN1) by coding the first random number (RN1) with the fourth information retrieved from the fourth storage means;

-10-

transmitting the first anti-duplication variable authentication number (ADVAN1) from the second site to the first site, and receiving the ADVAN1 at the first site;

receiving a personal identification number (PIN) or a password (Pw) supplied by the first party at the first site;

retrieving the first information associated with the first party from the first storage means only if the PIN or the password of the first party is determined to be authentic;

uncoding the received ADVAN1 by using the retrieved first information to derive a first recovered random number (RRN1);

retrieving the second information associated with the second party from the second storage means;

generating a second anti-duplication variable authentication number (ADVAN2) by coding the first recovered random number (RRN1) with the second information retrieved from the second storage means;

transmitting the second anti-duplication variable authentication number (ADVAN2) from the first site to the second site, and receiving the ADVAN2 at the second site;

retrieving the third information associated with the second party from the third storage means;

-11-



uncoding the received ADVAN2 by using the retrieved third information to derive a second recovered random number (RRN2); and

authenticating the first party if the first random number (RN1) corresponds to the second recovered random number (RRN2).

121. The method of claim 120 wherein the first information stored in the first storage means is secret, and the second information stored in the second storage means is non-secret, and the third information stored in the third storage means is secret, and the fourth information stored in the fourth storage means is non-secret.

122. A method for authenticating a second party at a second site by a first party at a first site, wherein first information associated with the first party is previously stored in a first storage means at the first site, second information associated with the second party is previously stored in a second storage means at the first site, third information associated with the second party is previously stored in a third storage means at the second site, and fourth information associated with

the first party is previously stored in a fourth storage means at the second site, the method comprising the steps of;

generating a first random number (RN1) at the first site;

retrieving the second information associated with the second party from the second storage means at the first site;

generating a first anti-duplication variable authentication number (ADVAN1) by coding the first random number (RN1) with the second information retrieved from the second storage means;

transmitting the first anti-duplication variable authentication number (ADVAN1) from the first site to the second site, and receiving the first ADVAN1 at the second site;

retrieving the third information associated with the second party from the third storage means at the third site;

uncoding the received ADVAN1 by using the retrieved third information to derive a first recovered random number (RRN1);

retrieving the fourth information associated with the first party from the fourth storage means;

generating a second anti-duplication variable authentication number (ADVAN2) by coding the first recovered

random number (RRN1) with the fourth information retrieved from the fourth storage means;

transmitting the second anti-duplication variable authentication number (ADVAN2) from the second site to the first site, and receiving the ADVAN2 at the first site;

retrieving the first information associated with the first party from the first storage means;

uncoding the received ADVAN2 by using the retrieved first information to derive a second recovered random number (RRN2); and

authenticating the second party if the first random number (RN1) corresponds to the second recovered random number (RRN2).

123. The method of claim 122 wherein the first information stored in the first storage means is secret, and the second information stored in the second storage means is non-secret, and the third information stored in the third storage means is secret, and the fourth information stored in the fourth storage means is non-secret.

~~Sub 315~~ 124. A method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party, comprising the steps of:

receiving funds transfer information from the first party, including at least information for identifying the account of the first party, and information for identifying the account of the second party, and a transfer amount;

generating a variable authentication number (VAN) using at least a portion of the received funds transfer information;

determining whether the funds transfer information is authentic by using the VAN; and

transferring funds from the account of the first party to the account of the second party if the funds transfer information and the VAN are determined to be authentic.

125. The method of claim 124 further comprising:

receiving from the first party a personal identification number (PIN) or a password;

generating the VAN by using the PIN or the password, and at least a portion of the funds transfer information;

determining whether the first party is authentic by using the PIN or the password;

determining whether the funds transfer information is authentic by using the VAN; and

debiting the account of the first party and crediting the account of the second party with the funds transfer amount if the funds transfer information is determined to be authentic.

*126.43* The method of claim *124.41* wherein the funds transfer comprises a payment made by the first party to the second party.

*Sub 16* 127. The method of claim 124 wherein the VAN is used to confirm, substantiate, acknowledge, authorize, reference or verify the transfer of funds.

*Sub 16* 128. The methods of claim 124 wherein the VAN is generated by using an error detection code derived by using at least a portion of the funds transfer information.

129. A method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party, the transfer being controlled by a third party, comprising the steps of receiving funds transfer

information, including at least information for identifying the account of the first party, and information for identifying the account of the second party, and a transfer amount from the first party, and other funds transfer information from the third party;

generating a variable authentication number (VAN) using at least a portion of the received funds transfer information;

determining whether the funds transfer information is authentic by using the VAN; and

transferring funds from the account of the first party to the account of the second party, under the control of the third party, if the funds transfer information and the VAN are determined to be authentic.

130. The method of claim 129 further comprising: receiving from the first party a personal identification number (PIN) or a password;

generating the VAN by using the PIN or the password, and at least a portion of the funds transfer information;

determining whether the first party is authentic by using the PIN or the password;

determining whether the funds transfer information is authentic by using the VAN; and

debiting the account of the first party, and crediting  
the account of the second party with the funds transfer amount if  
the funds transfer information is determined to be authentic.

*121-53* 121. The method of claim *129-51* wherein the funds  
transfer comprises a payment made by the first party to the  
second party.

*122-53* 122. The methods of claim 129 wherein the VAN is  
used to confirm, substantiate, acknowledge, authorize, reference  
or verify the transfer of funds.

133. The methods of claim 129 wherein the VAN is  
generated by using an error detection code derived by using at  
least a portion of the funds transfer information.

*123-53* 134. A method for authenticating the transfer of  
funds from an account associated with a first party to an account  
associated with a second party, the transfer being carried out by  
a third party, comprising the steps of:

receiving funds transfer information, including at  
least information for identifying the account of the first party,

and information for identifying the account of the second party,  
and information for identifying the account of the third party,  
and a transfer amount;

generating a first variable authentication number  
(VAN1) using at least a portion of the received funds transfer  
information, the VAN1 being associated with the transfer of funds  
from the account of the third party to the account of the second  
party;

determining whether the funds transfer information is  
authentic by using VAN1;

transferring the funds from the account of the third  
party to the account of the second party if the funds transfer  
information and the VAN1 are determined to be authentic;

generating a second variable authentication number  
(VAN2) using at least a portion of the received funds transfer  
information, the VAN2 being associated with the transfer of funds  
from the account of the first party to the account of the third  
party;

determining whether the funds transfer information is  
authentic by using VAN2; and



transferring the funds from the account of the first party to the account of the third party if the funds transfer information and the VAN2 are determined to be authentic.

*Sub 69*  
135. The method of claim 134 further comprising:  
receiving from the first party a personal identification number (PIN) or a password;  
generating the VAN by using the PIN or the password, and at least a portion of the funds transfer information;  
determining whether the first party is authentic by using the PIN or the password;  
determining whether the funds transfer information is authentic by using the VAN; and  
debiting the account of the first party and crediting the account of the second party with the funds transfer amount if the funds transfer information is determined to be authentic.

*Sub 72*  
136. The method of claim 134 wherein the funds transfer comprises a payment made by the first party to the second party

*Sub E 10*  
137. The methods of claim 134 wherein the VAN1 or the VAN2 are used to confirm, substantiate, acknowledge, authorize, reference or verify the transfer of funds.

*Sub E 10*  
138. The methods of claim 134 wherein the VAN1 or the VAN2 are generated by using an error detection code derived by using at least a portion of the funds transfer information.

*Sub E 10*  
139. A method for authenticating and securing the integrity of relevant information transmitted from a first party at a first site to a second party at a second site by using first information associated with the first party, the first information comprising a secret first key, a non-secret second key, and credential information, the first information being previously stored in a first storage means at the first site, and the credential information including information for authenticating the identity of the first party, and information for securing the second key to the first party, the credential information being previously generated by a third party by using a secret third key during prior issuance of a credential to the first party, and a fourth non-secret key associated with the third party being previously stored in a second storage means at

the second site, and the first key being used by the first party  
to generate a variable authentication number (VAN), the VAN, the  
second key and the fourth key being used by the second party to  
authenticate the first party and the integrity of the relevant  
information received from the first party, the method comprising  
the steps of:

receiving relevant information from the first party;  
deriving a first error detection code (EDC1) by using  
the relevant information;

retrieving the first information previously stored in  
the first storage means;

coding the EDC1 with the retrieved first key to  
generate the variable authentication number (VAN);

forming a message including at least the VAN, the  
second key, the credential information, and the relevant  
information;

transmitting the message from the first party at the  
first site to the second party at the second site, and receiving  
the message at the second site;

extracting the VAN, the second key, the credential  
information, and the relevant information from the message at the  
second site;

retrieving the fourth key from the second storage means  
at the second site;

determining if the identity of the first party is  
secured to the second key by using the credential information,  
the second key, and the fourth key;

rejecting the message if the identity of the first  
party is determined not to be secured to the second key;

uncoding the VAN using the second key to recover the  
first error detection code (EDC1);

deriving a second error detection code (EDC2) by using  
the relevant information;

comparing the first error detection code (EDC1) with  
the second error detection code (EDC2); and

authenticating the first party and the integrity of the  
relevant information if the first error detection code (EDC1) and  
the second error detection code (EDC2) correspond.

140. The method of claim 139 wherein the relevant  
information and the second information associated with the second  
party are previously stored in the second storage means, the  
second information comprising a secret fifth key and a non-secret  
sixth key and credential information, the credential information

being previously generated by a third party by using the secret third key during prior issuance of a credential to the second party, and a fourth non-secret key associated with the third party being previously stored in the first storage means at the first site, the method comprising the additional steps of:

the second party retrieving the credential and the sixth key from the second storage means;

the second party transmitting a message comprising at least the credential information and the sixth key from the second site to the first site, and the message being received at the first site;

the first party extracting the credential and the sixth key from the received message;

retrieving the fourth key from the first storage means at the first site;

determining if the identity of the second party is secured to the sixth key by using the credential information and the sixth key and the fourth key;

rejecting the message if the identity of the second party is determined not to be secured to the sixth key;

receiving or generating the sensitive information;

coding the sensitive information with the sixth key to generate secure coded sensitive information;

transmitting the secure coded sensitive information from the first site to the second site, and receiving the secure coded sensitive information at the second site;

the second party retrieving the fifth key from the second storage means; and

uncoding the secure coded sensitive information using the fifth key to recover the sensitive information.

~~141.67~~

The method of claim ~~140~~<sup>64</sup> wherein the sensitive information comprises a session key being subsequently used by the first and second parties to code and uncode information transferred between the first and second sites.

~~142.~~

The method of claim 140 wherein the first party is granted access to the first key in the first storage means only if the identity of the first party is authenticated by using a personal identification number (PIN) or a password (PW) belonging to the first party, and the second party is granted access to the fifth key in the second storage means only if the

identity of the second party is authenticated by using a personal identification number (PIN) or a password (PW) belonging to the second party.

143. The method of claim 139 wherein the first party is granted access to the first key in the first storage means only if the identity of the first party is authenticated by using a personal identification number (PIN) or a password (PW) belonging to the first party, and the second party is granted access to the fifth key in the second storage means only if the identity of the second party is authenticated by using a personal identification number (PIN) or a password (PW) belonging to the second party.--

REMARKS

Claims 64-74 and 90-143 are pending in this application. Claims 75-89 were canceled. New claims 108-143 were added to further define the invention. These new claims are believed to be drawn to the subject matter of Group I and thus should be examined with the elected invention.

Respectfully submitted,

LEON STAMBLER

5/7/97

(Date)

BY:



Leslie L. Kasten, Jr.

Registration No. 28,959

PANITCH SCHWARZE JACOBS & NADEL, P.C.

1601 Market Street, 36th Floor

Philadelphia, PA 19103

Telephone: (215) 567-2020

Facsimile: (215) 567-2991

LLK:eam



69916 U.S. PTO



06/16/97

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.

BY Elizabeth A. McLeod DATE 6/13/97

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit: 2211  
Leon Stambler :  
Appln. No.: 08/747,174 : Examiner: B. Zimmerman  
Filed: November 12, 1996 :  
For: METHOD FOR SECURING :  
INFORMATION RELEVANT TO A : Attorney Docket  
TRANSACTION (as amended) : No. 6074-105

RECEIVED  
JUL 10 1997  
GROUP 2200

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

The Supplemental Information Disclosure Statement submitted herewith is being filed before the mailing date of a first Office Action on the merits. 37 CFR 1.97(b).

It is requested that the reference listed on the attached Information Citation Form PTO-1449 be considered by the Patent Examiner with the above-identified application and be made of record herein.

Independent consideration and acknowledgement of the listed reference is respectfully requested.

195JN2/102587.1

- 1 -

Respectfully submitted,

LEON STAMBLER

6/13/97

(Date)

BY: Clark Jablon

Clark A. Jablon

Registration No. 35,039

PANITCH SCHWARZE JACOBS & NADEL, P.C.

1601 Market Street, 36th Floor

Philadelphia, PA 19103

Telephone: (215) 567-2020

Facsimile: (215) 567-2991

CAJ:LLK:eam



69916 U.S. PTO



06/16/97 I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.

BY Elizabeth A. McLeod DATE 6/13/97

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit: 2211  
Leon Stambler :  
Appln. No.: 08/747,174 : Examiner: B. Zimmerman  
Filed: November 12, 1996 :  
For: METHOD FOR SECURING :  
INFORMATION RELEVANT TO A : Attorney Docket  
TRANSACTION (as amended) : No. 6074-1U5

RECEIVED  
JUL 10 1997  
GROUP 2200

THIRD SUPPLEMENTAL PRELIMINARY AMENDMENT

This correspondence is being filed before receipt of a first Office Action on the merits. Please enter this paper before substantive examination of elected claims 64-74 and 90-107 (claims 90-92 now cancelled in favor of new claims 144-146) and claims 108-143 filed May 7, 1997 which are believed to be drawn to the subject matter of Group I.

No fee is believed to be due for filing this paper. However, if any fee is due, please charge the fee to Deposit Account No. 16-0235.

PSJN2/102534.1

Please amend the above-identified application as follows, without prejudice:

In the Claims:

Amend the claims as follows:

*Sub 94*  
72. (Amended) A method for coding first information, the method comprising the step of:

coding the first information using second information and then coding the result using third information, [wherein] the second or third information [was] being previously generated [and stored] during an enrollment process, [and] wherein the second or third information are not derivable from each other, the second information being previously stored in a first storage means, the third information being previously stored in a second storage means, and the second or third information being retrieved solely by at least one predetermined party from the first or second storage means.

Cancel claims 90-92.

*Sub 99*  
105. (Twice Amended) In a computer system comprising a memory containing computer information stored in a controlled

27  
LP  
memory area to which access is granted only upon proper authentication of an authorized user of the computer system, the memory further including a stored control program for interacting with a user and for making a determination as to whether the user is an authorized user, the memory further including a first area, not readily accessible to a user, the first memory area containing a first revisable code and a second area containing a second revisable code, a method of authentication of a user comprising the steps of:

receiving in the computer system identification information associated with the user;

generating first coded authentication information using the received identification information associated with the user;

retrieving the first revisable code from the first memory area and the second revisable code from the second memory area and deriving therefrom second coded authentication information;

deriving a third revisable code using the retrieved first revisable code and the first coded authentication information;

22  
6  
Cmt  
comparing the retrieved second revisable code with  
the derived third revisable code;  
granting access to the computer information stored  
in the controlled memory area to the user only if the second and  
third revisable codes compare favorably.

108. (Amended) A method for authenticating a first  
party by using information stored in a credential, the credential  
being previously issued to the first party by a second party,  
wherein information previously stored in the credential comprises  
at least a variable authentication number (VAN) and other non-  
secret credential information, the method comprising the steps  
of:

3  
p  
0  
previously coding at least a portion of the other non-  
secret credential information with first information associated  
with the second party to derive a variable authentication number  
(VAN);

previously storing the VAN and the other non-secret  
credential information in the credential;

retrieving the VAN and the other non-secret credential  
information stored in the credential;

retrieving second information associated with the  
second party previously stored in a storage means associated with  
at least one of the parties;

uncoding the VAN using the second information  
associated with the second party to derive the at least a portion  
of the other non-secret credential information; and

authenticating the first party if the at least a  
portion of the other non-secret credential information retrieved  
from the credential corresponds to the at least a portion of the  
other non-secret credential information uncoded from the VAN.

110. (Amended) The method of claim 108 wherein the at  
least a portion of the other non-secret credential information  
comprises a name and a non-secret key associated with the first  
party.

111. (Amended) A method for issuing a credential to a  
first party by a second party, the method comprising the steps  
of:

the second party receiving non-secret information  
associated with the first party;



the second party authenticating at least a portion of the received non-secret information associated with the first party;

denying issuance of the credential if at least a portion of the received non-secret information associated with the first party is determined not to be authentic;

coding at least a portion of the received non-secret information associated with the first party with first information associated with the second party to derive a variable authentication number (VAN);

storing the VAN and at least a portion the received information associated with the first party, and other information associated with the second party, in the credential; and

issuing the credential to the first party.

112. (Amended) The method of claim 111 wherein at least a portion of the non-secret information associated with the first party comprises the name and a non-secret key associated with the first party.

24  
2  
113. (Amended) A method for authenticating a first party by using information stored in a credential, the credential being previously issued to the first party by a second party, wherein information previously stored in the credential comprises at least a variable authentication number (VAN) and other non-secret credential information, the method comprising the steps of:

2  
11.4  
previously generating a first error detection code (EDC1) by using at least a portion the other non-secret credential information[:];

previously coding the first error detection code (EDC1) with first information associated with the second party to derive a variable authentication number (VAN)[:];

previously storing the VAN and the other non-secret credential information in the credential;

retrieving the VAN and the other non-secret credential information stored in the credential;

deriving a second error detection code (EDC2) by using at least a portion of the retrieved other non-secret credential information;

EF  
10/1/13  
retrieving second information associated with the  
second party previously stored in a storage means associated with  
at least one of the parties;

uncoding the VAN using the second information  
associated with the second party to derive a third error  
detection code (EDC3); and

authenticating the first party and at least a portion  
of the non-secret information stored in the credential if the  
second error detection code (EDC2) corresponds to the third error  
detection code (EDC3).

115. (Amended) The method of claim 113 wherein the at  
least a portion of the other non-secret credential information  
comprises a name and a non-secret key associated with the first  
party.

116. (Amended) A method for issuing a credential to a  
first party by a second party, the method comprising the steps  
of:

the second party receiving non-secret information  
associated with the first party;

the second party authenticating at least a portion of the received non-secret information associated with the first party;

denying issuance of the credential if at least a portion of the received non-secret information associated with the first party is determined not to be authentic;

generating an error detection code (EDC) by using at least a portion the received non-secret information associated with the first party;

coding the error detection code (EDC) by using information associated with the second party to derive a variable authentication number (VAN);

storing the VAN and at least a portion the received non-secret information associated with the first party, and other information associated with the second party, in the credential; and

issuing the credential to the first party.

117. (Amended) The method of claim 116 wherein at least a portion of the non-secret information associated with the first party comprises the name and a non-secret key associated with the first party.

26 40 39  
119. (Amended) The method of claim 118 wherein after authentication occurs, the first party is authorized access to information or programs stored at the second site.

46 41  
128. (Amended) The method[s] of claim 124 wherein the VAN is generated by using an error detection code derived by using at least a portion of the funds transfer information.

31 17  
129. (Amended) A method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party, the transfer being controlled by a third party, the method comprising the steps of:  
receiving funds transfer information, including at least information for identifying the account of the first party, and information for identifying the account of the second party, and a transfer amount from the first party, and other funds transfer information from the third party;  
generating a variable authentication number (VAN) using at least a portion of the received funds transfer information;  
determining whether the funds transfer information is authentic by using the VAN; and

transferring funds from the account of the first party to the account of the second party, under the control of the third party, if the funds transfer information and the VAN are determined to be authentic.

130. (Amended) The method of claim 129 further comprising the steps of:

receiving from the first party a personal identification number (PIN) or a password;

generating the VAN by using the PIN or the password, and at least a portion of the funds transfer information;

determining whether the first party is authentic by using the PIN or the password;

determining whether the funds transfer information is authentic by using the VAN; and

debiting the account of the first party, and crediting the account of the second party with the funds transfer amount if the funds transfer information is determined to be authentic.

132. (Amended) The method[s] of claim 129 wherein the VAN is used to confirm, substantiate, acknowledge, authorize, reference or verify the transfer of funds.

55  
133. (Amended) The method[s] of claim 129 wherein the VAN is generated by using an error detection code derived by using at least a portion of the funds transfer information.

9  
135. (Amended) The method of claim 134 further comprising:  
receiving from the first party a personal identification number (PIN) or a password;  
generating the [VAN] VAN2 by using the PIN or the password, and at least a portion of the funds transfer information;  
determining whether the first party is authentic by using the PIN or the password;  
determining whether the funds transfer information is authentic by using the [VAN] VAN2; and  
debiting the account of the first party and crediting the account of the second party with the funds transfer amount if the funds transfer information is determined to be authentic.

137. (Amended) The method[s] of claim 134 wherein the VAN1 or the VAN2 are used to confirm, substantiate, acknowledge, authorize, reference or verify the transfer of funds.

10  
2  
1004  
138. (Amended) The method[s] of claim 134 wherein the  
VAN1 or the VAN2 are generated by using an error detection code  
derived by using at least a portion of the funds transfer  
information.

Add new claims 144-146 as follows:

11  
2  
Sub 125  
--144. A method of issuing a credential to a first  
party at a first site, by a second party at a second site,  
wherein the first party is authenticated during at least one  
stage of a subsequent transaction by using the credential,  
wherein the information stored in the credential comprises at  
least a first variable authentication number VAN1, information  
for identifying the first party, a non-secret key associated with  
the first party, and information for identifying the second  
party, and first and second storage means at the first site, the  
first storage means being used to store a secret key associated  
with the first party, the secret key being accessible only to a  
party with knowledge of a pre-determined personal identification  
number (PIN) or password, the second storage means being used to  
store the non-secret key associated with the first party, and  
third and fourth storage means at the second site, the third  
storage means being used to store a secret key associated with



the second party, the secret key being accessible only to a pre-authorized party, the fourth storage means being used to store a non-secret key associated with the second party, the method comprising the steps of:

11  
receiving information for identifying the first party, and a pre-determined personal identification number (PIN) or password, from the first party;

retrieving the secret key associated with the first party from the first storage means, only if the personal identification number (PIN) or password, is determined to be authentic;

generating a second variable authentication number VAN2 by coding at least a portion of the information for identifying the first party with the secret key associated with the first party;

retrieving the non-secret key associated with the first party from the second storage means;

forming a message including at least the VAN2, the non-secret key associated with the first party, and the information for identifying the first party;

transmitting the message from the first party at the first site to the second party at the second site, and receiving the message at the second site;

extracting the VAN2, the non-secret key associated with the first party, and the information for identifying the first party from the message at the second site;

using at least a portion of the information for identifying the first party to authenticate the identity of the first party;

denying issuance of the credential if at least a portion of the information for identifying the first party is determined not to be authentic;

retrieving the secret key associated with the second party from the third storage means at the second site;

generating a first variable authentication number VAN1 by coding the second variable authentication number VAN2 with the secret key associated with the second party;

storing in the credential at least the VAN1, the non-secret key associated with the first party, at least a portion of the information for identifying the first party, and information for identifying the second party;

11  
7  
10  
4  
11

issuing the credential to the first party,  
wherein the method for authenticating the first party and the  
credential during at least one state of a subsequent transaction,  
comprising the steps of:  
retrieving the information previously stored in the  
credential;  
receiving the non-secret key associated with the first  
party and the non-secret key associated with the second party;  
uncoding the first variable authentication number VAN1  
using the non-secret key associated with the second party to  
generate a second variable authentication number VAN2;  
uncoding the second variable authentication number VAN2  
using the non-secret key associated with the first party to  
recover information for identifying the first party;  
authenticating the credential, and the first party who  
was issued the credential, if the information for identifying the  
first party retrieved from the credential corresponds to the  
information for identifying the first party recovered from the  
second variable authentication number VAN2.

145. <sup>71</sup> The method of claim <sup>70</sup> 144 wherein the non-secret  
key associated with the second party is retrieved from the fourth

-16-

61

storage means and stored in the credential, prior to issuing the credential.

*146*  
*146* The method of claim 144 wherein prior to the step of denying issuance of the credential if at least a portion of the information for identifying the first party is determined not to be authentic, the method comprising the additional steps of:

uncoding the second variable authentication number VAN2 by using the non-secret key associated with the first party to recover the at least a portion of the information for identifying the first party; and

comparing the recovered at least a portion of the information for identifying the first party with the at least a portion of the information for identifying the first party extracted from the received message.--

#### REMARKS

Claims 64-74 and 93-146 are pending in this application. Claims 72, 105, 108, 110-113, 115-117, 119, 128-130, 132, 133, 135, 137 and 138 were amended to further define the invention and/or to improve their form. Claims 90-92 were

17-  
*62*

canceled and their subject matter was incorporated into new  
claims 144-146.

Respectfully submitted,

LEON STAMBLER

6/13/97

(Date)

BY: Clark A. Jablon

Clark A. Jablon

Registration No. 35,039

PANITCH SCHWARZE JACOBS & NADEL, P.C.

1601 Market Street, 36th Floor

Philadelphia, PA 19103

Telephone: (215) 567-2020

Facsimile: (215) 567-2991

CAJ:LLK:eam



UNITED STATES DEPARTMENT OF COMMERCE  
Patent and Trademark Office

Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, DC 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/747,174	11/12/96	STAMBLER	L 6074-1-U5

82M1/0812  
PANITCH SCHWARZE JACOBS & NADEL  
1601 MARKET STREET  
36TH FLOOR  
PHILADELPHIA PA 19103-2398

EXAMINER  
ZIMMERMAN, B

ART UNIT	PAPER NUMBER
2211	12

DATE MAILED: 08/12/97

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

<b>Office Action Summary</b>	Application No. <b>08/747,174</b>	Applicant(s) <b>Stambler</b>
	Examiner <b>Brian Zimmerman</b>	Group Art Unit <b>2211</b>

☒ Responsive to communication(s) filed on Jun 16, 1997

☐ This action is **FINAL**.

☐ 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.

A shortened statutory period for response to this action is set to expire 3 month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

**Disposition of Claims**

☒ Claim(s) 64-74 and 93-146 is/are pending in the application.

Of the above, claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

☐ Claim(s) \_\_\_\_\_ is/are allowed.

☒ Claim(s) 64-74 and 93-146 is/are rejected.

☐ Claim(s) \_\_\_\_\_ is/are objected to.

☐ Claims \_\_\_\_\_ are subject to restriction or election requirement.

**Application Papers**

☒ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on \_\_\_\_\_ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on \_\_\_\_\_ is ☐ approved ☐ disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. § 119**

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some\* ☐ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) \_\_\_\_\_.

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\*Certified copies not received: \_\_\_\_\_

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

**Attachment(s)**

☐ Notice of References Cited, PTO-892

☒ Information Disclosure Statement(s), PTO-1449, Paper No(s). 3

☐ Interview Summary, PTO-413

☒ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

— SEE OFFICE ACTION ON THE FOLLOWING PAGES —

### **DOUBLE PATENTING REJECTION**

1. The non-statutory double patenting rejection, whether of the obviousness-type or non-obviousness-type, 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. *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); and *In re Goodman*, 29 USPQ2d 2010 (Fed. Cir. 1993).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(b) and © may be used to overcome an actual or provisional rejection based on a non-statutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.78(d).

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).

2. Claims 64-74, 93-146 are rejected under the judicially created doctrine of double patenting over claims 1-19 of U. S. Patent No. 5524073 or alternatively claims 1-22 of U. S. Patent No. 5267314, since the claims, if allowed, would improperly extend the "right to exclude" already granted in the patent.

The subject matter claimed in the instant application is fully disclosed in the patent and is covered by the patent since the patent and the application are claiming common subject matter, as follows: secure authorization technique.

Furthermore, there is no apparent reason why applicant was prevented from presenting claims corresponding to those of the instant application during prosecution of the application which matured into a patent. *In re Schneller*, 397 F.2d 350, 158



08/17714  
2211

3

USPQ 210 (CCPA 1968). See

#### **ART REJECTION**

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

5 (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10

4. Claims 64-74,93-146 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman. Hellman shows the multi-party secure transaction system as is claimed. See the abstract, figure 1, and col. 2 lines 53+. Hellman shows the secure method of transmitting information which is to be sent between the communicating parties. It is verily well known to send coded information or noncoded information (digital or analog) between stations in an encrypted manner, and here by claiming both, the applicant has effectively shown that this is not essential to the operation of the claimed device. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have send coded or noncoded information over the Hellman system since this information is verily common in the art at the time of the invention.

20

5. Claims 64-74,93-146 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maurer. Maurer clearly shows the multi-party secure transaction system which

08/717714  
2211

4

is claimed. Maurer shows the secure method of transmitting information which is to be sent between the communicating parties. It is verily well known to send coded information or noncoded information (digital or analog) between stations in an encrypted manner, and here by claiming both, the applicant has effectively shown that  
5 this is not essential to the operation of the claimed device. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have send coded or noncoded information over the Maurer system since this information is verily common in the art at the time of the invention.

