

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

LEON STAMBLER,

Plaintiff,

v.

AMAZON.COM, INC., et al

Defendants.

§
§
§
§
§
§
§
§

CIVIL ACTION NO. 2:09-cv-310

JURY TRIAL DEMANDED

PLAINTIFF'S OPENING CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	DISPUTED CONSTRUCTIONS	4
	A. “transferring funds from the first account of the first party to the second account of the second party if” – ‘302 Patent, claims 41, 51	4
	1. “Transferring” is not limited to crediting and debiting.....	4
	2. Defendants improperly construe “funds” as “the transfer amount”	5
	B. “party” – ‘302 claims 41, 44, 47 and 53; 148 Patent, claims 4, 34 and 35	6
	C. “coding” – ‘302 Patent, claims 7; ‘148 Patent, claim 35	6
	D. “coding the EDCI using a secret key of the originator” – ‘148 Patent, claim 35	7
	E. “and then coding the result using third information” – ‘302 Patent, claim 7	7
	F. “variable authentication number (VAN)”	9
	1. Stambler’s construction is consistent with prior constructions.....	9
	2. Stambler’s construction is that given the term by the specification	9
	G. “using at least a portion of the received funds transfer information” – ‘302 Patent, claim 41, 51.....	10
	H. “secret key of the payor/first party/originator” – ‘148 Patent, claims 1, 28, 34, and 35.....	11
	1. Stambler’s construction is based on the patent’s description of “joint key”	12
	2. The remaining attributes of the “secret key of the payor/first party/originator” are dictated by the claim language.....	13
	3. Defendants’ construction does not read on a preferred embodiment	13
	I. “including the VAN with the instrument for subsequent use in attesting to the authenticity of the instrument” – ‘148 Patent, claim 34	14
	J. “the originator’s VAN being usable to determine the authenticity of the one or more pieces of payment information” – ‘148 Patent, claim 35.....	14

K. “the VAN being used for attesting to authenticity of the payor and document information” – ‘148 Patent, claim 28.....	15
1. VAN being used for attesting to the authenticity of the payor	15
2. Defendants’ construction does not clarify the scope of the claim	16
L. “the VAN attesting to the authenticity of the first party and the first information” – ‘148 Patent, claim 1	16
M. “authentic” – ‘302 Patent, claims 41, 51	17
N. “credential” – ‘302 Patent, claims 7, 47, 55.....	18
O. “trusted entity / party” – ‘302 Patent, claims 7, 47, 53	19
P. “previously issued”	20
1. Claim 7.....	21
2. Claim 47	22
3. Claim 51.....	22
Q. “first/second storage means” – ‘302 patent, claim 41.....	23
R. “information for identifying the first/second account of the first/second party” – ‘302 Patent, claim 41	24
S. “one or more pieces of payment information including an amount, information for identifying the recipient party or the originator party, a date, and a check control or serial number” – ‘148 Patent, claim 35.....	25
T. “check control or serial number” – ‘148 Patent, claim 35	26
U. “descriptive details of the first party” – ‘148 Patent, claim 4	26
V. “instrument for transferring funds” / “payment instrument” – ‘148 Patent, claims 1, 28, 34, 35.....	27
W. “error detection code” – ‘302 Patent, claim 48; ‘148 Patent, claim 35.....	28
X. “including the VAN with the instrument” – ‘148 Patent, claim 34	28

Y. “attaching the VAN to the instrument” – ‘148 Patent, claim 1.....	29
Z. “appending the VAN to the payment instrument” – ‘148 Patent, claim 28	29
AA. “accounts receivable” / “accounts payable” – ‘302 Patent, claim 44	30
III. CONCLUSION.....	30

TABLE OF AUTHORITIES

CASES

<i>Acumed LLC v. Stryker Corp.</i> 483 F.3d 800 (Fed. Cir. 2007).....	5
<i>Black v. Ce Soir Lingerie Co.</i> 06-cv-544, 2007 U.S. Dist. LEXIS90962 (E.D. Tex. Dec. 11, 2007)	4
<i>Credle v. Bond</i> 25 F.3d 1566 (Fed. Cir. 1994).....	20
<i>Duratech Indus. Int’l, Inc. v. Bridgeview Mfg., Inc.</i> 292 Fed. Appx. 931 (Fed. Cir. 2008).....	23
<i>Oatey Co. v. IPS Corp.</i> 514 F.3d 1271 (Fed. Cir. 2008).....	5
<i>Phillips v. AWH Corp.</i> 415 F.3d 1303 (Fed. Cir. 2005).....	9
<i>Seal-Flex, Inc. v. Athletic Track & Court Const.</i> 172 F.3d 836 (Fed. Cir. 1999).....	20
<i>Source Search Techs., LLC v. Lending Tree, LLC</i> No. 04-4420, 2006 U.S. Dist. LEXIS 79651 (D.N.J. Oct. 16, 2006).....	23

OTHER

35 U.S.C. § 112, ¶ 6.....	23
Manual of Patent Examining Procedure § 608.01(i) (7th ed. 1997).....	20

I. INTRODUCTION

This case involves two patents issued to Leon Stambler — U.S. Patents 5,793,302 and 5,974,148 (the “Stambler patents”). The Stambler patents are titled “Method for Securing Information Relevant to a Transaction” and share a common specification. At issue are 19 terms that were already construed by this Court¹ and 15 additional terms designated by Defendants.

The Stambler patents disclose novel methods to authenticate parties and information involved in transactions. (1:15-21.)² Authentication refers to a plurality of concepts, including: (1) ensuring that a message has arrived exactly as it was sent, referred to as data integrity authentication; (2) ensuring that a message came from the stated source, referred to as data origin authentication, or (3) verifying the identity of an individual, which is referred to as entity authentication. (Ex. F at 360, 363, 365, 367; Ex. G at 30, 140-41, 385.)

To assist the Court in construing the disputed terms, an overview of the funds transfer embodiments illustrated by FIGS. 6-8 of the Stambler patents follows. These embodiments demonstrate the enrollment of a payment originator (FIG. 6), the creation of a check (FIG. 7), and the redemption and verification of the check (FIGS. 8A and 8B). Although the embodiments of FIGS. 6-8 are described in the context of creating and authenticating a paper check, the Stambler patents explain that these embodiments (and the disclosed concepts) apply equally to electronic funds transfers and a “paperless/cashless” transaction system, which completes “funds transfer” transactions (e.g., a purchase) “entirely electronically.” (5:28-30; 24:4-7.)³

FIG. 6 illustrates enrollment of an originator at his bank. First, the originator provides personal information (*e.g.*, a tax ID number), and the bank verifies his identity. (4:2-11.) Then the bank opens an account and creates a file for the originator, and the originator selects a secret

¹ *Stambler v. JPMorgan Chase & Co., et al.*, Case No. 08-cv-204-DF-CE (“*JPMorgan*”) and *Stambler v. Merrill Lynch & Co., Inc., et al.*, Case No. 08-cv-462-DF-CE (“*Merrill Lynch*”).

² Column:line, FIG., and Abstract references are to the ‘302 patent, attached as Exhibit A.

³ The patents also describe credential issuing and authentication systems. (*See, e.g.*, 12:35-13:39.)

personal identification number (“PIN”), which is irreversibly coded and transferred to the bank. (4:13-51.) The coded PIN is later used by the originator and the originator’s bank to generate cryptographic keys used to code or uncode funds transfer instructions (*e.g.*, a check).

FIG. 7 illustrates a method for generating a check. (4:52-53.) First, the originator inputs funds transfer information (*e.g.*, the originator’s tax ID number (“TIN”), the recipient’s TIN, an amount, and other information) into a computer or terminal. (4:53-60.) The originator then inputs his PIN, which is irreversibly coded to produce a coded PIN. (5:3-6.)

The coded PIN, together with information related to the funds transfer recipient (*e.g.*, the recipient’s TIN), are coded together to generate a cryptographic key called the “joint key” or “joint code.” (5:3-15.) The joint key is then used to code the funds transfer information to generate what the Stambler patents call a “variable authentication number” (“VAN”). (5:9-22.) The VAN is included with the funds transfer information to create the check. (5:25-34.)

FIGS. 8A and 8B illustrate methods for redeeming a check generated according to FIG. 7. (5:55-58.) In FIG. 8A, the check recipient first enters his PIN into a bank terminal. (5:62-66.) The PIN is irreversibly coded and transmitted, along with other information (*e.g.*, the recipient’s TIN) to the recipient’s bank. (5:66-6:40.) That bank accesses the recipient’s file using his TIN and verifies his identity with his coded PIN. (*Id.*) This is an example of entity authentication (*i.e.*, identity verification) — if the PIN is incorrect, the authentication fails. (6:38-40.) If the recipient’s identity is verified, his bank transfers the information from the check to the originator’s bank. (6:43-45.)

In FIG. 8B, the originator’s bank receives the funds transfer instructions and the VAN from the recipient’s bank, which is requesting authorization to pay. (6:43-45.) Using the originator’s TIN, the originator’s bank accesses the originator’s file and retrieves information used to derive

the originator's coded PIN. (6:46-55.) The terminal then generates a joint key by coding the originator's coded PIN (derived by the bank) with the recipient's TIN. (6:66-7:2.) The originator's bank then uses that joint key to uncode the VAN included with the check and compares the resulting information with the received funds transfer instructions. (7:2-11; FIG. 7, uncoder 58, comparator 60.) If they match, the funds transfer instructions are presumed to be unaltered (data integrity authentication) and to have come from the originator (data origin authentication). (7:16-20.)

Alternatively, the system authenticating the funds transfer information generates a new VAN by coding the funds transfer information with the separately generated joint key. (7:12-15.) This newly generated VAN is compared with the received VAN to authenticate the check. (Id.) If the VANs match, the funds transfer instructions are presumed to be unaltered (data integrity authentication) and to have come from the originator (data origin authentication). (7:16-20.)

As discussed above, three aspects of authentication are implicated in FIGS. 6-8B. Entity authentication is implicated when the check recipient cashes a check in FIG. 8A. The recipient's coded PIN is compared with a coded PIN stored by the bank to verify the recipient's identity. Data integrity authentication is implicated when the information uncoded from a VAN is compared with the received funds transfer information to determine if the information has been changed. And data origin authentication is involved when a VAN is coded or uncoded using the joint key. Because the joint key is created using the originator's coded PIN, a VAN created using the joint key corroborates that the VAN was, in fact, created by the originator.

II. DISPUTED CONSTRUCTIONS⁴

A. “transferring funds from the first account of the first party to the second account of the second party if” – ‘302 Patent, claims 41, 51

Stambler’s Construction	Defendants’ Construction
to cause funds to pass from the first account to the second account, including by debiting or crediting or by instructing another to debit or credit	debiting (i.e., deducting) the transfer amount from the first account and crediting (i.e., adding) the transfer amount to the second account if . . .

Stambler’s proposed construction is rooted in the ordinary meaning of “transfer,” the claims, and preferred embodiments described in the specification. Defendants’ construction fails because it disregards the plain meaning of “transfer” and excludes preferred embodiments.

1. “Transferring” is not limited to crediting and debiting.

“All claim construction begins with the words of the claims.” *See, e.g., Black v. Ce Soir Lingerie Co.*, 06-cv-544, 2007 U.S. Dist. LEXIS90962, at *30 (E.D. Tex. Dec. 11, 2007). The ordinary meaning of “transfer” is “to cause to pass from one place to another.” (Ex. I at 1900.) Thus, “transferring funds from the first account of the first party to the second account of the second party” means “to cause funds to pass from the first account to the second account.” Defendants’ construction, however, eschews the meaning of “transferring” and improperly constricts the broadly claimed “transferring funds” to include **only** crediting and debiting.

Moreover, Defendants’ proposed construction contradicts the claims. Claim 1 of the ‘148 patent, for example, recites “[a] method of **transferring funds** from a first party to a second party...” in which funds are “transferred” by “**creating an instrument** by the first party **for transferring funds** to the second party....” The claim does not include a “transferring” step. Thus, the claims require that “transferring funds” encompasses creating instructions (*e.g.*, an instrument) that cause funds to pass between accounts — not just crediting and debiting.

⁴ The Joint Claim Construction and Prehearing Statement [Dkt. No. 388] identifies the disputed terms and phrases. Since filing the joint statement, the parties have agreed that “payor” and “payer” refer to the same party and mean “a person or entity who pays, or who is to make a payment.”

Defendants' proposed construction also violates the doctrine of claim differentiation. Dependent claims are presumed to narrow and further limit the independent claims from which they depend. *See, e.g., Acumed LLC v. Stryker Corp.*, 483 F.3d 800, 806 (Fed. Cir. 2007). Independent claims 41 and 51 of the '302 patent include a "transferring funds" step. Dependent claims 42 and 52, which depend from claims 41 and 51, respectively, further recite "debiting the first account of the first party and crediting the second account of the second party." The claimed "crediting" and "debiting" steps narrow the claimed "transferring" step, confirming that "transferring" is broader than Defendants' proposed construction.

Further, Defendants' construction contradicts the specification, which uses "transferring" broadly and does not restrict it to "crediting" and "debiting." For example, in the embodiments of FIGS. 6-8 and 13, "transferring funds" may be accomplished by **dispensing paper money** from an ATM machine or cashing a check. (7:44-50.) Alternatively, "transferring funds" may be accomplished by an originator's bank debiting the originator's account and **instructing** a recipient's bank to credit the recipient's account. (7:28-30, 39-45.) By limiting "transferring" to "crediting" and "debiting", Defendants' construction excludes these preferred embodiments. *See, e.g., Oatey Co. v. IPS Corp.*, 514 F.3d 1271, 1276 (Fed. Cir. 2008) ("We normally do not interpret claims in a way that excludes embodiments disclosed in the specification.").

2. Defendants improperly construe "funds" as "the transfer amount".

Defendants' construction must also be rejected because it conflates and disregards the meaning of distinct claim terms in different claims — "transferring funds" and "the transfer amount." Claims 41 and 51 broadly recite a step for "transferring funds." Dependent claims 42 and 52, which depend from claims 41 and 51, respectively, more narrowly recite debiting and crediting a specific "funds transfer amount." Nowhere do the Stambler patents limit the "transferring **funds**" to the "funds transfer amount" or equate the meaning of those terms.

B. “party” – ‘302, claims 41, 44, 47 and 53; 148 Patent, claims 4, 34 and 35

Stambler’s Construction	Defendants’ Construction
a person or entity, computer system(s), or a person or entity using a computer system(s)	a person or legal entity, including computer systems put in use by that person or entity

The parties agree that the term “party” includes a person or entity, or a person or entity using a computer system. At issue is whether a computer system, by itself, can be a “party.”

Compelling intrinsic evidence confirms that a computer system – by itself – can be a “party.” During prosecution, Stambler described claim 124 of the ‘302 patent (issued claim 41) in the context of the disclosed “paperless/cashless transaction system.” (Ex. H at 54-55.) Stambler clearly explained to the USPTO that “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.*” (*Id.*) Thus, the file history clearly establishes that a “party” can be a computer system.

The patent claims further confirm that a computer system – separate from a person or entity that owns or uses the computer system – may be a “party.” Each of claims 17, 39, and 88 of the ‘302 patent recite “the second party being a person *or a computer program.*” (Ex. A at claims 17, 39, 88.) And claims 7, 25, and 73 of the ‘302 patent refer to a “computer program,” by itself, *as an entity.* (Ex. A at claims 7 (“the entity comprising a person or a computer program”), 73 (“the first entity and the second entity being a person, or a computer program”), 25). Defendants’ construction of “party” contradicts this intrinsic evidence and must be rejected.

C. “coding” – ‘302 Patent, claims 7; 148 Patent, claim 35

Stambler’s Construction	Defendants’ Construction
transforming information by applying a known algorithm	transforming original information into coded information by applying a known algorithm but excluding transforming coded information back into its original state

Stambler’s proposed construction for “coding” is battle-tested — it was adopted by the Delaware court, agreed to by all parties in the *JPMorgan* case, and again adopted by the Court in *Merrill Lynch*. (Ex. C at 6; Ex. D at 18-19; Ex. E at 4.) Moreover, it is rooted in the express

disclosure of coding found in the Stambler patents, which describes coding information using a “coder” that “may be *any form of such device utilizing a known algorithm.*” (3:37-39.) Thus, in express terms, the patents describe the function of a “coder” as expansively as possible. Defendants’ construction is a transparent attempt to tack on an “exclusion” for non-infringement.

D. “coding the EDC1 using a secret key of the originator” – ‘148 Patent, claim 35

Stambler’s Construction	Defendants’ Construction
transforming the EDC1 by applying a known algorithm using a secret key of the originator	reversibly transforming the EDC1 by applying a known algorithm using a secret key of the originator

The parties’ constructions are identical except that Defendants’ construction includes the limitation “reversibly.” But nothing in the claims suggests that “coding” is limited to “reversibly” transforming the EDC1, and as noted above, a coder “may be *any form* of such device utilizing a known algorithm.” By 1992, both irreversible and reversible coding algorithms were well-known. (Ex. G at 268, 449.) Defendants’ attempt to tack on the unfounded “reversibly” limitation must be rejected.⁵

E. “and then coding the result using third information” – ‘302 Patent, claim 7

Stambler’s Construction	Defendants’ Construction
and thereafter transforming the result by applying a known algorithm using third information	reversibly transforming the result by applying a known algorithm using a key (the third information) without intervening operations

There are three disputed aspects of this phrase: (1) whether the limitation “reversibly” should be imported into the construction of coding; (2) when the “coding” must occur (*i.e.*, the meaning of “and then”); and (3) whether the claimed “third information” is strictly limited to a “key.”

First, as discussed directly above, there is no basis in the claims, specification, or file history for limiting “coding” to “reversibl[e]” transformations.

Second, the claim language recites two coding processes: “*coding* the first information using

⁵ In Delaware, the defendants asked the court to construe “coding” as “applying a *reversible*, symmetric encryption algorithm.” (Ex. J at 32.) The court rejected the defendants’ attempt to limit “coding” to reversible encryption, noting that the specification states “that a ‘coder’ . . . may be *any form* of such device utilizing a known algorithm.” (Ex. E at 4.)

second information and then ***coding*** the result using third information.” Defendants’ construction requires the second coding operation to take place “without intervening operations.” However, this limitation finds no support in the claim language and flatly contradicts the processes described in the Stambler patents. Indeed, the patents describe numerous instances where a first piece of information is coded using a second piece of information, and later — ***after intervening operations*** — the result of coding the first and second pieces of information is coded using a third piece of information. For example, the patents disclose that a VAN may be generated directly from INFO and information associated with at least one of the parties (*e.g.*, a tax identification number). (5:6-13, 22-25.) The VAN (*i.e.*, the “result”) is stored on a check illustrated in FIG. 7. Later, in the redemption process of FIG. 13, the VAN from the check is coded using the joint bank key (JBK) at element 256. However, this second coding process does not take place “without intervening operations.” As illustrated in FIG. 13, after the initial coding operation, the VAN is: (1) recorded on a check; (2) the check is given from the originator to the recipient; (3) the recipient presents the check to a redeemer (block 200); (4) the VAN is read from the check and stored (block 250); and (5) the VAN is passed from temporary storage to coder 256, where it is coded using a joint bank key (JBK) (*i.e.*, the third information). (13:4-62, 15:27-45.) Defendants’ construction plainly excludes such embodiments and must be rejected.

Finally, Defendants wrongly argue that the “third information” is limited to a “key.” But that construction is inconsistent with the ordinary meaning of “information” and contradicts the specification, which states 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 [joint key].” (5:22-24.) Accordingly, Defendants’ construction must be rejected.

F. “variable authentication number (VAN)”

Stambler’s Construction	Defendants’ Construction
an encoded variable number that can be used in verifying the identity of a party or the integrity of information or both, the number generated by coding information relevant to a transaction, document, or thing with either a joint key or information associated with or assigned or related to at least one party to the transaction or issuance of the document or thing	an encoded variable number constructed to allow verification that information is not fraudulent

Variable authentication number (“VAN”) is a term coined by Mr. Stambler. Where, as here, a claim term has no understood meaning in the art, the proper construction is the definition given the term in the specification. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1321 (Fed. Cir. 2005).

1. Stambler’s construction is consistent with prior constructions.

In a funds transfer context, a VAN is an encoded variable number used in verifying the integrity and origin of funds transfer instructions (*e.g.*, a check). In a credential context, a VAN is an encoded variable number used in authenticating a credential, which is used for purposes of determining identity. Thus, the VAN is “an encoded variable number that can be used in verifying the identity of a party or the integrity of information or both....” This portion of Stambler’s construction was adopted by the Court in the *JPMorgan* and *Merrill Lynch* cases. (Ex. C at 11-13; Ex. D at 9-10; Ex. E at 2.)

2. Stambler’s construction is that given the term by the specification.

Further, the VAN is, by definition, created using other information. Indeed, it is ***always*** created in one of two ways: by coding information with either a joint key (or code), or “generated directly from INFO and information associated with at least one of the parties, without the intermediate step of generating the [joint key].” (*See, e.g.*, 2:9-17; 5:9-25; 11:65-12:2.) How the VAN is created defines, in part, what it is. Thus, the proper construction of VAN must reflect that the VAN is created by coding information to be authenticated “with either a joint key or information associated with or assigned or related to at least one party to the

transaction or issuance of the document or thing.” (See 2:9-17; 5:9-25; 10:42-45 (assigning a number to a party for use in creating a joint key); 11:15-20 (the VAN / joint key is created using information “*related to*” the parties)).