It is noted that Maurer states also, the invention can be applied in any situation  
10 in which two parties have store a string of related digits. This, taken in context with the description of the prior art (by Maurer) suggests that Maurer was implying that his invention can also be used when the string of digits stored in the stations was related. The implication offered by Maurer is that the invention can be used if the strings ( $S_a$ ,  $S_b$ ) are related or are unrelated. Maurer discusses the strings as digits "selected" from  
15 a finite alphabet col. 5 line 40 , the suggestion of the relationship discussed on col. 5 lines 20+ is merely exemplary, not necessary. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have the strings ( $S_a$ ,  $S_b$ ) be unrelated to each other since it is known that un-related encryption codes increase the secure nature of the coded information.

20

08/717714  
2211

5

**OTHER PRIOR ART CITED**

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

5

**CONTACT INFORMATION**

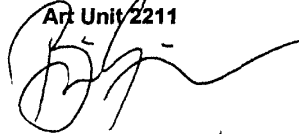
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brian Zimmerman whose telephone number is (703) 305-4796.

10 Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-4900.

15

703-305-4796  
August 11, 1997

Brian Zimmerman  
Patent Examiner  
Art Unit 2211



Attachment 12

The drawings submitted with this application were declared informal by the applicant. Accordingly they have not been reviewed by a draftsman at this time. When formal drawings are submitted, the draftsman will perform a review.

Direct any inquiries concerning drawing review to the Drawing Review Branch (703) 305-8404.

Substitute PTO-948



**UNITED STATES DEPARTMENT OF COMMERCE**  
**Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231

SERIAL NUMBER	FILING DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NO.
08/747,174	11/12/96	STAMBLER	L 6074-1-U5

B2M1/1027  
PANITCH SCHWARZE JACOBS & NADEL  
1601 MARKET STREET  
36TH FLOOR  
PHILADELPHIA PA 19103-2398

EXAMINER	
ZIMMERMAN, B	
ART UNIT	PAPER NUMBER
2211	13

DATE MAILED: 10/27/97

Please find below a communication from the EXAMINER in charge of this application.

Commissioner of Patents

<b>Interview Summary</b>	Application No. <b>08/747,174</b>	Applicant(s) <b>Stambler</b>
	Examiner <b>Brian Zimmerman</b>	Group Art Unit <b>2211</b>

All participants (applicant, applicant's representative, PTO personnel):

(1) Brian Zimmerman (3) \_\_\_\_\_

(2) Clark Jabalon (4) \_\_\_\_\_

Date of Interview Oct 24, 1997

Type: ☒ Telephonic ☐ Personal (copy is given to ☐ applicant ☐ applicant's representative).

Exhibit shown or demonstration conducted: ☐ Yes ☒ No. If yes, brief description: \_\_\_\_\_

Agreement ☐ was reached. ☐ was not reached.

Claim(s) discussed: \_\_\_\_\_

Identification of prior art discussed: \_\_\_\_\_

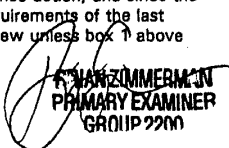
Description of the general nature of what was agreed to if an agreement was reached, or any other comments:  
The IDS filed 6/16/97 has been considered however it does not effect the merit of the rejection in the Office Action dated 8/12/97.

(A fuller description, if necessary, and a copy of the amendments, if available, which the examiner agreed would render the claims allowable must be attached. Also, where no copy of the amendments which would render the claims allowable is available, a summary thereof must be attached.)

1. ☐ It is not necessary for applicant to provide a separate record of the substance of the interview.

Unless the paragraph above has been checked to indicate to the contrary, A FORMAL WRITTEN RESPONSE TO THE LAST OFFICE ACTION IS NOT WAIVED AND MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP Section 713.04). If a response to the last Office action has already been filed, APPLICANT IS GIVEN ONE MONTH FROM THIS INTERVIEW DATE TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW.

2. ☐ Since the Examiner's interview summary above (including any attachments) reflects a complete response to each of the objections, rejections and requirements that may be present in the last Office action, and since the claims are now allowable, this completed form is considered to fulfill the response requirements of the last Office action. Applicant is not relieved from providing a separate record of the interview unless box 1 above is also checked.

  
**BRIAN ZIMMERMAN**  
**PRIMARY EXAMINER**  
**GROUP 2200**

Examiner Note: You must sign and stamp this form unless it is an attachment to a signed Office action.

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: ASSISTANT COMMISSIONER OF PATENTS, WASHINGTON, DC 20231, ON THE DATE INDICATED BELOW.



DATE: 11/7/97

PATENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re: Patent Application of : Group Art Unit 2211  
Leon Stambler :  
Serial No.: 08/747,174 : Examiner: B. Zimmerman  
Filed: November 12, 1996 :  
For: METHOD FOR SECURING : Attorney Docket  
INFORMATION RELEVANT TO A : No. 6074-1U5  
TRANSACTION (as amended)

**NOTICE OF CHANGE OF ADDRESS**

Please change the correspondence address of the attorneys of record in the above-identified patent application as follows:

**Panitch Schwarze Jacobs & Nadel, P.C.  
One Commerce Square  
2005 Market Street - 22nd Floor  
Philadelphia, PA 19103-7086**

The corresponding attorney and the telephone number are as indicated below.

Respectfully submitted,

November 7, 1997  
(Date)

By:

Clark A. Jablon  
**CLARK A. JABLON**  
Registration No. 35,039  
**PANITCH SCHWARZE JACOBS & NADEL, P.C**  
One Commerce Square  
2005 Market Street - 22nd Floor  
Philadelphia, PA 19103-7086  
Telephone: 215-965-1293  
Facsimile: 215-567-2991  
E-Mail: psjn@psjn.com

CAJ:eam

NOV 10 1997  
TYPE  
PATENT & TRADEMARK  
In re

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**AMENDMENT**

In the Claims:

11/21/1997 HARRISON 00000000 BAN:160235 00747174  
01 FC:202 02.00 CH  
02 FC:203 206.00 CH

-1-



Amend claims 64, 66, 67, 69, 70, 72-74, 93, 95-98, 100-108, 110-113, 115-118, 124-125, 127, 129-130, 132-140, 142-144 and 146 as follows:

~~64.~~ (Amended) A method for coding and storing information, comprising information associated with a party and other sensitive information, said information associated with a party being subsequently used to authenticate the party and authorize access, the method comprising [the steps of]:

previously receiving a first personal identification number (PIN<sub>1</sub>) from the party;  
previously deriving or accessing first coded authentication information by using the first PIN<sub>1</sub>;  
previously generating at least two numbers using the first coded authentication information, wherein at least one of the at least two numbers is an arbitrary number;  
previously storing each of the at least two numbers in one or more [first] storage means;  
[previously storing each of the at least two numbers in one or more second storage means;]  
retrieving each of the at least two numbers previously stored in the [first] one or more storage means;  
[retrieving each of the at least two numbers previously stored in the second one or more storage means;  
comparing each of the at least two numbers retrieved from the first one or more storage means with each of the at least two numbers retrieved from the second one or more storage means; and

authorizing access if each of the at least two numbers retrieved from the first one or more storage means and each of the at least two numbers retrieved from the second one or more storage means correspond to each other]

receiving a second personal identification number (PIN2) from a party to be authenticated;

deriving or accessing second coded authentication information by using the second PIN2;

combining each of the at least two numbers retrieved from the one or more storage means to derive third coded authentication information;

comparing the second coded authentication information with the third coded authentication information; and

authenticating the party and authorizing access if the second coded authentication information and third coded authentication information correspond to each other.

~~65.2~~ (Amended) The method of claim [65] ~~64~~<sup>1</sup> further comprising [the step of]:

coding said other sensitive information with said first or second or third coded authentication information to derive coded sensitive information.

~~65.3~~ (Amended) The method of claim [65] ~~64~~<sup>1</sup> further comprising [the step of]:

uncoding said coded sensitive information with said second or third coded authentication information to recover the other sensitive information.

~~5.4~~ (Amended) The method of claim ~~6.1~~ further comprising [the steps of]:

revising each of the at least two numbers at an arbitrary time; and

replacing each of the previous at least two numbers in the [first and second] one or more storage means with each of the revised at least two numbers.

~~7.5~~ (Amended) The method of claim ~~6.1~~ wherein at least [one of each of the at least two numbers is stored in the first] a first of the one or more storage means [and at least another of each of the at least two numbers is stored in the second one or more storage means, wherein the first and second one or more storage means are located at first and second respective sites] is located at a first site, and a second of the one or more storage means is located at a second site.

~~7.7~~ (Twice Amended) A method for coding first information, the method comprising [the step of]:

coding the first information using second information and then coding the result using third information, [the second or third information being previously generated during an enrollment process, wherein the second or third information are not derivable from each other, the second information being previously stored in a first storage means, the third information being previously stored in a second storage means, and the second or third information being retrieved solely by at least one predetermined party from the first or second storage means] at least one of the second and third information

184  
Amended

being associated with at least one entity; the entity comprising a person or a computer program, wherein a credential having non-secret information stored therein is previously issued to at least one entity by a trusted entity, the non-secret information including the second or third information.

15

73.8 (Amended) In a multi-party transaction system, a method for securing information relevant to a transaction, the method comprising [the steps of]:

coding the information relevant to the transaction using first information associated with a party to generate first coded transaction information;

coding the first coded transaction information using second information associated with more than one party to generate second coded transaction information, wherein [the first information associated with a party and the second information associated with more than one party are not derivable from each other] a credential having non-secret information stored therein is previously issued to at least one of the parties by a trusted party, the non-secret information including the first or second information.

24.9 (Amended) The method of claim 73.8 [wherein the] further comprising recovering information relevant to the transaction [is recovered comprising the steps of] by:

uncoding the second coded transaction information using the second information associated with the more than one party to recover the first coded transaction information; and

15  
2204

uncoding the first coded transaction information  
using third information associated with [a] the party to recover  
the information relevant to the transaction.

8

---

~~28~~<sup>10</sup> (Amended) A method for securing in escrow[,] and  
in trust, [information] a joint key associated with a first party  
and a second party and stored in a storage means associated with  
[a] the second party, wherein [at least a portion of the]  
escrowed or entrusted information [may be] was previously used  
for generating a [joint key, wherein] variable authentication  
number (VAN), the joint key [is] being derivable from information  
associated with the first party and information associated with  
[a] the second party, the VAN being subsequently used in  
authenticating the first party, the first party being enrolled by  
the second party and being issued a credential, the VAN being  
stored in the credential, the method comprising [the steps of]:

previously receiving information associated with  
the first party and information associated with the second party;

previously generating a joint key using the  
information associated with the first party, and the information  
associated with the second party; and

retaining in the storage means, in trust, at least  
the [information associated with the first party and the  
information associated with the second party which was previously  
used to generate the] joint key.

8

---

~~28~~<sup>11</sup> (Amended) The method of claim ~~25~~<sup>10</sup> wherein the  
second party is an agent, or an agency, or an official of an

117

agency, or an authority, or an administrator, or an entity entrusted with issuing [a] the credential.

1  
X  
su.4  
96. <sup>W</sup> (Amended) A method for enrolling and issuing a credential to a first party by a second party, and subsequently granting the first party access to a first storage means, [or other thing,] wherein the first party has a first personal identification number (PIN1), and the second party [has a second personal identification number (PIN2),] is previously granted authority to issue a credential to the first party. the first storage means, [or other thing,] being accessible only to a party with knowledge of the first PIN1 [or with knowledge of the second PIN2], the method of enrollment and issuing a credential comprising [the steps of]:

receiving information associated with the first party;

receiving information associated with the second party; [and]

storing in escrow and in trust the information associated with the first party and the information associated with the second party in a second storage means, wherein at least a portion of the information retrieved [subsequently] from the second storage means is used in enrolling the first party and issuing the credential; and

subsequently granting the first party access to the first storage means[, or other thing] by using the PIN1 or the credential.

~~97.~~<sup>13</sup> (Amended) The method of claim ~~96~~<sup>12</sup> wherein the second storage means is accessible for storing information therein only by a party with knowledge of [the] a second PIN (PIN2) known to at least the second party, such that if no party exists with knowledge of the second (PIN2), then information cannot be stored in the second storage means.

1  
J  
Amended  
98.<sup>14</sup> (Amended) A method for enrolling a first party by a second party, and subsequently granting the first party access to a first storage means, [or other thing,] wherein the first party has a first personal identification number (PIN1), and the second party has a second personal identification number (PIN2), the first storage means, [or other thing,] being accessible only to a party with knowledge of the first PIN1 or with knowledge of the second PIN2, the method of enrollment comprising [the steps of]:

receiving information associated with the first party;

receiving information associated with the second party;

coding the information associated with the first party and the information associated with the second party to generate a joint code; [and]

storing the joint code and the information associated with the second party in a second storage means[, wherein]; and

subsequently receiving and using PIN1 or PIN2, and retrieving and using the joint code and the information associated with the second party [retrieved subsequently from the

7  
2nd  
second storage means are used] in granting the first party access to the first storage means[, or other thing].

16  
100. (Amended) A method for granting a first party access to a first storage means, [or other thing,] subsequent to being enrolled by a second party, wherein the first party has a personal identification number (PIN), and wherein information associated with the second party was previously stored during enrollment in a second storage means, and a first joint code was previously generated and stored during enrollment in the second storage means, wherein the joint code was previously generated by using first coded authentication information derived or accessed from the personal identification number (PIN) of the first party and information associated with the second party, the method comprising [the steps of]:

receiving a personal identification number (PIN) from the first party and generating or accessing second coded authentication information using the PIN;

retrieving from the second storage means the information associated with the second party, and the first joint code;

coding the second coded authentication information and the information associated with the second party to generate a second joint code;

comparing the first joint code and the second joint code; and

granting the first party access to the first storage means, [or other thing,] if the first joint code corresponds to the second joint code.



101.17 (Amended) A method for authenticating a first party at first site by a second party at a second site and granting [a] the first party access to a first storage means at a second site, [or other thing, subsequent to being enrolled by a second party,] the second party being a person or a computer program, wherein the first party has a personal identification number (PIN), and wherein first information associated with the second party [was previously] is generated and stored [during enrollment] in a second storage means associated with the second party at the second site, and wherein first coded information previously derived or accessed by using the PIN of the first party was previously stored [during enrollment] in the second storage means, the method comprising [the steps of]:

generating the first information, and storing the first information in the second storage means;

receiving the PIN from the first party and  
deriving or accessing second coded information by using the PIN;

retrieving from the second storage means the first information [associated with the second party], [and] the first information being previously derived or accessed by using the PIN;

coding the first coded information previously derived or accessed by using the PIN and the first information associated with the second party to generate a first joint code;

coding the second coded information derived or accessed by using the PIN and the first information associated with the second party to generate a second joint code;

comparing the first joint code and the second joint code; and

authenticating the first party by the second party, and granting the first party access to the first storage means, [or other thing,] if the first joint code corresponds to the second joint code.

*102. 22* (Amended) In a computer system comprising a memory containing computer information or a first computer program stored in a controlled memory area to which access is granted only upon proper authentication of an authorized user of the computer system, the user including a person or a second computer program, the memory further including a stored control program for interacting with [a] the user and for making a determination as to whether the user is an authorized user, the memory further including a first area[, ] not readily accessible to a user, the first [memory] area containing a first revisable code, and a second area containing a second revisable code, a method of authentication of a user comprising [the steps of]:

receiving in the computer system identification information associated with the user;

generating or accessing first coded authentication information using the received identification information associated with the user;

retrieving the first revisable code from the first memory area and the second revisable code from the second memory area and deriving therefrom second coded authentication information;

comparing the first coded authentication information with the second coded authentication information;

authenticating the user, and granting access to  
the computer information or a first computer program stored in  
the controlled memory area to the user only if the first and  
second coded authentication information compare favorably.

8  
X  
103<sup>23</sup> (Amended) The method as recited in claim ~~102~~<sup>22</sup>  
further comprising [the step of] revising and storing the first  
and second revisable codes in the original respective memory  
areas only if the first and second coded authentication  
information compare favorably.

104<sup>24</sup> (Amended) The method as recited in claim ~~103~~<sup>23</sup>  
wherein computer information stored in the memory of the computer  
system may be reproduced, the method further comprising [the  
steps of]:

previously recording the second revisable code  
with the computer information to be reproduced;  
permitting the computer information to be  
reproduced only if the access has been granted to the user; and  
thereafter retrieving the second revisable code  
retrieved from the reproduced information and using the second  
revisable code to authenticate the user if the reproduced  
information is used or accessed.

9  
X  
105<sup>25</sup> (Three Times Amended) In a computer system  
comprising a memory containing computer information or a first  
computer program stored in a controlled memory area to which  
access is granted only upon proper authentication of an  
authorized user of the computer system, the user including a

*9*  
*claim 4*  
person or a second computer program. the memory further including a stored control program for interacting with a user and for making a determination as to whether the user is an authorized user, the memory further including a first area[,] not readily accessible to a user, the first [memory] area containing a first revisable code, and a second area containing a second revisable code, a method of authentication of a user comprising [the steps of]:

receiving in the computer system identification information associated with the user;

generating or accessing first coded authentication information using the received identification information associated with the user;

retrieving the first revisable code from the first memory area and the second revisable code from the second memory area [and deriving therefrom second coded authentication information];

deriving a third revisable code using the retrieved first revisable code and the first coded authentication information;

comparing the retrieved second revisable code with the derived third revisable code;

authenticating the user and granting access to the computer information or first computer program stored in the controlled memory area to the user only if the second and third revisable codes compare favorably.

*10*  
~~106.~~<sup>26</sup> (Amended) The method as recited in claim ~~105~~<sup>25</sup>  
further comprising [the step of] revising and storing the first

and second revisable codes in the original respective memory areas only if the second and third revisable codes compare favorably.

<sup>27</sup>  
~~187.~~ (Amended) The method as recited in claim <sup>25</sup>~~185~~ wherein computer information stored in the memory of the computer system may be reproduced, the method further comprising [the steps of]:

previously recording the second revisable code with the computer information to be reproduced;

permitting the computer information to be reproduced only if the access has been granted to the user; and

thereafter retrieving the second revisable code retrieved from the reproduced information and using the second revisable code to authenticate the user if the reproduced information is used or accessed.

---

<sup>28</sup>  
~~188.~~ (Three Times Amended) A method for authenticating a first party by using information stored in a credential, the credential being previously issued to the first party by a second party, wherein information previously stored in the credential comprises at least a non-secret variable authentication number (VAN) and other non-secret credential information, the method comprising [the steps of]:

previously irreversibly coding at least a portion of the other non-secret credential information to derive an irreversibly coded number, and further coding the irreversibly coded number with first information associated with the second party to derive a variable authentication number (VAN);

previously storing the VAN and the other non-secret credential information in the credential;

retrieving the VAN and the other non-secret credential information stored in the credential;

retrieving second information associated with the second party previously stored in a storage means associated with at least one of the parties;

uncoding the VAN using the second information associated with the second party to derive the [at least a portion of the other non-secret credential information] irreversibly coded number; and

authenticating the first party if the irreversibly coded number derived from at least a portion of the other non-secret credential information retrieved from the credential corresponds to the [at least a portion of the other non-secret credential information] irreversibly coded number uncoded from the VAN.

~~110.~~<sup>30</sup> (Twice Amended) The method of claim ~~100~~<sup>28</sup> wherein the at least a portion of the other non-secret credential information comprises [a name and] a non-secret key associated with the first party.

~~111.~~<sup>31</sup> (Twice Amended) A method for issuing a credential to a first party by a second party, the method comprising [the steps of]:

the second party receiving non-secret information associated with the first party;

the second party authenticating at least a portion of the received non-secret information associated with the first party;

denying issuance of the credential if at least a portion of the received non-secret information associated with the first party is determined not to be authentic;

coding at least a portion of the received non-secret information associated with the first party with first information associated with the second party to derive a variable authentication number (VAN);

storing in the credential the VAN and at least a portion of the received non-secret information associated with the first party, and other information associated with the second party[, in the credential]; and

issuing the credential to the first party.

~~112~~<sup>32</sup> (Twice Amended) The method of claim ~~111~~<sup>31</sup> wherein at least a portion of the non-secret information associated with the first party comprises [the name and] a non-secret key associated with the first party.

~~113~~<sup>33</sup> (Twice Amended) A method for authenticating a first party by using information stored in a credential, the credential being previously issued to the first party by a second party, wherein information previously stored in the credential comprises at least a non-secret variable authentication number (VAN) and other non-secret credential information, the method comprising [the steps of]:

previously generating a first error detection code (EDC1) by using at least a portion the other non-secret credential information;

previously coding the first error detection code (EDC1) with first information associated with the second party to derive a variable authentication number (VAN);

previously storing the VAN and the other non-secret credential information in the credential;

retrieving the VAN and the other non-secret credential information stored in the credential;

deriving a second error detection code (EDC2) by using at least a portion of the retrieved other non-secret credential information;

retrieving second information associated with the second party previously stored in a storage means associated with at least one of the parties;

uncoding the VAN using the second information associated with the second party to derive a third error detection code (EDC3); and

authenticating the first party and at least a portion of the non-secret information stored in the credential if the second error detection code (EDC2) corresponds to the third error detection code (EDC3).

115. <sup>35</sup> (Twice Amended) The method of claim <sup>33</sup> 113 wherein the at least a portion of the other non-secret credential information comprises [a name and] a non-secret key associated with the first party.



~~116~~<sup>36</sup>. (Twice Amended) A method for issuing a credential to a first party by a second party, the method comprising [the steps of]:

the second party receiving non-secret information associated with the first party;

the second party authenticating at least a portion of the received non-secret information associated with the first party;

denying issuance of the credential if at least a portion of the received non-secret information associated with the first party is determined not to be authentic;

generating an error detection code (EDC) by using at least a portion the received non-secret information associated with the first party;

[coding the error detection code (EDC) by using information associated with the second party to derive a variable authentication number (VAN);]

storing in the credential the [VAN] EDC and at least a portion the received non-secret information associated with the first party, and other information associated with the second party[, in the credential]; and

issuing the credential to the first party.

~~117~~<sup>37</sup>. (Twice Amended) The method of claim ~~116~~<sup>36</sup> wherein at least a portion of the non-secret information associated with the first party comprises [the name and] a non-secret key associated with the first party.

116. (Amended) A method for authenticating a first party at a first site by a second party at a second site, the second party being a person or a computer program, by using a personal identification number (PIN) [or a password (PW)] supplied by the first party at the first site, and further using a first random number (RN1) generated by the second party at the second site, the PIN [or password (PW)] being previously used to derive or access first coded authentication information, the first coded authentication information being previously stored in a storage means associated with the second party at the second site, the method comprising [the steps of]:

receiving a PIN [or a password (PW)] at the first site from a first party to be authenticated;

generating or accessing second coded authentication information using the received PIN [or password (PW)];

generating a first random number (RN1) at a second site by the second party;

storing the first random number (RN1) in the second storage means at the second site;

transmitting the first random number (RN1) from the second site to the first site;

receiving the first random number (RN1) at the first site by the first party;

coding the received first random number (RN1) and the second coded authentication information to derive a first anti-duplication variable authentication number (ADVAN1);

transmitting the first anti-duplication variable authentication number (ADVAN1) from the first site to the second site;

receiving the first anti-duplication variable authentication number (ADVAN1) at the second site by the second party;

retrieving the first coded authentication information from the storage means at the second site;

coding the first random number (RN1) and the first coded authentication information to generate a second anti-duplication variable authentication number (ADVAN2);

comparing the first anti-duplication variable authentication number (ADVAN1) and the second anti-duplication variable authentication number (ADVAN2); and

authenticating the first party by the second party if the first anti-duplication variable authentication number (ADVAN1) and the second anti-duplication variable authentication number (ADVAN2) correspond.

~~224.~~<sup>41</sup> (Amended) A method for authenticating the transfer of funds from [an] a first account associated with a first party to [an] a second account associated with a second party, the first account information being stored in a first storage means, and the second account information being stored in a second storage means, the method comprising [the steps of]:

receiving funds transfer information from the first party, including at least information for identifying the first account of the first party, and information for identifying the second account of the second party, and a transfer amount;

generating a variable authentication number (VAN) using at least a portion of the received funds transfer information;

a third party for determining whether the at least a portion of the received funds transfer information is authentic by using the VAN; and

transferring funds from the first account of the first party to the second account of the second party if the at least a portion of the received funds transfer information and the VAN are determined to be authentic.

<sup>42</sup>  
~~125.~~ (Amended) The method of claim ~~124~~<sup>41</sup> further comprising [the steps of]:

receiving from the first party [a personal identification number (PIN) or a password;] information for identifying the first party;

[generating the VAN by using the PIN or the password, and at least a portion of the funds transfer information;]

determining whether the first party is authentic by using the [PIN or the password;] information for identifying the first party;

determining whether the at least a portion of the received funds transfer information is authentic by using the VAN; and

debiting the first account of the first party and crediting the second account of the second party with the funds transfer amount if the at least a portion of the received funds transfer information is determined to be authentic.

<sup>45</sup>  
~~127.~~ (Amended) The method of claim ~~124~~<sup>41</sup> wherein the VAN is used to confirm, substantiate, acknowledge, authorize, reference, validate or verify the transfer of funds.

~~129~~<sup>51</sup> (Twice Amended) A method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party, [the transfer being controlled by a third party], a credential being previously issued to at least one of the parties by a trusted party, the information stored in the credential being non-secret, the method comprising [the steps of]:

receiving funds transfer information, including at least information for identifying the account of the first party, and information for identifying the account of the second party, and a transfer amount [from the first party, and other funds transfer information from the third party];

generating a variable authentication number (VAN) using at least a portion of the received funds transfer information;

determining whether the at least a portion of the received funds transfer information is authentic by using the VAN and the credential information; and

transferring funds from the account of the first party to the account of the second party [, under the control of the third party,] if the at least a portion of the received funds transfer information and the VAN are determined to be authentic.

~~130~~<sup>52</sup> (Twice Amended) The method of claim ~~129~~<sup>51</sup> further comprising [the steps of]:

receiving from the first party [a personal identification number (PIN) or a password] information for identifying the first party;

[generating the VAN by using the PIN or the password, and at least a portion of the funds transfer information;]

determining whether the first party is authentic by using the [PIN or the password] information for identifying the first party;

determining whether the at least a portion of the received funds transfer information is authentic by using the VAN; and

debiting the account of the first party, and crediting the account of the second party with the funds transfer amount if the at least a portion of the received funds transfer information is determined to be authentic.

---

~~132~~<sup>54</sup> (Twice Amended) The method of claim ~~132~~<sup>57</sup> wherein the VAN is used to confirm, substantiate, acknowledge, authorize, reference, validate or verify the transfer of funds.

---

~~57~~<sup>57</sup> ~~134~~<sup>57</sup> (Amended) A method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party, at least a part of the transfer being carried out by a third party, comprising [the steps of]:

receiving funds transfer information, including at least information for identifying the account of the first party, and information for identifying the account of the second party, and information for identifying the account of the third party, and a transfer amount;

generating a first variable authentication number (VAN1) using at least a portion of the received funds transfer information, the VAN1 being associated with the transfer of funds

from the account of the third party to the account of the second party;

determining whether the at least a portion of the received funds transfer information is authentic by using VAN1;

transferring the funds from the account of the third party to the account of the second party if the at least a portion of the received funds transfer information and the VAN1 are determined to be authentic;

generating a second variable authentication number (VAN2) using at least a portion of the received funds transfer information, the VAN2 being associated with the transfer of funds from the account of the first party to the account of the third party;

determining whether the at least a portion of the received funds transfer information is authentic by using VAN2; and

transferring the funds from the account of the first party to the account of the third party if the at least a portion of the received funds transfer information and the VAN2 are determined to be authentic.

<sup>58</sup>  
~~125.~~ (Amended) The method of claim ~~124~~<sup>59</sup> further comprising:

receiving from the first party [a personal identification number (PIN) or a password] information for identifying the first party;

[generating the VAN2 by using the PIN or the password, and at least a portion of the funds transfer information;]

determining whether the first party is authentic by using the [PIN or the password] information for identifying the first party;

determining whether the at least a portion of the received funds transfer information is authentic by using the VAN2; and

debiting the account of the first party and crediting the account of the [second] third party with the funds transfer amount if the at least a portion of the received funds transfer information [is] and the VAN2 are determined to be authentic.

136.57 (Amended) The method of claim 134.57 wherein the funds transfer comprises a payment made by the first party or the third party to the second party.

137.60 (Amended) The method of claim 134.57 wherein the VAN1 or the VAN2 are used to confirm, substantiate, acknowledge, authorize, reference, validate or verify the transfer of funds.

138.61 (Amended) The method of claim 134.57 wherein the VAN1 or the VAN2 are each generated by using an error detection code derived by using at least a portion of the funds transfer information.