The *Merrill Lynch* court declined to construe VAN in terms of how it is created, reasoning that the claims themselves illustrate the information used to generate it. (Ex. D at 9-10.) Stambler respectfully disagrees. Indeed, asserted claim 34 of the ‘148 patent does not state what information is coded using the secret key, and asserted claim 41 of the ‘302 patent does not expressly state that the VAN is generated using a key or information associated with a party. Accordingly, the claims themselves do not necessarily reflect how a VAN is created. Because the way a VAN is created partially defines what it is, the Court should adopt Stambler’s proposed construction, which is true to the claims and specification.

G. “using at least a portion of the received funds transfer information” – ‘302 Patent, claim 41, 51

Stambler’s Construction	Defendants’ Construction
Plain meaning; alternatively, using some, but not necessarily all, of the received funds transfer information	using at least some of the information for identifying the first account of the first party, at least some of the information for identifying the second account of the second party, and at least some of the transfer amount

Claims 41 and 51 recite the disputed claim language as follows:

receiving funds transfer information ... 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.*

“[T]he received funds transfer information” claimed in the “generating” step refers back to the “funds transfer information” received in the preceding step. Accordingly, “the received funds transfer information” includes “information for identifying the first account of the first party,” “information for identifying the second account of the second party,” and “a transfer amount.”

The limitation “generating a [VAN] using at least **a portion** of the received funds transfer information,” however, requires using only some of the information defined as the “received funds transfer information.” Indeed, using any portion of the “received funds transfer information” to create the VAN satisfies the claim. For example, generating a VAN using only “information for identifying the first account of the first party” — but not the “transfer amount” — satisfies the plain meaning of the claim language “using at least a portion of the received funds transfer information.”

Defendants’ construction re-writes claims 41 and 51. The claims do not require “using at least a portion” of **each** type of information in the “received funds transfer information” — they only require using a portion of **any** information in the “received funds transfer information.” Defendants’ construction turns the plain meaning of the claim language on its head.

H. “secret key of the payor/first party/originator” – ‘148 Patent, claims 1, 28, 34, and 35

Stambler’s Construction	Defendants’ Construction
a private key that is created by the payor/first party/originator, or an entity originating an instrument on the payor’s/first party’s/originator’s behalf, by coding information associated with or related to the payor/first party/originator, which is capable of being separately created by a party intended to authenticate the instrument	key that is generated by coding information associated with and known, prior to any coding, only by the payor/first party/originator party for use in any future transactions

Both parties disagree with the *Merrill Lynch* construction.⁶ (Ex. D at 10-11.)

The “secret key” terms appear in claims 1, 28, 34 and 35 of the ‘148 patent. These claims are “funds transfer” or “payment” methods. (Ex. B at claims 1, 28, 34, and 35.) In each of these claims, the “secret key” is used to create a VAN. (*Id.*) For example, claim 34 recites “the VAN being created using at least *a secret key of the first party.*” (*Id.* at claim 34.)

The **only** cryptographic key that (1) the specification describes as a “key” and (2) is used to

⁶ Although Stambler’s proposed construction was not adopted in *JPMorgan* or *Merrill Lynch*, Stambler believes his construction is sound and warrants reconsideration by the Court.

create the VAN in the funds transfer embodiments is the “joint key.” (FIGS. 7, 8B, 13D; 5:13-15.) **No** other “keys” for coding a VAN are disclosed in a funds transfer context. The “secret key” is clearly a specific embodiment of the joint key (or code). The Court should, thus, look to Stambler’s disclosure of the joint key to construe the term “secret key.”

1. Stambler’s construction is based on the patents’ description of “joint key.”

Stambler’s patents define the joint key (also called “joint code”)⁷ as a “**key**” that is created by coding information associated with one or more parties, which is capable of being separately created by the party authenticating the instrument. This mirrors the Abstract, which states:

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. ... **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 “Summary of the Invention” recites the same definition. (2:9-27.) And the specification confirms that definition as well. Specifically, the joint key in funds transfer embodiments is created by coding “information associated with **at least one of the parties involved in the transaction** (in this case, the originator and recipient).” (5:11-14; FIG. 7; 16:1-6.) An authenticating system later re-creates the joint key in the same manner. (6:66-7:2.)

The specification also explains that creation of the joint key by the payment originator preferably, but not necessarily, takes place at an originator’s terminal or computer using information provided by the originator. (4:53-54; FIG. 7.) Accordingly, as Stambler’s construction indicates, the “secret key” is “created by the payor/first party/originator, or an entity originating an instrument on the payor’s/first party’s/originator’s behalf.”

⁷ (5:13-15) (“the joint key (or code)....”)

2. The remaining attributes of the “secret key of the payor/first party/originator” are dictated by the claim language.

According to the specification, the joint key may be created by coding information associated with the payor/first party/originator, the second party/payee/recipient, or both. (5:11-14; FIG. 7.) The claim language “of the payor/first party/originator” specifies that the “secret key” of claims 1, 28, 34, and 35 is created by coding at least information associated with the payor/first party/originator. Accordingly, the proper construction must specify that the “secret key” is created using “information associated with the payor/first party/originator.”

Finally, the key of the “payor/first party/originator” is “secret.” “Secret” may be construed as “private,” which means “designed or intended for one’s exclusive use.” (See Ex. I at 1442.)

3. Defendants’ construction does not read on a preferred embodiment.

Moreover, Defendants’ construction is improper because it contradicts the specification and does not read on at least one preferred embodiment. Specifically, Defendants’ construction includes a limitation that the “secret key” of claims 28, 34, and 35 “is generated by coding information associated with and known, prior to any coding, **only by the payor/first party/originator party** for use in any future transactions.” In the funds transfer embodiments, however, the joint key is generated using information known to both **the originator and the originator’s bank**. As illustrated in FIG. 7, the transaction system codes the originator’s coded PIN with the check recipient’s TIN to produce the joint key. (5:3-10; FIG. 7, element 10, 28.) Defendants’ construction, which requires creating the key by coding “information ... known ... **only** by the payor/first party/originator[.]” ignores the fact that the originator’s bank maintains information from which it too can derive the joint key.

Lastly, Defendants’ construction reads unfounded limitations into the claim. The broadly disclosed joint key is created using “information associated with one or more of the parties

involved....” (Abstract.) Nothing in the Stambler patents requires that the joint key is created using “information associated with and known, prior to any coding, only by the payor....”

I. “including the VAN with the instrument for subsequent use in attesting to the authenticity of the instrument” – ‘148 Patent, claim 34

Stambler’s Construction	Defendants’ Construction
including the VAN with the instrument for subsequent use in verifying that the information in the instrument has not changed and verifying that the instrument originated from the first party	including the VAN with the instrument for subsequent use in verifying that the instrument is not fraudulent

Stambler’s construction was adopted in *JPMorgan* and accepted by all parties in *Merrill Lynch*. (Ex. C at 18-19; Ex. D at 7.) It reflects the ordinary meaning of “authenticate,” which means “ensuring that a message is genuine, has arrived exactly as it was sent and came from the stated source.” (Ex. F at 360.) And, it is consistent with the specification, which describes using a VAN to attest to the integrity of information and the origin of information. (See, e.g., 7:16-20.)

Defendants’ construction is unhelpful and confusing. The phrase “not fraudulent” can mean several things — indeed, the Stambler patents use the term “fraud” to refer to several distinct concepts, including unauthorized creation (*i.e.*, origination), unauthorized alteration, or unauthorized use. (See 1:29-34; 7:21-24; 20:13-15.) Thus, “not fraudulent,” as it appears in Defendants’ construction, is ambiguous and difficult for a jury to apply. It provides no guidance regarding the type of “fraud” the VAN must be used to prevent (*i.e.*, what the VAN is used to verify). Stambler’s construction, on the other hand, provides the clarity Defendants’ construction lacks without deviating from the ordinary meaning or intrinsic evidence.

J. “the originator’s VAN being usable to determine the authenticity of the one or more pieces of payment information” – ‘148 Patent, claim 35

Stambler’s Construction	Defendants’ Construction
the originator’s VAN being usable to verify that the one or more pieces of payment information has not changed and to verify that the one or more pieces of payment information originated from the originator party	the originator’s VAN being usable to verify that the one or more pieces of payment information are not fraudulent

Stambler's construction was accepted by the parties in *Merrill Lynch* and is based on the *JPMorgan* Court's construction for "including the VAN with the instrument for subsequent use in attesting to the authenticity of the instrument." (Ex. C at 18-19; Ex. D at 7.) Stambler's construction is true to the ordinary meaning of "authentic" and the specification, and it precisely defines that the VAN is used to verify "that the one or more pieces of payment information has not changed" and "that the one or more pieces of payment information originated from the originator." As discussed above, Defendants' use of the term "fraudulent" only injects ambiguity into the claim.

K. "the VAN being used for attesting to the authenticity of the payor and document information" – '148 Patent, claim 28

Stambler's Construction	Defendants' Construction
the VAN being used to verify that the instrument originated from the payor and that the at least a portion of the document information used to create the VAN has not changed	the VAN being used to verify that the identity of the payor and the document information used to create the VAN are not fraudulent

Stambler's construction is that adopted by the Court in the *JPMorgan* case and agreed to by the parties in the *Merrill Lynch* case. (Ex. C at 16-18; Ex. P at 17.) Claim 28 is a "payment method" in which a "payor" creates a "payment instrument" and a "VAN." The disputed phrase concerns the VAN – "the VAN being used for attesting to the authenticity of the payor and document information...."

1. VAN being used for attesting to the authenticity of the payor.

The parties dispute the meaning of the phrase "attesting to the authenticity of the payor." Stambler contends that the phrase refers to origin verification. Defendants contend that the phrase refers to identity verification. In *JPMorgan*, the Court specifically rejected the argument that the disputed claim language "attesting to the authenticity of the payor" requires identity verification. (Ex. C at 17.) Indeed, the notion that the VAN in Stambler's funds transfer embodiments could be used to verify identity is nonsensical. In such embodiments, the

originator of a funds transfer instrument is not present when the instrument is authorized and, thus, there is no need or ability to verify the originator's identity. (*See, e.g.*, 5:55-6:45; FIG. 8.) Rather, the VAN is used to ensure that the originator party did in fact create the instrument that is being authorized. This is a form of origin authentication, not identity authentication.

An analogy to the authentication processes in traditional paper check systems illustrates the flaws in Defendants' construction. When the recipient of a paper check presents the check to a bank, the bank does not "verify the identity of" the originator. Rather, the bank confirms that the check actually originated from the originator (*e.g.*, was not forged) using a signature on the check. Similarly, the VAN is used to confirm that the payor in fact originated, or authorized, the funds transfer instructions. If the information extracted from the VAN does not match the funds transfer instructions, the payor's bank determines that the instrument did not originate from the payor and rejects the transfer. (7:2-20.)

2. Defendants' construction does not clarify the scope of the claim.

As discussed above, the Stambler patents use the term "fraud" to refer to **several** activities: unauthorized creation (*i.e.*, origination), unauthorized alteration, *or* unauthorized use. (*See* 1:29-34; 7:21-24; 20:13-15.) Defendants' construction is unhelpful and ambiguous because it fails to clarify the types of fraud the VAN is used to prevent (*i.e.*, what the VAN is used to verify).

L. **"the VAN attesting to the authenticity of the first party and the first information" – '148 Patent, claim 1**

Stambler's Construction	Defendants' Construction
the VAN being used to verify that the first information originated from the first party and that the first information has not changed	the VAN being used to verify that the identity of the first party and the first information used to create the VAN are not fraudulent

Stambler's construction is based on the Court's prior constructions and the agreed construction for a similar phrase, "the VAN attesting to the authenticity of the payor and document information," in *Merrill Lynch*. (Ex. C at 16-18; Ex. P at 17.) The only difference

between the disputed phrase in this case and the phrase construed in *Merrill Lynch* is that claim 1 — at issue here — recites a “first party” and “first information” rather than a “payor” and “document information.” Because the scope of the disputed phrases is virtually identical, the construction for the two phrases should be consistent. As explained in Section II(K), Stambler’s construction properly defines what the VAN verifies, while Defendants’ construction is ambiguous and injects the concept of identity verification.

M. “authentic” – ‘302 Patent, claims 41, 51

Stambler’s Construction	Defendants’ Construction
This term is used differently in different contexts throughout the patents. ‘302 Patent, claims 41 and 51: determined to be unchanged, from a stated origin, or not fraudulent	not fraudulent

Although the parties in *JPMorgan* and *Merrill Lynch* did not propose constructions for “authentic,” by itself, prior constructions of phrases that include the term “authentic” confirm that “authentic” means “unchanged, from a stated origin, or not fraudulent.” (See Ex. C at 19-20; Ex. D at 20-22.) The *JPMorgan* and *Merrill Lynch* Courts correctly construed “determining whether the at least a portion of the received funds transfer information is **authentic** by using the VAN” as “using the VAN to determine that the at least a portion of the funds transfer **information has not changed** and to **determine the origin of the at least a portion of the received funds transfer information.**” (Ex. D at 20-21.) And the Courts correctly construed “if the at least a portion of the received funds transfer information and the VAN are determined to be authentic” as “if the at least a portion of the received funds transfer information is **unchanged** and the VAN is **not fraudulent.**” (Ex. C at 19-20.) Based on the Court’s prior constructions, it

is clear that the term “authentic” may mean “determined to be unchanged, from a stated origin, or not fraudulent.”⁸

N. “credential” – ‘302 Patent, claims 7, 47, 51

Stambler’s Construction	Defendants’ Construction
a non-secret document or information obtained from a trusted source that is transferred or presented for purposes of determining the identity of a party	a document or thing obtained from a trusted source that establishes the identity of a party when it is transferred or presented

With the exception of the word “non-secret,” Stambler’s construction is the same as the Court’s constructions in *JPMorgan* and *Merrill Lynch*. (Ex. C at 21-22; Ex. D at 11-12.) Stambler asks the Court to reconsider whether a “credential is “non-secret.” In the April 9, 2010 *JPMorgan* Claim Construction Order, the Court appears to agree that Stambler’s “credentials” are not-secret. (See Ex. C at 22 (“[A]s used in the patent, a credential is intended to be a document or information presented to another for review. As such, it would make sense that **the credential cannot be secret.**”) (emphasis added)). Yet the Court declined to include the adjective “non-secret” in its construction, reasoning that because claim 7 of the ‘302 patent states that the “credential” includes “non-secret information,” the term is unnecessary. (Ex. C at 22.) That reasoning breaks down, however, because other claims at issue in this case (specifically, asserted claim 47 of the ‘302 patent) recite a “credential” **without** explicitly requiring that the “credential” contain “non-secret information.” Stambler’s construction is thus **necessary** to clarify that — as the *JPMorgan* Court noted — that a “credential cannot be secret.” Moreover, this construction is on all fours with the specification. All of the disclosed credentials, and all information recorded on the disclosed credentials, is “non-secret.” And though “secret” information is used to create these credentials (e.g., the joint key), the “secret” information used

⁸ Given that the term “authentic” appears in separate contexts within claims 41 and 51, it may make sense to construe “authentic” in the context of the phrases in which the term appears rather than attempting to craft a one-size-fits-all construction. If so, Stambler’ proposes the constructions previously adopted by the Court for “if the at least a portion of the received funds transfer information and the VAN are determined to be authentic” and “determining whether the at least a portion of the received funds transfer information is authentic by using the VAN.” (See Ex. C at 19-20; Ex. D at 20-22.)

to create a credential is never stored in the credential. (*See, e.g.*, 11:33-13:39; FIGS. 11-12.)

The parties also dispute how a “credential” is used. Stambler’s construction accurately reflects the way “credentials” are described in the patents. Specifically, the Stambler patents identify passive instruments such as a driver’s license, social security card, and birth certificate as example “credentials.” (8:54-58.) Such credentials are presented as evidence of identity, and the receiving party or system uses the credential to verify identity. (12:30-34; FIG. 12.) However, such credentials — by themselves — do **not** “establish the identity of a party,” as required by Defendants’ construction. Rather, such credentials are documents or information **used for purposes of** determining the identity of the party presenting the credential. This is the same conclusion reached in *JPMorgan* and *Merrill Lynch*. (Ex. C at 21-22; Ex. D at 11-12.)

O. “trusted entity / party” – ‘302 Patent, claims 7, 47, 51

Stambler’s Construction	Defendants’ Construction
an entity / party that has the authority or ability to establish or confirm a party’s identity	an entity / party that has the officially recognized authority to establish or confirm a party’s identity

“Trusted party” and “trusted entity” appear in claims 7, 47, and 51, which claim a credential issued by a trusted entity, or party. Stambler’s construction was adopted by the Court in *Merrill Lynch* and is consistent with the patent disclosure. (Ex. D at 12.) Specifically, it reflects the broad range of disclosed credentials without improperly limiting the inventive concepts to a particular “officially recognized” environment. (1:28-32) (“Similarly passports, pay checks, motor vehicle registrations, diplomas, food stamps, wager receipts, medical prescriptions, birth certificates and other official documents are subject to forgery, fraudulent modification....”) The Stambler patents explain that the disclosed credential issuance systems and methods apply to “all types of credentials,” including **“all types of identification cards.”** (8:54-58 (emphasis added).) Thus, Mr. Stambler’s inventions find utility not only in the issuance of government identification cards (*e.g.*, a passport), but also in the issuance of credentials by non-government entities, such

as employee identification cards, security badges, and school identification cards.

Because the term “trusted party/entity” must include the types of parties/entities that issue the diverse credentials and identification cards disclosed by Stambler, it is improper to limit trusted entity to an entity that has “**officially recognized authority**,” as proposed by Defendants. Indeed, nothing in claims 7, 47, or 51 requires or suggests that the “trusted entity/party” must have “officially recognized authority.” Defendants’ construction should also be rejected because the concept of “officially recognized” authority is vague and ambiguous.

P. “previously issued”

The term “previously issued” appears in asserted claims 7, 47, and 51 of the ‘302 patent. Stambler’s constructions are the same as the constructions adopted in *JPMorgan* and *Merrill Lynch*. In those cases, the Court correctly held that “previously issued” means “issued before the execution of the steps recited in the claim,” and that the term does not give rise to an additional claim step. (Ex. C at 24-26; Ex. D at 20.)

Grammar and syntax can be important in construing claim terms. *See Credle v. Bond*, 25 F.3d 1566, 1571 (Fed. Cir. 1994). Indeed, the Federal Circuit recognizes that each step of a method claim usually begins with a present participle – verbs ending in “-ing.” *See id.* at 1572; *Seal-Flex, Inc. v. Athletic Track & Court Const.*, 172 F.3d 836, 849 (Fed. Cir. 1999). Method claims in the Stambler patents follow this convention. And, as is customary in method claims, each step in Stambler’s claims is offset using a semicolon or the conjunction “and.” Moreover, Stambler’s claims generally follow the common convention of indenting separate claim steps. *See* MPEP § 608.01(i) (7th ed. 1997) (“Where a claim sets forth a plurality of elements or steps, each element or step of the claim should be separated by a line indentation.”) (Ex. M.) Accordingly, the grammar and syntax of Stambler’s claims clearly identify each step in the claimed methods.

1. Claim 7.

Stambler's Construction	Defendants' Construction
"Wherein a credential having non-secret information stored therein is previously issued to at least one entity by a trusted entity" is a limitation but not a step of the claim. The term "previously issued" means issued before the execution of the steps recited in the claim.	"Wherein a credential having non-secret information stored therein is previously issued to at least one entity by a trusted entity" is a required step of the claim which occurs prior to "coding the information using second information."

The parties dispute whether the phrase "wherein a credential having non-secret information stored therein is previously issued to at least one entity by a trusted entity" is a descriptive phrase or a separate, additional step recited in the claimed method. As discussed above, Stambler identifies active steps of his method claims using present participles. Claim 7 is no different. Stambler recites two active steps: "**coding** the first information using second information" and "**coding** the result using third information." The two steps are offset by the conjunction "and." All other limitations in the claim relate to and limit the "coding" steps.

The phrase "**wherein** a credential having non-secret information stored therein is previously issued to at least one entity by a trusted entity" is a **condition** that limits the universe of information used in the "coding" steps of the claim. After reciting two "coding" steps, claim 7 defines what information is coded in the coding steps. First Stambler recites "at least one of the second and third information being associated with at least one entity." Stambler then further limits the claim by limiting the "at least one entity," reciting "wherein a credential having non-secret information stored therein is previously issued to at least one entity by a trusted entity." Thus the disputed language merely limits what information may be used in the two previously-recited coding steps, which are clearly identified as such.

Stambler's construction of the phrase "previously issued" as a condition rather than a step is also consistent with accepted usage of present and past participles. The present participle, ending in "-ing," denotes the verb's action as **in progress** or **incomplete** at the time expressed by

the sentence's principal verb – in this case “coding.” (Ex. L at 176.) The past participle “issued” denotes the verb's action as **complete**. (*Id.*) This is confirmed by the adverb “previously.”

2. Claim 47.

Stambler's Construction	Defendants' Construction
“At least one party being previously issued a credential by a trusted party” is a limitation but not a step in the claimed method. The term “previously issued” means “issued before the execution of the steps recited in the claim.”	“At least one party being previously issued a credential by a trusted party” is a required step of the claim that occurs prior to the other steps recited in the claim.

Claim 47 depends from claim 41, which recites “receiving,” “generating,” “determining,” and “transferring” steps. Claim 47 limits the method of claim 41 by requiring that at least one party to the funds transfer of claim 41 (*e.g.*, the “first party,” “second party,” or “third party”) was “previously issued a credential.” As is customary, the active steps of claim 41 are recited using present participles, and are indented and offset using semicolons or the conjunction “and.” By contrast, the disputed phrase “at least one party being **previously issued** a credential by a trusted party” does not share these features — it is **not** offset using semicolons and does **not** use a present participle. Indeed, the claim does not require “issuing a credential to at least one party” — an additional, active step — but merely requires “at least one party being **previously issued** a credential,” indicating that “being previously issued a credential” is a characteristic of at least one party. Defendants’ construction, which injects an additional “issuing” step, lacks evidentiary support and is a transparent attempt to create divided infringement that must be rejected.