139.63 (Amended) A method for authenticating and securing the integrity of relevant information transmitted from a first party at a first site to a second party at a second site by using first information associated with the first party, the first information comprising a secret first key, a non-secret



second key, and first credential information, the first information being previously stored in a first storage means at the first site, and the first credential information [including] comprising non-secret information [for authenticating the identity of the first party, and information] for securing the second key to the first party, the first credential information including a third error detection code (EDC3) being previously [generated] stored in the first credential by a third party [by using a secret third key] during prior issuance of [a] the first credential to the first party, [and a fourth non-secret key associated with the third] and the second key associated with the first party being previously stored in a second storage means at the second site, and the first key being used by the first party to generate a first variable authentication number (VAN1), the VAN1[,] and the second key [and the fourth key] being used by the second party to authenticate the first party and the integrity of the relevant information received from the first party, the method comprising [the steps of]:

receiving relevant information from the first party;  
deriving a first error detection code (EDC1) by using the relevant information;  
retrieving the first information previously stored in the first storage means;  
coding the EDC1 with the retrieved first key to generate the first variable authentication number (VAN1);  
forming a first message including at least the VAN1, [the second key,] the first credential information, and the relevant information;

transmitting the first message from the first party at the first site to the second party at the second site, and receiving the first message at the second site;

extracting the VAN<sub>1</sub>, [the second key,] the first credential information, and the relevant information from the first message at the second site;

retrieving the [fourth] second key from the second storage means at the second site;

determining if [the identity of] the first party is secured to the second key by using the first credential information[, the second key, and the fourth key] and the third error detection code (EDC3);

rejecting the first message if the [identity of the] first party is determined not to be secured to the second key;

uncoding the VAN<sub>1</sub> using the second key to recover the first error detection code (EDC1);

deriving a second error detection code (EDC2) by using the relevant information;

comparing the first error detection code (EDC1) with the second error detection code (EDC2); and

authenticating the first party and the integrity of the relevant information if the first error detection code (EDC1) and the second error detection code (EDC2) correspond.

<sup>140.64</sup> (Amended) The method of claim <sup>63</sup> 139 wherein [the relevant information and the] second information associated with the second party [are] is previously stored in the second storage means, the second information comprising a secret [fifth] third key and a non-secret [sixth] fourth key and second credential

information, the second credential information including a fourth error detection code (EDC4) being previously [generated] stored in the second credential by a third party [by using the secret third key] during prior issuance of [a] the second credential to the second party, [and a fourth non-secret key associated with the third party] and the non-secret fourth key being previously stored in the first storage means at the first site, the method further comprising [the additional steps of]:

the second party retrieving the second credential [and the sixth key] information from the second storage means;

the second party transmitting a second message comprising at least the second credential information [and the sixth key] from the second site to the first site, and the second message being received at the first site;

the first party extracting the second credential [and the sixth key] information from the received second message;

retrieving the [sixth] fourth key from the first storage means at the first site;

determining if [the identity of] the second party is secured to the [sixth] fourth key by using the second credential information and [the sixth key and the fourth key] the fourth error detection code (EDC4);

rejecting the second message if the [identity of the] second party is determined not to be secured to the [sixth] fourth key;

receiving or generating [the] sensitive information;

coding the sensitive information with the [sixth] fourth key to generate secure coded sensitive information;

transmitting the secure coded sensitive information  
from the first site to the second site, and receiving the secure  
coded sensitive information at the second site;

the second party retrieving the [fifth] third key from  
the second storage means; and

uncoding the secure coded sensitive information using  
the [fifth] third key to recover the sensitive information.

23  
24  
142.<sup>68</sup> (Amended) The method of claim 140<sup>64</sup> wherein the  
first party is granted access to the first key in the first  
storage means only if the identity of the first party is  
authenticated by using a personal identification number (PIN) [or  
a password (PW)] belonging to the first party, and the second  
party is granted access to the [fifth] third key in the second  
storage means only if the identity of the second party is  
authenticated [by using a personal identification number (PIN) or  
a password (PW) belonging to the second party].

143.<sup>65</sup> (Amended) The method of claim 139<sup>63</sup> wherein the  
first party is granted access to the first key in the first  
storage means only if the identity of the first party is  
authenticated by using a personal identification number (PIN) [or  
a password (PW)] belonging to the first party[, and the second  
party is granted access to the fifth key in the second storage  
means only if the identity of the second party is authenticated  
by using a personal identification number (PIN) or a password  
(PW) belonging to the second party].

~~144~~<sup>70</sup> (Amended) A method of issuing a credential to a first party at a first site, by a second party at a second site, wherein the first party is authenticated during at least one stage of a subsequent transaction by using the credential, wherein the information stored in the credential comprises at least a first variable authentication number VAN1, information for identifying the first party, a non-secret key associated with the first party, and information for identifying the second party, and first and second storage means at the first site, the first storage means being used to store a secret key associated with the first party, the secret key being accessible [only] to a party with knowledge of a pre-determined personal identification number (PIN) ~~or password~~, the second storage means being used to store the non-secret key associated with the first party, and third and fourth storage means at the second site, the third storage means being used to store a secret key associated with the second party, the secret key being accessible [only] to [a pre-] an authorized party, the fourth storage means being used to store a non-secret key associated with the second party, the method comprising [the steps of]:

receiving information for identifying the first party, and a pre-determined personal identification number (PIN) [or password,] from the first party;

retrieving the secret key associated with the first party from the first storage means, only if the personal identification number (PIN) [or password,] is determined to be authentic;

coding at least a portion of the information for identifying the first party to derive a first error detection code (EDC1):

generating a second variable authentication number VAN2 by coding [at least a portion of the information for identifying the first party] the EDC1 with the secret key associated with the first party;

retrieving the non-secret key associated with the first party from the second storage means;

forming a message including at least the VAN2, the non-secret key associated with the first party, the EDC1, and the information for identifying the first party;

transmitting the message from the first party at the first site to the second party at the second site, and receiving the message at the second site;

extracting the VAN2, the non-secret key associated with the first party, the EDC1, and the information for identifying the first party from the message at the second site;

using at least a portion of the information for identifying the first party to authenticate the identity of the first party;

denying issuance of the credential if at least a portion of the information for identifying the first party is determined not to be authentic;

retrieving the secret key associated with the second party from the third storage means at the second site;

generating a first variable authentication number VAN1 by coding the second variable authentication number VAN2 with the secret key associated with the second party;

-31-

storing in the credential at least the VAN1, the EDC1,  
the non-secret key associated with the first party, [at least a  
portion of the information for identifying the first party,] and  
information for identifying the second party;

issuing the credential to the first party;  
wherein the method for authenticating the first party and the  
credential during at least one [state] stage of a subsequent  
transaction, [comprising] comprises [the steps of]:

retrieving the information previously stored in the  
credential;

receiving or retrieving the non-secret key associated  
with the first party and the non-secret key associated with the  
second party;

uncoding the first variable authentication number VAN1  
using the non-secret key associated with the second party to  
[generate a] recover the second variable authentication number  
VAN2;

uncoding the second variable authentication number VAN2  
using the non-secret key associated with the first party to  
recover [information for identifying the first party] the EDC1;

authenticating the credential, and the first party who  
was issued the credential, if the [information for identifying  
the first party] EDC1 retrieved from the credential corresponds  
to the [information for identifying the first party] EDC1  
recovered from the second variable authentication number VAN2.

---

<sup>14672</sup>(Amended) The method of claim 144 wherein prior  
to [the step of] denying issuance of the credential if at least a  
portion of the information for identifying the first party is

determined not to be authentic, the method further comprising [the additional steps of]:

uncoding the second variable authentication number VAN2 by using the non-secret key associated with the first party to recover the [at least a portion of the information for identifying the first party] EDC1; [and]

comparing the recovered [at least a portion of the information for identifying the first party] EDC1 with the [at least a portion of the information for identifying the first party] EDC1 extracted from the received message; and

denying issuance of the credential if the extracted EDC1 and the recovered EDC1 do not match.

C  
Add new claims 147-179 as follows:

--~~147~~<sup>73</sup> A method for determining if an unauthorized duplication or alteration occurred in first transaction information (FXI) and in second transaction information (SXI), the FXI being originated by a second entity at a second site, and being transmitted to a first entity at a first site, the first entity and the second entity being a person, or a computer program, and the SXI being originated at the first site and being combined with the FXI to form first combined transaction information (FCX) at the first site, an anti-duplication variable authentication number (ADVAN1) being derived from the FCX and first information (FK1) associated with the first entity, the FK1 being previously stored in a first storage means at the first site and being solely accessible to the first entity, the ADVAN1, and the SXI being transmitted from the first site to the second site, the FXI and the SXI being authenticated at the second site, ✓

-33-

9/1



by using the ADVAN1, FXI, SXI, and second information (FK2) associated with the first entity, the FK2 being previously stored in a second storage means at the second site, a first transaction record storage means (FXR) being used at the first site, and a second transaction record storage means (SXR) being used at the second site, the FXR and SXR being used to store at least the FXI and the SXI, the method comprising:

generating or receiving first transaction information (FXI) at the second site, and storing the FXI in the second transaction record (SXR) storage means at the second site;

transmitting the FXI from the second site to the first site, and receiving the FXI at the first site;

storing the FXI in the first transaction record (FXR) storage means at the first site;

generating or receiving second transaction information (SXI) at the first site;

storing the SXI in the FXR storage means at the first site;

combining the FXI and the SXI to form first combined transaction information (FCX);

retrieving the first information (FK1) associated with the first entity from the first storage means, the FK1 being accessible only to the first entity;

coding the FCX with the retrieved FK1 to derive a first anti-duplication variable authentication number (ADVAN1);

transmitting the first anti-duplication variable authentication number (ADVAN1) and the SXI, from the first site to the second site, and receiving the ADVAN1 and the SXI at the second site;

storing the received ADVAN1 and the SXI in the SXR storage means at the second site; and

the second entity subsequently using the ADVAN1, the FXI, the SXI, and second information (FK2) associated with the first entity to determine if an unauthorized duplication or alteration occurred in the first transaction information (FXI) or in the second transaction information (SXI).

74  
148. The method of claim 147 wherein coding the FCX to derive the ADVAN1 further comprises:

irreversibly coding the FCX to derive a first error detection code (EDC1);

storing the EDC1 in the FXR storage means; and  
coding the EDC1 with the first information (FK1) associated with the first entity to derive the first anti-duplication authentication number (ADVAN1).

76  
149. The method of claim 147 wherein the first entity is authenticated by the second entity, and wherein the FXI comprises a first random number (RN1), and the SXI comprises a second random <sup>number</sup> variable (RN2).

77  
150. The method of claim 147 wherein FXI and SXI are both present.

75  
151. The method of claim 148 for further authenticating the integrity of the FXI, and for further authenticating the first entity by the second entity, the method further comprising:

retrieving the FXI, the SXI, and the ADVAN1 from the SXR storage means at the second site;  
retrieving the second information (FK2) associated with the first entity from the second storage means;  
uncoding the ADVAN1 by using the FK2 to recover the first error detection code (EDC1);  
combining the retrieved FXI and the retrieved SXI to form a second combined transaction information (SCX);  
irreversibly coding the second combined transaction information (SCX) to derive a second error detection code (EDC2);  
storing the second error detection code (EDC2) in the SXR storage means at the second site;  
comparing the recovered first error detection code (EDC1) and the derived second error detection code (EDC2); and  
the second entity (1) authenticating the first entity and determining that no unauthorized duplication or alteration occurred in first transaction information (FXI) if the recovered EDC1 and the derived EDC2 correspond; or (2) denying authentication to the first entity or determining that an unauthorized duplication or alteration occurred in first transaction information (FXI) if the recovered EDC1 and the derived EDC2 do not correspond.

182. The method of claim 147<sup>73</sup> for further determining if an unauthorized duplication or alteration occurred in the SXI, and for further authenticating the second entity by the first entity, by using a second anti-duplication variable identification number (ADVAN2) derived by the second entity, the

ADVAN2 being derived at the second site from the EDC2 and third information (SK3) associated with the second entity, the SK3 being previously stored in a third storage means at the second site, the SXI and the second entity being authenticated by the first entity by using the ADVAN2, the SXI, the FXI, and fourth information (SK4) associated with the second entity, the SK4 being previously stored in a fourth storage means at the first site, the method further comprising:

retrieving the second error detection code (EDC2) from the SXR storage means;

retrieving the third information (SK3) associated with the second entity from the third storage means at the second site;

coding the EDC2 with the SK3 to derive a second anti-duplication variable authentication number (ADVAN2);

transmitting the ADVAN2 from the second site to the first site, and receiving the ADVAN2 at the first site;

storing the ADVAN2 in the FXR storage means;

retrieving fourth information (SK4) associated with the second entity from the fourth storage means at the first site;

retrieving the ADVAN2 from the FXR storage means;

uncoding the ADVAN2 by using the SK4 to recover the second error detection code (EDC2);

retrieving the FXI, and the SXI from the FXR storage means;

combining the retrieved FXI and the retrieved SXI to form a third combined transaction information (TCX);

irreversibly coding the TCX to derive a third  
error detection code (EDC3);  
storing the third error detection code (EDC3) in  
FXR storage means;

comparing the derived third error detection code  
(EDC3) and the recovered second error detection code (EDC2); and  
the first entity (1) authenticating the second  
entity and determining that no unauthorized duplication, or  
alteration, occurred in ~~first~~ <sup>the second</sup> transaction information (FXI) <sup>SX1</sup> if  
the derived EDC3 and the recovered EDC2 correspond, or (2)  
denying authentication to the second entity or determining that  
an unauthorized duplication, or alteration, occurred in ~~first~~ <sup>the second</sup>  
transaction information (FXI) <sup>SX1</sup> if the derived EDC3 and the  
recovered EDC2 do not correspond.

<sup>79</sup>  
~~153~~. The method of claim ~~147~~ <sup>73</sup> for further securing  
the first and second information associated with the first entity  
to the first entity by using a credential previously issued to  
the first entity by a trusted entity, the information stored in  
the credential including at least the first or second information  
associated with the first entity, and a first variable  
authentication number (VAN1), the VAN1 being used to secure the  
first or second information to the first entity, authentication  
being denied if the first or second information associated with  
the first entity cannot be secured to the first entity by using  
VAN1.

<sup>80</sup>  
~~154~~. The method of claim ~~147~~ <sup>73</sup> for further securing  
the third and fourth information associated with the second

-38--

entity to the second entity by using a credential previously issued to the second entity by a trusted entity, the information stored in the credential including at least the third or fourth information associated with the second entity, and a second variable authentication number (VAN2), the VAN2 being used to secure the third or fourth information to the second entity, authentication being denied if the third or fourth information associated with the second entity cannot be secured to the second entity by using VAN2.

81/ 185. The method of claim 73 wherein the first entity has a personal identification number (PIN), the PIN being used to access the FK1 information stored in the first storage means, the method further comprising:

receiving a personal identification number (PIN) supplied by the first entity at the first site; and

retrieving the first information associated with the first entity from the first storage means only if the PIN of the first entity is determined to be authentic.

82/ 186. The method of claim 73 wherein a transaction number (XN) is used in conjunction with the FXI or the SXI to identify and retrieve transaction information from a storage means associated with an entity participant in a transaction, the method further comprising:

generating an XN at one of the first or second sites, and transmitting the XN to the other of the first or second sites;

storing the XN in the FXR storage means and SXR storage means associated with the transaction;

using the XN to identify the transaction, and as an index in retrieving relevant transaction information.

157.<sup>83</sup> The method of claim ~~147~~<sup>73</sup> wherein one of the first and second information associated with the first entity is secret, and the other of the first and second information associated with the first entity is non-secret.

158.<sup>84</sup> The method of claim ~~147~~<sup>73</sup> wherein one of the third and fourth information associated with the second entity is secret, and the other of the third and fourth information associated with the second entity is non-secret.

159.<sup>85</sup> The method of claim ~~147~~<sup>73</sup> wherein the same key, or either one of RN1 or RN2, is used subsequent to authentication, by each of the first and second entities to code and uncode information transmitted between the sites.

160.<sup>86</sup> The method of claim ~~147~~<sup>73</sup> for further authenticating the participation of the first entity in a transaction by a third entity at a third site, wherein the FXI comprises the XN and fifth information associated with the first entity, the fifth information being previously stored in a fifth storage means at the first site and also in a seventh storage means at the third site, and second information associated with the third entity being previously stored in sixth storage means at the first site, and first information associated with the

third entity being previously stored in an eighth storage means at the third site, the method further comprising:

retrieving the fifth information associated with the first entity from the fifth storage means at the first site;  
retrieving the XN from the FXR storage means;  
combining the XN and the fifth information to form a first information group (IG1);

irreversibly coding IG1 to derive a fourth error detection code (EDC4);

retrieving the second information associated with the third entity from the sixth storage means at the first site;  
coding the EDC4 with the second information associated with the third entity to derive a third anti-duplication authentication number (ADVAN3);

transmitting the ADVAN3 and the XN from the first site to the third site, and receiving the ADVAN3 and the XN at the third site;

retrieving the first information associated with the third entity from the eighth storage means at the third site;  
uncoding the ADVAN3 by using the first information associated with the third entity to recover the EDC4;

retrieving the fifth information from the seventh storage means at the third site;

combining the received XN and the fifth information to form a second information group (IG2);

irreversibly coding the IG2 to derive a fifth error detection code (EDC5);

comparing EDC4 and EDC5; and



authenticating the participation of the first entity in the transaction if the EDC4 and EDC5 match, or determining that the entity did not participate in the transaction if the EDC4 and EDC5 do not match.

87 73  
161. The method of claim 147 wherein the FXI is made secure in transmitting the FXI from the second site to the first site by coding the FXI with third information associated with the first entity to derive coded FXI, the third information associated with the first entity being previously stored in a ninth storage means at the second site, and by uncoding the coded FXI by using fourth information associated with the first entity, the fourth information associated with the first entity being previously stored in a tenth storage means at the first site, the method further comprising:

retrieving the third information associated with the first entity from the ninth storage means at the second site;

coding the FXI with the third information associated with the first entity to derive a coded FXI at the second site;

transmitting the coded FXI from the second site to the first site, and receiving the coded FXI at the first site;

retrieving the fourth information associated with the first entity from the tenth storage means at the first site; and

uncoding the coded FXI by using fourth information associated with the first entity to recover the FXI at the first site.

21  
cont.

~~162~~<sup>18</sup>. The method of claim ~~101~~<sup>17</sup> wherein the second party is authenticated by the first party, wherein third information associated with the first party is generated and stored in a third storage means at the first site, and fourth information associated with the second party was previously stored in the third storage means, and fifth information associated with the second party was previously stored in a fourth storage means at a second site, the method further comprising:

generating the third information associated with the first party;  
storing the third information in the third storage means;  
retrieving the third information associated with the first party, and the fifth information associated with the second party;  
coding the fifth information and the third information to generate a third joint code;  
retrieving the fourth information associated with the second party;  
uncoding the third joint code using the fourth information to recover the third information;  
comparing the generated third information and the recovered third information; and  
authenticating the second party if the generated third information corresponds to the recovered third information.

~~163~~<sup>19</sup>. The method of claim ~~162~~<sup>18</sup> wherein a credential previously issued to the second party by a trusted party is used

by the first party to verify that the fourth information is secured to the second party.

27  
X  
C  
(  
164.<sup>20</sup> The method of claim 162<sup>18</sup> wherein the first information associated with the second party, and the third information associated with the first party each comprise a random number.

165.<sup>38</sup> The method of claim 164<sup>36</sup> further comprising:  
coding the error detection code (EDC) by using first information associated with the second party to derive a variable authentication number (VAN), and  
storing the VAN in the credential.

166.<sup>88</sup> A method for authenticating a first party at a first site by a second party at a second site, the second party being a person or a computer program, by using a personal identification number (PIN) supplied by the first party at the first site, and further using a first random number (RN1) generated by the second party at the second site, the PIN being previously used to derive or access first coded authentication information, the first coded authentication information being previously stored in a storage means associated with the second party at the second site, the method comprising:

receiving a PIN at the first site from a first party to be authenticated;

generating or accessing second coded authentication information using the received PIN;

generating a first random number (RN1) at a second site by the second party;

storing the first random number (RN1) in the second storage means at the second site;

transmitting the first random number (RN1) from the second site to the first site;

receiving the first random number (RN1) at the first site by the first party;

coding the received first random number (RN1) and the second coded authentication information to derive a first anti-duplication variable authentication number (ADVAN1), the first anti-duplication variable authentication number (ADVAN1) further being derived by irreversibly coding the received first random number (RN1) to derive a first error detection code (EDC1), and coding the first error detection code (EDC1) with the second coded authentication information to thereby derive the first anti-duplication variable authentication number (ADVAN1);

transmitting the first anti-duplication variable authentication number (ADVAN1) from the first site to the second site;

receiving the first anti-duplication variable authentication number (ADVAN1) at the second site by the second party;

retrieving the first coded authentication information from the storage means at the second site;

uncoding the received first anti-duplication variable authentication number (ADVAN1) by using the first coded authentication information to recover the first error detection code (EDC1);

retrieving the first random number (RN1) from the storage means at the second site;

irreversibly coding the retrieved first random number (RN1) to derive a second error detection code (EDC2);

comparing the first error detection code (EDC1) and the second error detection code (EDC2); and

authenticating the first party by the second party if the first error detection code (EDC1) and the second error detection code (EDC2) correspond.

*7/27/94*  
*g*  
*second*  
*g*  
<sup>47</sup>167. The method of claim <sup>41</sup>124 for further securing the transfer of funds, at least one party being previously issued a credential by a trusted party, the credential information including information associated with the at least one party, and a variable authentication number (VAN), the VAN being used to secure at least a portion of the credential information to the at least one party, authentication and the transfer of funds being denied to the at least one party if the at least a portion of the credential information cannot be secured to the at least one party by using the VAN.

<sup>66</sup>168. The method of claim <sup>63</sup>139 wherein a second variable authentication number (VAN2) is stored in the first credential during prior issuance of the first credential, the VAN2 being generated by coding the EDC3 with a third secret key associated with the third party, and wherein a fourth non-secret key associated with the third party is previously stored in the second storage means at the second site, the fourth key being used by the second party to authenticate the first credential

information, and following the step of retrieving the second key from the second storage means at the second site, the method further comprising:

retrieving the fourth key from the second storage means at the second site;

extracting the EDC3 and the VAN2 from the first credential information in the received first message;

uncoding the VAN2 using the fourth key to recover the third error detection code (EDC3);

determining if the extracted EDC3 and the recovered EDC3 correspond;

rejecting the first message if the extracted EDC3 and the recovered EDC3 do not correspond.

169. The method of claim 164 wherein a third variable authentication number (VAN3) is stored in the second credential during prior issuance of the second credential, the VAN3 being generated by coding the EDC4 with a third secret key associated with the third party, and a fourth non-secret key associated with the third party being previously stored in the first storage means at the first site, the fourth key being used by the first party to authenticate the second credential information, and following the step of retrieving the fourth key from the first storage means at the first site, the method further comprising:

retrieving the fourth key from the first storage means at the first site;

extracting the EDC4 and the VAN3 from the second credential information in the received second message;

-47-

uncoding the VAN3 using the fourth key to recover  
the fourth error detection code (EDC4);

determining if the extracted EDC4 and the  
recovered EDC4 correspond;

rejecting the second message if the extracted EDC4  
and the recovered EDC4 do not correspond.

170<sup>48</sup>. The method of claim 124<sup>41</sup> wherein the first party  
and the second party are the same party.

171<sup>49</sup>. The method of claim 120<sup>48</sup> wherein the second  
storage means comprises a credential.

172<sup>50</sup>. The method of claim 124<sup>41</sup> wherein the first  
storage means comprises a credential, and the second storage  
means comprises a credential.

173<sup>44</sup>. The method of claim 126<sup>43</sup> wherein prior to  
payment being made to the second party, the first party is  
presented with the second party's invoice, and after the payment  
is made to second party, the accounts receivable associated with  
the second party, and the accounts payable associated with the  
first party are updated.

174<sup>21</sup>. The method of claim 162<sup>18</sup> wherein the third  
information associated with the second party, and the fourth  
information associated with the first party, each comprise a  
random number.

175<sup>56</sup>. The method of claim ~~123~~<sup>51</sup> for further securing the transfer of funds, at least one party being previously issued a credential by a trusted party, the credential information including information associated with the at least one party, and a ~~variable~~<sup>second</sup> authentication number (VAN~~0~~), the VAN~~1~~ being used to secure at least a portion of the credential information to the at least one party, authentication and the transfer of funds being denied to the at least one party if the at least a portion of the credential information cannot be secured to the at least one party by using the VAN~~0~~.

176<sup>62</sup>. The method of claim ~~134~~<sup>57</sup> for further securing the transfer of funds, at least one party being previously issued a credential by a trusted party, the credential information including information associated with the at least one party, and a variable authentication number (VAN~~2~~), the VAN~~3~~ being used to secure at least a portion of the credential information to the at least one party, authentication and the transfer of funds being denied to the at least one party if the at least a portion of the credential information cannot be secured to the at least one party by using the VAN~~2~~.

177<sup>87</sup>. In a check or payment instrument transaction system, a method for issuing a check or payment instrument by an originator to a recipient, information associated with the check or payment instrument comprising (1) information associated with the originator, (2) information associated with the recipient, and (3) other information which includes at least an amount of the check or payment instrument, the method comprising:



receiving the information associated with the  
originator and the recipient, and the other information including  
at least the amount;

deriving a variable authentication number (VAN) using  
at least a portion of the received information;

associating the received information and the VAN with  
the check or payment instrument; and

issuing the check or payment instrument.

*178.90* The method of claim *177.89* wherein the check or  
payment instrument is authenticated by using at least a portion  
of the information associated with the check or payment  
instrument and the VAN.

*179.91* A method for securing in escrow and in trust, a  
portion of information used to derive a joint key, the joint key  
being associated with a first party and a second party and being  
stored in a storage means associated with the second party,  
wherein escrowed or entrusted information was previously used for  
generating a variable authentication number (VAN), the joint key  
being derivable from information associated with the first party  
and information associated with the second party, the VAN being  
subsequently used in authenticating the first party, the first  
party being enrolled by the second party and being issued a  
credential, the VAN being stored in the credential, the method  
comprising:

previously receiving information associated with  
the first party and information associated with the second party;

127  
previously generating a joint key using the  
information associated with the first party, and the information  
associated with the second party; and  
retaining in the storage means, in trust, at least  
a portion of information used to derive the joint key.--

**REMARKS**

Claims 64, 66, 67, 69, 93, 95-119 and 124-179 are pending in this application. Claims 64-69, 70, 72-74, 93, 95-98, 100-108, 110-113, 115-118, 124-125, 127, 129-130, 132-140, 142-144 and 146 were amended to improve their form. Furthermore, claims 72, 73, 93, 96, 98, 124 and 129 were amended to more particularly point out, and distinctly claim the invention. Claims 65, 68, 94 and 120-123 were canceled. Claim 64 was further amended to incorporate the limitations of claim 65 therein. New claims 147-179 are presented to further define the invention. Withdrawal of all pending rejections is respectfully requested for the reasons set forth below.

**Status of Application Drawings**

The Examiner is requested to review the Submission of Proposed Drawing Amendment filed on November 12, 1997, and to forward the formal drawings filed on November 12, 1997 for review by the Draftsperson. The outstanding Office Action does not indicate that either of these papers were received or reviewed.

**Double patenting rejection**

-51-

NO page 52

(2) PINS - The present invention also includes the feature of using a personal identification number (PIN) to execute transactions. As described in part on page 3, line 28 through page 4, line 3, each user selects a PIN upon enrollment in the system. The PIN is secret, does not exist in an uncoded form, and cannot be recovered from other information anywhere in the system. During or after enrollment, a non-secret identification code and a secret code are also stored in a user's file at the user associated computer facility. When a user participates in a transaction, the user is required to utilize his or her PIN, which after being coded is used to derive a coded arbitrary number. Subsequently, this arbitrary code is compared to another such code which is generated from a reconstituted version of the coded PIN, in order to authenticate the user's identity. The PIN is another important feature of the present invention which minimizes the vulnerability of the system to imposters and the like.

The use of a PIN is recited in independent claims 64, 96, 98, 100, 101, 118, 144 and 166.

(3) multiple revisable owner codes - Fig. 6 discloses the generation of a revisable owner code (ROC). To generate an ROC, a PIN is received from a party. The PIN is coded to produce a coded PIN (CPN). The CPN is then coded using a predetermined arbitrary number to produce the ROC. The predetermined arbitrary number and the ROC are stored in a storage means at a location associated with the party, wherein the CPN is derivable from the predetermined arbitrary number and the ROC.

As discussed in part on page 12, line 29 through page 13, line 3, security considerations may warrant revising the ROC

from time to time independent of any transaction. To accomplish this task (i.e., to create multiple revisable codes), the CPN could be reconstituted from the current ROC and RN as in block 52 of Fig. 8B. Next, a new RN is used with the CPN to generate a revised ROC, making use of a coder in the same manner as coder 20 of Fig. 6. The user's new RN and ROC are stored and accessed, and CPN need only be reproduced at the bank where the user maintains an account.

The use of multiple revisable codes to authenticate a user is recited in independent claims 102 and 105.