3. Claim 51.

The parties do not appear to dispute the scope of the term “previously issued” in claim 51. To the extent Defendants allege the disputed limitation is an additional claim step, Defendants’ construction must be rejected for the reasons described above.

Q. “first/second storage means” – ‘302 patent, claim 41

Stambler’s Construction	Defendants’ Construction
This element is not subject to 35 U.S.C. § 112, ¶ 6: a first/second place for storing information, which may include a computer file Alternatively, if the Court concludes this element is subject to 35 U.S.C. § 112, ¶ 6: <u>Function</u>: storing the first/second account information <u>Structure</u>: documents, files, memory or other computer storage, tables, personal storage media	This term is a means plus function limitation as defined by 35 U.S.C. § 112, ¶ 6: <u>Function</u>: storing the first/second party’s account information. <u>Structure</u>: first/second party’s bank’s computer

Stambler’s construction was adopted in *Merrill Lynch*. Defendants contend that “first storage means” and “second storage means” are means-plus-function limitations governed by 35 U.S.C. § 112, ¶ 6, though the *Merrill Lynch* Court explicitly rejected that argument and ruled that “‘storage means’ was well defined in the art at the time of the invention.” (Ex. D at 16-17.) That ruling is firmly rooted in Federal Circuit case law,⁹ district court decisions,¹⁰ and technical dictionaries.¹¹ The Court also found that the “the claim is not drafted in standard § 112, ¶ 6 format (*e.g.*, “means for [performing a function]”)” and, thus, U.S.C. § 112, ¶ 6 does not apply. (Ex. D at 16-17.) The *Merrill Lynch* Court’s ruling is sound and should be affirmed here.

Even if the Court reverses the September 24 ruling and finds that the claim terms are subject to 35 U.S.C. § 112, ¶ 6, Defendants’ proposed function disregards the claim language and improperly reads “the first/second **party’s** account information” into the claim. Claim 41 recites that the first/second account is “**associated with**” the first/second party — not that it **is** the first/second party’s account. Moreover, the disclosure is replete with structure corresponding to storing account information that is not included in Defendants’ proposal, including computer

⁹ *Duratech Indus. Int’l, Inc. v. Bridgeview Mfg., Inc.*, 292 Fed. Appx. 931, 933 (Fed. Cir. 2008) (A claim term avoids § 112, ¶ 6 “if the claim term is used in common parlance or by persons of skill in the pertinent art to designate structure, even if the term covers a broad class of structures”).

¹⁰ *Source Search Techs., LLC v. Lending Tree, LLC*, No. 04-4420, 2006 U.S. Dist. LEXIS 79651, at *53-56 (D.N.J. Oct. 16, 2006) (refusing to construe “storage means” as means-plus-function).

¹¹ (Ex. K at 72, 149, 168-69, 221, 290, 302, 339.)

files and storage (FIG 6, Element 22; FIG 8A, element 68; FIG 8B, element 50; 4:9-11), bank cards (4:11-13), and terminals (24:4-9). Further, dependent claims 49 and 50 recite that the “storage means” can be a credential, which can be a document or storage media. (9:54-60.)

Lastly, Defendants’ proposed structure improperly limits the claimed structure to a “first/second party’s *bank’s* computer.” That construction fails because it excludes the “paperless/cashless embodiment” of Mr. Stambler’s patents — the specific embodiment cited during prosecution as supporting this claim. (Ex. H at 54-55.) In that embodiment, “a *payment recipient’s terminal* ... stores information to identify the precise location of the recipient’s account.” (24:7-9.) Thus, the payment recipient may be the party selling a good or service, such as a retailer — which is not a bank. (24:4-7.)

R. “information for identifying the first/second account of the first/second party” – ‘302 Patent, claim 41

Stambler’s Construction	Defendants’ Construction
information that is used to identify an account associated with the first/second party	information that is used to identify a precise record of debit and/or credit transactions particular to the first/second party

The parties agree that the language “information for identifying” means “information that is used to identify.” The parties’ dispute what “the first/second account of the first/second party” means. Specifically, the parties’ dispute the relationship of the first and second accounts to the first and second parties, and whether “account” needs to be construed.

Stambler’s construction accurately identifies the first and second accounts as accounts “associated with” the first and second parties. Claim 41’s preamble describes “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 claim’s “receiving” step recites “receiving . . . information for identifying *the* first account of the first party, and information for identifying *the* second account of the second party.” Stambler’s use of the article “the” before “first account”

and “second account” confirms that the disputed terms find antecedent in the previous phrases “a first account **associated with** a first party” and “a second account **associated with** a second party.” Thus, “the first account of the first party” and “the second account of the second party” are accounts “associated with” the first and second parties, respectively.

Defendants’ construction identifies the first and second accounts as accounts that are “particular to” the first and second parties. That construction must be rejected because it fails to comport with the claim language itself, which identifies the first and second accounts as accounts that are “associated with” the first and second parties.

Finally, it is unnecessary for the Court to construe “account” because the term has a well understood meaning, and Stambler uses the term in its ordinary sense. An “account” is “a precise list or enumeration of financial transactions.” (Ex. I at 12; Ex. O at 3.) It is not limited to “a record of debit and/or credit transactions,” as proposed by Defendants.

S. “one or more pieces of payment information including an amount, information for identifying the recipient party or the originator party, a date, and a check control or serial number” – ‘148 Patent, claim 35

Stambler’s Construction	Defendants’ Construction
one or more pieces of the following payment information: an amount, information for identifying the recipient party or the originator party, a date, and a check control or serial number	one or more pieces of payment information, the one or more pieces of payment information including each of the following: an amount, information for identifying the recipient party or the originator party, a date, and a check control or serial number

The parties’ dispute whether the claimed payment instrument must include all, or just one of, “one or more pieces of payment information.” Stambler’s construction, which was adopted by the *JPMorgan* Court and agreed to by the parties in *Merrill Lynch*, aligns with, and is required by, the phrase “one or more pieces of payment information.” (Ex. C at 27-28; Ex. D at 7.) That phrase — “**one or more**” — leaves no question that the claim is satisfied when one “piece” of payment information is included with the instrument. Defendants’ construction turns a blind eye

to the plain meaning of the term and demands that the instrument include ***all*** the recited pieces of payment information. That construction contradicts the claim language and must be rejected.

T. “check control or serial number” – ‘148 Patent, claim 35

Stambler’s Construction	Defendants’ Construction
a value that is used to identify an instrument	a unique number for determining the identity of the instrument

A serial number is “a number that is one of a series and is used for identification.” (Ex. I at 1647.) A check serial number, which Stambler calls a check control number, is a serial number assigned to a check in a series of checks. (See Ex. Q at 3:37-38.) Stambler’s construction is consistent with the ordinary meaning of “check control or serial number.” Defendants’ construction, however, imposes an additional limitation — “uniqueness” — that finds no support in the specification or the claims. Although the patents describe embodiments in which a check control/serial number is used to determine that an instrument is not a duplicate, nothing in the specification requires that a check control/serial number is “unique.” (7:21-24, 14:36-41.) Indeed, check control numbers (*e.g.*, 101, 102, 103...) are often used in connection with account numbers to detect duplicates. Yet different customers might have checks with the same serial number. Accordingly, Defendants’ construction is improper.

U. “descriptive details of the first party” – ‘148 Patent, claim 4

Stambler’s Construction	Defendants’ Construction
information that describes a feature of the first party	personal information that identifies a first party

Claim 4 states that “the secret key is obtained by the first party using a PIN, or using ***descriptive details, of the first party.***” Stambler’s construction is consistent with the ordinary meaning of that claim language. Descriptive means “serving to describe,” and detail means “an individual part.” (Ex. I at 505, 508.) It follows that “descriptive details of the first party” means “information that describes a feature of the first party.” Defendants’ construction should be

rejected because it disregards the plain meaning of the claim language. While “descriptive detail” may identify a party, it is not required to do so.

Stambler’s construction is also consistent with the specification. As discussed above, the claimed “secret key” is an embodiment of the disclosed joint key. *See* Section II(H). The specification states that a joint key is “generated using information associated with at least one of the parties involved in the transaction.” (5:11-12.) Information that describes a feature of the first party is “information ***associated with***” at least one of the parties to a transaction. The specification does ***not*** require that the joint key is generated using information that “identifies” a party, as Defendants allege. For example, the specification discloses using a person’s telephone number to access a file that contains information (ROC and CPN) used to derive the joint key. (4:8-43.) The telephone number, which is used to obtain the joint key, is information that describes a feature of a party, but it is plainly ***not*** “information that ***identifies*** the first party” because a telephone number may identify with numerous parties (*e.g.*, different members of a household).

V. “instrument for transferring funds” / “payment instrument” – ‘148 Patent, claims 1, 28, 34, 35

Stambler’s Construction	Defendants’ Construction
“instrument for transferring funds”: a document (including paper or electronic) that is used to transfer funds to a recipient party	“instrument for transferring funds”: a financial document (including paper or electronic) that includes all the information necessary to transfer funds to a recipient party
“payment instrument”: a document (including paper or electronic) that is used to transfer funds to a recipient party in connection with a [payment]	“payment instrument”: a financial document (including paper or electronic) that includes all the information necessary to transfer funds to a recipient party in connection with a payment

Stambler’s constructions were adopted by the *JPMorgan* Court and agreed to by the parties in *Merrill Lynch*. (Ex. C at 20; Ex. D at 7.) Defendants’ construction should be rejected because the term “***financial*** document” is unclear and superfluous. It is unclear what a “financial

document” is, and the term “financial” is wholly unnecessary because the parties agree that the claimed instruments are used for “transferring funds” and that a “payment instrument” is used “in connection with a payment.”

Defendants’ constructions should also be rejected to the extent they require an “instrument” to include “***all the information necessary*** to transfer funds to a recipient party.” The limitation “all the information necessary to transfer funds” finds no support in the intrinsic record. Moreover, the asserted claims explicitly recite what information the claimed “instrument” must include. For example, claim 1 (from which asserted claim 4 depends) recites “the instrument including the first information and the [VAN],” and “the first information including an amount and information for identifying the first party or the second party.”

W. “error detection code” – ‘302 Patent, claim 48; ‘148 Patent, claim 35

Stambler’s Construction	Defendants’ Construction
the result of applying an algorithm for coding information that, when applied to original information, creates coded information wherein changes to the coded information can be detected without complete recovery of the original information	an algorithm for coding information that, when applied to original information, creates coded information wherein changes to the coded information can be detected without complete recovery of the original information

Stambler asks the Court to clarify that the claimed “error detection code” is the result of applying an algorithm. Claim 35, for example, recites “creating an error detection code (EDC1) by coding one or more pieces of payment information.” In the claimed contexts, error detection code clearly refers to the **result** of applying an algorithm rather than the algorithm itself.

X. “including the VAN with the instrument” – ‘148 Patent, claim 34

Stambler’s Construction	Defendants’ Construction
<i>No construction necessary beyond the meaning of the terms VAN and instrument.</i> including the [VAN] with the [instrument]	the VAN accompanying the instrument

The Court’s constructions for the terms “VAN” and “instrument” will resolve any question concerning the scope of the phrase “including the VAN with the instrument.” Defendants

apparently believe that the term “including” is ambiguous. The term “including” is an ordinary word that Stambler uses in its ordinary sense. For instance, the specification states that in an electronic transaction, “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.” (5:28-32.) In this context, as in other contexts in the patent, Stambler uses “including” according to its ordinary meaning “taking in as a part, an element, or a member.”¹² Defendants’ construction should be rejected as inconsistent with the ordinary meaning of the claim language and a transparent attempt to narrow the claim language. Stambler is unaware of any objective source that defines “including” as “accompanying.” (See Ex. I at 913; Ex. N at 576.)

Y. “attaching the VAN to the instrument” – ‘148 Patent, claim 1

Stambler’s Construction	Defendants’ Construction
joining or connecting the [VAN] to the [instrument]	the VAN joined to the instrument

Stambler’s construction is consistent with the ordinary meaning of the claim language. The two most common definitions of “attach” are “to fasten, secure, or **join**” and “**to connect** as an adjunct or associated condition or part.” (Ex. I at 118.) Defendants’ construction should be rejected because it disregards the breadth of the claimed “attaching” by limiting the term to joining. Defendants’ construction also changes the verb tense of the phrase (*i.e.*, joined).

Z. “appending the VAN to the payment instrument” – ‘148 Patent, claim 28

Stambler’s Construction	Defendants’ Construction
joining or connecting the [VAN] to the [payment instrument]	the VAN joined to the end of the instrument

Defendants’ construction should be rejected because the common meaning of “appending” is not limited to joining “to the end.” (See Ex. I at 88.) Nor is there any support in the intrinsic record for adding this limitation. Additionally, the specification discloses imprinting a VAN on a physical check and including the VAN with an electronic instrument. It is unclear what

¹² Should the Court construe the word “include,” Stambler proposes “taking in as a part, an element, or a member.”

constitutes “the end of” a check or “the end of” an electrical signal. Additionally, Defendants’ construction changes the verb tense of the phrase (*i.e.*, joined).

AA. “accounts receivable” / “accounts payable”– ‘302 Patent, claim 44

Stambler’s Construction	Defendants’ Construction
“accounts receivable”: a record that indicates a monetary value owed	“accounts receivable”: balances of multiple accounts of funds due from one or more debtors
“accounts payable”: a record that indicates a monetary value due to be paid	“accounts payable”: balances of multiple accounts of funds due to one or more creditors

The parties dispute whether “accounts receivable” and “accounts payable” refer to a single record, or whether the terms must refer to multiple records (*i.e.*, “balances of multiple accounts”). Stambler’s constructions are consistent with the ordinary meaning of “accounts receivable” and “accounts payable,” which simply mean “money owed to a company” and “money owed by a company,” respectively. (Ex. O at 211, 244.) Defendants’ constructions should be rejected to the extent they require that the claimed terms include multiple records (*i.e.*, “balances of multiple accounts”). For example, accounts receivable may include indications of monetary value owed for one account (*e.g.*, when a company has only one customer account) or monetary value owed for multiple accounts (*e.g.*, when a company has multiple customer accounts). In fact, an accounts receivable might even be empty (*e.g.*, when a company has no customers). The same is true with respect an account payable. Accounts payable may include indications of monetary value owed for one account (*e.g.*, when a company owes money to only one creditor) or monetary value owed for multiple accounts (*e.g.*, when a company owes money to multiple creditors). And an accounts receivable might even be empty (*e.g.*, when a company has no creditors).

III. CONCLUSION

For the foregoing reasons, Stambler asks that the Court adopt his proposed constructions.

Dated: October 6, 2010.

Respectfully submitted,

/s/ Brent N. Bumgardner
Texas State Bar No. 00795272
Attorney-in-Charge
Edward R. Nelson, III
Texas State Bar No. 00797142
Christie B. Lindsey
Texas State Bar No. 24041918
Ryan P. Griffin
Texas State Bar No. 24053687
NELSON BUMGARDNER CASTO, P.C.
3131 West 7th Street, Suite 300
Fort Worth, Texas 76107
(817) 377-9111
Fax (817) 377-3485
bbumgardner@nbclaw.net
enelson@nbclaw.net
clindsey@nbclaw.net
rgriffin@nbclaw.net

Eric M. Albritton
Texas State Bar No. 00790215
ALBRITTON LAW FIRM
P.O. Box 2649
Longview, TX 75606
(903) 757-8449
(903) 758-7397 (fax)
ema@emafirm.com

T. John Ward, Jr.
Texas State Bar No. 00794818
WARD & SMITH LAW FIRM
111 W. Tyler Street
Longview, Texas 75601
(903) 757-6400
(903) 757-2323 (fax)
jw@jwfirm.com

Ronald A. Dubner
Texas State Bar No. 06149000
4965 Preston Park, Suite 560
Plano, Texas 75093
(972) 964-6500
(972) 964-6533 (fax)
rondub@gte.com

**ATTORNEYS FOR PLAINTIFF
LEON STAMBLER**

CERTIFICATE OF SERVICE

I hereby certify that on the 6th day of October, 2010, I electronically filed the foregoing document with the clerk of the court for the U.S. District Court, Eastern District of Texas, Marshall Division, using the electronic case filing system of the court. The electronic case filing system sent a "Notice of Electronic Filing" to the attorneys of record who have consented in writing to accept this Notice as service of this document by electronic means.

/s/ Brent N. Bumgardner

Exhibit 1

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

LEON STAMBLER,

CIVIL ACTION NO. 2:09-cv-310

Plaintiff,

v.

AMAZON.COM, INC., et al,

Defendants.

**DECLARATION OF RYAN P. GRIFFIN
IN SUPPORT OF PLAINTIFF'S
OPENING CLAIM CONSTRUCTION
BRIEF**

I, Ryan P. Griffin, say and declare as follows:

1. I am an attorney licensed to practice in the State of Texas and am an associate in the law firm of Nelson Bumgardner Casto P.C., counsel of record for Leon Stambler. This declaration is based on my own personal knowledge and if called as a witness I would and could competently testify thereto.

2. Attached hereto as Exhibit A is a true and accurate copy of U.S. Patent No. 5,793,302 issued to Leon Stambler on August 11, 1998.

3. Attached hereto as Exhibit B is a true and accurate copy of U.S. Patent No. 5,974,148 issued to Leon Stambler on October 26, 1999.

4. Attached hereto as Exhibit C is a true and accurate copy of the April 9, 2010 claim construction order in the case styled *Stambler v. JPMorgan Chase & Co., et al.*, No. 08-204-DF-CE (E.D. Tex.).

5. Attached hereto as Exhibit D is a true and accurate copy of the September 24, 2010 claim construction order in the case styled *Stambler v. Merrill Lynch & Co., Inc., et al.*, No. 08-462-DF-CE (E.D. Tex.).

6. Attached hereto as Exhibit E is a true and accurate copy of the January 29, 2003 claim construction order in the case styled *Stambler v. RSA Security Inc., et al.*, No. 01-65-SLR (D. Del.).

7. Attached hereto as Exhibit F are true and accurate excerpts from D.W. Davies & W.L. Price, *Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer* (John Wiley & Sons 1989).

8. Attached hereto as Exhibit G are true and accurate excerpts from Dennis Longley et al., *Information Security: Dictionary of Concepts, Standards and Terms* (Stockton Press 1992).

9. Attached hereto as Exhibit H are true and accurate excerpts from a response to the United States Patent and Trademark Office dated November 7, 1997.

10. Attached hereto as Exhibit I are true and accurate excerpts from *The American Heritage Dictionary of the English Language* (3d ed. 1992).

11. Attached hereto as Exhibit J are true and accurate excerpts from Defendant's Opening Markman Brief, dated October 15, 2002, which was made in support of the defendants' claim constructions in the case styled *Stambler v. RSA Security Inc., et al.*, No. 01-65 (SLR) (D. Del.).

12. Attached hereto as Exhibit K are true and accurate excerpts from *Computer Dictionary* (Microsoft Press 1991).

13. Attached hereto as Exhibit L are true and accurate excerpts from *The Chicago Manual of Style* (15th ed. The University of Chicago Press 2003).

14. Attached hereto as Exhibit M are true and accurate excerpts from *Manual of Patent Examining Procedure* (6th ed. rev. 3 1997).

15. Attached hereto as Exhibit N are true and accurate excerpts from *Webster's New Collegiate Dictionary* (1981).

16. Attached hereto as Exhibit O are true and accurate excerpts from Dictionary of Business (Fitzroy Dearborn 1998).

17. Attached hereto as Exhibit P are true and accurate excerpts from the P.R. 4-5 chart filed by the parties in the case styled *Stambler v. Merrill Lynch & Co., Inc., et al.*, No. 08-462-DF-CE (E.D. Tex.).

18. Attached hereto as Exhibit Q are true and accurate excerpts from U.S. Patent No. 4,404,649 issued to Nunley et al. on September 13, 1983.

Dated: October 6, 2010

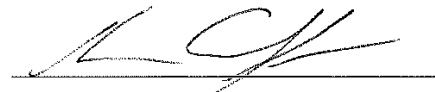

Ryan P. Griffin

Exhibit “A”

US005793302A

United States Patent [19]

[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.⁶ 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	Haltof .	
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

Shiple C., "I threw away my checkbook", PC-Computing, vol. 3, No. 11, pp. 112, 114-115, 118-120, Nov. 1990.

Iida J., "Electronic Presentation 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 Magnaplane Corporation Issues Three-Month Report to Stockholders", PR Newswire, 1 page, Nov. 11, 1992.

Byles T., "More Companies Are Paying Bills Electronically", Journal of Commerce, p. 2B, May 5, 1988.

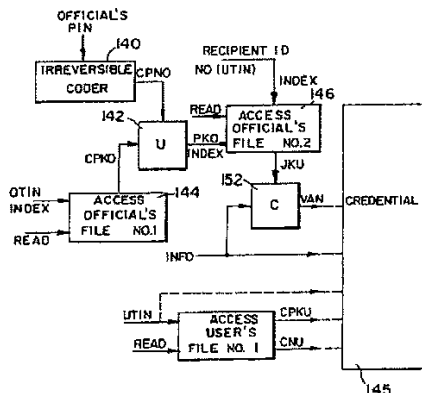
Carreker J.D., "Strides in Electronic Checking Transforming Payment System", vol. 68, No. 3, pp. 18-19, 22, 24, 26, 28, 30, Mar. 1992.

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 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.

91 Claims, 15 Drawing Sheets



5,793,302

Page 2

U.S. PATENT DOCUMENTS

4,283,599	8/1981	Atalla .	4,992,783	2/1991	Zdunek et al. .	
4,302,810	11/1981	Bouricius et al. .	4,995,082	2/1991	Schnorr	380/23
4,304,990	12/1981	Atalla .	5,016,274	5/1991	Micali et al. .	
4,317,957	3/1982	Sendrow .	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	Chesarek .	5,161,244	11/1992	Maurer	380/43
4,405,829	9/1983	Rivest et al. .	5,163,098	11/1992	Dahbura .	
4,423,287	12/1983	Zeidler .	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	Decavele 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	Schlaflly .	5,267,314	11/1993	Stambler .	
4,740,890	4/1988	William .	5,283,829	2/1994	Anderson .	
4,747,050	5/1988	Brachtl et al. .	5,297,202	3/1994	Kapp et al. .	
4,755,940	7/1988	Brachtl 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	Abraham et al. .	5,327,563	7/1994	Singh .	
4,823,264	4/1989	Deming .	5,341,428	8/1994	Schatz .	
4,908,861	3/1990	Brachtl 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	Gorog .	5,465,299	11/1995	Matsumoto et al. .	
4,965,568	10/1990	Atalla et al. .	5,473,690	12/1995	Grimouprez et al. .	
4,977,595	12/1990	Ohta et al. .	5,530,755	6/1996	Pailles et al. .	
			5,677,955	10/1997	Doggett et al. .	

U.S. Patent

Aug. 11, 1998

Sheet 1 of 15

5,793,302

FIG. 1

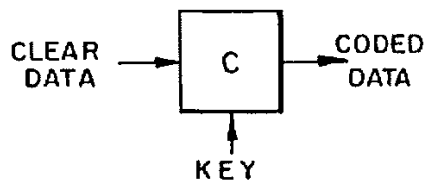


FIG. 2

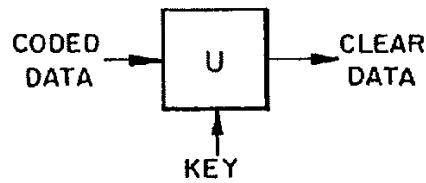


FIG. 3

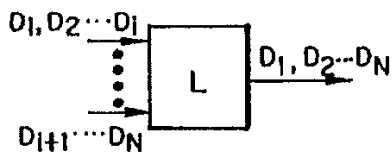


FIG. 4

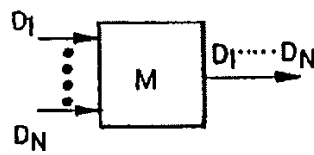


FIG. 5

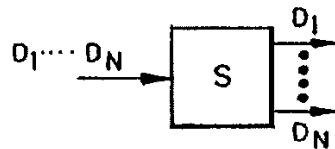
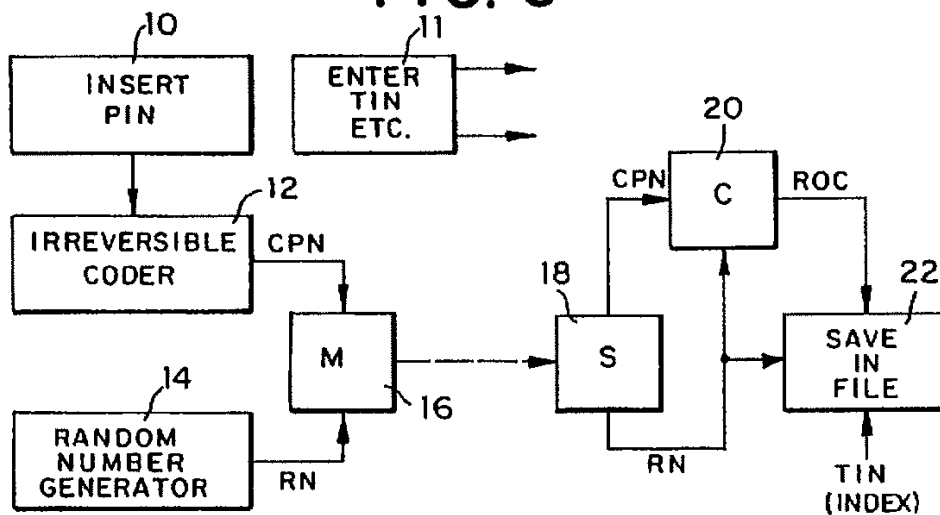


FIG. 6

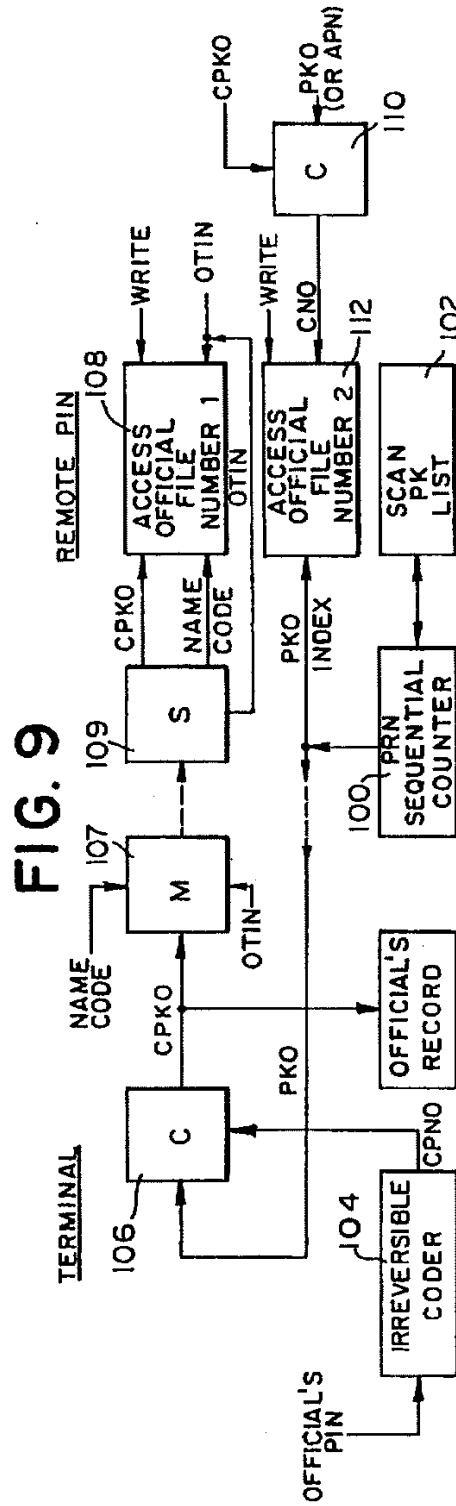
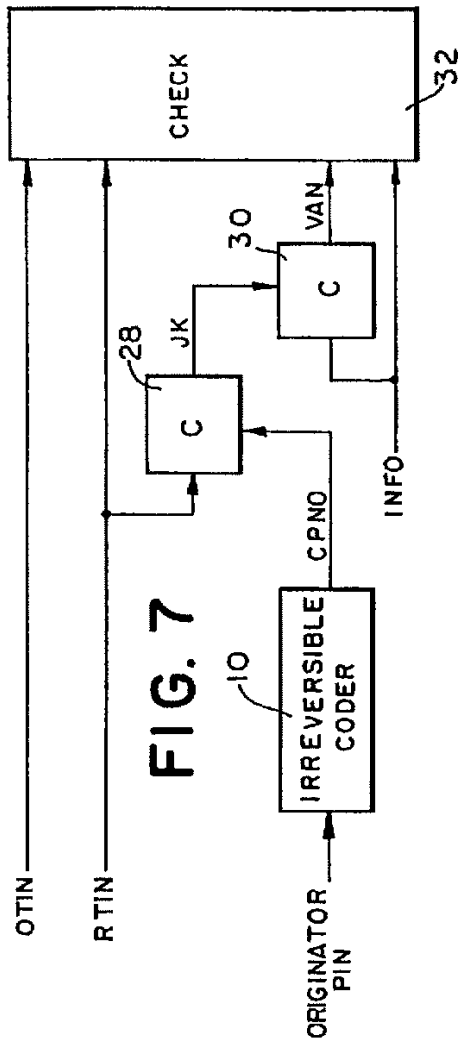


U.S. Patent

Aug. 11, 1998

Sheet 2 of 15

5,793,302

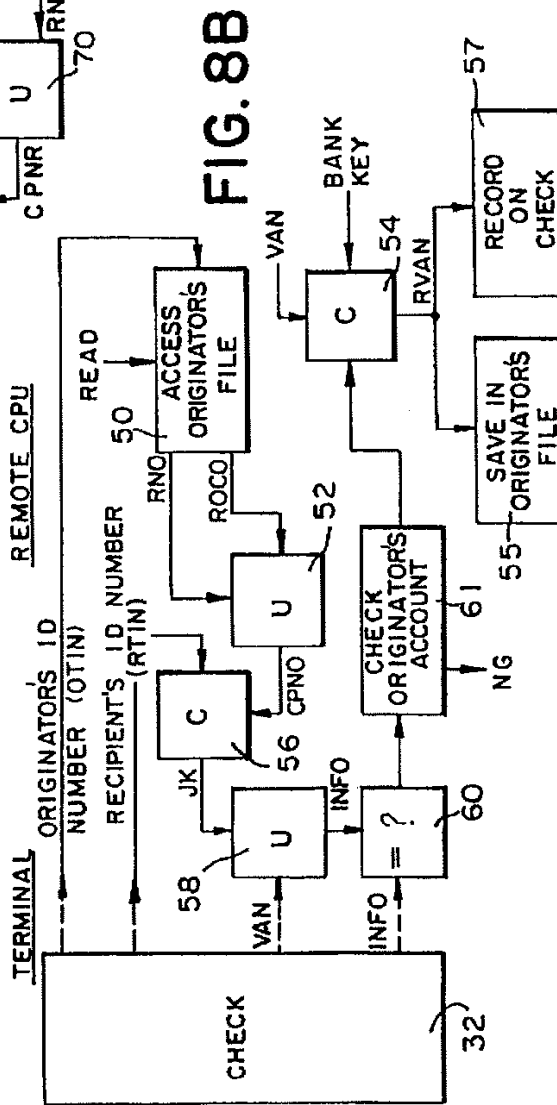
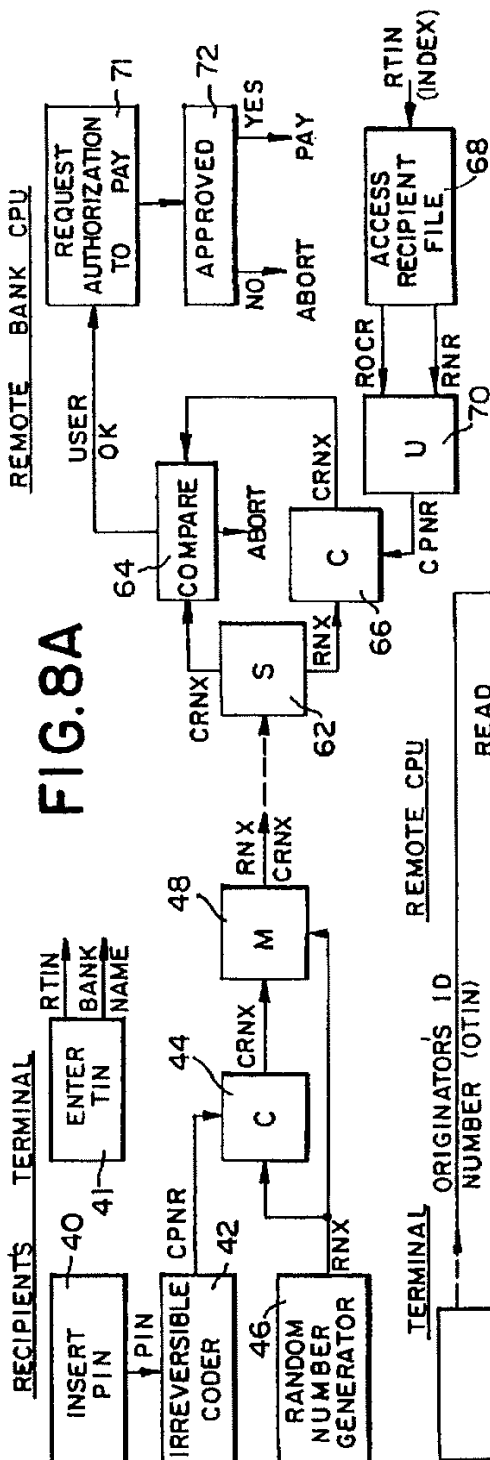


U.S. Patent

Aug. 11, 1998

Sheet 3 of 15

5,793,302



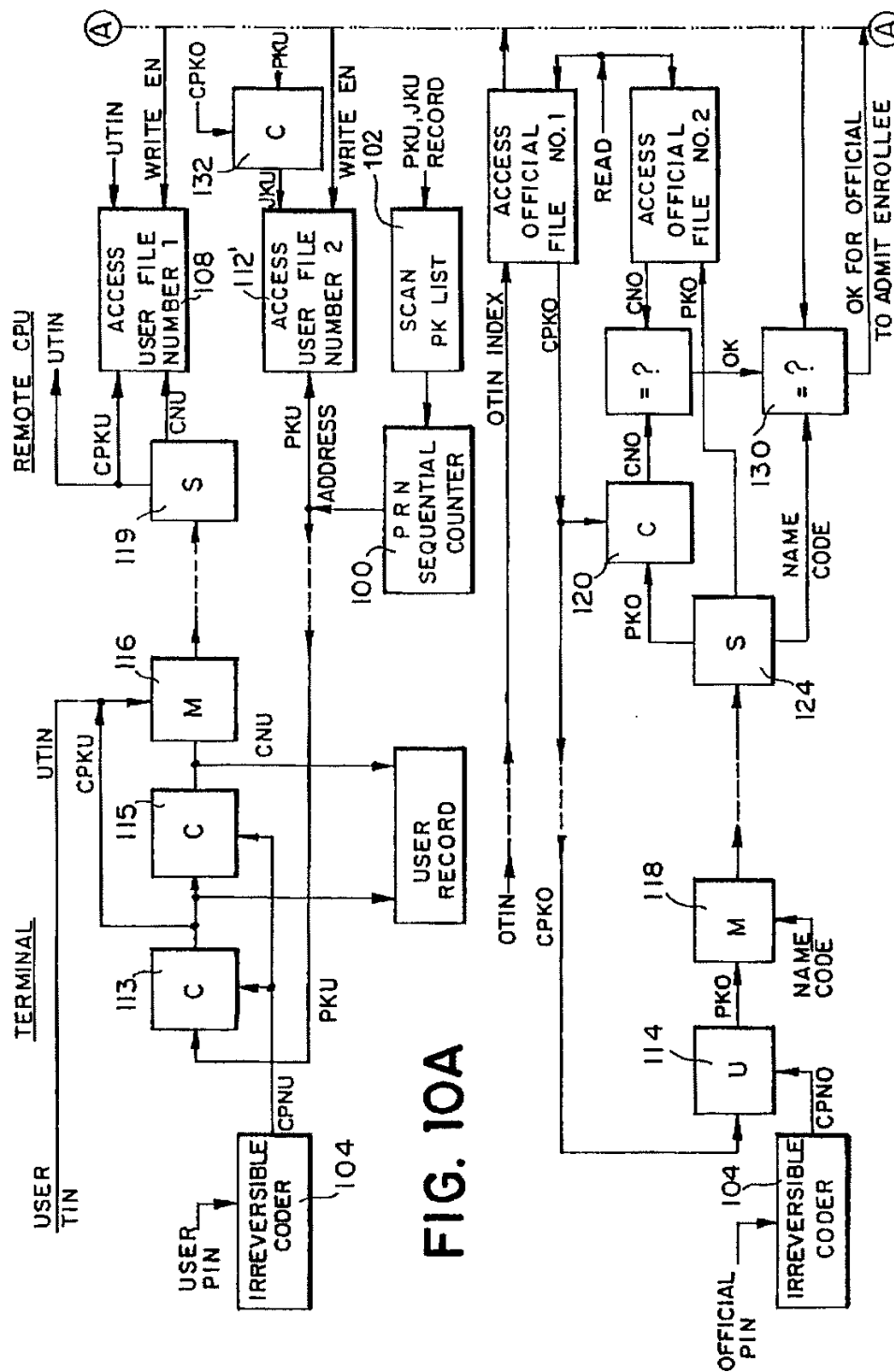


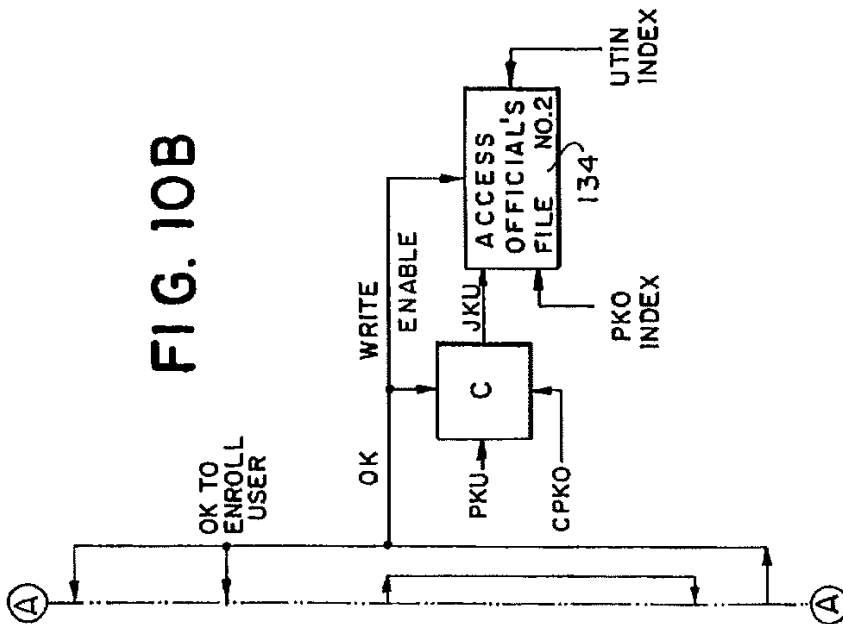
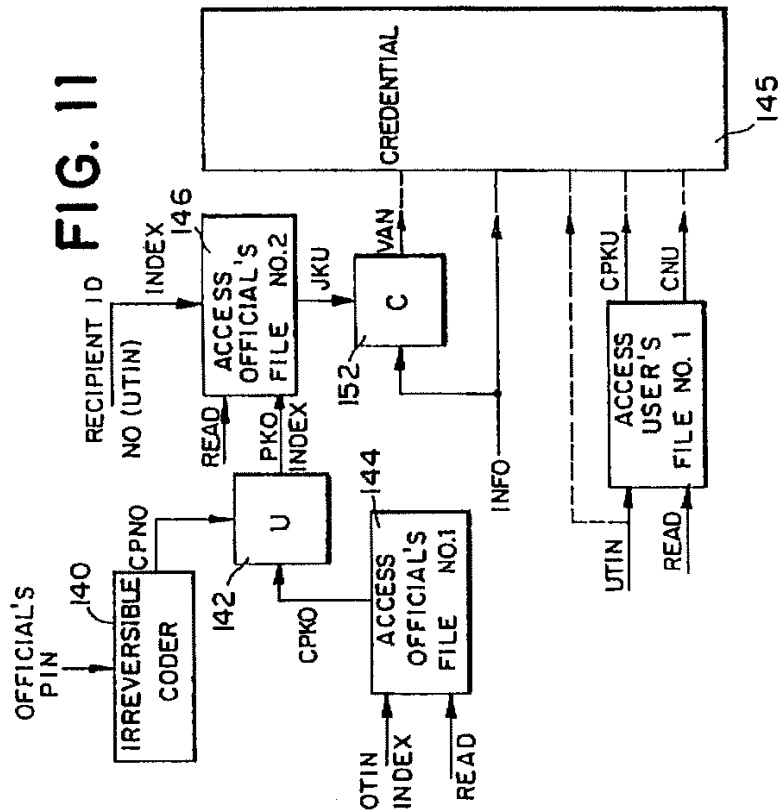
FIG. 10A