(4) Use of a third party to authenticate a VAN and transfer of funds, and use of originator, recipient and payment information to derive a VAN.

When a transaction, document or thing needs to be authenticated, information associated with at least one of the parties involved (e.g., an originator and/or a recipient) is coded to produce a joint code. This joint code is then utilized to code information relevant to the transaction, document or record, in order to produce a variable authentication number (VAN) or code at the initiation of the transaction. This VAN is thereafter associated with the transaction and is recorded on the document or thing, along with the original information that was coded. During subsequent stages of the transaction, only parties capable of reconstructing the joint code will be able to uncode the VAN properly in order to re-derive the information.

As described in part on page 48, lines 1-27, the present invention may be used as paperless/cashless transaction system, in which "funds transfer" transactions, such as purchases, occur without the use of money, or checks. In this

system, the payment originator uses a payment recipient's terminal which stores information to identify the precise location of the recipient's account. Alternatively, an originator PIN, information identifying an originator account and a recipient account, and funds transfer information (INFO) which includes a payment amount are entered directly into a terminal of this system by the payment originator. The system initially generates a VAN, (OVAN), by using the payment information (INFO) in conjunction with the identification information associated with the payment originator and payment recipient. The payment originator is authenticated using the originator PIN using a method described above. The system then approves or disapproves the payment based upon an authentication of the VAN, and the "joint" identification information associated with the participants, and the availability of funds, or credit. Such transactions are carried on entirely electronically, the participant's bank accounts are credited and debited automatically..."

In this scheme, the payment originator is a first party, the recipient is a second party, and the system which approves or disapproves the payment is a third party.

The use of a third party to authenticate a VAN and transfer of funds is recited in claim 124. The use of originator, recipient and payment information to derive a VAN is recited in claim 177.

(5) Securing a joint key, or a portion of information used to derive the joint key, in escrow or in trust -

This feature is related to the credential issuance process described in Fig. 11 and is described in part on page 23, lines 1-26, as follows:

The issuing process continues with the official entering his PIN, which is applied to an irreversible coder 140 to produce his CPNO, which is applied as a key input to an uncoder 142. At block 144, the official's TIN, OTIN is utilized as an index to access the official's "File 1", so that CPKO may be read therefrom and applied as the input to uncoder 142. Uncoder 142 therefore performs the same process as uncoder 114 of Fig. 10 to produce PKO. At block 146, PKO and UTIN are utilized as address indices to access the official's "File 2" and JKU is read therefrom. The information INFO on the credential is applied as the data input to a coder 152 and JKU is applied as the key input, whereby coder 152 codes the INFO to produce a VAN, which is recorded on the credential. After recording the VAN on the credential, the joint key, JKU, may be erased from the official's File 2, where it was stored (*or held in escrow or in trust*), until the credential was issued. Alternately, the authentic JKU may be replaced with a false or dummy JK for security purposes. This completes the issuance of the credential 145. It should be noted that the joint key JKU stored in the official's File No. 2 can only be used in a transaction if a party exists with knowledge of the official's PIN, since this PIN is required to access the official's File No. 2 (at block 146). Thus, a person who does not have knowledge of the official's PIN (such as an unscrupulous person trying to issue a fraudulent credential) cannot legitimately issue a credential. (bolding and italics added for emphasis)

The feature of securing a joint key in escrow or in trust is recited in claim 93. The feature of securing a portion of information used to derive the joint key is recited in claim 179. With respect to claim 179, one example of securing a portion of information used to derive the joint key is shown in Figs. 10A, 10B and 11, wherein CPKO which is used to derive the joint key is stored in element 144.

(6) Two-stage funds transfer - Figs. 13A-13E and corresponding text on page 26, line 25 through page 27, line 11 disclose a three party check transaction scheme. The participating parties

in this transaction are the check originator whose account is to be debited, the check recipient to whom the check is drawn, and the check redeemer who is cashing the check for the recipient or accepting it in payment for goods or services, and whose account is to be credited. In this manner, the check recipient does not have to deposit the check in his or her bank as is typically done. Instead, the check recipient uses the check itself by presenting it to a merchant (who replaces the check recipient's bank as the check redeemer) to pay for goods or services.

This feature is recited in claim 134 wherein the check originator is the first party, the check recipient is the third party, and the check redeemer is the second party. Also, in claim 134, VAN2 corresponds to OVAN in Figs. 13A-13E, and VAN1 corresponds to RDBVAN in Fig. 13C and to OBVAN in Fig. 13D. VAN1 is associated with the transfer of funds from the check recipient (third party) to the check redeemer (second party).

In the first stage of the process, the funds are transferred from the account of the check recipient (third party) to the account of the check redeemer (second party). In the second stage of the process, the funds are transferred from the account of the check originator (first party) to the account of the check recipient (third party).

(7) Anti-duplication transaction number to authenticate a party-

Referring to Fig. 8A, as described on page 15, line 25 through page 16, line 16, it is possible to use an unsecured link between the mixer 48 and the sorter 62 because CRNX and RNX, not CPNR, are transmitted from the mixer 48 to the sorter 62.

However, a security problem still exists in using an unsecured line between the mixer 48 and the sorter 62 because the signal



can be recorded and then played back later to attempt to fraudulently authenticate a fraudulent transaction. In an alternate embodiment of the present invention, an anti-duplication variable authentication number (ADVAN) is generated at the recipient's terminal by coding at least a transmission date and time with the CPNR by a coder. The ADVAN is then mixed with the CRNX and the RNK by the mixer 48 and sent to the remote bank CPU over the unsecured line to the sorter 62. At the remote bank CPU, the CPNR which is generated by the uncoder 70 is used to uncode the ADVAN to regenerate the transmission date and time. The signal received over the unsecured line is then authenticated by comparing the regenerated transmission date and time to a reception date and time (that is, the date and time at which the signal was received at the remote bank CPU). In this manner, the recipient and transaction are further authenticated.

Alternately, as described in part on page 41, lines 33-36, an anti-duplication VAN (ADVAN) is generated from a transaction sequence number (TSN) using coder 1610 of Fig. 16.

The use of the ADVAN to authenticate a party is recited in claim 147.

#### Hellman

Hellman discloses a system for allowing authorized parties to a conversation (conversers) to converse privately even though an unauthorized party (eavesdropper) intercepts all of their communications, and for allowing conversers on an insecure channel to authenticate each other's identity (column 2, lines 7-13). In Hellman's system, the first converser or first party

receives a public key (i.e., transformed signal  $Y_1$  or  $Y_2$ ) from a second converser or second party (column 2, lines 35-68 and column 4, lines 1-50). The second converser transmits the public key to the first party over an unsecured data communications channel, or the first party obtains the public key from a public directory. The second converser places the transformed second signal in a public directory as the second converser's means of identification (column 2, lines 58-61).

Hellman's system does not disclose or suggest any of the seven features described above. Each independent claim includes at least one of the seven features. Thus, Hellman cannot render obvious any of the pending independent claims, or any of the dependent claims which incorporate the respective features therein.

#### Maurer

Maurer discloses a method of generating a shared cipher key which is subsequently used for encrypting and decrypting information to be sent between two communicating stations A and B over an error-free public communications channel. A common (broadcast) transmitting source sends an identical data string to the stations A and B. The cipher key is generated based upon a difference in the information content of data strings  $S_a$  and  $S_b$  respectively received by the two stations A and B. The information difference is caused by different noise levels in the channels associated with the common transmitting source and the receivers of the two stations A and B. (If there is no noise anywhere in the system, there would be no information difference since both stations A and B receive the same data string.)

To generate the cipher key, station A generates an error-control information string C from the data string  $S_a$ , and transmits the string C to the station B over a public channel. Station B generates string D and a decision bit F which is based on a predetermined reliability function of string ( $S_b$ , C, D). If the reliability function is greater than a predetermined threshold, then decision bit F is assigned a value of "1". Otherwise it is assigned a value of "0". Bit F is then sent from station B to station A over the public channel. Strings  $S_a$  and  $S_b$  are tagged acceptable when F is 1. These steps are repeated a number of times resulting in a corresponding number of tagged strings. The tagged strings are concatenated to form the shared cipher key. Maurer does not teach or suggest the concept of authentication of a party. At best, Maurer is concerned with authenticating data passing from one station to another without regard to authentication of an individual party who may be involved in generating or passing the data.

Maurer's system does not disclose or suggest any of the seven features described above. Each independent claim includes at least one of the seven features. Thus, Maurer cannot render obvious any of the pending independent claims, or any of the dependent claims which incorporate the respective features therein.

For at least the reasons set forth above, withdrawal of the § 103(a) rejections over Hellman and Maurer is respectfully requested.

**Conclusion**

Insofar as the Examiner's rejections have been fully addressed, the instant application is in condition for allowance. A Notice of Allowability of all pending claims is therefore earnestly solicited.

Respectfully submitted,

LEON STAMBLER

11/7/97

(Date)

BY:

Clark A. Jablon

Clark A. Jablon  
Registration No. 35,039  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
One Commerce Square  
2005 Market Street, 22nd Floor  
Philadelphia, PA 19103-7086  
Telephone: (215) 567-2020  
Facsimile: (215) 567-2991

CAJ:eam

GAU 2211

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.



BY Elizabeth L. Infante

DATE: November 7, 1997

2302  
10/30/97

**PATENT**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In Re.:	Patent application of	:
	Leon Stambler	: Group Art Unit 2211
		:
Appln. No.:	08/747,174	:
		: Examiner: B. Zimmerman
Filed:	November 12, 1996	:
		: Attorney Docket
For:	METHOD FOR SECURING	: No. 6074-1U5
	INFORMATION RELEVANT TO A	:
	TRANSACTION (as amended)	:

**AMENDMENT COVER SHEET**

Transmitted herewith is an Amendment in the above identified application.

☒ [X] A verified statement to establish small entity status under 37 CFR 1.9 and 1.27 is

☒ [X] already on file;

☐ [ ] enclosed.

☐ [ ] No additional fee is required.

☐ [ ] An Information Disclosure Statement with one copy of each of the cited patents is also attached.

The fee has been calculated as shown below:

					SMALL ENTITY		LARGE ENTITY	
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NO. PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDIT FEE	RATE	ADDIT. FEE
TOTAL	84	(-)	65	= 19	X11	\$209	X22	\$
INDEP.	22	(-)	23	= 0	X41	\$	X82	\$
1ST PRESENTATION OF MULTIPLE DEPENDENT CLAIMS					+\$135	\$	+\$270	\$
TOTAL						\$209	TOTAL	\$

- ☐ The applicant(s) hereby petition(s) for any extension of time which may be required in connection with the filing of the enclosed paper(s). (Petition and Fee for \_\_\_\_\_ month(s) extension is enclosed.)
- ☒ The Assistant Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 16-0235. One additional copy of this sheet is attached for accounting purposes.
- ☒ The above calculated additional claim fees \$209.00.
- ☒ Any additional fees under 37 CFR 1.16 or 1.17.

Respectfully submitted,

LEON STAMBLER

November 7, 1997  
(Date)

By: Clark Jablon  
CLARK A. JABLON  
Registration No. 35,039  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
One Commerce Square  
2005 Market Street - 22nd Floor  
Philadelphia, PA 19103-7086  
Telephone: (215) 965-1293  
Facsimile: (215) 567-2991  
E-Mail: psjn@psjn.com

CAJ:eam  
Enclosures

PSJN2/131590.1

-2-

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: BOX AF, ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.



BY: Elizabeth A. McLeod DATE: November 7, 1997

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

#16

In re: Patent Application of : Group Art Unit: 2211  
Leon Stambler :  
:   
Appln. No.: 08/747,174 : Examiner: B. Zimmerman  
:   
Filed: November 12, 1996 :  
:   
For: METHOD FOR SECURING :  
INFORMATION RELEVANT TO A : Attorney Docket  
TRANSACTION (as amended) : No. 6074-1U5

TERMINAL DISCLAIMER TO OBVIATE A  
DOUBLE PATENTING REJECTION (37 CFR 1.321(g))

IDENTIFICATION OF PERSON MAKING THIS DISCLAIMER

I, Leslie L. Kasten, Jr. represent that I am a representative authorized to sign on behalf of Leon Stambler, who is the owner of the above-identified unassigned application.

EXTENT OF DISCLAIMANT'S INTEREST

The extent of the interest in this invention that the disclaimant owns is in the whole of this invention.

11/21/1997 15:06:00 00000007 000160235 08747174  
01 FC:248 35.00 CH

-1-

**DISCLAIMER**

The owner of the above-identified application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the present application which would extend beyond the expiration date of the full statutory term defined in 35 U.S.C. § 154 to § 156 and § 173 of U.S. Patent Nos. 5,267,314 and 5,524,073. The owner of the above-identified application hereby agrees that any patent so granted on the present application shall be enforceable only for and during such period that it and U.S. Patent Nos. 5,267,314 and 5,524,073 are commonly owned. This agreement runs with any patent granted on the present application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner of the above-identified application does not disclaim any terminal part of any patent granted on the present application that would extend to the expiration date of the full statutory term defined in 35 U.S.C. § 154 to § 156 and § 173 of the prior patent, in the event that it later: expires for failure to pay a maintenance fee, is held unenforceable or is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or is terminally disclaimed under 37 C.F.R. § 1.321, has all claims canceled by a re-examination certificate, or is in any manner terminated prior to the expiration of its full statutory term.



**FEE STATUS AND PAYMENT**

(37 CFR 1.20(d))

This application is entitled to Small Entity status. A verified statement was previously filed in original Application No. 07/977,385 and such status is still proper and desired.

Charge Deposit Account No. 16-0235 in the sum of \$55.00.

Also, charge Deposit Account No. 16-0235 for any fee deficiency.

A duplicate of this disclaimer is attached.

Respectfully submitted,

LEON STAMBLER

11/7/97 BY: Leslie L. Kasten, Jr.  
(Date)  
Leslie L. Kasten, Jr.  
Registration No. 28,959  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
One Commerce Square  
2005 Market Street - 22nd Floor  
Philadelphia, PA 19103-7086  
Telephone: (215) 567-2020  
Facsimile: (215) 567-2991

LLK:CAJ:eam



**UNITED STATES DEPARTMENT OF COMMERCE  
Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/747,174	11/12/96	STAMBLER	6074-1-U5

LM32/0102  
PANITCH SCHWARZE JACOBS & NADEL  
ONE COMMERCE SQUARE  
2005 MARKET STREET 22ND FLOOR  
PHILADELPHIA PA 19103-7086

EXAMINER

ZIMMERMAN, B

ART UNIT

2735

PAPER NUMBER

#17

DATE MAILED:

01/02/98

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

<b>Notice of Allowability</b>	Application No. <b>08/747,174</b>	Applicant(s) <b>Stambler</b>
	Examiner <b>Brian Zimmerman</b>	Group Art Unit <b>2735</b>

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 and Issue Fee Due or other appropriate communication will be mailed in due course.

☒ This communication is responsive to amendment filed 11/10/97

☒ The allowed claim(s) is/are 64, 66, 67, 69-74, 93, 95-119, and 124-179

☐ The drawings filed on \_\_\_\_\_ are acceptable.

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some\* ☐ None of the CERTIFIED copies of the priority documents have been received.

☐ received in Application No. (Series Code/Serial Number) \_\_\_\_\_

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\*Certified copies not received: \_\_\_\_\_

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

A SHORTENED STATUTORY PERIOD FOR RESPONSE to comply with the requirements noted below is set to EXPIRE THREE MONTHS FROM THE "DATE MAILED" of this Office action. Failure to timely comply will result in ABANDONMENT of this application. Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

☐ Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL APPLICATION, PTO-152, which discloses that the oath or declaration is deficient. A SUBSTITUTE OATH OR DECLARATION IS REQUIRED.

☒ Applicant MUST submit NEW FORMAL DRAWINGS

☐ because the originally filed drawings were declared by applicant to be informal.

☒ including changes required by the Notice of Draftsperson's Patent Drawing Review, PTO-948, attached hereto or to Paper No. 12

☒ including changes required by the proposed drawing correction filed on Nov 12, 1996, which has been approved by the examiner.

☐ including changes required by the attached Examiner's Amendment/Comment.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the reverse side of the drawings. The drawings should be filed as a separate paper with a transmittal letter addressed to the Official Draftsperson.

☐ Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Any response to this letter should include, in the upper right hand corner, the APPLICATION NUMBER (SERIES CODE/SERIAL NUMBER). If applicant has received a Notice of Allowance and Issue Fee Due, the ISSUE BATCH NUMBER and DATE of the NOTICE OF ALLOWANCE should also be included.

Attachment(s)

☐ Notice of References Cited, PTO-892

☐ Information Disclosure Statement(s), PTO-1449, Paper No(s) \_\_\_\_\_

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

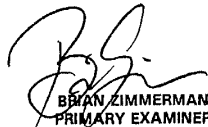
☐ Notice of Informal Patent Application, PTO-152

☐ Interview Summary, PTO-413

☐ Examiner's Amendment/Comment

☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

☐ Examiner's Statement of Reasons for Allowance

  
**BRIAN ZIMMERMAN**  
 PRIMARY EXAMINER  
 ART UNIT 2735



UNITED STATES DEPARTMENT OF COMMERCE  
Patent and Trademark Office

Address: Box ISSUE FEE  
COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231

NOTICE OF ALLOWANCE  
AND ISSUE FEE DUE

- ☐ Note attached communication from the Examiner  
☐ This notice is issued in view of applicant's communication filed

SERIES CODE/SERIAL NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT	DATE MAILED
First Named Applicant				

TITLE OF INVENTION

ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEE DUE	DATE DUE

**THE APPLICATION IDENTIFIES ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED.**

**THE ISSUE FEE 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.**

**HOW TO RESPOND TO THIS NOTICE:**

- I. Review the SMALL ENTITY Status shown above.  
If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:
  - A. If the status is changed, pay twice the amount of the FEE DUE shown above and notify the patent and Trademark Office of the change in status, or
  - B. If the Status is the same, pay the FEE DUE shown above.
- II. Part B of this notice should be completed and returned to the Patent and Trademark Office (PTO) with your ISSUE FEE. Even if the ISSUE FEE has already been paid by charge to deposit account, Part B should be completed and returned. If you are charging the ISSUE FEE to your deposit account, Part C of this notice should also be completed and returned.
- III. All communications regarding this application must give series code (or filing date), serial number and batch number. Please direct all communication prior to issuance to Box ISSUE FEE unless advised to contrary.

If the SMALL ENTITY is shown as NO:

- A. Pay FEE DUE shown above, or
- B. File verified statement of Small Entity Status before, or with, pay of 1/2 the FEE DUE shown above.

**IMPORTANT REMINDER: 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.**



I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.

BY: Elizabeth A. McLeod

DATE: 12/23/97

RECEIVED  
JAN 14 1998  
Publishing Division  
Correspondence File (2)

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re: Patent Application of Leon Stambler : Group Art Unit 111  
: :  
: :  
Appln. No.: 08/747,174 : Examiner: B. Zimmerman  
: :  
Filed: November 12, 1996 : :  
: :  
For: METHOD FOR SECURING : Attorney Docket  
INFORMATION RELEVANT TO A : No. 6074-1U5  
TRANSACTION (as amended) : :

**SECOND SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT**

1. The Second Supplemental Information Disclosure Statement (IDS) transmitted herewith is being filed after the mailing date of the first Office Action on the merits, but before the mailing date of either a final action under § 1.113 or a notice of allowance under § 1.311.

2. Accompanying this transmittal is a certification as specified in 37 CFR 1.97(e).

**Certification Under 37 C.F.R. § 1.97(e)**

I hereby certify that no item of information in the Second Supplemental IDS filed herewith was cited in a communication from a foreign patent office in a counterpart foreign application or, to my knowledge after making reasonable inquiry, was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of this Second Supplemental IDS. 37 CFR 1.97(e)(2).

3. It is requested that the enclosed references listed on the attached Second Supplemental IDS Form PTO-1449 be considered by the Patent Examiner in connection with the above-identified application and be made of record therein.

These references are being made of record because Applicant recently became aware of U.S. Patent No. 5,677,955 (Doggett et al.) and the references cited therein. With respect to the publications cited in the patent, only the publications having publication dates before the effective filing date of the present application (which is November 17, 1992) are cited. Furthermore, Applicant was not able to obtain copies of two of the articles cited in the publication section which predate the effective filing date of the present application, namely, the articles entitled "Industry Players Discuss...Dec. 20, 1990" and "New, Practical ACH...Apr. 26, 1990." Nor is Applicant aware of the contents of such articles. Accordingly, neither of these articles are cited either.

Independent consideration and acknowledgment of the enclosed references are respectfully requested.

Respectfully submitted,

LEON STAMBLER

12/23/97

(Date)

By:

Clark A. Jablon

CLARK A. JABLON

Registration No. 35,039

PANITCH SCHWARZE JACOBS & NADEL, P.C.

One Commerce Square

2005 Market Street - 22nd Floor

Philadelphia, PA 19103-7086

Telephone: (215) 965-1923

Facsimile: (215) 567-2991

E-Mail: psjn@psjn.com

CAJ:eam  
Enclosure

Form PTO-1449 (REV. 8-83)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY DOCKET NO.: 6074-1U5		APPLICATION NO.: 08/747,174	
<b>SECOND SUPPLEMENTAL INFORMATION DISCLOSURE CITATION</b> (Form PTO-1449 Modified 5/95) (Use several sheets if necessary)				APPLICANT: Leon Stambler		FILING DATE: November 12, 1996 GROUP ART UNIT: 2211 2935	
				FILING DATE: November 12, 1996			
<b>U.S. PATENT DOCUMENTS</b>							
EX. INIT	DOCU- MENT	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB- CLASS	FILING DATE IF APPROPRIATE
Bt		4,264,808	04/1981	Owens <i>et al.</i>	-	-	
		4,423,287	12/1983	Zeidler	-	-	
		4,823,264	04/1989	Deming	-	-	
		5,187,351	02/1993	Clary	-	-	
		5,191,613	03/1993	Graziano <i>et al.</i>	-	-	
		5,218,637	06/1993	Angebaud <i>et al.</i>	-	-	
		5,224,162	06/1993	Okamoto <i>et al.</i>	-	-	
		5,283,829	02/1994	Anderson	-	-	
		5,297,202	03/1994	Kapp <i>et al.</i>	-	-	
		5,321,751	06/1994	Ray <i>et al.</i>	-	-	
		5,326,959	07/1994	Perazza	-	-	
		5,453,601	09/1995	Rosen	-	-	
		5,455,407	10/1995	Rosen	-	-	
		5,465,299	11/1995	Matsumoto <i>et al.</i>	-	-	
		5,473,690	12/1995	Grimonprez <i>et al.</i>	-	-	
Bt		5,530,755	06/1996	Pailles <i>et al.</i>	-	-	
<b>FOREIGN PATENT DOCUMENTS</b>							
EX. INIT	DOCU- MENT	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB- CLASS	TRANSLATION YES NO
<b>OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)</b>							
Bt		Shipley C., "I threw away my checkbook", PC-Computing, vol. 3, No. 11, pp. 112, 114-115, 118-120, Nov. 1990.					
		Diamond S., "Check Processing Takes a New Turn", Computers in Banking, vol. 5, No. 3, pp. 50-55, March 1988.					
EXAMINER				DATE CONSIDERED 4/1/96			
*EXAMINER: Initial if citation 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.							

Form PTO-1449 (REV. 8-83)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY DOCKET NO.: 6074-1U5		APPLICATION NO.: 08/747,174	
SECOND SUPPLEMENTAL INFORMATION DISCLOSURE CITATION  (Form PTO-1449 Modified 5/93) (Use several sheets if necessary)				APPLICANT: Leon Stambler			
				FILING DATE: November 12, 1996		GROUP ART UNIT: 2211 2735	
<b>U.S. PATENT DOCUMENTS</b>							
EX. INIT	DOCU- MENT	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB- CLASS	FILING DATE IF APPROPRIATE
Bt		5,677,955	10/1997	Doggett <i>et al.</i>	—	—	
<b>FOREIGN PATENT DOCUMENTS</b>							
EX. INIT	DOCU- MENT	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB- CLASS	TRANSLATION YES NO
<b>OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)</b>							
Bt		Iida J., "Electronic Presentment Due for N.Y. Test", American Banker, vol. 157, No. 143, p. 3, July 27, 1992.					
Bt		Torrez A., "Banking Industry Looks at Changing Check Guarantees", The Business Journal-Phoenix & The Valley of the Sun, vol. 9, No. 29, pp. 13-14, May 29, 1989.					
Bt		Sullivan D., "Bank Technology Trick or Treat?", Bankers Monthly, vol. 109, No. 11, pp. 10, 12-14, 18, 20, November 1992.					
Bt		Seidenberg, "Bell Companies Now Testing Smart Card Offering Increased Feature Functionality", Card News, vol. 5, No. 10, pp. 5-6, May 21, 1990.					
Bt		"General Magnaplate Corporation Issues Three-Month Report to Stockholders", PR Newswire, 1 page, November 11, 1992.					
Bt		Bytes T., "More Companies Are Paying Bills Electronically", Journal of Commerce, p. 2B, May 5, 1988.					
Bt		Carreker J.D., "Strides in Electronic Checking Transforming Payment System", vol. 68, No. 3, pp. 18-19, 22, 24, 26, 28, 30, March 1992.					
EXAMINER		B. Zimmerman		DATE CONSIDERED 4/1/98			
*EXAMINER: Initial if citation 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.							



50  
110 - 1552 10/11/97  
7/19/98  
PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit: 2735  
Leon Stambler **Received** :  
Appln. No.: 08/747,174 MAR 16 1998 : Examiner: B. Zimmerman  
Filed: November 12, 1996 **Group 2700** : Batch No. V91  
For: METHOD FOR SECURING : Allowed: January 2, 1997  
INFORMATION RELEVANT TO A : Attorney Docket  
TRANSACTION (as amended) : No. 6074-1U5

HAND-DELIVERED TO  
EXAMINING GROUP ART UNIT 2735

COMMUNICATION

This communication is being submitted to facilitate three outstanding issues in the above-identified matter. Applicant's undersigned representative has attempted to address the issues through numerous telephone calls with the Examiner since receipt of the Notice of Allowability. However, the Examiner did not have access to the application file to assist in resolving the issue. The Examiner suggested that this correspondence be filed to more quickly resolve the outstanding issues. Applicant requests that all issues be resolved before the due date of the Issue Fee, which is April 2, 1998.

The outstanding issues are as follows:

(1) A Second Supplemental Information Disclosure Statement (IDS) was filed on December 23, 1997 and was apparently

not yet matched up with the application file when the Examiner issued the Notice of Allowability on January 2, 1998. Applicant requests that the Second Supplemental IDS be formally considered and that a signed copy of the PTO-1449s be provided to the Applicant before the due date of the Issue Fee.

Enclosed herewith are the following items related to the Second Supplemental IDS:

(a) Copy of Second Supplemental IDS and PTO-1449s as filed. Due to the large number of cited references, additional copies are not enclosed. Copies will be provided upon request if the PTO cannot locate the originally filed papers.

(b) Postcard receipt for such papers bearing a PTO mailroom stamp of December 29, 1997.

(2) The formal drawings filed with the application on November 12, 1996 (which incorporates the changes in the proposed drawing amendment filed concurrently therewith and approved by the Examiner) were either accidentally overlooked by the Examiner or are missing from the file. Receipt of the formal drawings was not acknowledged in the Examiner's Office Action of October 27, 1997 or in the Notice of Allowability dated January 2, 1998. Review of the formal drawings was requested upon filing of the application and during prosecution of the application. See page 51 of the Amendment filed November 7, 1997. However, the Notice of Allowability states that formal drawings are required.

Applicant requests that the formal drawings be formally reviewed by the Draftsperson and that the result of the review be provided to the Applicant before the due date of the formal drawings, which is April 2, 1998.

Enclosed herewith are the following items related to the formal drawings:

(a) Copy of "Transmittal of Formal Drawings Prior to Notice of Allowance" filed November 12, 1996" and copy of enclosed drawings.

(b) Postcard receipt for such papers bearing a PTO mailroom stamp of November 12, 1996.

(3) Small Entity status was requested for this application in the filing transmittal letter, and an additional request was made to correct the status after receipt of the filing receipt. Neither request appears to have been processed, and the Notice of the Allowance states that the application has a large entity status. Applicant requests that the small entity status be granted before the due date of the issue fee, which is April 2, 1998.

Enclosed herewith are the following items related to the small entity status:

(a) Copy of application transmittal letter requesting the small entity status.

(b) Copy of "Request for Corrected Filing Receipt" to correct the status.

(c) Postcard receipt for item (b) bearing a PTO mailroom stamp of May 22, 1997.

Also enclosed concurrently with this paper is an Amendment After Allowance to correct formal matters. Please consider this paper prior to the issue fee deadline of April 2, 1998.

Please telephone Applicant's undersigned attorney if additional information or materials are needed to resolve any of the outstanding issues.