U.S. Patent

Aug. 11, 1998

Sheet 5 of 15

5,793,302



U.S. Patent

Aug. 11, 1998

Sheet 6 of 15

5,793,302

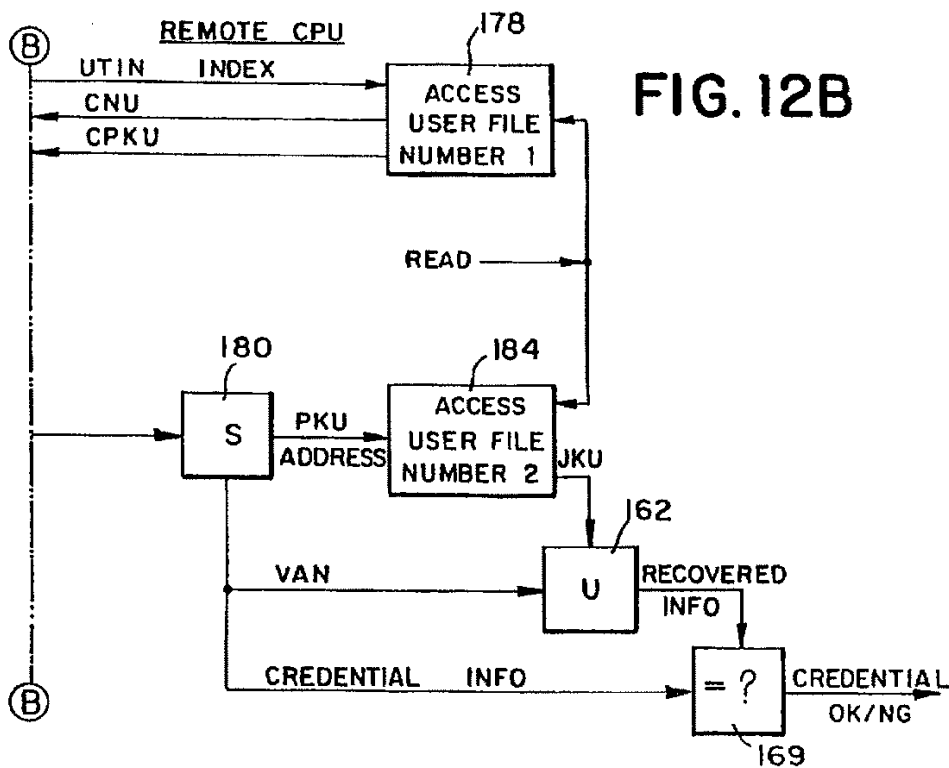
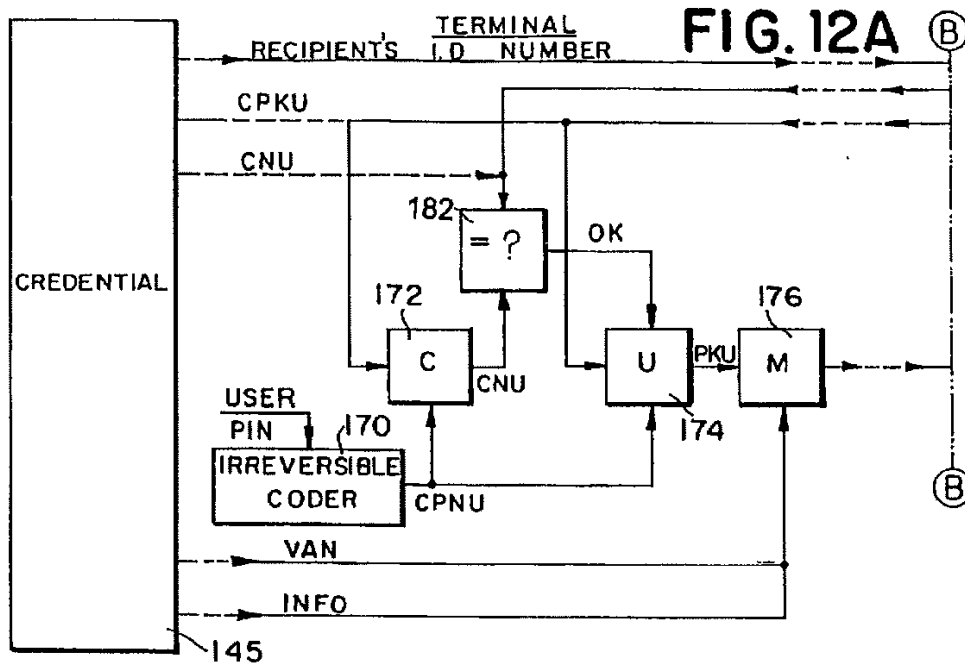
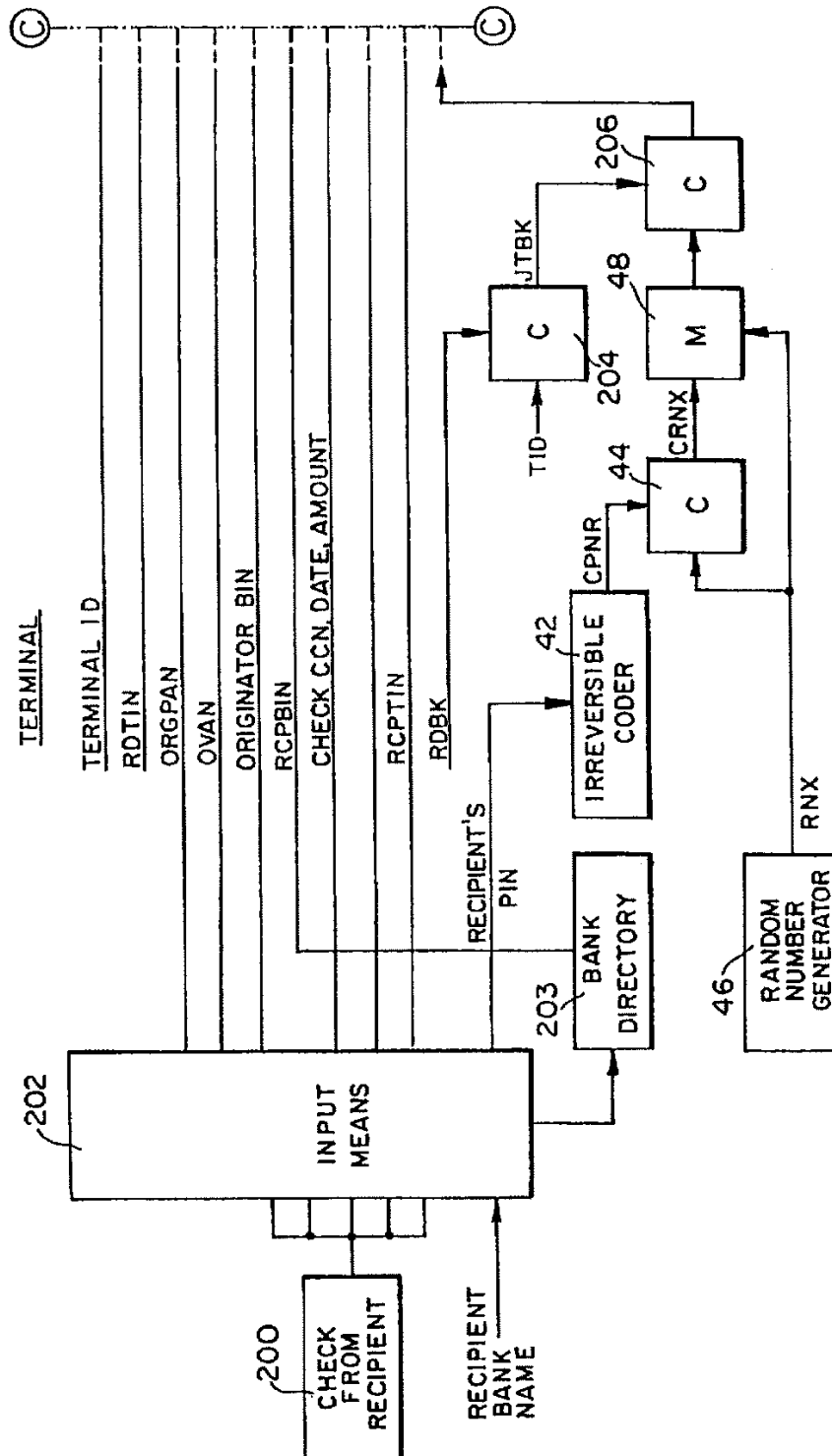


FIG. 13A



U.S. Patent

Aug. 11, 1998

Sheet 8 of 15

5,793,302

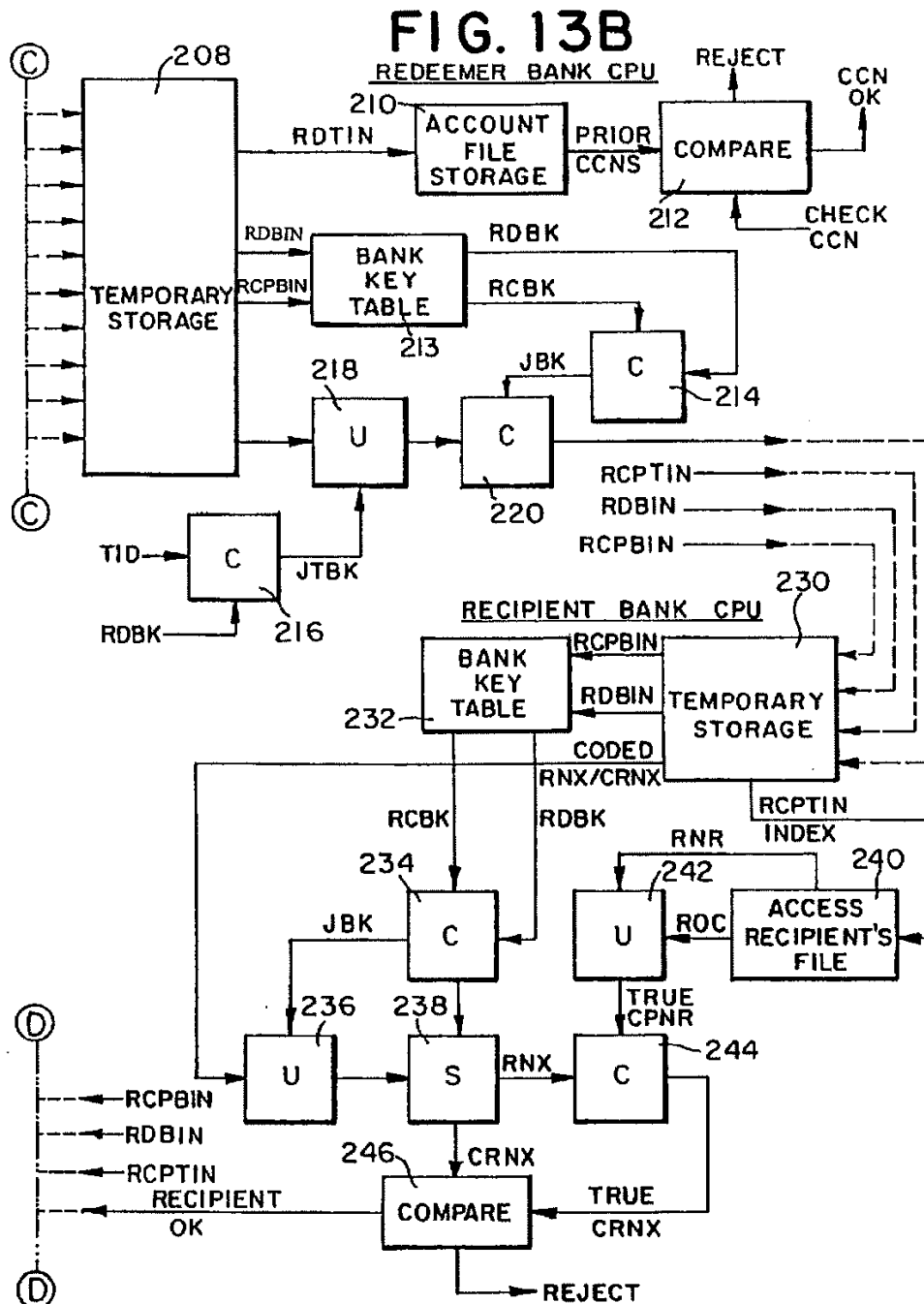


FIG. 13C

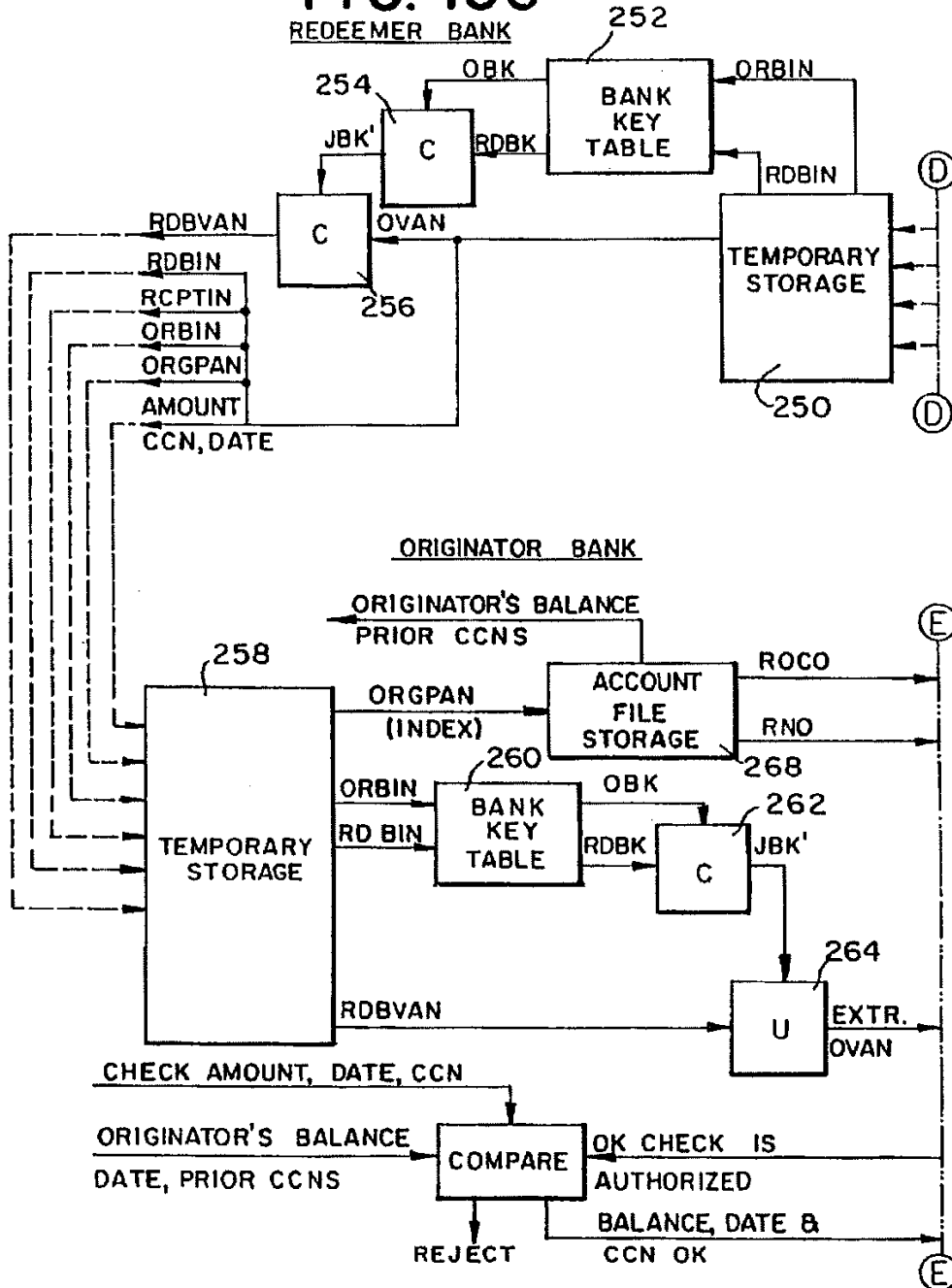
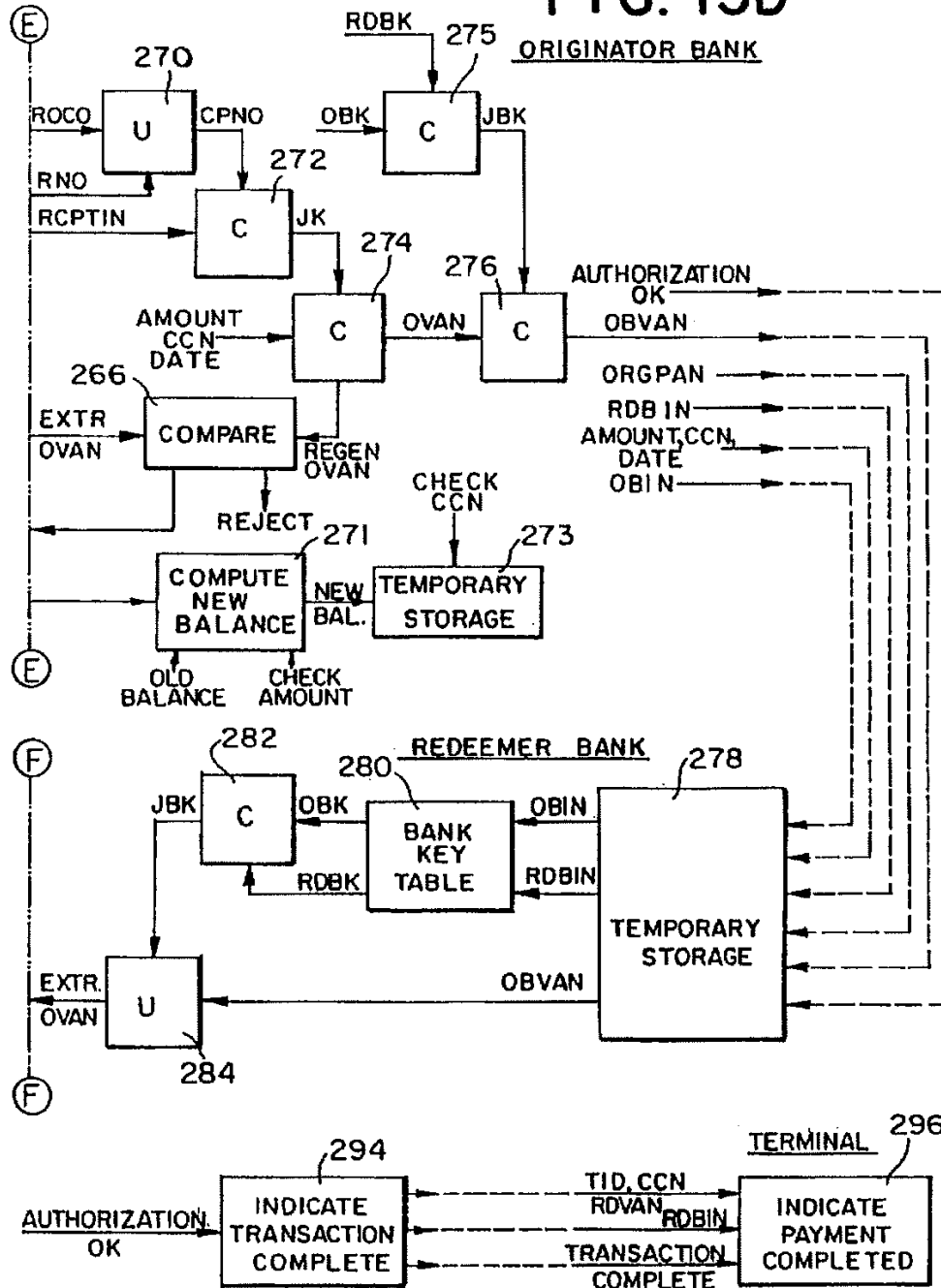


FIG. 13D

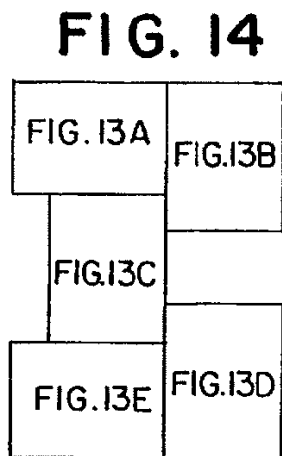
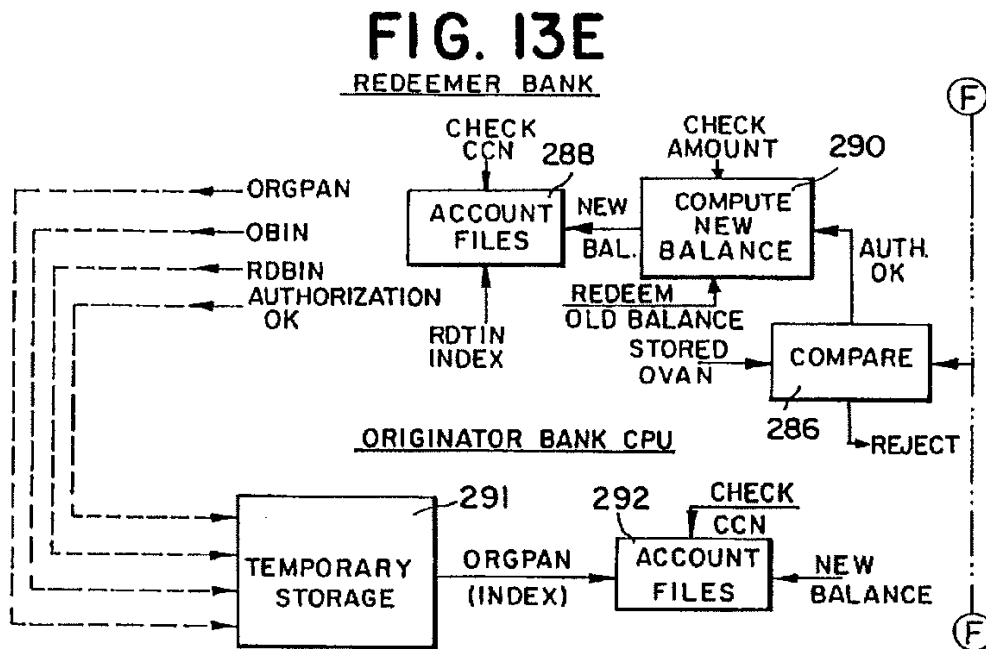