Respectfully submitted,

LEON STAMBLER

March 18, 1998 BY: Clark A. Jablon  
(Date)  
Clark A. Jablon  
Registration No. 35,039  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
One Commerce Square  
2005 Market Street, 22nd Floor  
Philadelphia, PA 19103-7086  
Telephone: (215) 965-1293  
Facsimile: (215) 567-2991

CAJ:eam

Form PTO-1449 (REV. 8-83)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY DOCKET NO.: 6074-1U5		APPLICATION NO.: 08/747,174	
SECOND SUPPLEMENTAL INFORMATION DISCLOSURE CITATION  (Form PTO-1449 Modified 5/93) (Use several sheets if necessary)				APPLICANT: Leon Stambler			
				FILING DATE: November 12, 1996		GROUP ART UNIT: 2211	
<b>U.S. PATENT DOCUMENTS</b>							
EX. INIT	DOCU- MENT	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB- CLASS	FILING DATE IF APPROPRIATE
		4,264,808	04/1981	Owens <i>et al.</i>			
		4,423,287	12/1983	Zeidler			
		4,823,264	04/1989	Deming			
		5,187,351	02/1993	Clary			
		5,191,613	03/1993	Graziano <i>et al.</i>			
		5,218,637	06/1993	Angebaud <i>et al.</i>			
		5,224,162	06/1993	Okamoto <i>et al.</i>			
		5,283,829	02/1994	Anderson			
		5,297,202	03/1994	Kapp <i>et al.</i>			
		5,321,751	06/1994	Ray <i>et al.</i>			
		5,326,959	07/1994	Perazza			
		5,453,601	09/1995	Rosen			
		5,455,407	10/1995	Rosen			
		5,465,299	11/1995	Matsumoto <i>et al.</i>			
		5,473,690	12/1995	Grimonprez <i>et al.</i>			
		5,530,755	06/1996	Pailles <i>et al.</i>			
<b>FOREIGN PATENT DOCUMENTS</b>							
EX. INIT	DOCU- MENT	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB- CLASS	TRANSLATION YES NO
<b>OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)</b>							
		Shipley C., "I threw away my checkbook", PC-Computing, vol. 3, No. 11, pp. 112, 114-115, 118-120, Nov. 1990.					
		Diamond S., "Check Processing Takes a New Turn", Computers in Banking, vol. 5, No. 3, pp. 50-55, March 1988.					
EXAMINER				DATE CONSIDERED			
*EXAMINER: Initial if citation 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.							

Form PTO-1449 (REV. 8-83)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY DOCKET NO.: 6074-1U5		APPLICATION NO.: 08/747,174	
SECOND SUPPLEMENTAL INFORMATION DISCLOSURE CITATION  (Form PTO-1449 Modified 5/93) (Use several sheets if necessary)				APPLICANT: Leon Stambler			
				FILING DATE: November 12, 1996		GROUP ART UNIT: 2211	
<b>U.S. PATENT DOCUMENTS</b>							
EX. INIT	DOCU- MENT	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB- CLASS	FILING DATE IF APPROPRIATE
		5,677,955	10/1997	Doggett <i>et al.</i>			
<b>FOREIGN PATENT DOCUMENTS</b>							
EX. INIT	DOCU- MENT	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB- CLASS	TRANSLATION YES NO
<b>OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)</b>							
		Iida J., "Electronic Presentment Due for N.Y. Test", American Banker, vol. 157, No. 143, p. 3, July 27, 1992.					
		Torrez A., "Banking Industry Looks at Changing Check Guarantees", The Business Journal-Phoenix & The Valley of the Sun, vol. 9, No. 29, pp. 13-14, May 29, 1989.					
		Sullivan D., "Bank Technology Trick or Treat?", Bankers Monthly, vol. 109, No. 11, pp. 10, 12-14, 18, 20, November 1992.					
		Seidenberg, "Bell Companies Now Testing Smart Card Offering Increased Feature Functionality", Card News, vol. 5, No. 10, pp. 5-6, May 21, 1990.					
		"General Magnaplate Corporation Issues Three-Month Report to Stockholders", PR Newswire, 1 page, November 11, 1992.					
		Byles T., "More Companies Are Paying Bills Electronically", Journal of Commerce, p. 2B, May 5, 1988.					
		Carreker J.D., "Strides in Electronic Checking Transforming Payment System", vol. 68, No. 3, pp. 18-19, 22, 24, 26, 28, 30, March 1992.					
EXAMINER				DATE CONSIDERED			
*EXAMINER: Initial if citation 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.							

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of Leon Stambler : Group Art Unit: 2735  
: Received :  
: MAR 16 1998 :  
Appln. No.: 08/747,174 : Examiner: B. Zimmerman  
: Group 2700 :  
Filed: November 12, 1996 : Batch No. V91  
: Allowed: January 2, 1997  
For: METHOD FOR SECURING :  
INFORMATION RELEVANT TO A : Attorney Docket  
TRANSACTION (as amended) : No. 6074-1U5

HAND-DELIVERED TO  
EXAMINING GROUP ART UNIT 2735

U.S. Patent & Trademark Office  
Office of Publications  
Query and Correspondence Branch  
Crystal Plaza 2 - Room 6C30  
Washington, DC 20231

AMENDMENT AFTER ALLOWANCE (37 CFR 1.312(a))

1. Please make the following amendment to the application:

In the Claims

Claim 144, line 13: delete "or password".

Claim 147, line 15: after "site" (first occurrence),  
insert --,--.

Claim 149, line 4: delete "variable" and insert  
therefor --number--.

Claim 152, line 42: delete "first" and insert therefor  
--the second--.

line 42: delete "(FXI)" and insert therefor  
--(SXI)--.

line 43: delete "first" and insert therefor  
--the second--.

line 46: delete "(FXI)" and insert therefor  
--(SXI)--.

Claim 167, line 5: after "a", insert --second--.

line 5: delete "(VAN), the VAN" and insert  
therefor --(VAN1), the VAN1--.

line 10: delete "VAN" and insert therefor  
--VAN1--.

Claim 175, line 5: after "a", insert --second--.

line 5: delete "(VAN), the VAN" and insert  
therefor --(VAN1), the VAN1--.

line 10: delete "VAN" and insert therefor  
--VAN1--.

Claim 176, line 5: after "a", insert --third--.

line 5: delete "(VAN), the VAN" and insert  
therefor --(VAN3), the VAN3--.

line 10: delete "VAN" and insert therefor  
--VAN3--.



2. The type of amendment submitted herewith is a correction of formal matters. These corrections are needed for proper disclosure or protection of the invention and requires no substantial amount of additional work on the part of the USPTO to process. No additional search or examination is required to process this amendment.

The amendment to claim 144 is being submitted to correct an obvious oversight in deleting the "password" from this portion of the claim.

The amendment to claim 147 is being submitted to improve the form of the claim.

The amendment to claim 149 is being submitted to correct an obvious grammatical error.

The amendment to claim 152 is being submitted to correct an obvious mislabeling of a claimed element.

The amendments to claims 167, 175 and 176 are being submitted to correct an obvious oversight in distinguishing a newly recited VAN from a previously recited VAN or VANs.

3. The issue fee has not been paid.

4. No fee is believed to be due. However, please charge Deposit Account No. 16-0235 for any fees that may be required by the filing of this paper.

Respectfully submitted,

LEON STAMBLER

March 18, 1998 BY: Clark Jablon  
(Date)  
Clark A. Jablon  
Registration No. 35,039  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
One Commerce Square  
2005 Market Street, 22nd Floor  
Philadelphia, PA 19103-7086  
Telephone: (215) 567-2020  
Facsimile: (215) 567-2991

CAJ:eam

PAT # 5793302  
8-11-98

PATENT  
BOX ISSUE FEE

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.

BY: Louise Train DATE: March 30, 1998

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of Leon Stambler : ATTN: OFFICIAL DRAFTSPERSON  
Appln. No.: 08/747,174  
Filed: November 12, 1996 : Batch No. V91  
For: METHOD FOR SECURING INFORMATION RELEVANT TO TRANSACTION (as amended) : Allowed: January 2, 1997  
: Attorney Docket No. 6074-1U5

RECEIVED  
MAY 12 1998  
Publishing Division  
RECEIVED  
APR 02 1998  
Publishing Division  
Correspondence Files (04)

RECEIVED  
APR 01 1998  
Publishing Division  
16

COMMUNICATION REGARDING FORMAL DRAWINGS

No formal drawings are believed to be due for the above-identified patent application. The Notice of Allowability stating that formal drawings are required is an error, as explained below.

On March 18, 1998 a "Communication" was hand-delivered to the Examiner in charge of the above-identified application regarding the formal drawings in this case. In that Communication, Applicants undersigned representative responded to the Notice of Allowability as follows:

The formal drawings filed with the application on November 12, 1996 (which incorporates the changes in the proposed drawing amendment filed concurrently therewith and approved by the Examiner) were either accidentally overlooked by the Examiner or are missing from the file. Receipt of the formal drawings was not acknowledged in the Examiner's Office Action of October 27, 1997 or in the Notice of Allowability dated January 2, 1998. Review of the formal drawings was requested upon filing of the application and during prosecution of the application. See page 51 of the Amendment filed November 7, 1997. However, the Notice

of Allowability states that formal drawings are required. Applicant requests that the formal drawings be formally reviewed by the Draftsperson and that the result of the review be provided to the Applicant before the due date of the formal drawings, which is April 2, 1998.

Please telephone Applicant's undersigned attorney if additional information or materials are needed to resolve any of the outstanding issues.

Respectfully submitted,

LEON STAMBLER

3/30/98 BY: Clark A. Jablon  
(Date)  
Clark A. Jablon  
Registration No. 35,039  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
One Commerce Square  
2005 Market Street, 22nd Floor  
Philadelphia, PA 19103-7086  
Telephone: (215) 965-1293  
Facsimile: (215) 567-2991

CAJ:lcd



UNITED STATES DEPARTMENT OF COMMERCE  
Patent and Trademark Office

Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, DC 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/747,174	11/12/96	STAMBLER	6074-1-05

LM32/0403  
PANITCH SCHWARZE JACOBS & NADEL  
ONE COMMERCE SQUARE  
2005 MARKET STREET 22ND FLOOR  
PHILADELPHIA PA 19103-7086

EXAMINER  
ZIMMERMAN, B

ART UNIT	PAPER NUMBER
2735	21

DATE MAILED: 04/03/98

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

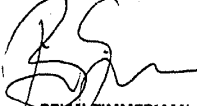
<b>Response to Rule 312 Communication</b>	Application No. <b>08/747,174</b>	Applicant(s) <b>Stambler</b>
	Examiner <b>Brian Zimmerman</b>	Group Art Unit <b>2735</b>

☐ The petition filed on \_\_\_\_\_ under 37 CFR 1.312(b) is granted. The paper has been forwarded to the examiner for consideration on the merits.

☒ The amendment filed on Mar 18, 1998 under 37 CFR 1.312 has been considered, and has been:

- ☐ entered.
- ☒ entered as directed to matters of form not affecting the scope of the invention (Order 3311).
- ☐ disapproved. See explanation below.
- ☐ entered in part. See explanation below.

*SEE Attachment*

  
**BRIAN ZIMMERMAN**  
**PRIMARY EXAMINER**  
**ART UNIT 2735**


The formal drawing filed 3/18/98 have been reviewed. No copy of previously filed formal drawings could be found in the file. Enclosed, find attached Draftsman's Review PTO 948.

The Small Entity Status of the application has been corrected. A new Notice of Allowance and Issue Fee Due has been mailed.

Please find enclosed, a copy of the 2 sheets of IDS filed by the applicant on 12/29/97.

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-3900.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brian Zimmerman whose telephone number is (703) 305-4796.

  
Brian Zimmerman  
Patent Examiner  
Art Unit 2735

703-305-4796  
April 02, 1998

08/74717

NOTICE OF DRAFTERPERSON'S  
PATENT DRAWING REVIEW

The drawing filed (insert date)

12/11/97

A. ☐ not objected to by the Drafterperson under 37 CFR 1.84 or 1.152.B. ☒ objected to by the Drafterperson under 37 CFR 1.84 or 1.152 as indicated below. The Examiner will require submission of new, corrected drawings when necessary. Corrected drawings must be submitted according to the instructions on the back of this notice.1. DRAWINGS. 37 CFR 1.84(a): Acceptable categories of drawings:  
Black ink. Color.☐ Color drawing are not acceptable until petition is granted.☐ Fig.(s) \_\_\_\_\_☐ Pencil and non black ink is not permitted. Fig.(s) \_\_\_\_\_

## 2. PHOTOGRAPHS. 37 CFR 1.84(b)

☐ Photographs are not acceptable until petition is granted.☐ 3 full-tone sets are required. Fig.(s) \_\_\_\_\_☐ Photographs not properly mounted (must bristol board or photographic double-weight paper). Fig.(s) \_\_\_\_\_☐ Poor quality (half-tone). Fig.(s) \_\_\_\_\_

## 3. TYPE OF PAPER. 37 CFR 1.84(c)

☐ Paper not flexible, strong, white and durable.☐ Fig.(s) \_\_\_\_\_☐ Erasures, alterations, overwritings, interlineations, folds, copy machine marks not acceptable. (too thin)☐ Mylar, vellum paper is not acceptable (too thin).☐ Fig.(s) \_\_\_\_\_

## 4. SIZE OF PAPER. 37 CFR 1.84(f): Acceptable sizes:

☐ 21.0 cm by 29.7 cm (DIN size A4)☐ 21.6 cm by 27.9 cm (8 1/2 x 11 inches)☐ All drawings sheets not the same size.☐ Sheet(s) \_\_\_\_\_

## 5. MARGINS. 37 CFR 1.84(g): Acceptable margins:

Top 2.5 cm Left 2.5 cm Right 1.5 cm Bottom 1.0 cm  
SIZE: A4 SizeTop 2.5 cm Left 2.5 cm Right 1.5 cm Bottom 1.0 cm  
SIZE: 8 1/2 x 11☒ Margins not acceptable. Fig.(s) 9, 10, 11, 12, 13, 14, 15, 16☒ Top (T) \_\_\_\_\_ Left (L) 13A-13C, 13E☒ Right (R) \_\_\_\_\_ Bottom (B) 15A, 15C, 16

## 6. VIEWS. CFR 1.84(h)

REMINDER: Specification may require revision to correspond to drawing changes.

☐ Views connected by projection lines or lead lines.☐ Fig.(s) \_\_\_\_\_

Partial views. 37 CFR 1.84(h)(2)

☐ Brackets needed to show figure as one entity.☐ Fig.(s) \_\_\_\_\_☐ Views not labeled separately or properly.☐ Fig.(s) \_\_\_\_\_☐ Enlarged view not labeled separately or properly.☐ Fig.(s) \_\_\_\_\_

## 7. SECTIONAL VIEWS. 37 CFR 1.84(h)(3)

☐ Hatching not indicated for sectional portions of an object.☐ Fig.(s) \_\_\_\_\_☐ Sectional designation should be noted with Arabic or

Roman numbers. Fig.(s) \_\_\_\_\_

## 8. ARRANGEMENT OF VIEWS. 37 CFR 1.84(i)

☐ Words do not appear on a horizontal, left-to-right fashion when page is either upright or turned, so that the top becomes the right side, except for graphs. Fig.(s) \_\_\_\_\_☐ Views not on the same plane on drawing sheet. Fig.(s) \_\_\_\_\_

## 9. SCALE. 37 CFR 1.84(k)

☐ Scale not large enough to show mechanism without crowding when drawing is reduced in size to two-thirds in reproduction.☐ Fig.(s) \_\_\_\_\_

## 10. CHARACTER OF LINES, NUMBERS, &amp; LETTERS. 37 CFR 1.84(l)

☒ Lines, numbers & letters not uniformly thick and well defined, clean, durable and black (poor line quality).☒ Fig.(s) 9, 11

## 11. SHADING. 37 CFR 1.84(m)

☐ Solid black areas pale. Fig.(s) \_\_\_\_\_☐ Solid black shading not permitted. Fig.(s) \_\_\_\_\_☐ Shade lines, pale, rough and blurred. Fig.(s) \_\_\_\_\_

## 12. NUMBERS, LETTERS, &amp; REFERENCE CHARACTERS. 37 CFR 1.84(p)

☒ Numbers and reference characters not plain and legible.☒ Fig.(s) 9☐ Figure legends are poor. Fig.(s) \_\_\_\_\_☐ Numbers and reference characters not oriented in the same direction as the view. 37 CFR 1.84(p)(3) Fig.(s) \_\_\_\_\_☐ English alphabet not used. 37 CFR 1.84(p)(3) Fig.(s) \_\_\_\_\_☐ Numbers, letters and reference characters must be at least .32 cm (1/8 inch) in height. 37 CFR 1.84(p)(3) Fig.(s) \_\_\_\_\_

## 13. LEAD LINES. 37 CFR 1.84(q)

☐ Lead lines cross each other. Fig.(s) \_\_\_\_\_☐ Lead lines missing. Fig.(s) \_\_\_\_\_

## 14. NUMBERING OF SHEETS OF DRAWINGS. 37 CFR 1.84(t)

☐ Sheets not numbered consecutively, and in Arabic numerals beginning with number 1. Fig.(s) \_\_\_\_\_

## 15. NUMBERING OF VIEWS. 37 CFR 1.84(u)

☐ Views not numbered consecutively, and in Arabic numerals, beginning with number 1. Fig.(s) \_\_\_\_\_

## 16. CORRECTIONS. 37 CFR 1.84(w)

☐ Corrections not made from PTO-948 dated \_\_\_\_\_

## 17. DESIGN DRAWINGS. 37 CFR 1.152

☐ Surface shading shown not appropriate. Fig.(s) \_\_\_\_\_☐ Solid black shading not used for color contrast.☐ Fig.(s) \_\_\_\_\_

COMMENTS

REVIEWER

JS

DATE

1/1/98

TELEPHONE NO.

ATTACHMENT TO PAPER NO.

21

PTO COPY



62K-1000  
8/11/98  
5793202

4170  
5/10/98  
750.5  
FEB 13 1998

RECEIVED  
FEB 23 1998

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON, DC 20231, ON THE DATE INDICATED BELOW.

BY: [Signature] DATE: February 11, 1998

BOX ISSUE FEE  
PATENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re: Patent Application of Leon Stambler : Office of Publications  
Appl. No.: 08/747,174 : Batch No. V91  
Filed: November 12, 1996 : Allowed January 2, 1998  
For: METHOD FOR SECURING INFORMATION RELEVANT TO A TRANSACTION : Attorney Docket No. 6074-1US

RECEIVED  
MAY 28 1998

Publishing Division  
Allowed Files (01)

RECEIVED  
APR - 7 98  
GROUP 2600

**TRANSMITTAL LETTER**

Although it is Applicant's opinion that the claims filed by way of amendment are substantially embraced in the statement of invention or in the claims originally filed, Applicant herewith files a Supplemental Declaration for precautionary purposes under 37 CFR 1.67.

Respectfully submitted,

2/11/98 By: Clark Jablon  
(Date)

CLARK A. JABLON  
Registration No. 35,039  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
One Commerce Square  
2005 Market Street - 22nd Floor  
Philadelphia, PA 19103-7086  
Telephone: (215) 567-2020  
Facsimile: (215) 567-2991  
E-Mail: psjn@psjn.com

CAJ/wj  
Enclosure

PSJ&N File No. 6074-1U5

**SUPPLEMENTAL DECLARATION**  
(Related Application)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed, as amended by any and all amendments entered during the prosecution of the patent application identified herein, and for which a patent is sought on the invention entitled **Method For Securing Information Relevant To A Transaction** the specification of which was filed on **November 12, 1996** as Application No. **08/747,174**.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any and all amendments entered during the prosecution of the application identified herein and during the prosecution of the related patent applications identified below.

I acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application(s) in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose information material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

<u>08/446,369</u> (Application No.)	<u>May 22, 1995</u> (Filing Date)	<u>Abandoned</u> (Status-patented, pending, abandoned)
<u>08/122,071</u> (Application No.)	<u>September 14, 1993</u> (Filing Date)	<u>Patented</u> (Status-patented, pending, abandoned)
<u>07/977,385</u> (Application No.)	<u>November 17, 1997</u> (Filing Date)	<u>Patented</u> (Status-patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made 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 so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issues thereon.

Full name of sole or  
first inventor Leon Stambler

Inventor's Signature Leon Stambler

Date 02/03/98

Residence Parkland, Florida

Citizenship U.S.A.

Post Office 7803 Boulder Lane  
Address Parkland, Florida 33067

**PATENT**

**BOX ISSUE FEE**

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.

BY: Louis Stein DATE: April 28, 1998 22  
8

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re: Patent Application of : ATTN: OFFICIAL DRAFTSPERSON  
Leon Stambler :  
Appln. No.: 08/747,174 :  
Filed: November 12, 1996 : Batch No. V91  
: Allowed: January 2, 1997  
For: METHOD FOR SECURING :  
INFORMATION RELEVANT TO A : Attorney Docket  
TRANSACTION (as amended) : No. 6074-1U5

RECEIVED  
Publishing Division  
MAY 04 1998  
11

**TRANSMITTAL OF FORMAL DRAWINGS**

In accordance with the Notice of Allowability accompanying the Notice of Allowance mailed January 2, 1998, and the Communication mailed April 3, 1998 stating that the originally filed formal drawings are missing from the application file, enclosed are fifteen (15) sheets of formal drawings, Figs. 1 through 16, concerning the above-identified application.

It is respectfully submitted that the enclosed copies of formal drawings place this application in condition to be issued, the issue fee having already been paid.

Respectfully submitted,

**LEON STAMBLER**

4/28/98 BY: Clark A. Jablon  
(Date)

Clark A. Jablon  
Registration No. 35,039  
**PANITCH SCHWARZE JACOBS & NADEL, P.C.**  
One Commerce Square  
2005 Market Street, 22nd Floor  
Philadelphia, PA 19103-7086  
Telephone: (215) 965-1293  
Facsimile: (215) 567-2991

CAJ:lcd

PSJN2/163221.1

APPROVED	O.G. FIG.
BY	CLASS SUBCLASS
DRAFTSMAN	

5793302

FIG. 1

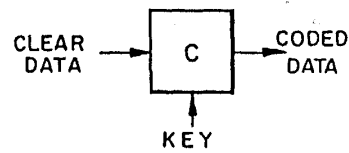


FIG. 2

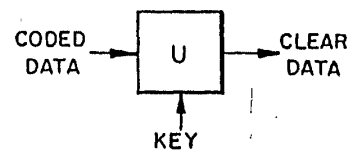


FIG. 3

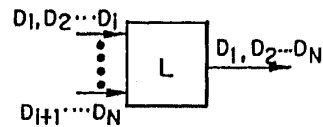


FIG. 4

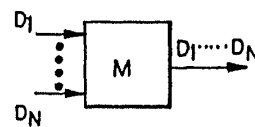


FIG. 5

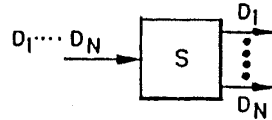
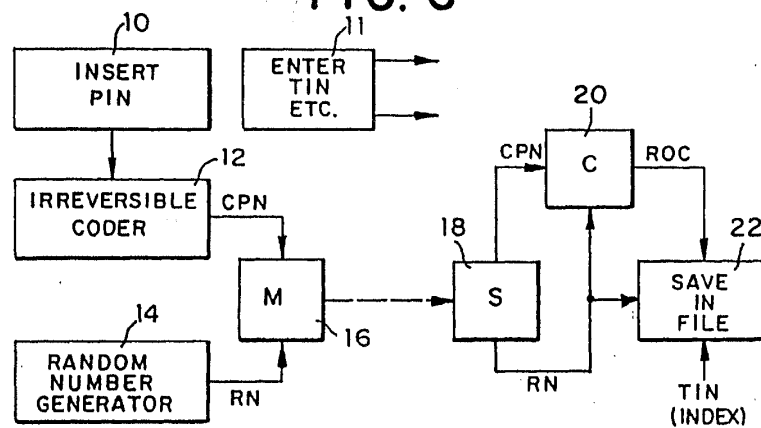
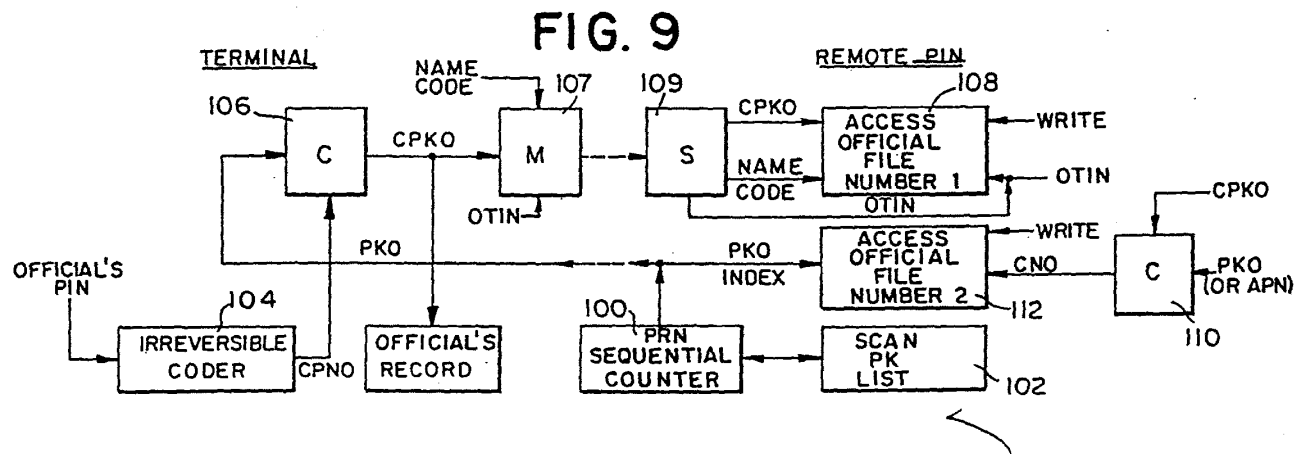
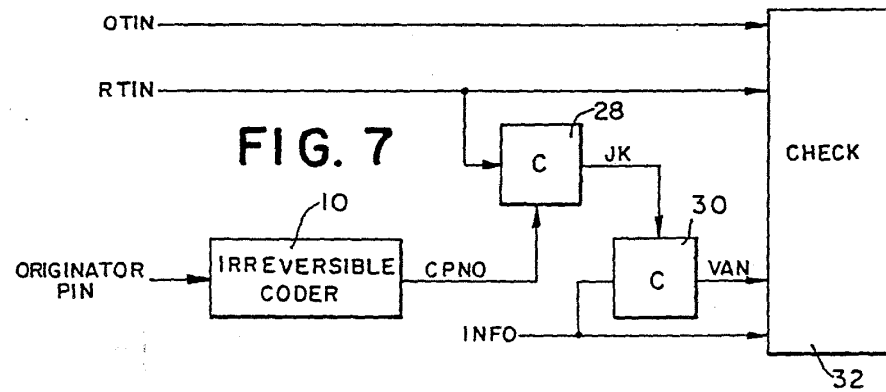


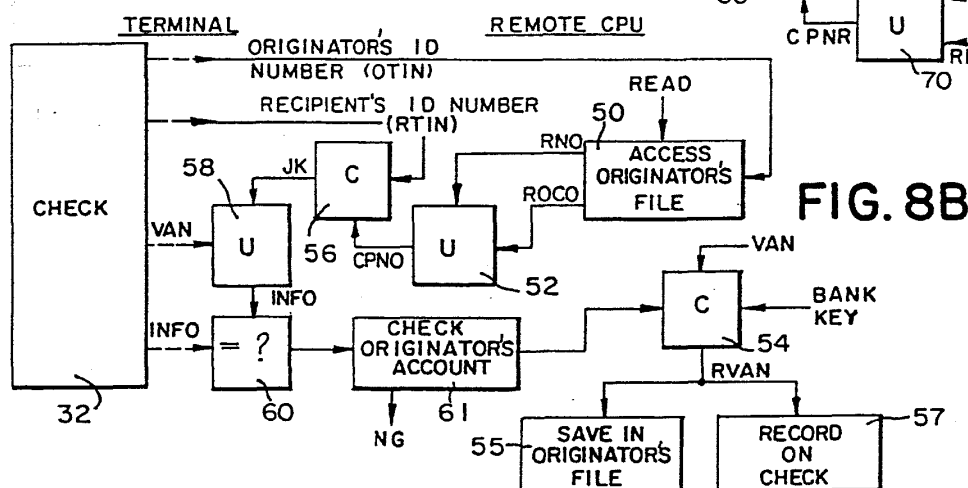
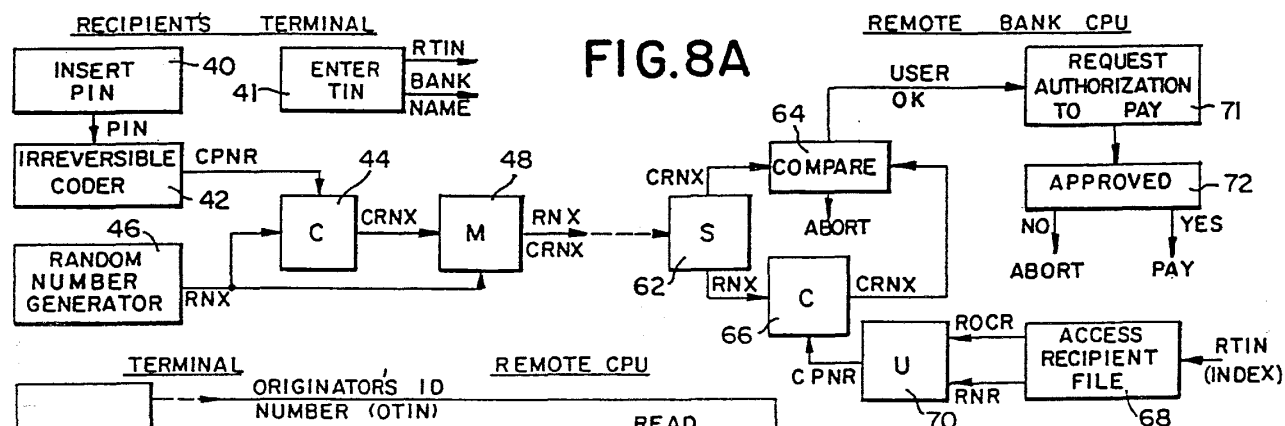
FIG. 6



APPROVED	O.G. FIG.
BY	CLASS / SUBCLASS
DRAFTSMAN	



APPROVED	O.G. FIG.
BY	CLASS
DRAFTSMAN	SUBCLASS





APPROVED	O.G. FIG.
BY	CLASS / SUBCLASS
DRAFTSMAN	

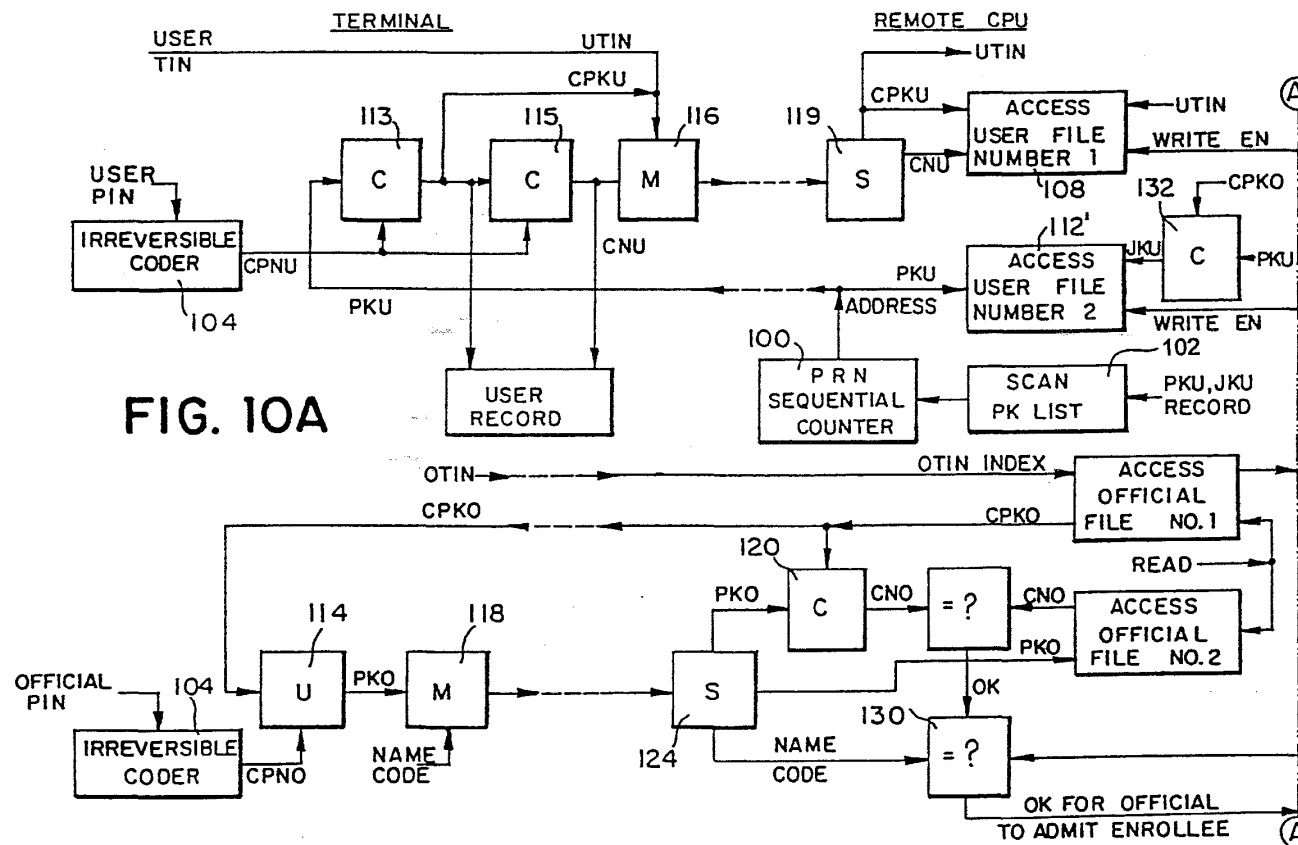
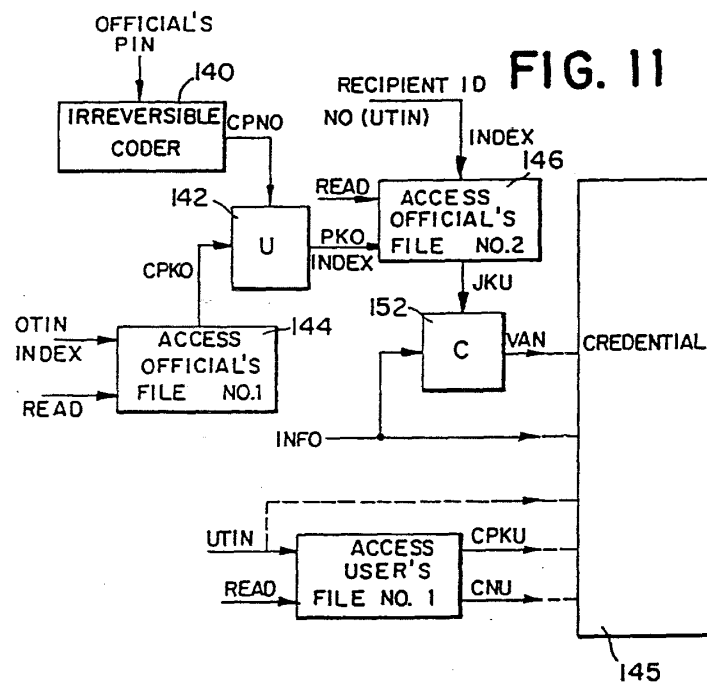
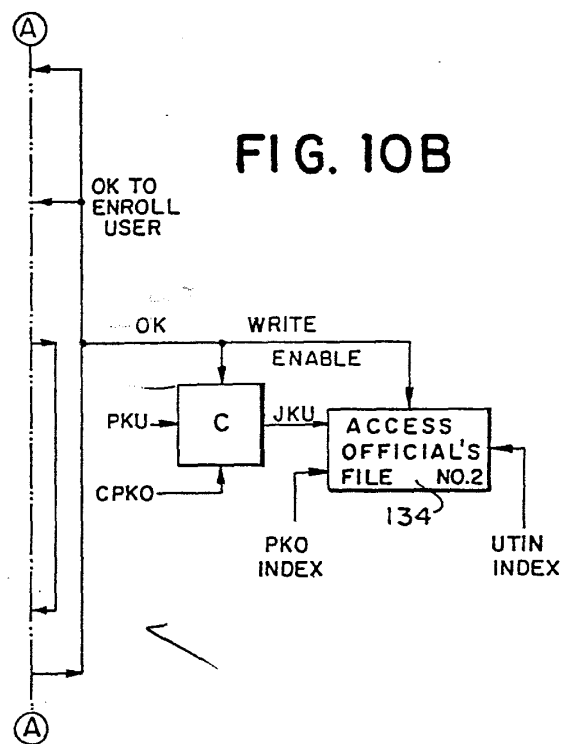
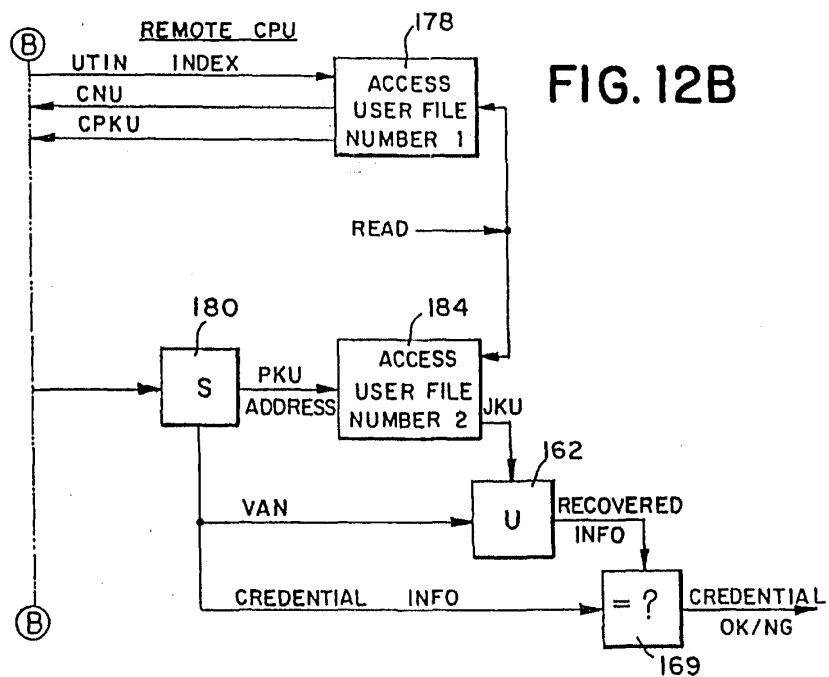
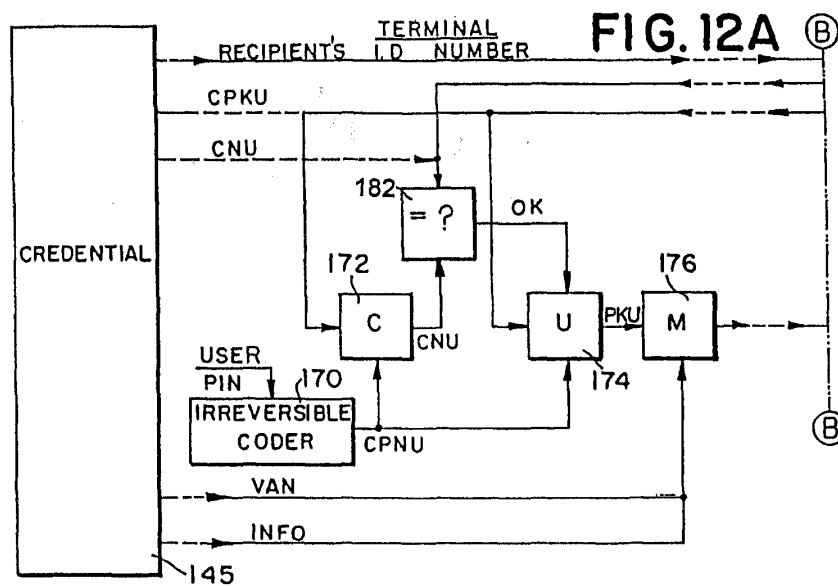


FIG. 10A

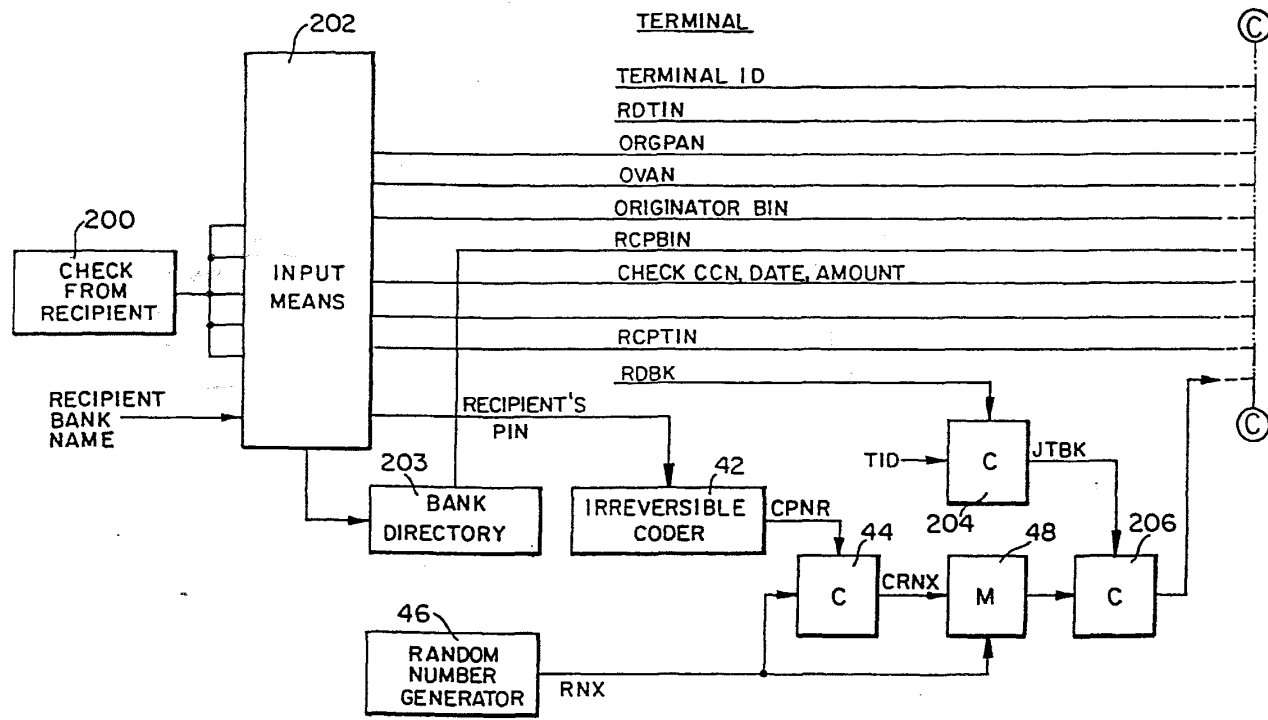
APPROVED	O.G. FIG.
By	CLASS
DRAFTSMAN	SUBCLASS