U.S. Patent

Aug. 11, 1998

Sheet 11 of 15

5,793,302

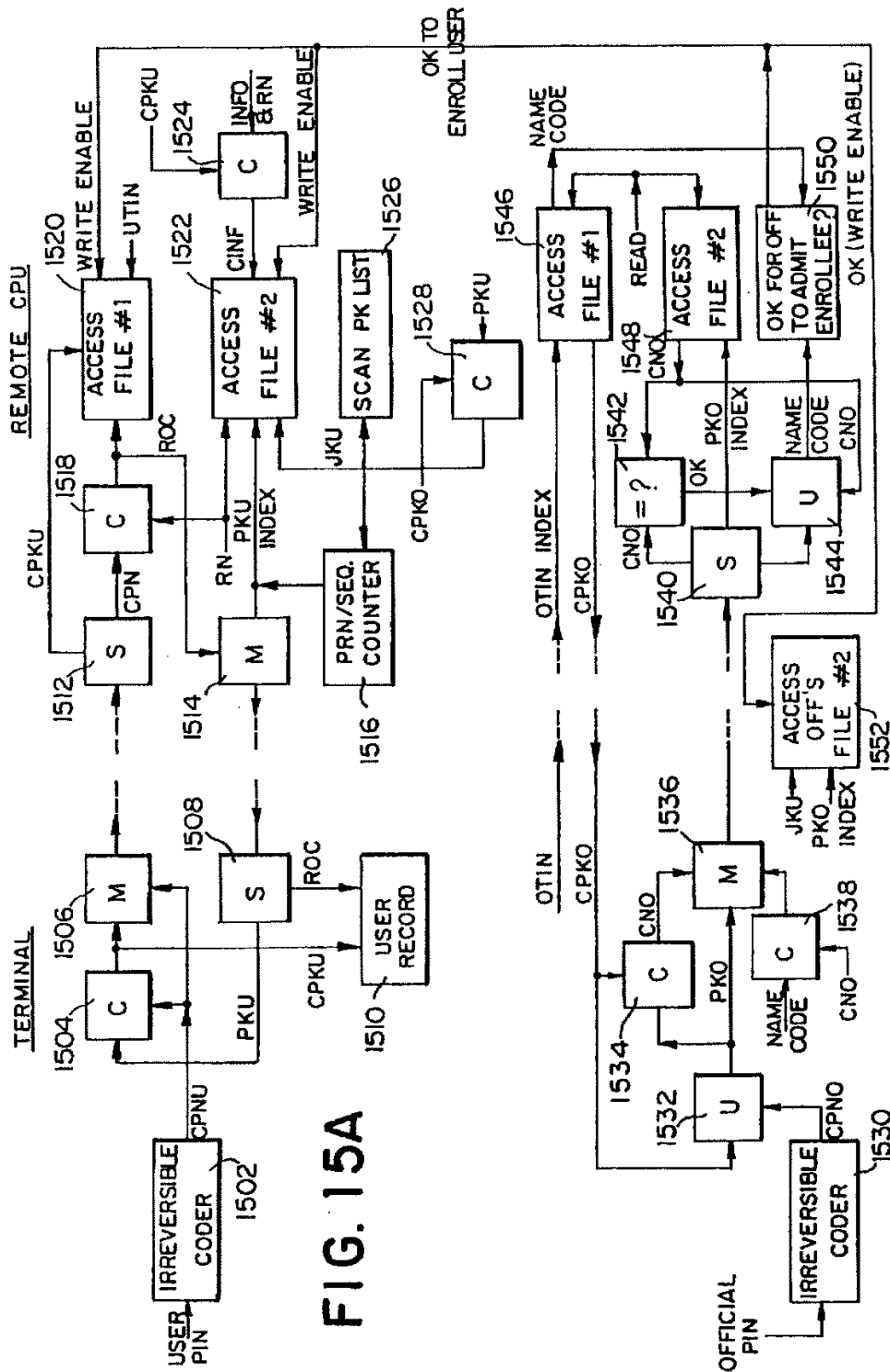


U.S. Patent

Aug. 11, 1998

Sheet 12 of 15

5,793,302



U.S. Patent

Aug. 11, 1998

Sheet 13 of 15

5,793,302

CREDENTIAL ISSUE PROCESSING AGENCY TERMINAL / COMPUTER

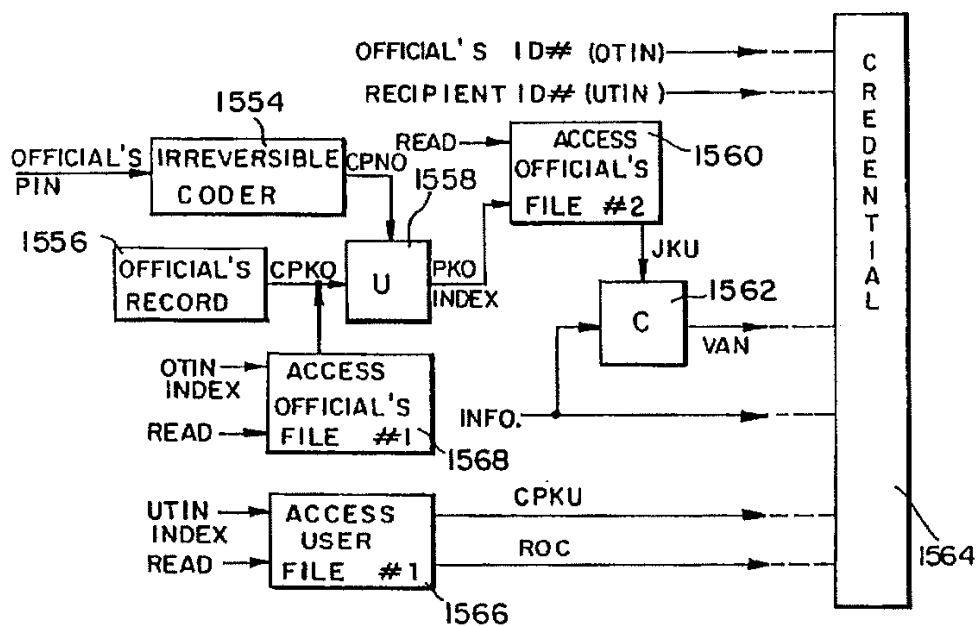


FIG. 15B

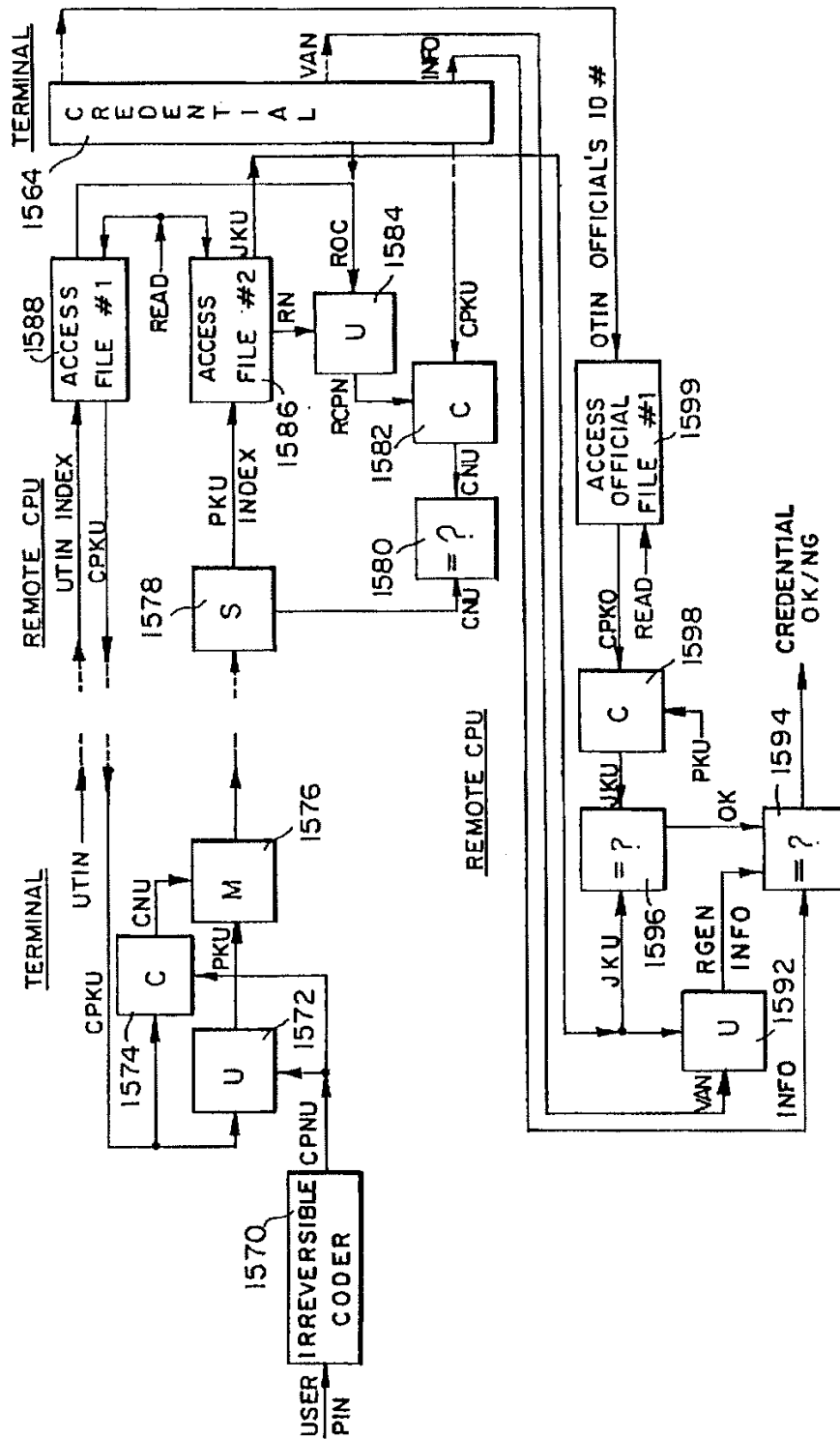


FIG. 15C

U.S. Patent

Aug. 11, 1998

Sheet 15 of 15

5,793,302

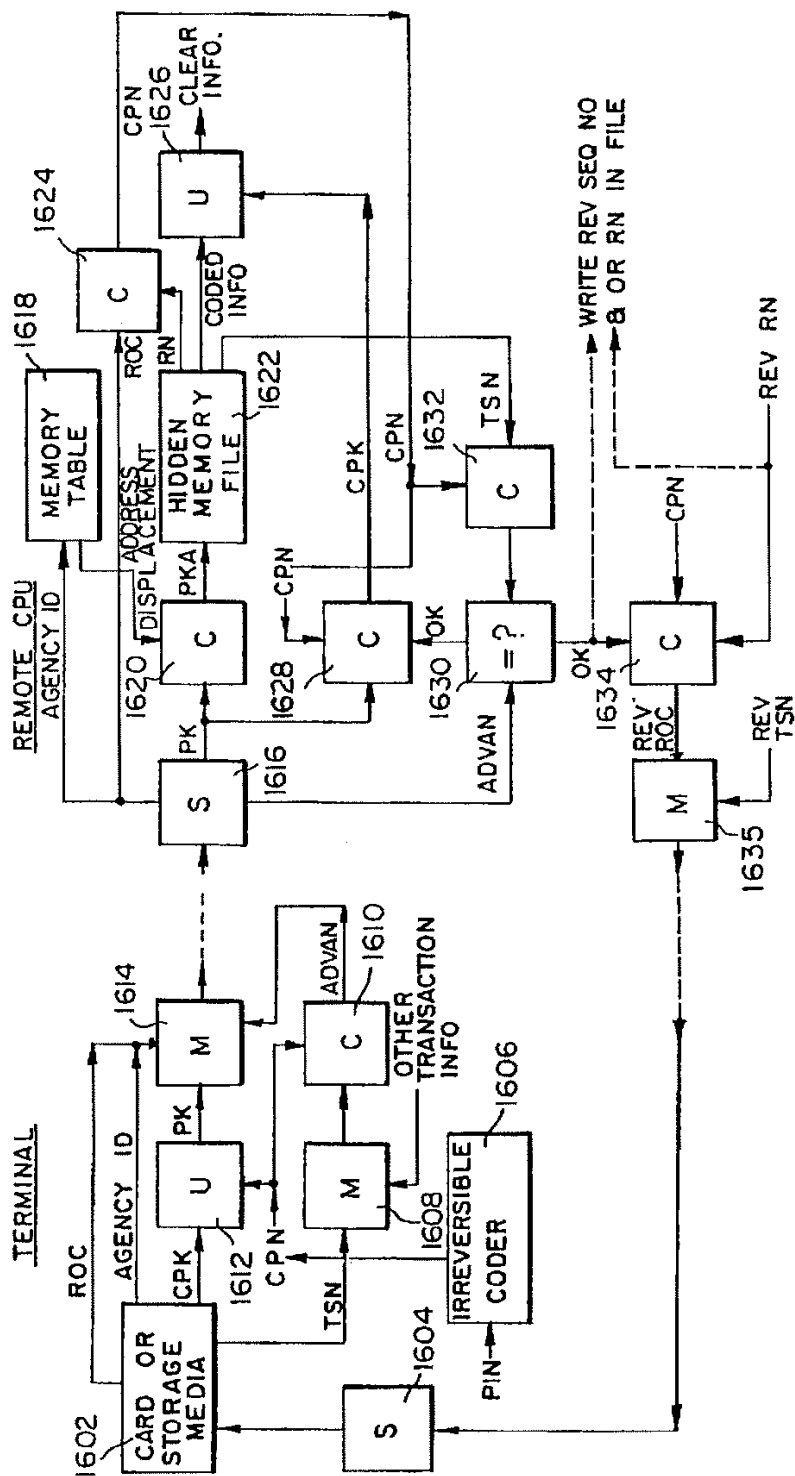


FIG. 16

5,793,302

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,

2

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;

5,793,302

3

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 uncoded 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

4

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

5,793,302

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) RNX 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 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 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 CRNX and RNX, 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 CRNX and RNX, with CRNX being applied to a comparison 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). ROC and RNR therefrom, 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 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 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 ROC and random number, RNO, are extracted from the originator's file at block 50. ROC 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

5,793,302

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 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

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 RNX 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, 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 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 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 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 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-

5,793,302

9

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, 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.

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.

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 the present embodiment offers an additional level of security in that, not

10

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 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 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 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 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 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 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

5,793,302

11

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 CPKO 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. Alternatively, 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,

12

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. 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. 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

5,793,302

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, RCPTIN, and the recipient'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 RCPTIN, 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,

5,793,302

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 RNK and CRNX produced by coder 220. Uncoder 236 therefore reverses the process of coder 220, yielding the mixture of RNK and CRNX as an output. This mixture is applied as an input to a sorter 238, to recover RNK 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 RNK 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 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 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).

5,793,302

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 1540, 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

5,793,302

19

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 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

20

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 alternate 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 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 revisable 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 (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

5,793,302

21

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.

22

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

5,793,302

23

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

24

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.

5,793,302

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

5,793,302

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.

5,793,302

29

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 codes 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

30

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

5,793,302

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 (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);

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 (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 (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

5,793,302

33

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.

34

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.

5,793,302

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

5,793,302

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 (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 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

5,793,302

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 (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. The method of claim 73 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).

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.

5,793,302

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 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. 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 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:

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;

5,793,302

43

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.

44

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.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 5,793,302

Page 1 of 3

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: 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 Scaled this
Thirtieth Day of March, 1999

Attest:



Q. TODD DICKINSON

Attesting Officer

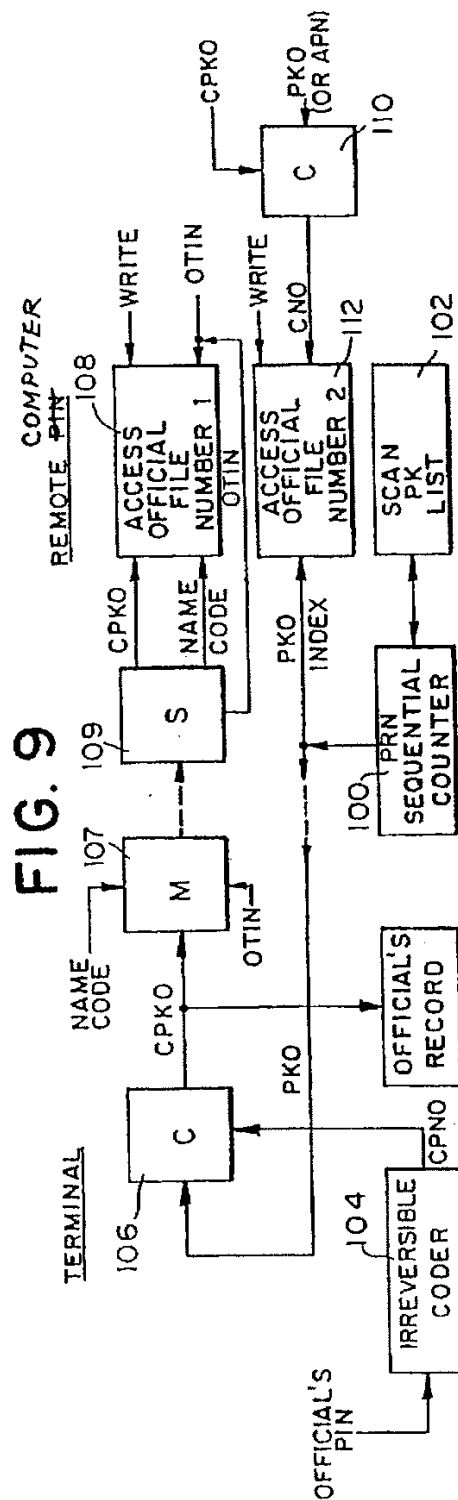
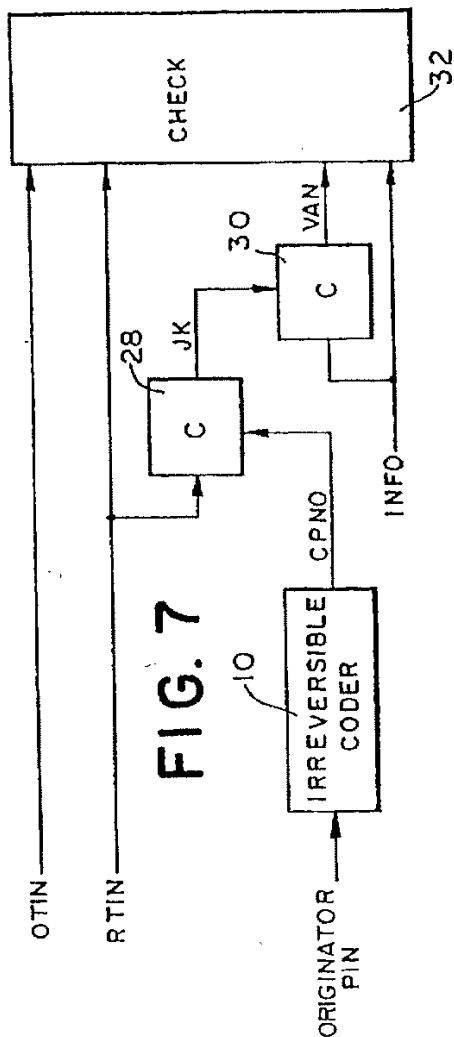
Acting Commissioner of Patents and Trademarks

U.S. Patent

Aug. 11, 1998

Sheet 2 of 15

5,793,302

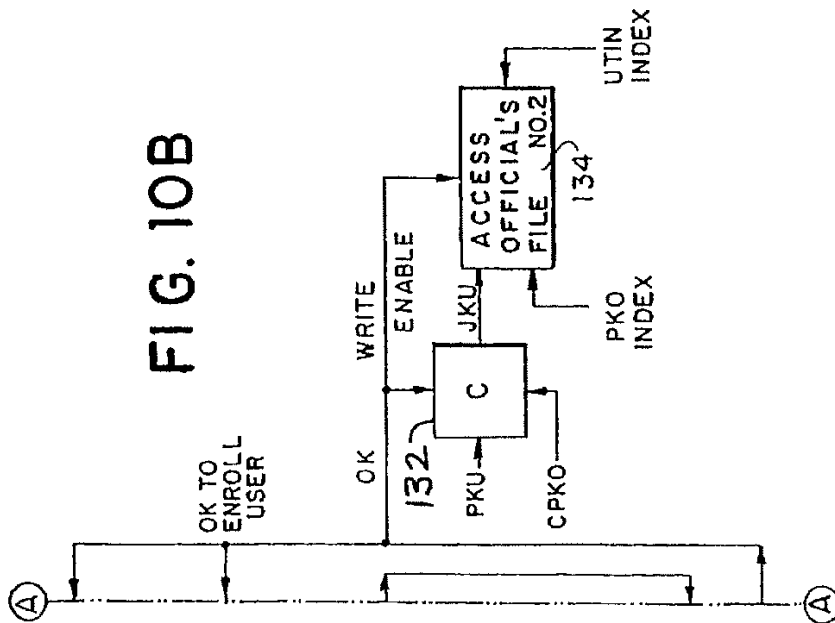
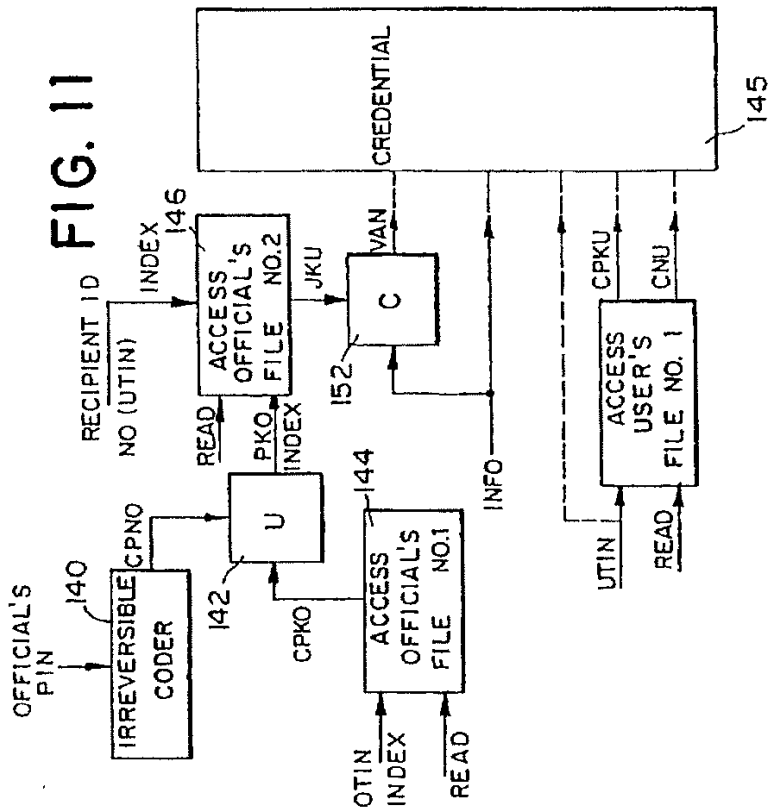


U.S. Patent

Aug. 11, 1998

Sheet 5 of 15

5,793,302



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:



Q. TODD DICKINSON

Attesting Officer

Acting Commissioner of Patents and Trademarks

Exhibit “B”

United States Patent [19]
Stambler

[11] **Patent Number:** **5,974,148**
[45] **Date of Patent:** ***Oct. 26, 1999**

[54] **METHOD FOR SECURING INFORMATION
RELEVANT TO A TRANSACTION**

[76] Inventor: **Leon Stambler**, 7803 Boulder La.,
Parkland, Fla. 33067

[*] Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

[21] Appl. No.: **08/855,561**

[22] Filed: **May 13, 1997**

Related U.S. Application Data

[62] Division of application No. 08/747,174, Nov. 12, 1996, Pat. No. 5,793,302, which is a continuation of application No. 08/446,369, May 22, 1995, abandoned, which is a division of application No. 08/122,071, Sep. 14, 1993, Pat. No. 5,524,073, which is a division of application No. 07/977,385, Nov. 17, 1992, Pat. No. 5,267,314.

[51] Int. Cl.⁶ **H04L 9/00**

[52] U.S. Cl. **380/25; 380/24**

[58] Field of Search **380/23-35**

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. .
4,208,575 6/1980 Haltof .
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 .

(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.
Diamond S., "Check Processing Takes a New Turn", Computers in Banking, vol. 5, No. 3, pp. 50-55, Mar. 1988.
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.

(List continued on next page.)

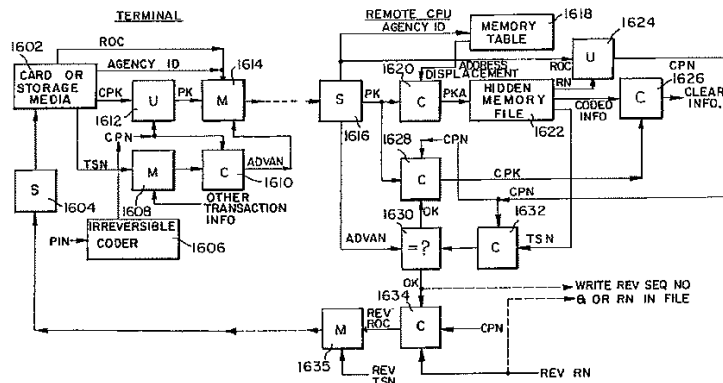
Primary Examiner—Salvatore Cangialosi
Attorney, Agent, or Firm—Akin, Gump, Strauss, Hauer & Feld, L.L.P.

[57]

ABSTRACT

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.

35 Claims, 15 Drawing Sheets



5,974,148

Page 2

U.S. PATENT DOCUMENTS

4,264,808	4/1981	Owens et al. .	5,054,066	10/1991	Riek .	
4,268,715	5/1981	Atalla .	5,067,155	11/1991	Bianco et al. .	
4,281,215	7/1981	Atalla .	5,161,244	11/1992	Maurer .	
4,283,599	8/1981	Atalla .	5,163,098	11/1992	Dahbura .	
4,302,810	11/1981	Bouricius et al. .	5,168,520	12/1992	Weiss .	
4,304,990	12/1981	Atalla .	5,187,351	2/1993	Clary .	
4,317,957	3/1982	Sendrow .	5,191,613	3/1993	Graziano et al. .	
4,319,079	3/1982	Best .	5,196,840	3/1993	Liech et al. .	
4,328,414	5/1982	Atalla .	5,199,066	3/1993	Logan .	
4,386,266	5/1983	Chesarek .	5,218,637	6/1993	Angebaud et al.	380/25
4,405,829	9/1983	Rivest et al. .	5,224,162	6/1993	Okamoto et al.	380/24
4,423,287	12/1983	Zeidler .	5,233,658	8/1993	Bianco et al. .	
4,471,163	9/1984	Donald et al. .	5,267,314	11/1993	Stambler	380/25
4,498,000	2/1985	Decavcic et al. .	5,283,829	2/1994	Anderson	380/24
4,590,470	5/1986	Koenig .	5,297,202	3/1994	Kapp et al.	380/23
4,605,820	8/1986	Campbell, Jr. .	5,321,751	6/1994	Ray et al.	380/25
4,665,396	5/1987	Dieleman .	5,326,959	7/1994	Perazza .	
4,686,357	8/1987	Duono et al. .	5,327,563	7/1994	Singh .	
4,720,859	1/1988	Aaro et al. .	5,341,428	8/1994	Schatz .	
4,734,858	3/1988	Schlafly .	5,367,572	11/1994	Weiss .	
4,740,890	4/1988	William .	5,400,403	3/1995	Fahn et al. .	
4,747,050	5/1988	Brachtl et al. .	5,453,601	9/1995	Rosen .	
4,755,940	7/1988	Brachtl et al. .	5,455,407	10/1995	Rosen .	
4,797,920	1/1989	Stein .	5,465,299	11/1995	Matsumoto et al.	380/23
4,799,061	1/1989	Abraham et al. .	5,473,690	12/1995	Grimonprez et al.	380/24
4,823,264	4/1989	Deming .	5,524,073	6/1996	Stambler	380/24
4,908,861	3/1990	Brachtl et al. .	5,530,755	6/1996	Pailles et al.	380/23
4,928,098	5/1990	Dannhaeuser .	5,555,303	9/1996	Stambler	380/25
4,933,969	6/1990	Marshall et al. .	5,646,998	7/1997	Stambler	380/25
4,935,962	6/1990	Austin .	5,677,955	10/1997	Doggett et al.	380/24
4,947,028	8/1990	Gorog .				
4,965,568	10/1990	Atalla et al. .				
4,977,595	12/1990	Ohta et al. .				
4,992,783	2/1991	Zdunek et al. .				
4,995,082	2/1991	Schnorr 380/23				
5,016,274	5/1991	Micali et al. .				
5,023,908	6/1991	Weiss .				

OTHER PUBLICATIONS

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, Mar. 1992.

U.S. Patent

Oct. 26, 1999

Sheet 1 of 15

5,974,148

FIG. 1

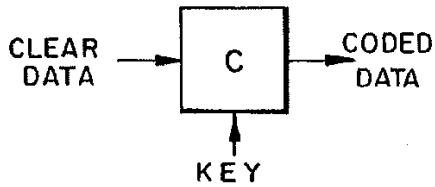


FIG. 2

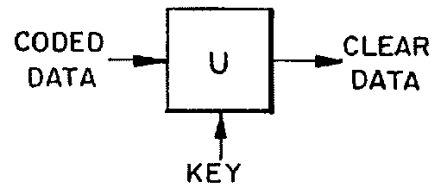


FIG. 3

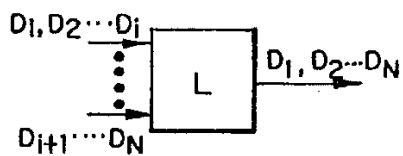


FIG. 4

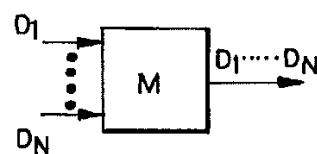


FIG. 5

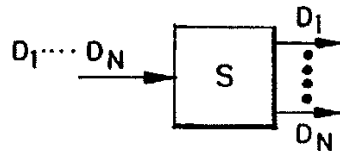
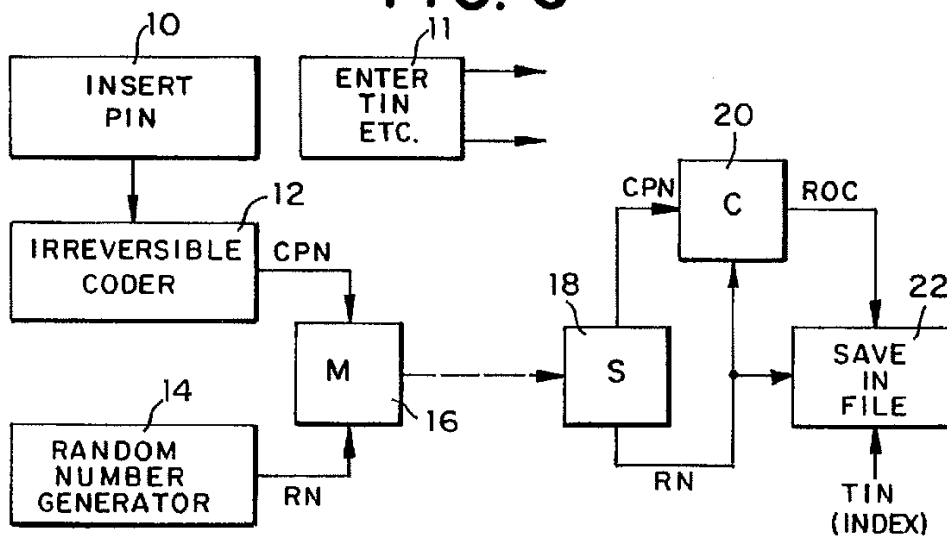


FIG. 6



U.S. Patent

Oct. 26, 1999

Sheet 2 of 15

5,974,148

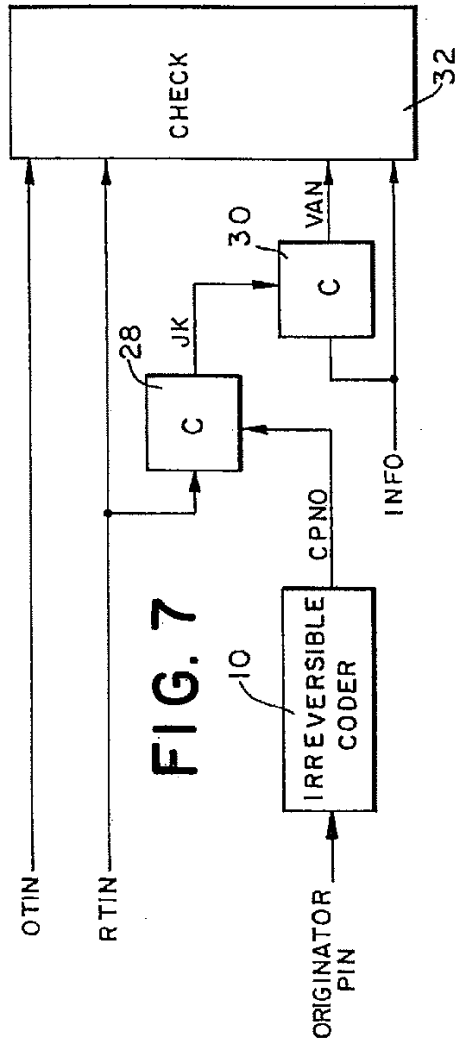
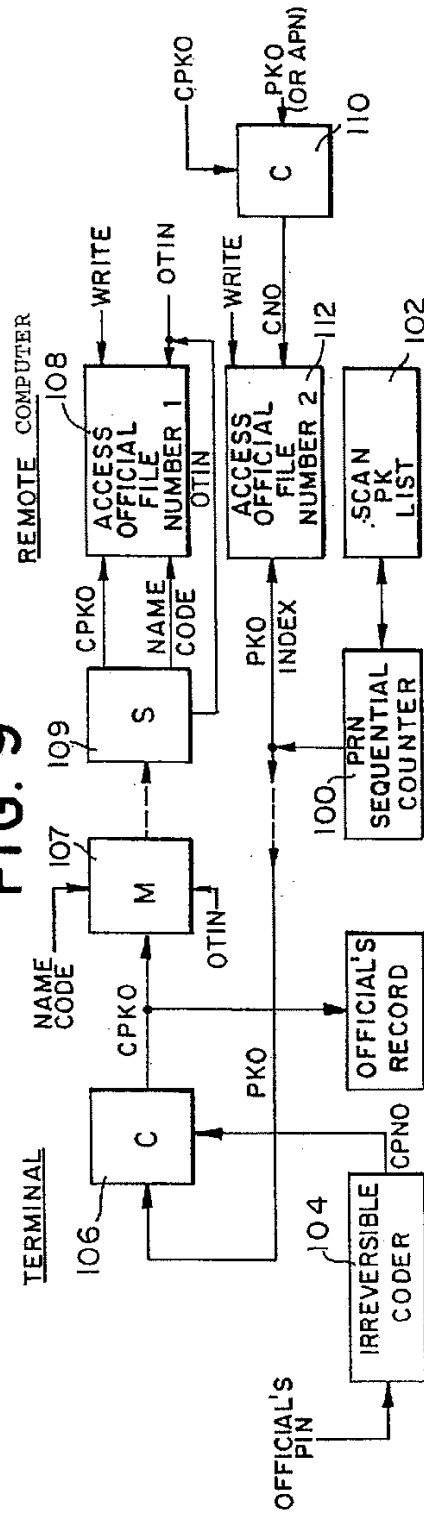
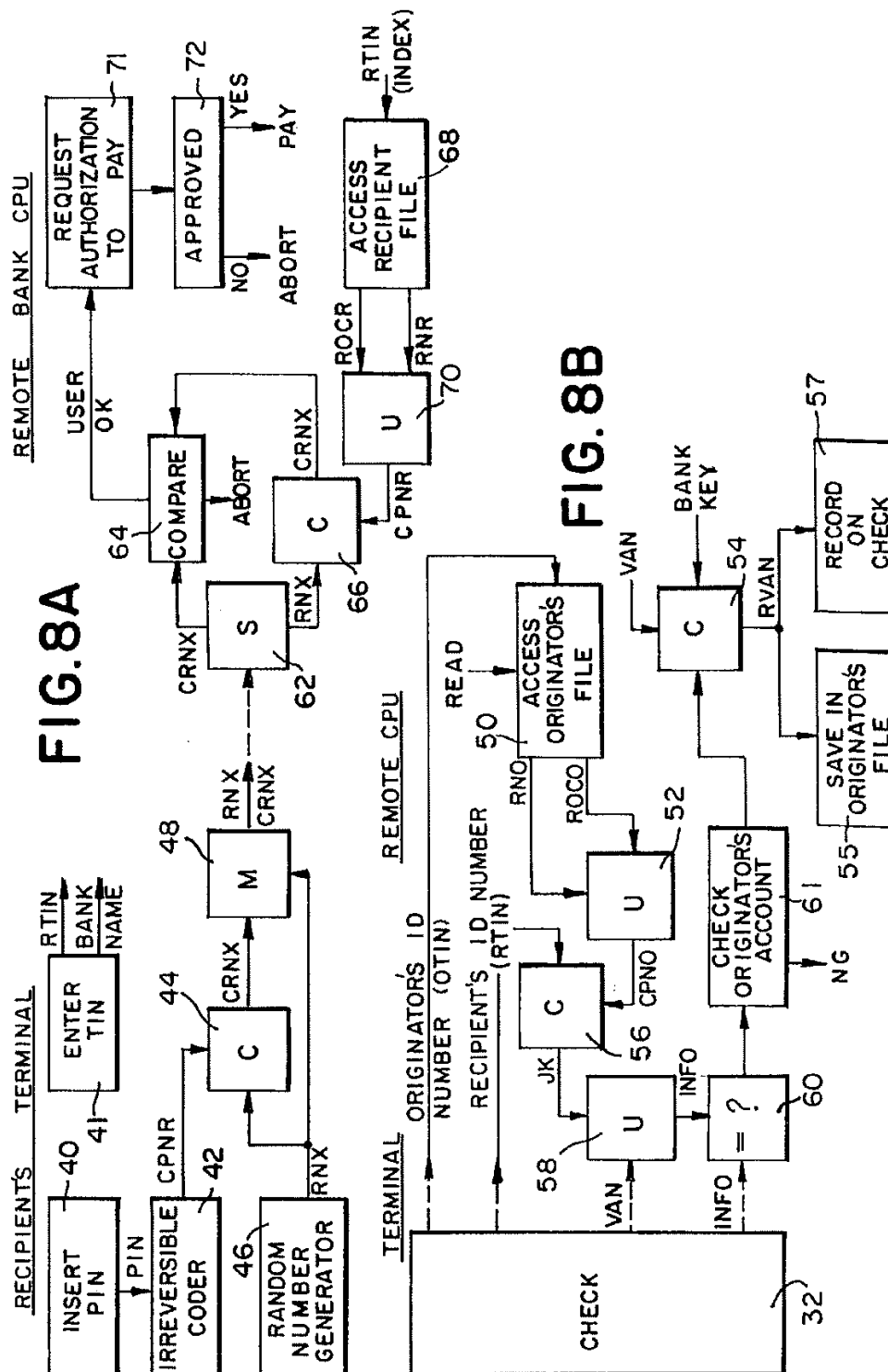