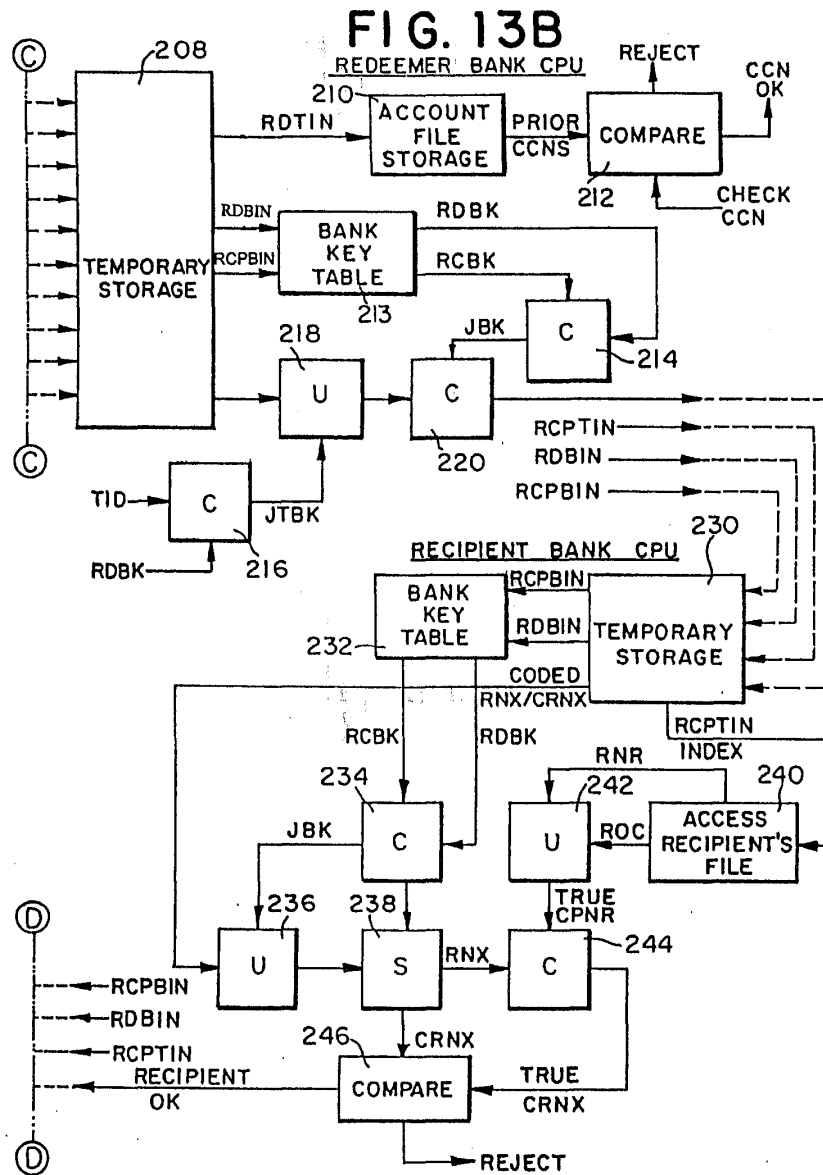
APPROVED	O.G. FIG.	
BY	CLASS	SUBCLASS
DRAFTSMAN		



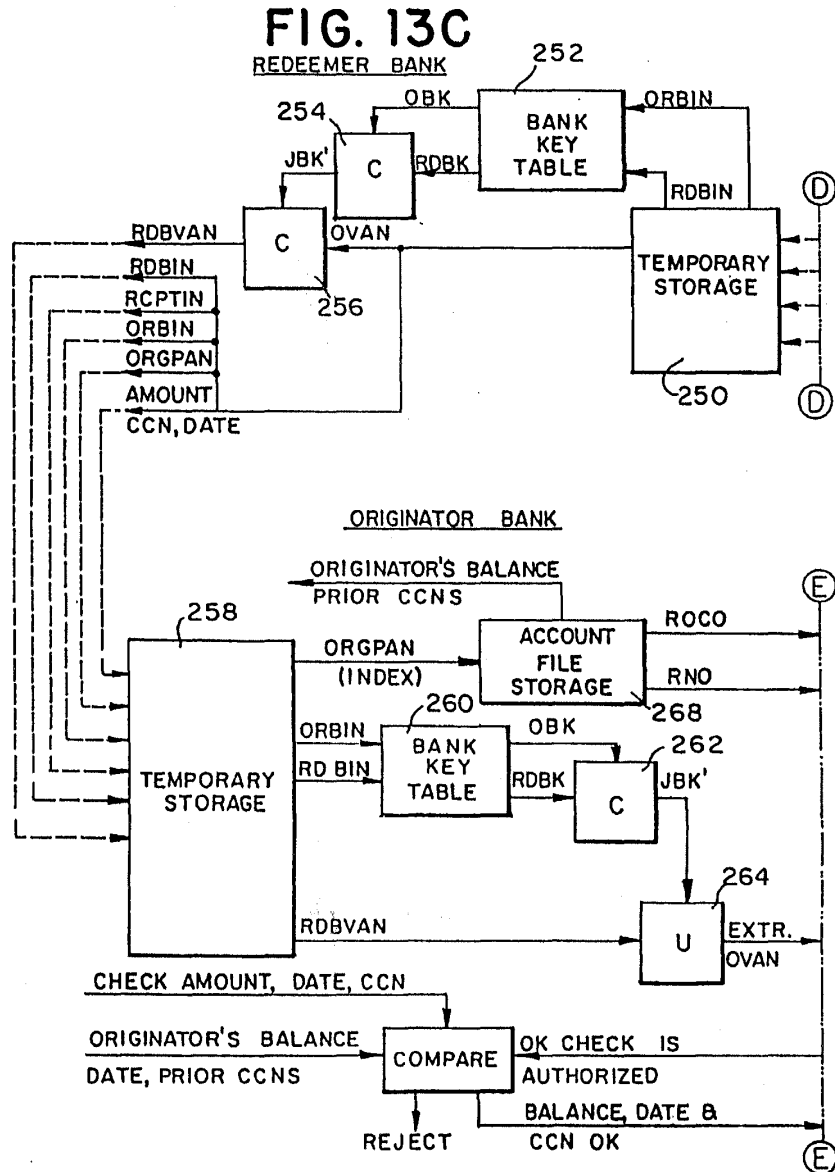
# FIG. 13A



APPROVED	O.G. FIG.	
BY	CLASS	SUBCLASS
DRAFTSMAN		

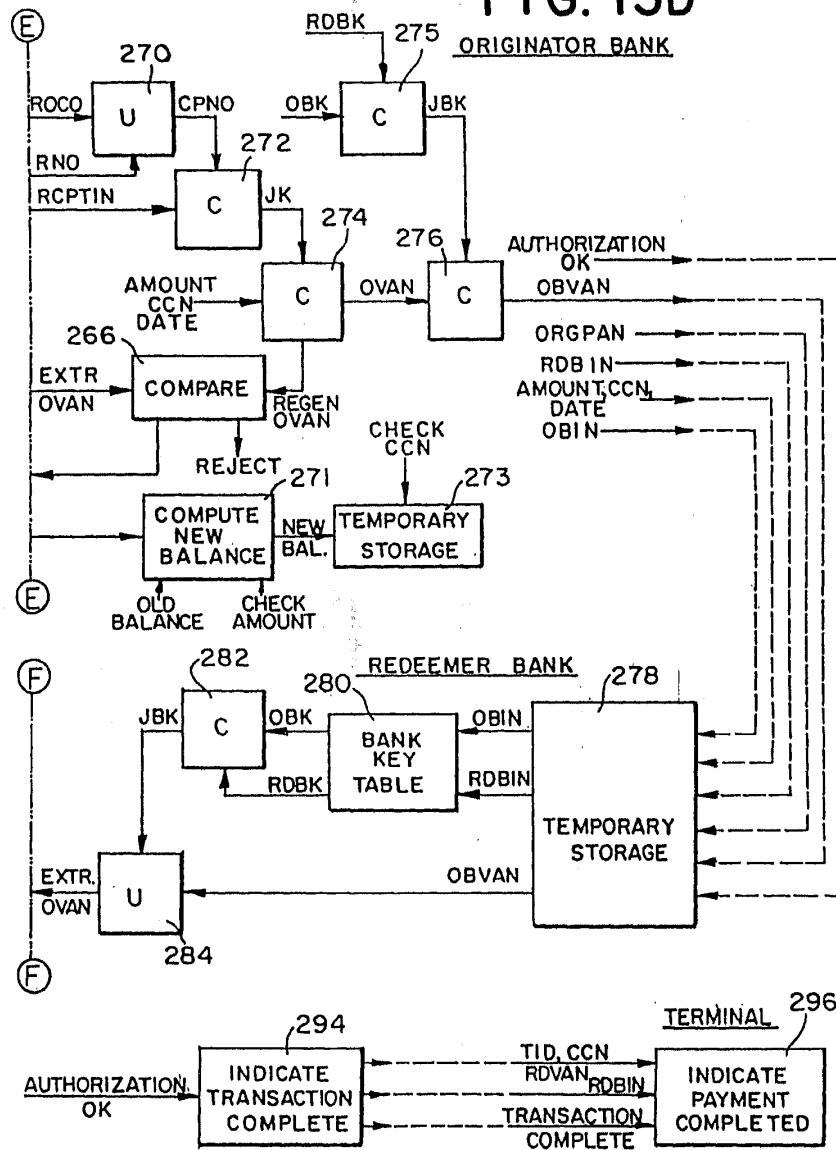


APPROVED	O.G. FIG.	
BY	CLASS	SUBCLASS
DRAFTSMAN		

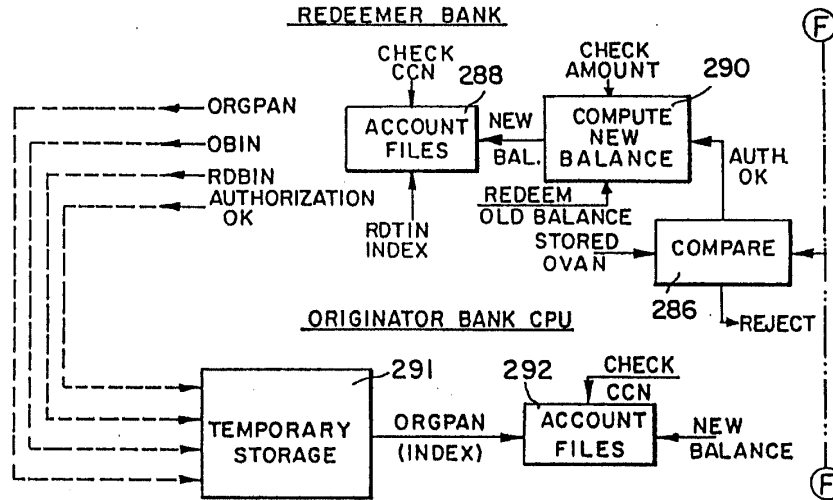


APPROVED	O.G. FIG.	
BY	CLASS	SUBCLASS
DRAFTSMAN		

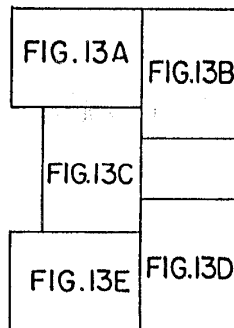
FIG. 13D



**FIG. 13E**

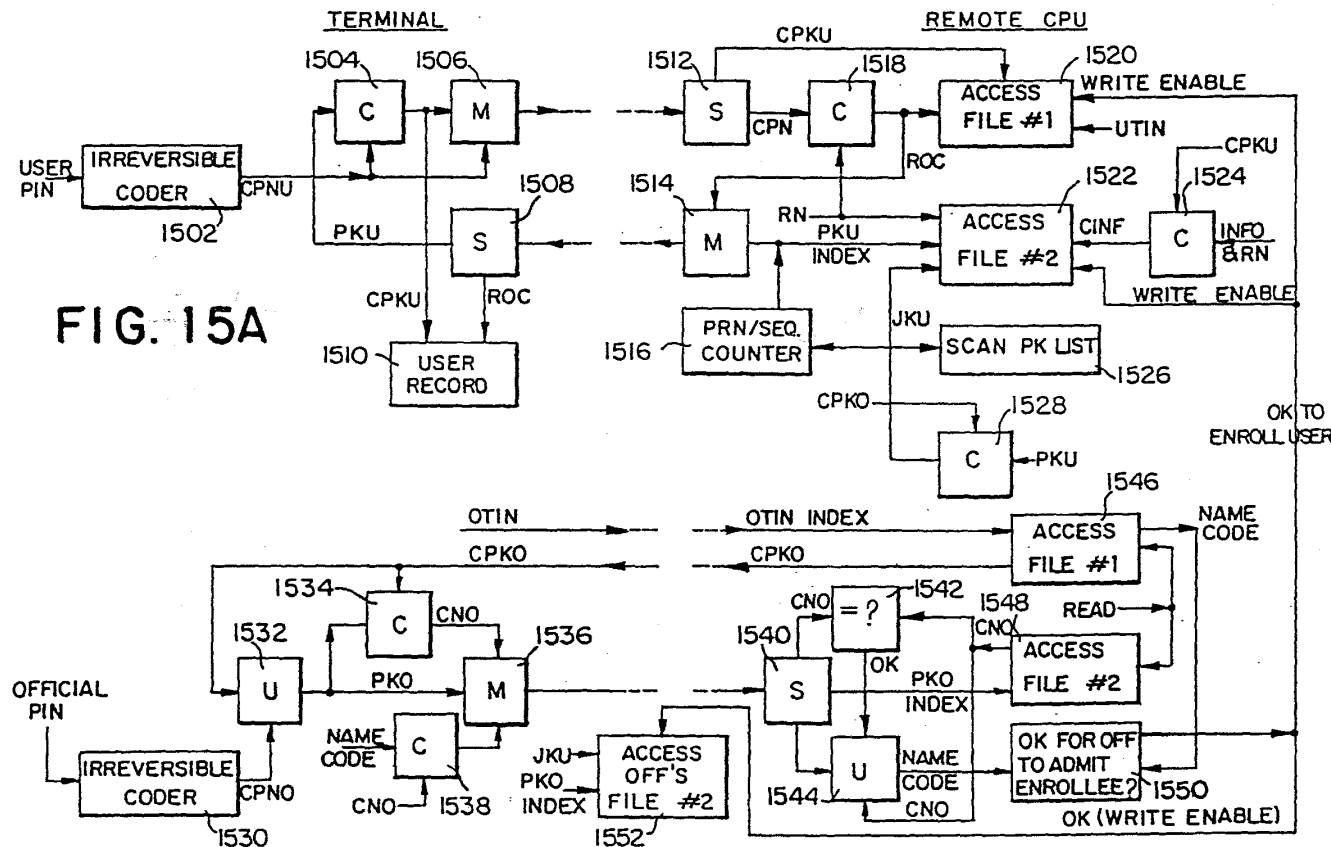


**FIG. 14**





APPROVED	O.G. FIG.
BY	CLASS
DRAFTSMAN	SUBCLASS



APPROVED	O.G. FIG.
BY	CLASS   SUBCLASS
DRAFTSMAN	

CREDENTIAL ISSUE PROCESSING AGENCY TERMINAL/COMPUTER

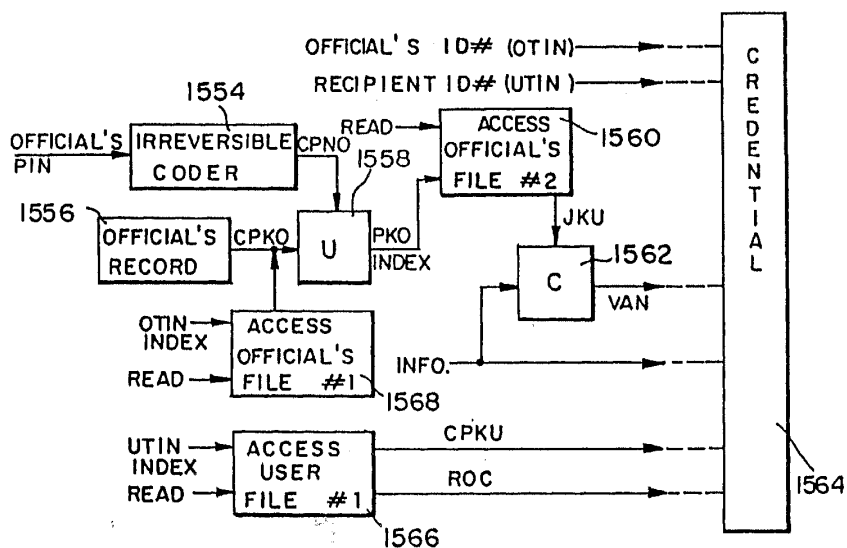


FIG. 15B

APPROVED	O.G. FIG.
BY	CLASS
DRAFTSMAN	SUBCLASS

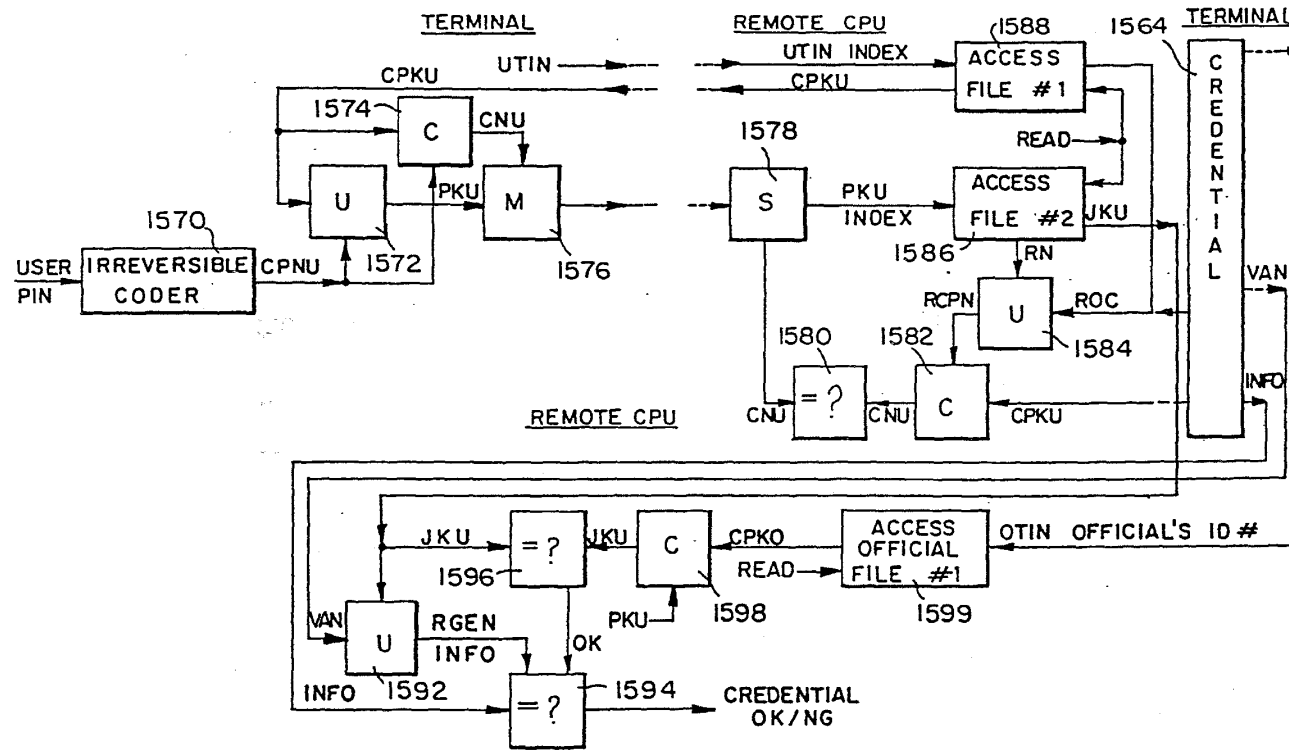


FIG. 15C

APPROVED	O.G. FIG.
BY	CLASS
DRAFTSMAN	SUBCLASS

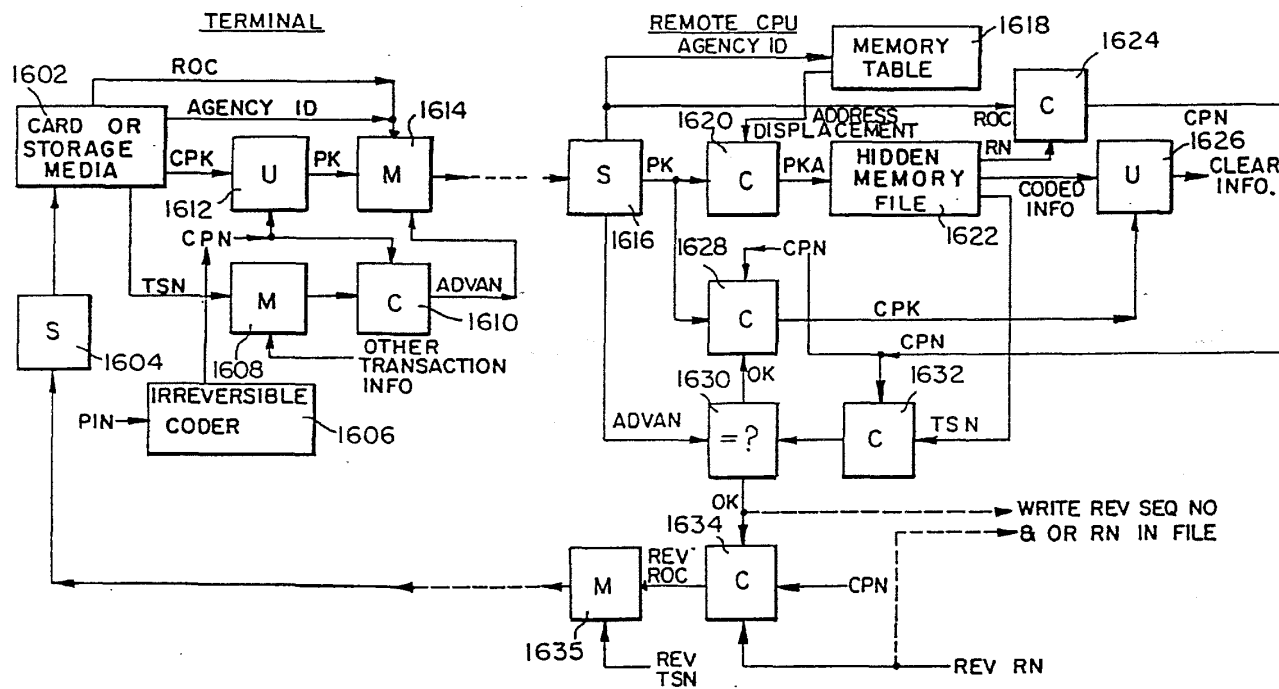


FIG. 16

# PART B—ISSUE FEE TRANSMITTAL

**INSTRUCTIONS:** This form should be used for transmitting the ISSUE FEE. Blocks 2 through 6 should be completed where appropriate. Other correspondence including the Issue Fee Receipt, the Patent, advance orders and notification of maintenance fees will be mailed to addressee entered in Block 1 unless you direct otherwise, by: (a) specifying a new correspondence address in Block 3 below; or (b) providing the PTO with a separate "EE ADDRESS" for maintenance fee notifications with the payment of Issue Fee or thereafter. See reverse for Certificate of Mailing.

1. CORRESPONDENCE ADDRESS		2. INVENTOR(S) ADDRESS CHANGE (Complete only if there is a change)	
<b>RECEIVED</b> Publishing Division  APR 01 1998  PANITCH SCHWARZE JACOBS & NADEL ONE COMMERCE SQUARE 2005 MARKET STREET 22ND FLOOR PHILADELPHIA PA 19103-7086		INVENTOR'S NAME Street Address City, State and ZIP Code CO-INVENTOR'S NAME Street Address City, State and ZIP Code <input type="checkbox"/> Check if additional changes are on reverse side	

SERIES CODE/SERIAL NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT	DATE MAILED
08/747,174	11/12/96	091	ZIMMERMAN, B	2735 01/02/98

First Named Applicant	STAMBLER, LEON
FILE OF INVENTION	METHOD FOR SECURING INFORMATION RELEVANT TO A TRANSACTION (AS AMENDED)

ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEE DUE	DATE DUE
2 6074-1-U5	340-825.340	V91	UTILITY	NO	\$1320.00	04/02/98
				YES	640.00	

4/03/1998 CASHBY 00000047 DAN:160235 08747174  
 1 FC:242 660.00 CH  
 2 FC:561 30.00 CH

Correspondence address change (Complete only if there is a change)	4. For printing on the patent front page, list the names of not more than 3 registered patent attorneys or agents OR, alternatively, the name of a firm having as a member a registered attorney or agent. If no name is listed, no name will be printed.
	1. Panitch 2. Schwarze 3. Jacobs & Nadel, P.C.

DO NOT USE THIS SPACE

ASSIGNMENT DATA TO BE PRINTED ON THE PATENT (print or type)	
NAME OF ASSIGNEE:	
ADDRESS (CITY & STATE OR COUNTRY)	
<input type="checkbox"/> This application is NOT assigned. <input type="checkbox"/> Assignment previously submitted to the Patent and Trademark Office. <input type="checkbox"/> Assignment is being submitted under separate cover. Assignments should be directed to Box ASSIGNMENTS. PLEASE NOTE: Unless an assignee is identified in Block 5, no assignee data will appear on the patent. Inclusion of assignee data is only appropriate when an assignment has been previously submitted to the PTO or is being submitted under separate cover. Completion of this form is NOT a substitute for filing an assignment.	5a. The following fees are enclosed: <input type="checkbox"/> Issue Fee <input type="checkbox"/> Advance Order - # of Copies 5b. The following fees should be charged to: 16-0235 DEPOSIT ACCOUNT NUMBER (ENCLOSE PART C) <input checked="" type="checkbox"/> Issue Fee <input checked="" type="checkbox"/> Advance Order - # of Copies 10 <input checked="" type="checkbox"/> Any Delinquencies in Enclosed Fees The COMMISSIONER OF PATENTS AND TRADEMARKS is requested to apply the Issue Fee to the application identified above. (Authorized Signature) <i>Josh Z. [Signature]</i> (Date) 3/30/98 NOTE: The Issue Fee will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the Patent and Trademark Office.

1. TRANSMIT THIS FORM WITH FEE CERTIFICATE OF MAILING ON REVERSE

PTOL-85B (REV.12-93)(0651-0033)

### Certificate of Mailing

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to:

Box ISSUE FEE

Commissioner of Patents and Trademarks  
Washington, D.C. 20231

on March 30, 1998  
(Date)

Dana Yost Hartman  
(Name of person making deposit)

Dana Yost Hartman  
(Signature)

3/30/98  
(Date)

Note: If this certificate of mailing is used, it can only be used to transmit the Issue Fee. 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.

Burden Hour Statement: This form is estimated to take .2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Office of Information Systems, Patent and Trademark Office, Washington, D.C. 20231, and to the Office of Information and Regulatory Affairs, Office of Management and Budget, (Project 0651-0033), Washington, D.C. 20503. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner of Patents and Trademarks, Box Issue Fee, Washington, DC 20231.

The  
United  
States  
of  
America



Form PTO-1584 (Rev. 2/97)

PTO UTILITY GRANT

Paper Number 23

The Commissioner of Patents  
and Trademarks

*Has received an application for a patent for a new and useful invention. The title and description of the invention are enclosed. The requirements of law have been complied with, and it has been determined that a patent on the invention shall be granted under the law.*

Therefore, this

United States Patent

*Grants to the person(s) having title to this patent the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States of America or importing the invention into the United States of America for the term set forth below, subject to the payment of maintenance fees as provided by law.*

*If this application was filed prior to June 8, 1995, the term of this patent is the longer of seventeen years from the date of grant of this patent or twenty years from the earliest effective U.S. filing date of the application, subject to any statutory extension.*

*If this application was filed on or after June 8, 1995, the term of this patent is twenty years from the U.S. filing date, subject to an statutory extension. If the application contains a specific reference to an earlier filed application or applications under 35 U.S.C. 120, 121 or 365(c), the term of the patent is twenty years from the date on which the earliest application was filed, subject to any statutory extension.*

*Bruce Lehman*  
Commissioner of Patents and Trademarks

*Andrea J. Morton*  
Attest

(RIGHT INSIDE)

FP-LOW

T. # 5793,302  
8-11-98 24

PATENT  
BOX ISSUE FEE

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.

BY: Priscilla Driscoll DATE: April 28, 1998 # 54

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re: Patent Application of : ATTN: OFFICIAL DRAFTSPERSON  
Leon Stambler :  
Appln. No.: 08/747,174 :  
Filed: November 12, 1996 : Batch No. V91  
: Allowed: January 2, 1997  
For: METHOD FOR SECURING :  
INFORMATION RELEVANT TO A : Attorney Docket  
TRANSACTION (as amended) : No. 6074-1U5

**PETITION FOR EXTENSION OF TIME**

Applicant in the above-identified application hereby petitions for a one-month extension of time to and including May 2, 1998 for responding to the Notice of Allowability mailed January 2, 1998. A Transmittal of Formal Drawings accompanies this Petition.

Please charge the extension fee of \$55.00 and any additional fees, or credit any overpayment, to the account of Panitch Schwarze Jacobs & Nadel, P.C., Deposit Account No. 16-0235. One additional copy of this document is enclosed for accounting purposes.

Respectfully submitted,

LEON STAMBLER

5/07/1998 CASHBY 00000054 160235 08747174

1 FC:215 55.00 CN

4/28/98  
(Date)

BY: Clark Jablon  
Clark A. Jablon  
Registration No. 35,039  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
One Commerce Square  
2005 Market Street, 22nd Floor  
Philadelphia, PA 19103-7086  
Telephone: (215) 965-1293  
Facsimile: (215) 567-2991

MGB:CAJ:lcd  
Enclosures

PS/N2/163223.1



Cancel this request <sup>correction</sup> included in request under  
1.323 PATENT #25

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: ASSISTANT COMMISSIONER OF PATENTS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.

BY Elyabeth A. [Signature] DATE 12/14/98

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re:	U.S. Patent No.	: Group Art Unit: 2735
	5,793,302	:
		:
Issued:	August 11, 1998	: Examiner: B. Zimmerman
		:
For:	METHOD FOR SECURING	: Attorney Docket
	INFORMATION RELEVANT	: No. 6074-1U5
	TO A TRANSACTION	:

#25 [Signature]

Attention: Decision and Certificate of Correction  
Branch of the Patent Issue Division

REQUEST FOR CERTIFICATE OF CORRECTION  
OF PATENT FOR PTO MISTAKE (37 CFR 1.322(a))

1. Attached, in duplicate, is Form PTO-1050, with at least one copy being suitable for printing.
2. The exact page and line number where the error is shown correctly in the application file is:

Correction to column 38, line 64: see page 33, line 28  
(first word) of the Amendment mailed November 7, 1997 (filed by  
the USPTO on November 10, 1997).

3. Please send the Certificate to:

Clark A. Jablon, Esq.  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
One Commerce Square  
2005 Market Street, 22nd Floor  
Philadelphia, PA 19103-7086

Respectfully submitted,

LEON STAMBLER

12/14/98  
(Date)

Clark Jablon  
CLARK A. JABLON  
Reg. No. 35,039  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
One Commerce Square  
2005 Market Street, 22nd Floor  
Philadelphia, PA 19103-7086  
Telephone: (215) 567-2020  
Facsimile: (215) 567-2991

CAJ:eam

PATENT

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: ASSISTANT COMMISSIONER OF PATENTS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.

BY Elizabeth A. McLeod DATE 12/14/98

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: U.S. Patent No. : Group Art Unit: 2735  
5,793,302 :  
Issued: August 11, 1998 : Examiner: B. Zimmerman  
For: METHOD FOR SECURING : Attorney Docket  
INFORMATION RELEVANT : No. 6074-1U5  
TO A TRANSACTION :

#256ms

Attention: Decision and Certificate of Correction  
Branch of the Patent Issue Division

REQUEST FOR CERTIFICATE OF CORRECTION  
OF PATENT FOR APPLICANT'S MISTAKE (37 CFR 1.323)

1. It is noted that errors appear in this patent of a minor nature or character, as more fully described below. The errors occurred in good faith. Correction thereof does not involve such changes in the patent as would constitute new matter or would require reexamination. A certificate of correction is requested.

1/04/1999 BLANKING 00000000 16025 573202  
1/04/1999 00000011 16025 573202  
1 FC:145 100.00 CH

PSJNZ/204804.1

-1-

APPROVED

MAR 1 1999  
FOR THE COMMISSIONER OF PAT. & T.M.

2. Attached hereto, in duplicate, is Form PTO-1050, with at least one copy being suitable for printing.

3. The exact location in the specification and drawings where the errors occur in the application file are listed below, along with the associated page and line numbers in the application file and patent:

Correction to column 38, line 64: see page 33, line 28 of the Amendment mailed November 7, 1997 (filed by the USPTO on November 10, 1997). The missing comma between the first occurrences of "site" and "the" was an obvious grammatical mistake. The addition of the comma does not change the meaning or scope of the claim.

Correction to Fig. 9: The reference to a "Remote PIN" should have read "Remote Computer" to be consistent with column 8, lines 61-66 of the patent (page 17, lines 1-6 of the application).

Correction to Fig. 10B: The coder should be labeled as block "132" to be consistent with column 11, lines 15-20 of the patent (page 21, lines 27-33 of the application).

The above-identified corrections are fully supported by the original specification and thus do not constitute new matter. Correction is thus believed to be permitted.

Also attached hereto for the Examiner's convenience are copies of the above-noted drawing sheets showing the corrections in red.

4. Please send the Certificate to:

Clark A. Jablon, Esq.  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
One Commerce Square  
2005 Market Street, 22nd Floor  
Philadelphia, PA 19103-7086

5. Please pay the fee of \$100.00, as required by 37 CFR 1.20(a),  
as follows:

Charge Deposit Account No. 16-0235 the sum of \$100.00.

A duplicate of this request is attached.

Respectfully submitted,

LEON STAMBLER

12/14/98  
(Date)

Clark Jablon

CLARK A. JABLON  
Reg. No. 35,039  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
One Commerce Square  
2005 Market Street, 22nd Floor  
Philadelphia, PA 19103-7086  
Telephone: (215) 567-2020  
Facsimile: (215) 567-2991

CAJ:eam

Staple  
Here  
Only !

PRINTERS TRIM LINE

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. 5,793,302  
DATED August 11, 1998  
INVENTOR(S) Leon Stambler

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 38, line 64: after "second", insert --site--.

MAILING ADDRESS OF SENDER:

Clark A. Jablon  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
One Commerce Square  
2005 Market Street, 22nd Floor  
Philadelphia, PA 19103-7086

FORM PTO 1050 (Rev. 2-93)

PATENT NO. 5,793,302

No. of add'l copies  
@ 50¢ per page



PSJN2/204841.1

Staple  
Here  
Only!

PRINTER'S TRIM LINE

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : 5,793,302  
DATED : August 11, 1998  
INVENTOR(S) : Leon Stambler

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

*note*  
*Note*  
*Note*  
Column 38, line 64: before "the" (second occurrence), insert <sup>*site,*</sup> ~~---~~ *Orndt HICK*  
Sheet 2, Fig. 9: Change "REMOTE PIN" to --REMOTE COMPUTER--, as shown on the attached page.  
Sheet 5, Fig. 10B: Add a label "132" to the coder block, as shown on the attached page.

MAILING ADDRESS OF SENDER:

Clark A. Jablon  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
One Commerce Square  
2005 Market Street, 22nd Floor  
Philadelphia, PA 19103-7086

PATENT NO. 5,793,302

No. of add'l copies  
@ 50¢ per page



FORM PTO 1050 (Rev. 2-93)

PSJN2/204857.1

NOTICE RE: CERTIFICATES OF CORRECTION

# 26

Paper ...

DATE : 2-8-99

TO : Supervisor, Art Unit 2735

SUBJECT : Certificate of Correction Request in Patent No. 5,799,302

A response to the following question(s) is requested with respect to the accompanying request for a certificate of correction.

- ☒ 1. Would the change(s) requested under 37 CFR 1.323 constitute new matter or require reexamination of the application?
- ☒ 2. Would the change(s) requested under 37 CFR 1.323 materially affect the scope or meaning of the claims allowed by the examiner in the patent?
- ☐ 3. Applicant disagrees with change(s) initialed and dated by Examiner in lieu of an Examiner's Amendment. Should the change request be granted?
- ☐ 4. With respect to the change(s) requested, correcting Office errors, should the patent read as shown in the certificate of correction?
- ☐ 5. If the amendment filed \_\_\_\_\_ had been considered by the Examiner, would the amendment have been entered?

PLEASE RESPOND WITHIN 7 DAYS AND RETURN THE FILE TO  
ROOM 809, PKI  
201

*Trina Smith*  
Patent Assistant

TO: CERTIFICATES OF CORRECTION BRANCH

DATE:

The decision regarding the change(s) requested in the certificate of correction is shown below.

- |                                 |  |   |
|---------------------------------|--|---|
| 1. <input type="checkbox"/> YES | <input checked="" type="checkbox"/> NO | <input type="checkbox"/> Comments below |
| 2. <input type="checkbox"/> YES | <input checked="" type="checkbox"/> NO | <input type="checkbox"/> Comments below |
| 3. <input type="checkbox"/> YES | <input type="checkbox"/> NO            | <input type="checkbox"/> Comments below |
| 4. <input type="checkbox"/> YES | <input type="checkbox"/> NO            | <input type="checkbox"/> Comments below |
| 5. <input type="checkbox"/> YES | <input type="checkbox"/> NO            | <input type="checkbox"/> Comments below |

☐ Comments \_\_\_\_\_

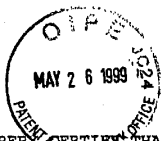
\_\_\_\_\_ 2/23/99

MICHAEL HORABIK  
SUPERVISOR PATENT EXAMINER  
GROUP 2700

*Michael Horabik*  
Supervisor

2735  
Art Unit





Cofc

PATENT

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: ASSISTANT COMMISSIONER OF PATENTS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.

BY Elizabeth A. McLeod DATE 5/24/99

1115

#27 Jan

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: U.S. Patent No. : Group Art Unit: 2735  
5,793,302 :  
Issued: August 11, 1998 : Examiner: B. Zimmerman  
For: METHOD FOR SECURING : Attorney Docket  
INFORMATION RELEVANT : No. 6074-1U5  
TO A TRANSACTION

JUN - 9 1999

Attention: Decision and Certificate of Correction  
Branch of the Patent Issue Division

STATUS REQUEST LETTER FOR PREVIOUSLY FILED  
CERTIFICATE OF CORRECTION OF PATENT FOR PTO MISTAKE

On December 14, 1998, Applicant filed a "Request for Certificate of Correction of Patent for PTO Mistake" and a "Request for Certificate of Correction of Patent for Applicant's Mistake."

On March 30, 1999, a Certificate of Correction was issued for the corrections set forth in the "Request for Certificate of Correction of Patent for Applicant's Mistake." However, the Certificate of Correction did not include the corrections set forth in the "Request for Certificate of

PSJN2/232035.1

APPROVED

AUG 24 1999

Mary J. [Signature]  
FOR THE COMMISSIONER OF PAT. & T.M.

Correction of Patent for PTO Mistake," nor was a second Certificate of Correction for the mistake set forth in that request.

Please review this matter and let us know the processing status of the "Request for Certificate of Correction of Patent for PTO Mistake." A copy of the following documents are enclosed to assist in this matter:

1. Copy of "Request for Certificate of Correction of Patent for PTO Mistake."
2. Copy of stamped postcard receipt showing a receipt date of December 15, 1998 by the Certificate of Correction Branch.

Respectfully submitted,

LEON STAMBLER

5/24/99  
(Date)

Clark Jablon  
CLARK A. JABLON  
Reg. No. 35,039  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
One Commerce Square  
2005 Market Street, 22nd Floor  
Philadelphia, PA 19103-7086  
Telephone: (215) 567-2020  
Facsimile: (215) 567-2991

CAJ:eam

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : 5,793,302  
DATED : August 11, 1998  
INVENTOR(S) : Leon Stambler

Page 1 of 3

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 38, line 64: before "the" (second occurrence), insert --,--.

Sheet 2, Fig. 9: Change "REMOTE PIN" to --REMOTE COMPUTER--.

Sheet 5, Fig. 10B: Add a label "132" to the coder block.

Signed and Sealed this  
Thirtieth Day of March, 1999

Attest:



Q. TODD DICKINSON

Attesting Officer

Acting Commissioner of Patents and Trademarks

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. 5,793,302  
DATED August 11, 1998  
INVENTOR(S) Leon Stambler

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 38, line 64: after "second", insert --site--.

Signed and Sealed this  
Twenty-first Day of September, 1999

Attest:



Attesting Officer

Q. TODD DICKINSON

Acting Commissioner of Patents and Trademarks

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. 5,793,302  
DATED August 11, 1998  
INVENTOR(S) Leon Stambler

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 38, line 64: after "second", insert --site--.

MAILING ADDRESS OF SENDER:

Clark A. Jablon  
PANITCH SCHWARZE JACOBS & NADEL, P.C.  
One Commerce Square  
2005 Market Street, 22nd Floor  
Philadelphia, PA 19103-7086

FORM PTO 1050 (Rev. 2-93)

PATENT NO. 5,793,302

No. of add'l copies  
@ 50¢ per page



PSJN2/204841.1

May-07-2008 14:38 From-PATTON BOGGS,LLP

T-021 P 002/006 F-797

U.S. Patent No. 5,793,302  
Issued: August 11, 1998

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED

In Re Application: Leon Stambler

MAY 13 2008

Patent No.: 5,793,302

OFFICE OF PETITIONS

Issued: August 11, 1998

For: Method for Securing Information Relevant to  
a Transaction

U.S. Patent and Trademark Office, 05/12/2008 DALLIN 00000008 5793302  
P.O. Box 979070  
St. Louis, MO 63197-9000 01 FC11559 1210.00 OP

REQUEST FOR ACCEPTANCE OF PAYMENT OF DEFICIENCY OWED

Dear Sir:

With regard to the referenced patent, inventor, Leon Stambler (hereinafter "Stambler"), hereby notifies the Patent and Trademark Office that small entity status is no longer appropriate pursuant to 37 C.F.R. § 1.27(g)(2) and that the claim for small entity status is hereby withdrawn.

Without deceptive intent, on August 11, 2005, an 8th year maintenance fee in the amount of \$1,150.00 was paid for the referenced patent. As Stambler was not entitled to small entity status on that date for the referenced patent, the payment submitted for the 8th year maintenance fee was deficient. The current 8th year maintenance fee pursuant to 37 CFR 1.20(f) is \$2,360.00. In addition, it is believed that a surcharge of \$130.00 is also required. The following is an itemization of the deficient payment:

475313

1

PAGE 2/6 \* RCVD AT 5/7/2008 3:40:24 PM [Eastern Daylight Time] \* SVR:USPTO-EFAXF-6/22 \* DNIS:2736500 \* CSID:+ \* DURATION (mm-ss):01:36

U.S. Patent No. 5,793,302  
Issued: August 11, 1998

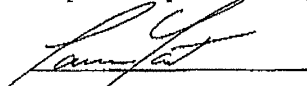
Fee Type:	8th Year Maintenance Fee
Fee Actually Paid:	\$1,150.00
Maintenance Fee Deficiency:	\$1,210.00
Surcharge Deficiency:	\$130.00
Total Deficiency:	\$1,340.00

Submitted herewith is Form PTO-2038 authorizing payment of the deficiency amount of \$1,340.00. It is believe that no additional fees are due with the filing of this Request. However, if any additional fees are due or any overpayments have been made, please charge or credit Patton Boggs' Deposit Account No. 50-2816.

In view of the forgoing, the USPTO is respectfully requested to accept payment of the deficiency owed. The USPTO is requested to call the undersigned with any questions relating to this payment.

Dated this 7th day of May, 2008.

Respectfully submitted,



Lawrence R. Youst  
Reg. No. 38,795  
Patton Boggs, LLP  
2001 Ross Avenue, Suite 3000  
Dallas, Texas 75201  
Tel 214.758.3414  
Fax 214.758.1550

May-07-2008 14:37, From-PATTON BOGGS,LLP

T-021 P.001/006 F-787

RECEIVED

MAY 13 2008

OFFICE OF PETITIONS

Approved for use through 09/30/2007. OMB 0851-0031  
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE  
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.

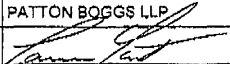
TRANSMITTAL FORM	
U.S. Patent Number	5,793,302
Issued	August 11, 1998
U.S. Patent App. No.	08/747,174
Inventor	Leon Stambler
Attorney Docket Number	TBD
Total Number of Pages in This Submission	4

**ENCLOSURES (Check all that apply)**

<input type="checkbox"/> Fee Transmittal Form	<input type="checkbox"/> Drawing(s)	<input type="checkbox"/> After Allowance Communication to TC
<input type="checkbox"/> Fee Attached	<input type="checkbox"/> Licensing-related Papers	<input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences
<input type="checkbox"/> Amendment/Reply	<input type="checkbox"/> Petition	<input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
<input type="checkbox"/> After Final	<input type="checkbox"/> Petition to Convert to a Provisional Application	<input checked="" type="checkbox"/> Request for Acceptance of Payment of Deficiency Owed - Maintenance Fee
<input type="checkbox"/> Affidavits/declaration(s)	<input checked="" type="checkbox"/> Power of Attorney, Revocation/Change of Correspondence Address	<input checked="" type="checkbox"/> Fee Address Indication Form
<input type="checkbox"/> Extension of Time Request	<input type="checkbox"/> Terminal Disclaimer	<input checked="" type="checkbox"/> Other Enclosure(s) (please identify below): Credit Card Payment Form
<input type="checkbox"/> Express Abandonment Request	<input type="checkbox"/> Request for Refund	
<input type="checkbox"/> Information Disclosure Statement	<input type="checkbox"/> CD, Number of CD(s)	
<input type="checkbox"/> Certified Copy of Priority Document(s)	<input type="checkbox"/> Landscape Table on CD	
<input type="checkbox"/> Reply to Missing Parts/Incomplete Application		
<input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53		

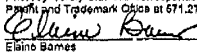
Remarks

**SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT**

Firm Name	PATTON BOGGS LLP		
Signature			
Printed name	Lawrence R. Youst		
Date	May 7, 2008	Reg. No.	38,795

Certificate of Transmission Under 37 C.F.R. § 1.8

I hereby certify that this correspondence is being transmitted by facsimile to the United States Patent and Trademark Office at 671.273.6500 on May 7, 2008.

  
Elaine Barnes

475360

PAGE 1/6 \* RCVD AT 5/7/2008 3:40:24 PM [Eastern Daylight Time] \* SVR:USPTO-EFXXRF-6/22 \* DNIS:2736500 \* CSID:\* \* DURATION (mm:ss):01:36





UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS  
UNITED STATES PATENT AND TRADEMARK OFFICE  
P.O. BOX 1450  
ALEXANDRIA, VA 22313-1450  
www.uspto.gov

Paper No. 28

LAWRENCE R. YOUST  
2001 ROSS AVENUE  
SUITE 3000  
DALLAS TX 75201

**COPY MAILED**

AUG 08 2008

In re Patent No. 5,793,302 :  
Issue Date: August 11, 1998 :  
Application No. 08/747,174 :  
Filed: November 12, 1996 :  
Attorney Docket No. 6074-1-US :

NOTICE

This is a notice regarding your request for acceptance of a fee deficiency submission under 37 CFR 1.28.

The Office no longer investigates or rejects original or reissue applications under 37 CFR 1.56. 1098 Off. Gaz. Pat. Office 502 (January 3, 1989). Therefore, nothing in this Notice is intended to imply that an investigation was done.

Your fee deficiency submission under 37 CFR 1.28 is hereby **ACCEPTED**.

Petitioner authorized payment of the deficiency amount of \$1,340.00. However, there is no surcharge required for late payment of maintenance fee when notifying the office the change of entity. Therefore, the \$130.00 surcharge will not be charged.

This application is no longer entitled to small entity status. Accordingly, all future fees paid in this application must be paid at the large entity rate.

Inquiries related to this communication should be directed to the undersigned at (571) 272-3213.

Cheryl Gibson-Baylor  
Petitions Examiner  
Office of Petitions

Irvin Dingle  
Petitions Examiner

# PATENT APPLICATION FEE DETERMINATION RECORD

Effective October 1, 1996

Application or Docket Number

08/1747174

## CLAIMS AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA
BASIC FEE		
TOTAL CLAIMS	24	24
INDEPENDENT CLAIMS	13	10
MULTIPLE DEPENDENT CLAIMS PRESENT		

\* If the difference in column 1 is less than zero, enter "0" in column 2

## CLAIMS AS AMENDED - PART II

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT	(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
AMENDMENT A			
Total	13	13	1
Independent	3	3	1
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM			

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT	(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
AMENDMENT B			
Total	10	10	1
Independent	3	3	1
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM			

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT	(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
AMENDMENT C			
Total	10	10	21
Independent	3	3	9
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM			

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.

SMALL ENTITY OR OTHER THAN SMALL ENTITY

RATE	FEE	OR	RATE	FEE
X\$11=	264	OR	X\$22=	528
X40=	400	OR	X80=	
+130=		OR	+260=	
TOTAL	1049	OR	TOTAL	

SMALL ENTITY OR OTHER THAN SMALL ENTITY

RATE	ADDITIONAL FEE	OR	RATE	ADDITIONAL FEE
X\$11=		OR	X\$22=	
X40=		OR	X80=	
+130=		OR	+260=	
TOTAL		OR	TOTAL	

RATE	ADDITIONAL FEE	OR	RATE	ADDITIONAL FEE
X\$11=		OR	X\$22=	
X40=		OR	X80=	
+130=		OR	+260=	
TOTAL		OR	TOTAL	

RATE	ADDITIONAL FEE	OR	RATE	ADDITIONAL FEE
X\$11=	281	OR	X\$22=	562
X40=	360	OR	X80=	
+130=		OR	+260=	
TOTAL	591	OR	TOTAL	1122

PATENT APPLICATION FEE DETERMINATION RECORD					Application or Docket Number	
Effective December 16, 1991					747174	
<b>CLAIMS AS FILED - PART I</b>					SMALL ENTITY OR OTHER THAN SMALL ENTITY	
(Column 1)		(Column 2)				
FOR	NUMBER FILED	NUMBER EXTRA		RATE	FEE	
BASIC FEE					270.00	
TOTAL CLAIMS	minus 20 =	*		x \$44 =		
INDEPENDENT CLAIMS	minus 3 =	*		x \$44 =		
MULTIPLE DEPENDENT CLAIM PRESENT				+ \$44 =		
				TOTAL		
* If the difference in column 1 is less than zero, enter "0" in column 2						
<b>* CLAIMS AS AMENDED - PART II</b>					SMALL ENTITY OR OTHER THAN SMALL ENTITY	
(Column 1)		(Column 2)		(Column 3)		
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDITIONAL FEE
	Total	* 91	Minus	** 65	= 26	x \$10 = 260
	Independent	* 24	Minus	*** 22	= 2	x \$36 = 72
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				+ \$110 =	
					TOTAL ADDIT. FEE	336
(Column 1)		(Column 2)		(Column 3)		
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDITIONAL FEE
	Total	*	Minus	**	=	x \$10 =
	Independent	*	Minus	***	=	x \$36 =
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				+ \$110 =	
					TOTAL ADDIT. FEE	
(Column 1)		(Column 2)		(Column 3)		
AMENDMENT C	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDITIONAL FEE
	Total	*	Minus	**	=	x \$10 =
	Independent	*	Minus	***	=	x \$36 =
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				+ \$110 =	
					TOTAL ADDIT. 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.						

Form PTO-875  
(Rev. 12 91)

Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

**U.S. DEPARTMENT OF COMMERCE**  
Patent and Trademark Office

1ST EXAMINER *Simm*

DATE 1/27/11

2ND EXAMINER

DATE \_\_\_\_\_

APPLICATION NUMBER  
**08/747174**

☒

FILING DATE					
MONTH		DAY		YEAR	
1	1	1	2	9	6

**SPECIAL  
HANDLING**

2

GROUP ART UNIT			
2	2	4	2

CLASS

3	A	X
---	---	---

SHEETS OF  
DRAWING

0	1	5
---	---	---

TOTAL CLAIMS		
0	4	4

INDEPENDENT  
CLAIMS

4	1	3
---	---	---

**SMALL  
ENTITY?**  
☒

FILING FEE			
1	0	4	9

**FOREIGN  
LICENSE**  
☒

ATTORNEY DOCKET NUMBER

6	8	7	4	-	/		4	5			
---	---	---	---	---	---	--	---	---	--	--	--

CONT	STATUS
CODE	CODE

PARENT APPLICATION  
SERIAL NUMBER

PCT APPLICATION SERIAL NUMBER

**PARENT PATENT  
NUMBER**

**PARENT FILING  
DATE**

2	2	8	4	4	6	3	6	9
1	1	8	1	2	2	7	7	1
1	1	7	9	7	7	3	8	5

P	C	T	/				/						
P	C	T	/				/						
P	C	T	/				/						
P	C	T	/				/						
P	C	T	/				/						

100	5	5	2	4	<del>8</del>	7	3
50	5	2	6	7	3	1	4
10							
1							

<del>8</del>	5	2	2	9	5
<del>8</del>	9	1	4	9	3
1	1	1	7	9	

**FOREIGN  
PRIORITY  
CLAIMED**

**COUNTRY  
CODE**

PCT/FOREIGN APPLICATION SERIAL NUMBER

**FOREIGN  
FILING DATE**

MONTH DAY YEAR

## MPI Family Report (Family Bibliographic and Legal Status)

In the MPI Family report, all publication stages are collapsed into a single record, based on identical application data. The bibliographic information displayed in the collapsed record is taken from the latest publication.

**Report Created Date:** 2008-08-19

**Name of Report:**

**Number of Families:** 1

**Comments:**

### Table of Contents

1. US5793302A 19980811 STAMBLER; LEON US	
Method for securing information relevant to a transaction .....	4



MicroPatent Patent Index - an enhanced INPADOC database

**Family1****7 records in the family.****US5524073A 19960604**

[ no drawing available]

**(ENG) Secure transaction system and method utilized therein****Inventor(s):** STAMBLER LEON US**Application No:** US 12207193 A**Filing Date:** 19930914**Issue/Publication Date:** 19960604

**Abstract:** (ENG) A transaction system is disclosed wherein, when a transaction, document or thing needs to be authenticated, information associated with one or more of the parties involved is coded together to produce a joint code. This joint code is then utilized to code information relevant to the transaction, document or record, in order to produce a variable authentication number (VAN) at the initiation of the transaction. This VAN is thereafter associated with the transaction and is recorded on the document or thing, along with the original information that was coded. During subsequent stages of the transaction, only parties capable of reconstructing the joint code will be able to uncode the VAN properly in order to re-derive the information. The joint code serves to authenticate the parties, and the comparison of the re-derived information against the information recorded on the document serves to authenticate the accuracy of that information.

**Priority Data:** US 12207193 19930914 A N; US 97738592 19921117 A 3 Y;**Related Application(s):** 07/977385 19921117 5267314 GRANTED**IPC (International Class):** G07F00712; G07F00710; H04L00932**ECLA (European Class):** G07F00710E; G07F00708E4; G07F00710C6; H04L00932R**US Class:** 705075; 705002; 713176**Agent(s):** Panitch Schwarze Jacobs & Nadel**Examiner Primary:** Cangialosi, Salvatore**US Post Issuance:**

--US Expiration Date: 20040604 20040803 DUE TO FAILURE TO PAY MAINTENANCE FEES

--US Certificate of Correction: 19960910 a Certificate of Correction was issued for this Patent

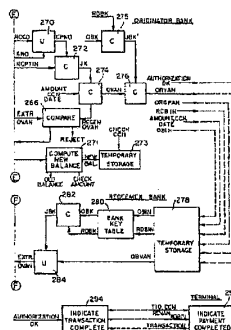
**Legal Status:**

Date	+/-	Code	Description
19960910	( )	CC	CERTIFICATE OF CORRECTION
20040803	(-)	FP	EXPIRED DUE TO FAILURE TO PAY MAINTENANCE FEE

Effective date: 20040604;



MicroPatent Patent Index - an enhanced INPADOC database

**US5646998A 19970708****(ENG) Secure transaction system and method utilized therein****Inventor(s):** STAMBLER LEON US**Application No:** US 44547795 A**Filing Date:** 19950522**Issue/Publication Date:** 19970708

**Abstract:** (ENG) A transaction system is disclosed wherein, when a transaction, document or thing needs to be authenticated, information associated with one or more of the parties involved is coded together to produce a joint code. This joint code is then utilized to code information relevant to the transaction, document or record, in order to produce a variable authentication number (VAN) at the initiation of the transaction. This VAN is thereafter associated with the transaction and is recorded on the document or thing, along with the original information that was coded. During subsequent stages of the transaction, only parties capable of reconstructing the joint code will be able to uncode the VAN properly in order to re-derive the information. The joint code serves to authenticate the parties, and the comparison of the re-derived information against the information recorded on the document serves to authenticate the accuracy of that information.

**Priority Data:** US 44547795 19950522 A N; US 12207193 19930914 A 3 Y; US 97738592 19921117 A 3 Y;**Related Application(s):** 08/122071 19930914 5524073 GRANTED 07/977385 19921117 5267314 GRANTED**IPC (International Class):** G07F00712; G07F00710; H04L00932**ECLA (European Class):** G07F00708E4; G07F00710C6; G07F00710E; H04L00932; H04L00932R2**US Class:** 705076; 713185**Agent(s):** Panitch Schwarze Jacobs & Nadel, P**Examiner Primary:** Cangialosi, Salvatore**US Post Issuance:**

--US Expiration Date: 20050708 20050906 DUE TO FAILURE TO PAY MAINTENANCE FEES

**Legal Status:**

Date	+/-	Code	Description
20050906	(-)	FP	EXPIRED DUE TO FAILURE TO PAY MAINTENANCE FEE Effective date: 20050708;



MicroPatent Patent Index - an enhanced INPADOC database

**US5555303A 19960910****(ENG) Secure transaction system and method utilized therein****Inventor(s):** STAMBLER LEON US

[ no drawing available]

**Application No:** US 44561295 A**Filing Date:** 19950522**Issue/Publication Date:** 19960910

**Abstract:** (ENG) A transaction system is disclosed wherein, when a transaction, document or thing needs to be authenticated, information associated with one or more of the parties involved is coded together to produce a joint code. This joint code is then utilized to code information relevant to the transaction, document or record, in order to produce a variable authentication number (VAN) at the initiation of the transaction. This VAN is thereafter associated with the transaction and is recorded on the document or thing, along with the original information that was coded. During subsequent stages of the transaction, only parties capable of reconstructing the joint code will be able to uncode the VAN properly in order to re-derive the information. The joint code serves to authenticate the parties, and the comparison of the re-derived information against the information recorded on the document serves to authenticate the accuracy of that information.

**Priority Data:** US 44561295 19950522 A N; US 12207193 19930914 A 3 Y; US 97738592 19921117 A 3 Y;**Related Application(s):** 08/122071 19930914 PENDING 07/977385 19921117 5267314 GRANTED**IPC (International Class):** G07F00712; G07F00710; H04L00932**ECLA (European Class):** G07F00708E4; G07F00710C6; G07F00710E; H04L00932; H04L00932R2**US Class:** 705075; 713176; 713193**Agent(s):** Panitch Schwarze Jacobs & Nadel, P**Examiner Primary:** Cangialosi, Salvatore**US Post Issuance:**

--US Expiration Date: 20040910 20041109 DUE TO FAILURE TO PAY MAINTENANCE FEES

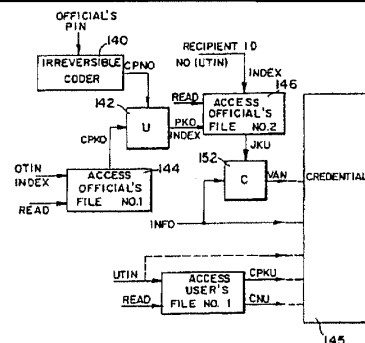
**Legal Status:**

Date	+/-	Code	Description
20041109	(-)	FP	EXPIRED DUE TO FAILURE TO PAY MAINTENANCE FEE Effective date: 20040910;



MicroPatent Patent Index - an enhanced INPADOC database



**US5793302A 19980811****(ENG) Method for securing information relevant to a transaction****Assignee:** STAMBLER; LEON US**Inventor(s):** STAMBLER LEON US**Application No:** US 74717496 A**Filing Date:** 19961112**Issue/Publication Date:** 19980811

**Abstract:** (ENG) A transaction system wherein, when a transaction, document or thing needs to be authenticated, information associated with one or more of the parties involved is coded together to produce a joint code. This joint code is then utilized to code information relevant to the transaction, document or record, in order to produce a variable authentication number (VAN) at the initiation of the transaction. This VAN is thereafter associated with the transaction and is recorded on the document or thing, along with the original information that was coded. During subsequent stages of the transaction, only parties capable of reconstructing the joint code will be able to uncode the VAN properly in order to re-derive the information. The joint code serves to authenticate the parties, and the comparison of the re-derived information against the information recorded on the document serves to authenticate the accuracy of that information.

**Priority Data:** US 12207193 19930914 A A; US 44636995 19950522 A I; US 74717496 19961112 A I; US 97738592 19921117 A A;

**Related Application(s):** 01 01; 01 01

**IPC (International Class):** G07F00712; G07F00710; H04L00932

**ECLA (European Class):** G07F00708E4; G07F00710C6; G07F00710E

**US Class:** 34000586; 34000541; 380043; 380045

**Publication Language:** ENG

**Filing Language:** ENG

**Agent(s):** Panitch Schwarze Jacobs & Nadel, P

**Examiner Primary:** Zimmerman, Brian

**US Post Issuance:**

--US Certificate of Correction: 19990330 a Certificate of Correction was issued for this patent; 19990921 a Certificate of Correction was issued for this patent

--US Litigations: Leon Stambler Leon Stambler 20010202 Delaware 01-065-SLR Final judgment is entered in favor of defendants and against plaintiff on all his claims of infringement under the '148 patent, the '541 patent, and the '302 patent. Defendant's motion for dismissal is granted in part, and defendants' invalidity counterclaims with respect to claims 1, 16 and 35 of the '148 patent and claim 12 of the '302 patent are dismissed without waiver and without prejudice as moot. Final judgment is entered against defendants and in favor of



MicroPatent Patent Index - an enhanced INPADOC database

**Legal Status:**

Date	+/-	Code	Description
19990330	()	CC	CERTIFICATE OF CORRECTION
19990921	()	CC	CERTIFICATE OF CORRECTION

**Assignee:** STAMBLER; LEON US

**Inventor(s):** STAMBLER LEON US

Application No: US 85556197 A

**Filing Date:** 19970513

**Issue/Publication Date:** 19991026

**Abstract:** (ENG) A transaction system is disclosed wherein, when a transaction, document or thing needs to be authenticated, information associated with one or more of the parties involved is coded together to produce a joint code. This joint code is then utilized to code information relevant to the transaction, document or record, in order to produce a variable authentication number (VAN) at the initiation of the transaction. This VAN is thereafter associated with the transaction and is recorded on the document or thing, along with the original information that was coded. During subsequent stages of the transaction, only parties capable of reconstructing the joint code will be able to decode the VAN properly in order to re-derive the information. The joint code serves to authenticate the parties, and the comparison of the re-derived information against the information recorded on the document serves to authenticate the accuracy of that information.

**Priority Data:** US 12207193 19930914 A R; US 44636995 19950522 A R; US 74717496 19961112 A R; US 85556197 19970513 A I; US 97738592 19921117 A R;

**Related Application(s):** 01 01; 01 01; 01 01 01

**IPC (International Class):** G07F00712; G07F00710

**ECLA (European Class):** G07F00710E; G07F00708E4; G07F00710C6



*MicroPatent Patent Index - an enhanced INPADOC database*

**US Class:** 705075; 705076

**Publication Language:** ENG

**Filing Language:** ENG

**Agent(s):** Akin, Gump, Strauss, Hauer & Feld, LP.

**Examiner Primary:** Cangialosi, Salvatore

**US Post Issuance:**

--US Expiration Date: 20071026 20071218 DUE TO FAILURE TO PAY MAINTENANCE FEES

--US Litigations: Leon Stambler Leon Stambler 20010202 Delaware

01-065-SLR Final judgment is entered in favor of defendants and against plaintiff on all his claims of infringement under the '148 patent, the '541 patent, and the '302 patent. Defendant's motion for dismissal is granted in part, and defendants' invalidity counterclaims with respect to claims 1, 16 and 35 of the '148 patent and claim 12 of the '302 patent are dismissed without waiver and without prejudice as moot. Final judgment is entered against defendants and in favor of plaintiff on defendants' invalidity counterclaims and affirmative defenses with respect to claim 27 of the '541 patent and claim 34 of the '302 patent. Defendants' motion for judgment as a matter of law of non-infringement of claim 27 of the '541 patent under the doctrine of equivalents is granted, and judgment is entered in favor of defendants and against plaintiff on his claim of infringement of claim 27 of the '541 patent. Verisign's motion for summary judgment of non-infringement of claim 12 of the '302 patent under the doctrine of equivalents (D.I. 274) is granted, and judgment is entered in favor of Verisign and against plaintiff on his claim of infringement of claim 12 of the '302 patent. So ordered this 17th day of April 2003 in Wilmington, Delaware. At Wilmington this 14th day of November, 2003, consistent with the memorandum opinion issued this same day; It is ordered that plaintiff Leon Stambler's motion for judgment as a matter of law, or in the alternative, for a new trial is denied. (D.I. 460), Sue L. Robinson, United States District Judge

**Legal Status:**

Date	+/-	Code	Description
20071218	(-)	FP	EXPIRED DUE TO FAILURE TO PAY MAINTENANCE FEE Effective date: 20071026;



MicroPatent Patent Index - an enhanced INPADOC database

**US5936541A 19990810****(ENG) Method for securing information relevant to a transaction****Assignee:** STAMBLER; LEON US**Inventor(s):** STAMBLER LEON US**Application No:** US 87211697 A**Filing Date:** 19970610**Issue/Publication Date:** 19990810

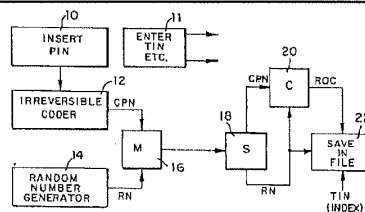
**Abstract:** (ENG) <p>A transaction system is disclosed wherein, when a transaction, document or thing needs to be authenticated, information associated with one or more of the parties involved is coded together to produce a joint code. This joint code is then utilized to code information relevant to the transaction, document or record, in order to produce a variable authentication number (VAN) at the initiation of the transaction. This VAN is thereafter associated with the transaction and is recorded on the document or thing, along with the original information that was coded. During subsequent stages of the transaction, only parties capable of reconstructing the joint code will be able to uncode the VAN properly in order to re-derive the information. The joint code serves to authenticate the parties, and the comparison of the re-derived information against the information recorded on the document serves to authenticate the accuracy of that information.</p>

**Priority Data:** US 12207193 19930914 A A; US 44636995 19950522 A A; US 87211697 19970610 A A; US 97738592 19921117 A A;

**Related Application(s):** 08/122071 19930914 5524073 GRANTED 07/977385 19921117 5267314 GRANTED; 08/446369 19950222 ABANDONED

**IPC (International Class):** H04K00100**ECLA (European Class):** G07F00708E4; G07F00710C6; G07F00710E; H04L00932**US Class:** 34000522; 380045; 705075; 705076**Agent(s):** Panitch, Schwarze, Jacobs & Nadel, P**Examiner Primary:** Zimmerman, Brian**US Post Issuance:**

--US Litigations: Leon Stambler RSA Security, Inc., et al 20010202 Delaware 01-065-SLR Final judgment is entered in favor of defendants and against plaintiff on all his claims of infringement under the '148 patent, the '541 patent, and the '302 patent. Defendant's motion for dismissal is granted in part, and defendants' invalidity counterclaims with respect to claims 1, 16 and 35 of the '148 patent and claim 12 of the '302 patent are dismissed without waiver and without prejudice as moot. Final judgment is entered against defendants and in favor of plaintiff on defendants' invalidity counterclaims and affirmative defenses with respect to claim 27 of the '541 patent and claim 34 of the '302 patent. Defendants' motion for judgment as a matter of law of non-infringement of claim 27 of the '541 patent under the doctrine of equivalents is granted, and judgment is entered in favor of defendants and against plaintiff on his claim of infringement of claim 27 of the '541 patent. Verisign's motion for summary judgment of non-infringement of claim 12 of the '302 patent under the doctrine of equivalents (D.I. 274) is granted, and judgment is entered in favor of Verisign and against plaintiff on his claim of infringement of claim 12 of the '302 patent. So ordered this 17th day of April



MicroPatent Patent Index - an enhanced INPADOC database

2003 in Wilmington, Delaware. At Wilmington this 14th day of November, 2003, consistent with the memorandum opinion issued this same day; It is ordered that plaintiff Leon Stambler's motion for judgment as a matter of law, or in the alternative, for a new trial is denied. (D.I. 460), Sue L. Robinson, United States District Judge

**Legal Status:** There is no Legal Status information available for this patent

**US5267314A 19931130**

**(ENG) Secure transaction system and method utilized therein**

**Assignee:** STAMBLER LEON US

**Inventor(s):** STAMBLER LEON US

**Application No:** US 97738592 A

**Filing Date:** 19921117

**Issue/Publication Date:** 19931130

**Abstract:** (ENG) A transaction system is disclosed wherein, when a transaction, document or thing needs to be authenticated, information associated with one or more of the parties involved is coded together to produce a joint code. This joint code is then utilized to code information relevant to the transaction, document or record, in order to produce a variable authentication number (VAN) at the initiation of the transaction. This VAN is thereafter associated with the transaction and is recorded on the document or thing, along with the original information that was coded. During subsequent stages of the transaction, only parties capable of reconstructing the joint code will be able to uncode the VAN properly in order to re-derive the information. The joint code serves to authenticate the parties, and the comparison of the re-derived information against the information recorded on the document serves to authenticate the accuracy of that information.

**Priority Data:** US 97738592 19921117 A Y;

**IPC (International Class):** G07F00712; G07F00710; H04L00932

**ECLA (European Class):** G07F00710E; G07F00708E4; G07F00710C6; H04L00932R

**US Class:** 713176; 705075; 713178; 713193

**Agent(s):** Panitch Schwarze Jacobs & Nadel

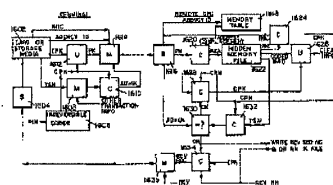
**Examiner Primary:** Cangialosi, Salvatore

**US Post Issuance:**

--US Expiration Date: 20051130 20060124 DUE TO FAILURE TO PAY MAINTENANCE FEES

**Legal Status:**

Date	+/-	Code	Description
20060124	(-)	FP	EXPIRED DUE TO FAILURE TO PAY MAINTENANCE FEE Effective date: 20051130;



MicroPatent Patent Index - an enhanced INPADOC database

U.S.P.T.O. Maintenance Report

Patent Bibliographic Data				08/19/2008 09:38 AM	
Patent Number:	5793302		Application Number:	08747174	
Issue Date:	08/11/1998		Filing Date:	11/12/1996	
Title:	METHOD FOR SECURING INFORMATION RELEVANT TO A TRANSACTION				
Status:	12th year fee window opens: 08/11/2009			Entity:	Large
Window Opens:	08/11/2009	Surcharge Date:	02/12/2010	Expiration:	N/A
Fee Amt Due:	Window not open	Surchg Amt Due:	Window not open	Total Amt Due:	Window not open
Fee Code:	1553	MAINTENANCE FEE DUE AT 11.5 YEARS			
Surcharge Fee Code:					
Most recent events (up to 7):	05/14/2008 05/14/2008 05/09/2008 05/07/2008 08/11/2005 11/27/2001		Payor Number Assigned. Payer Number De-assigned. Pat Hldr no Longer Claims Small Ent Stat Payment of Maintenance Fee under 1.28(c). Payment of Maintenance Fee, 8th Yr, Small Entity. Payment of Maintenance Fee, 4th Yr, Small Entity. --- End of Maintenance History ---		
Address for fee purposes:	LAWRENCE R. YOUST 2001 Ross Avenue Suite 3000 DALLAS, TX 75201				