FIG. 9



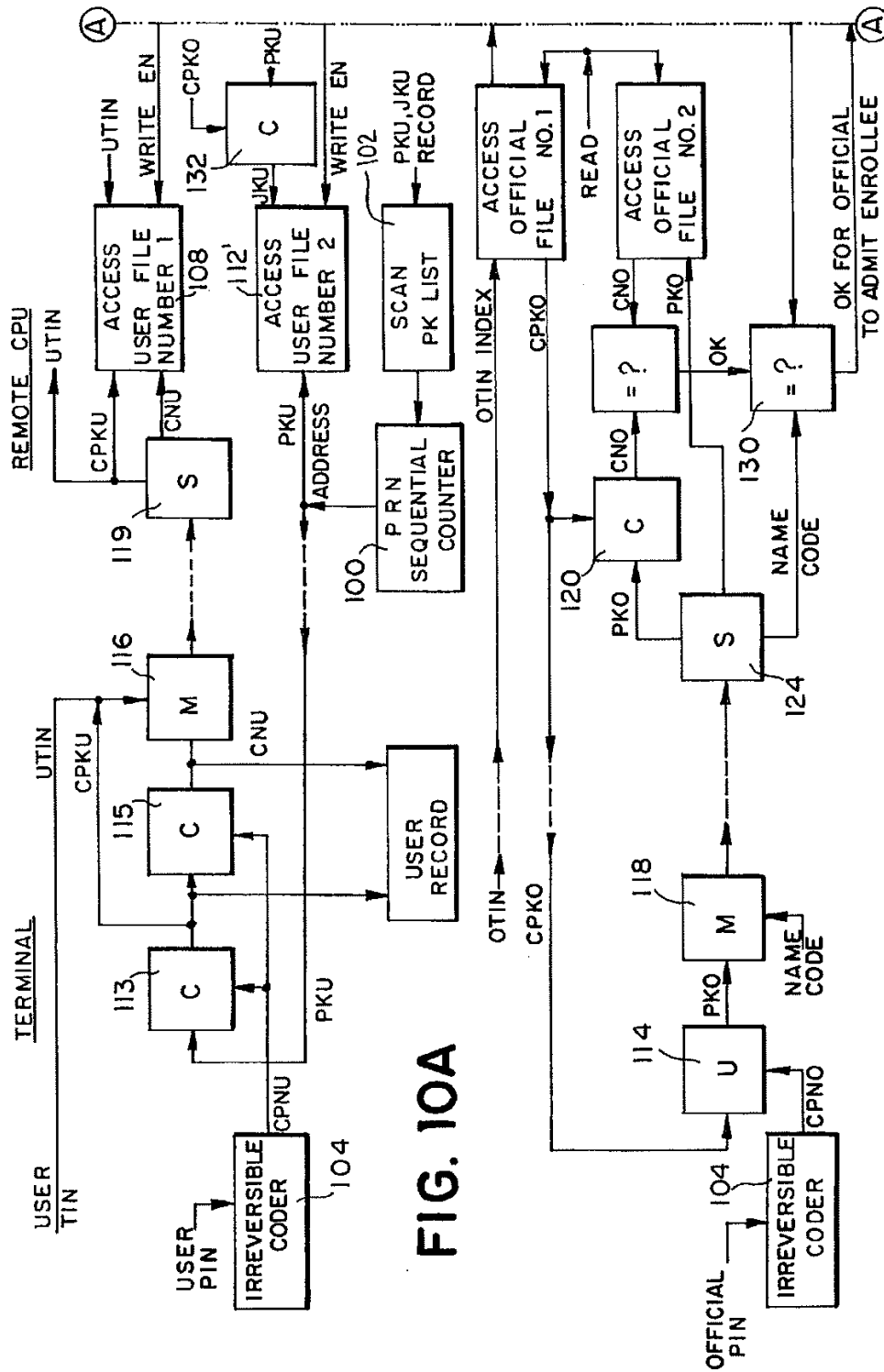


U.S. Patent

Oct. 26, 1999

Sheet 4 of 15

5,974,148

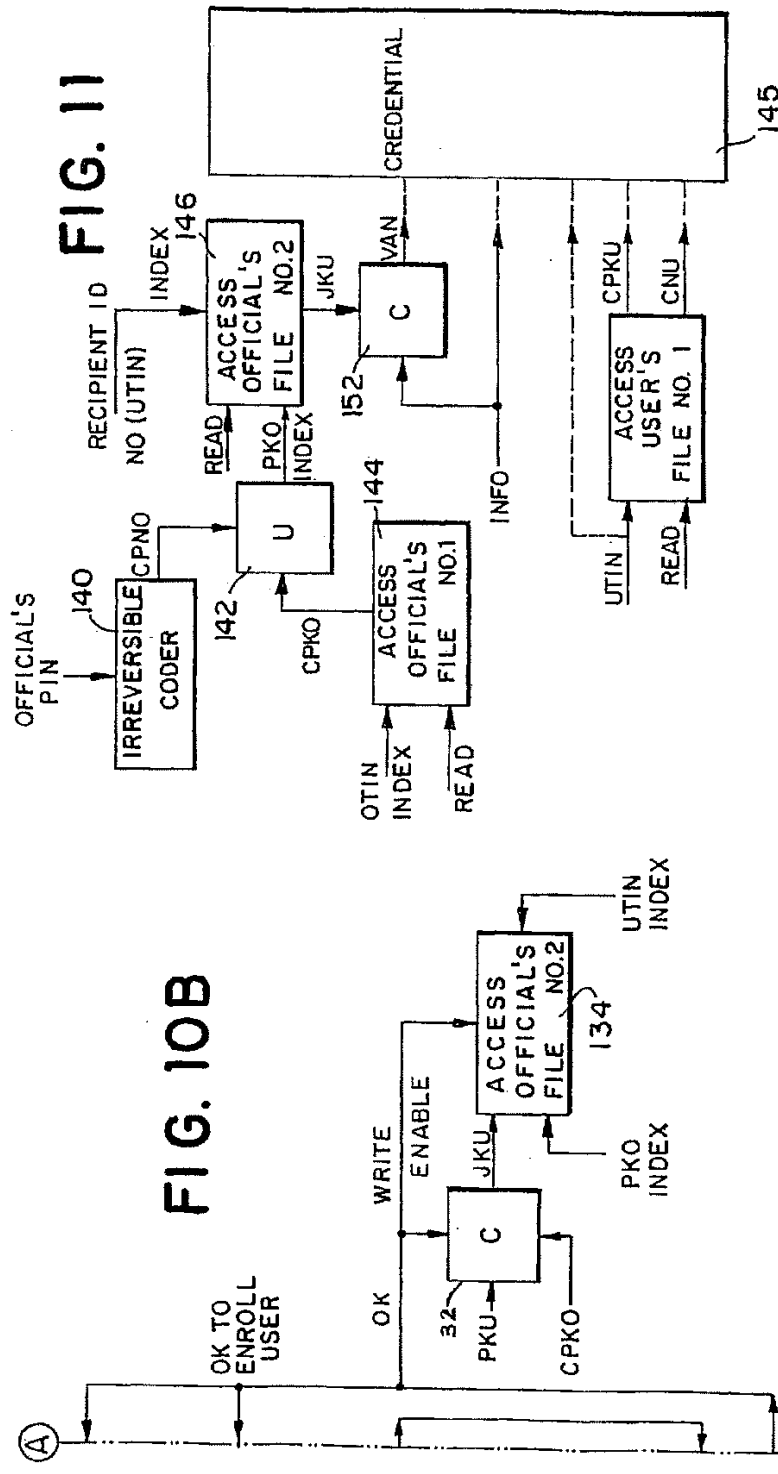


U.S. Patent

Oct. 26, 1999

Sheet 5 of 15

5,974,148

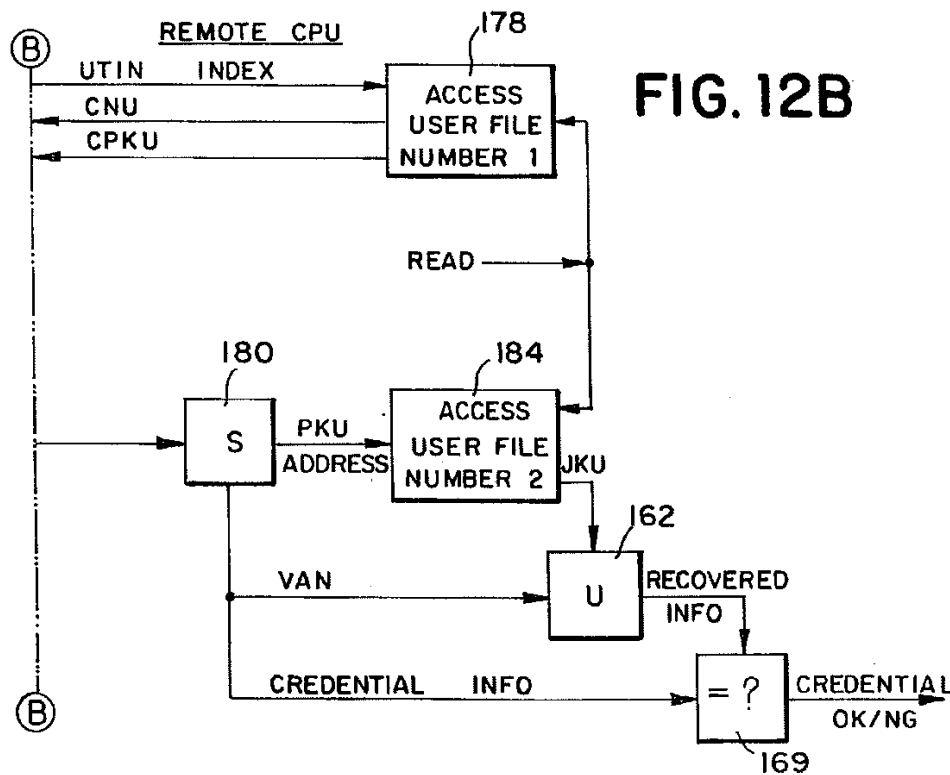
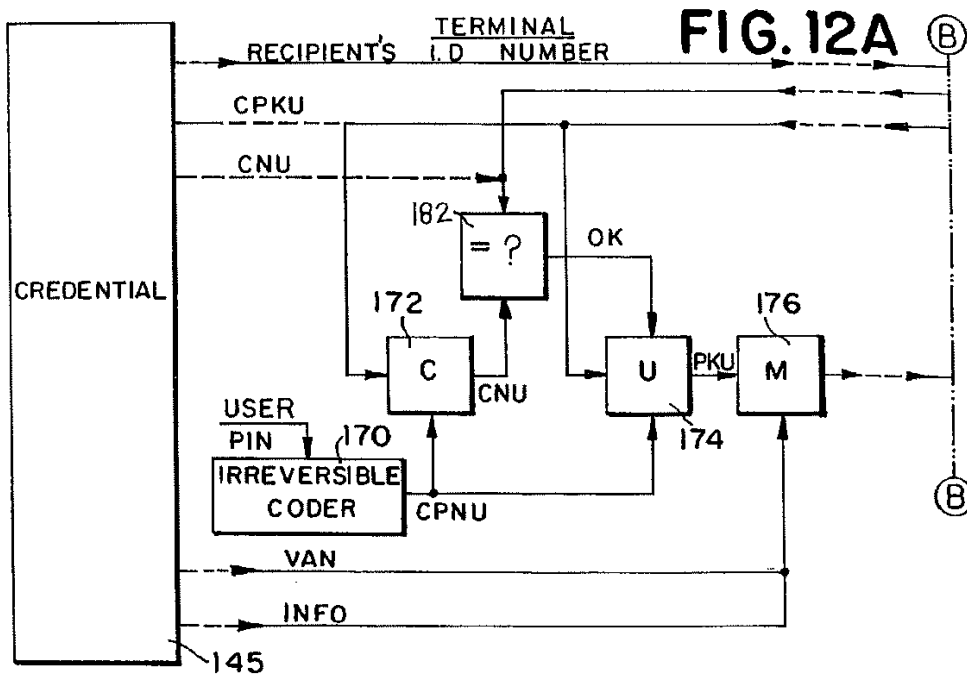


U.S. Patent

Oct. 26, 1999

Sheet 6 of 15

5,974,148



U.S. Patent

Oct. 26, 1999

Sheet 8 of 15

5,974,148

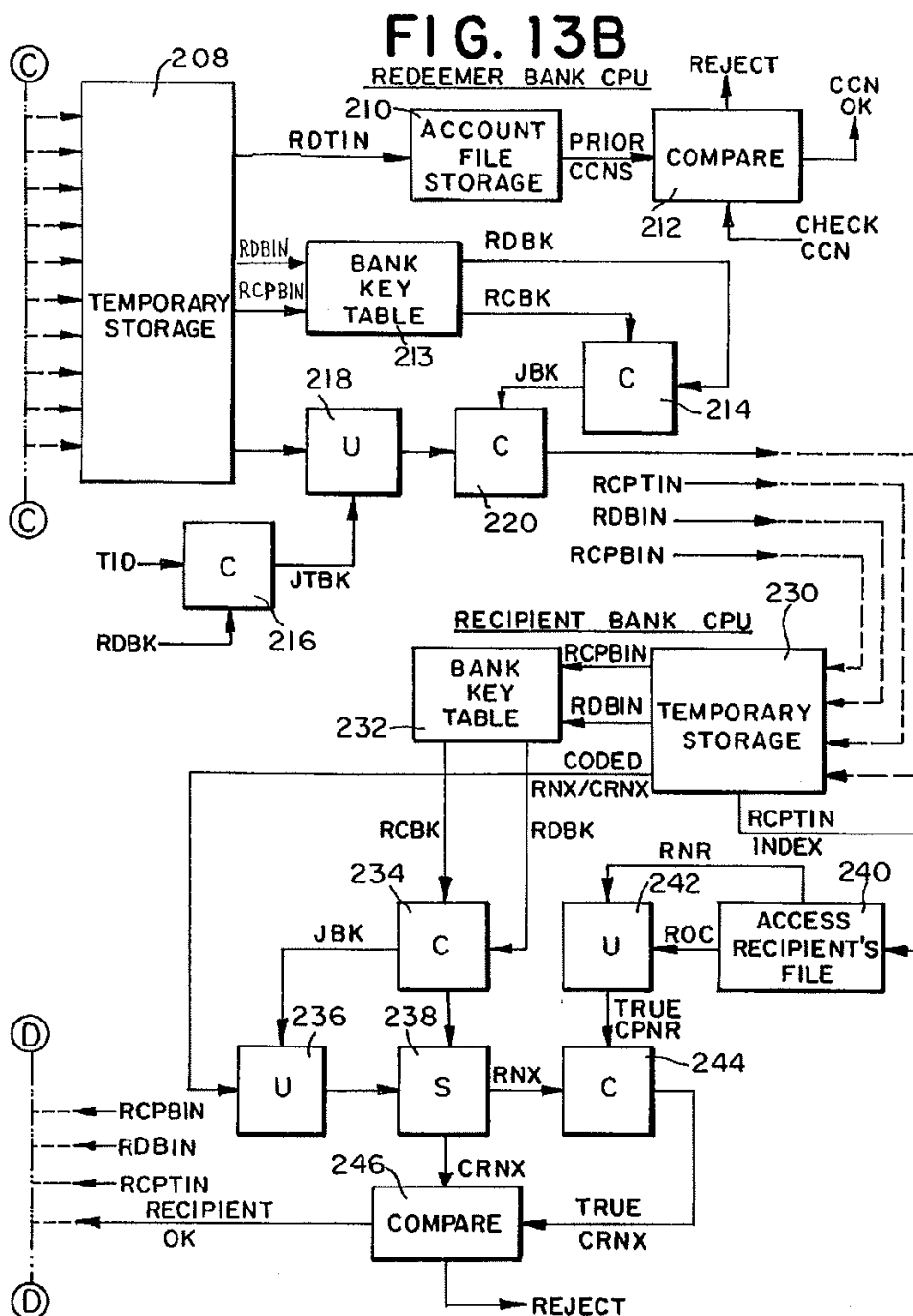
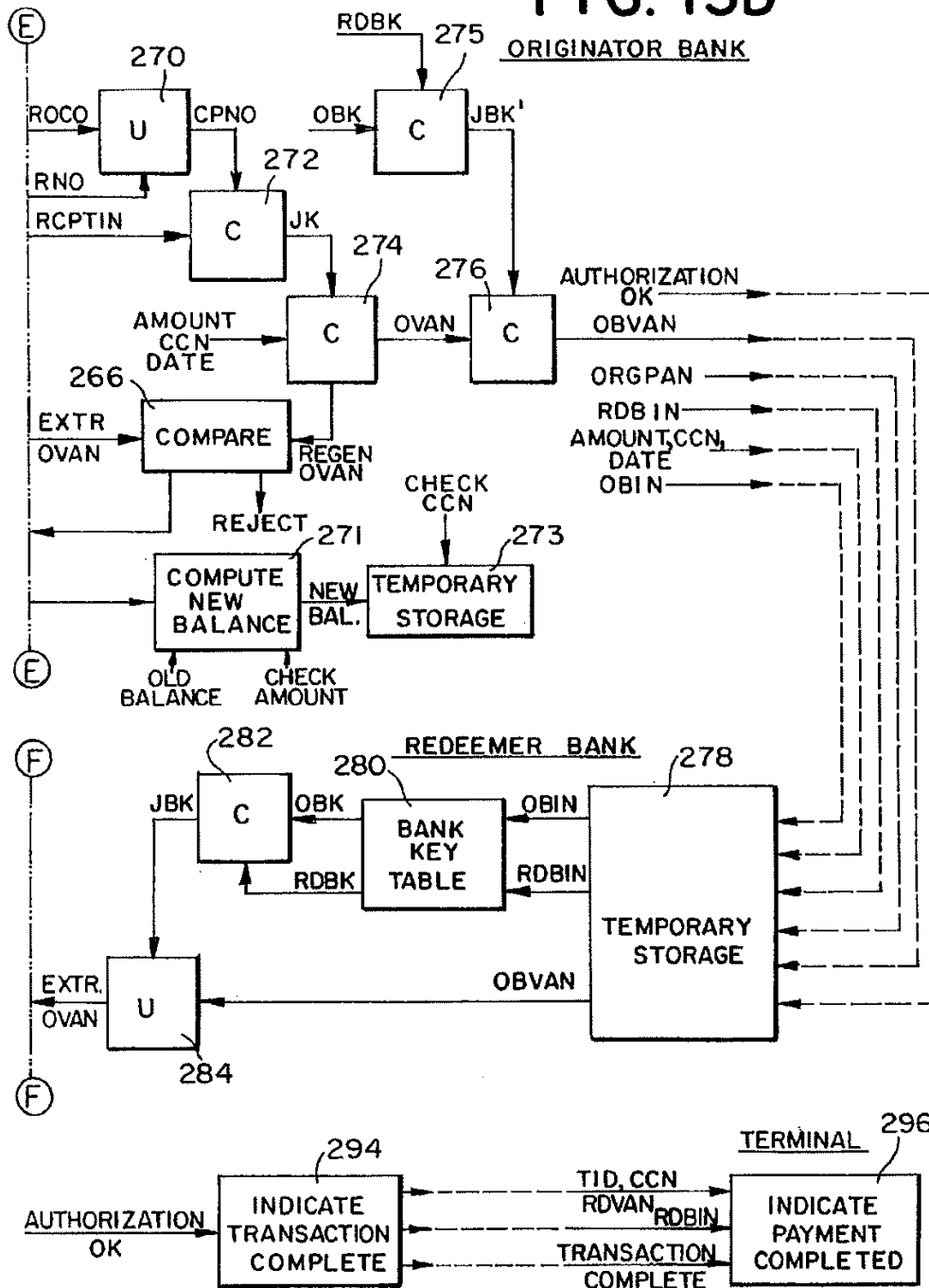


FIG. 13D



U.S. Patent

Oct. 26, 1999

Sheet 11 of 15

5,974,148

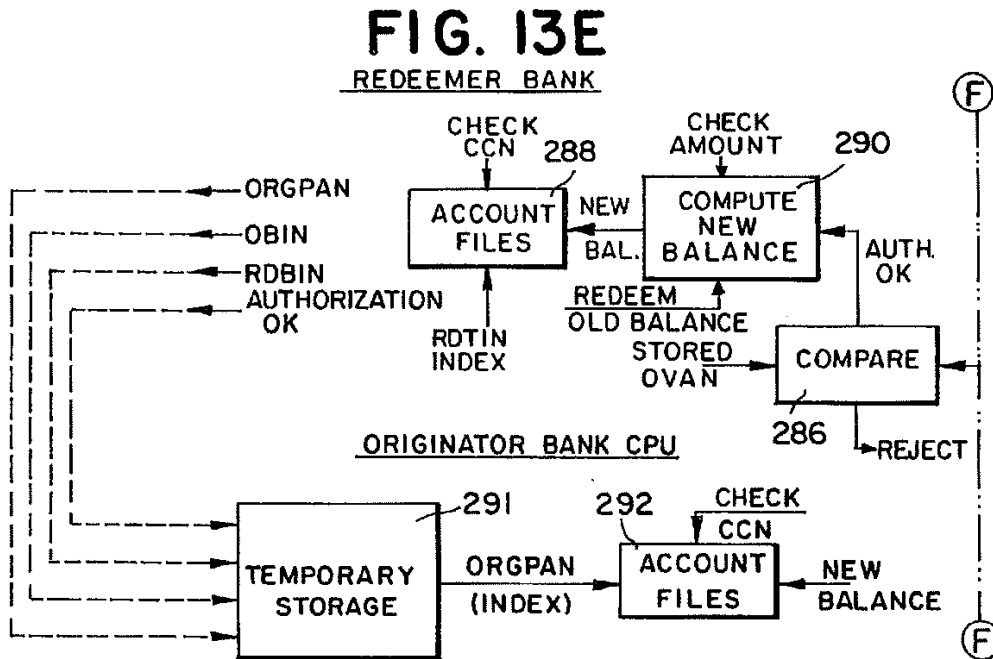
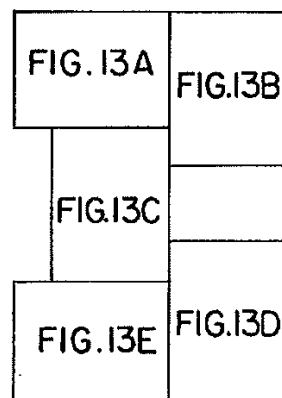


FIG. 14



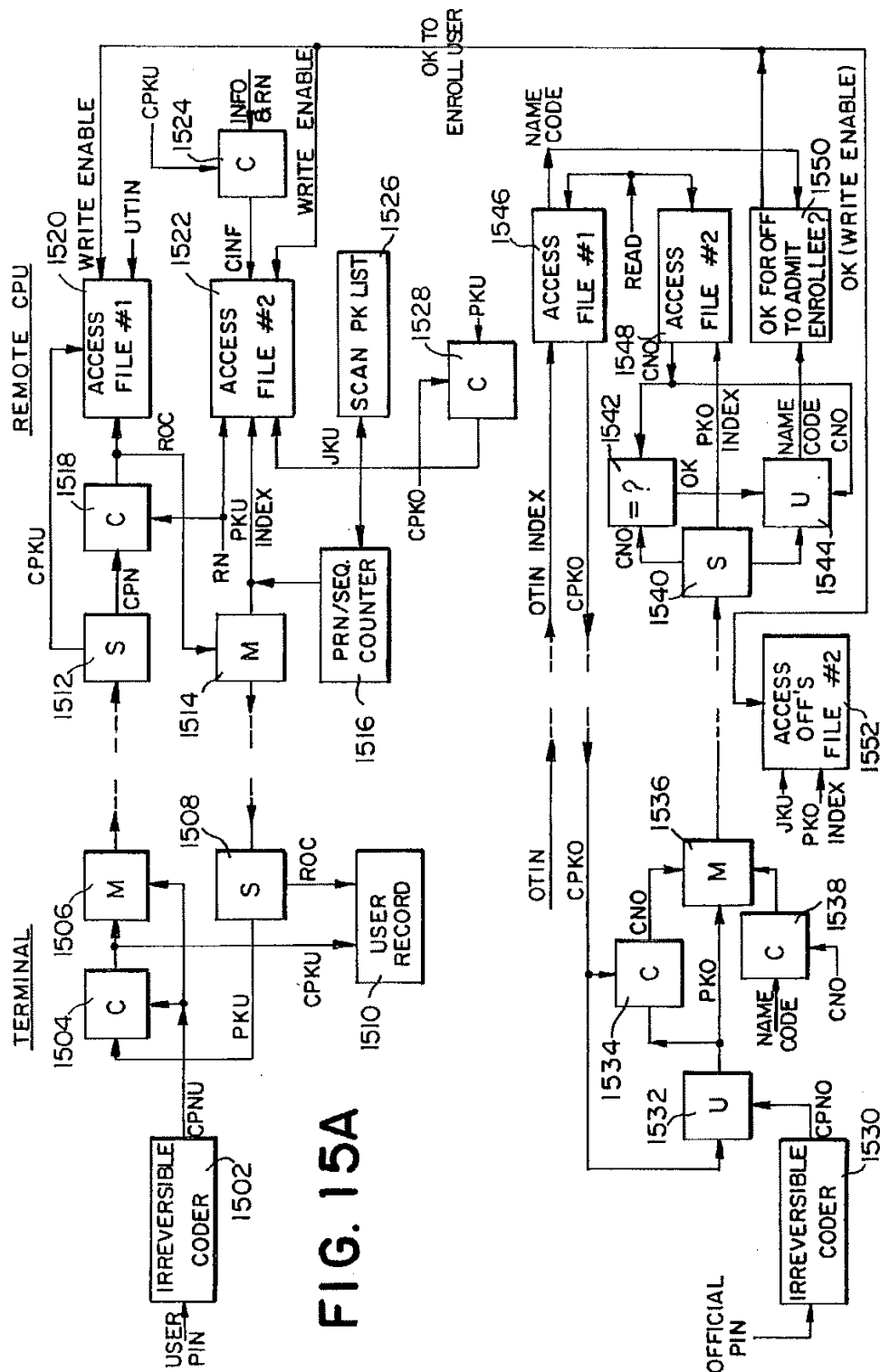


FIG. 15A

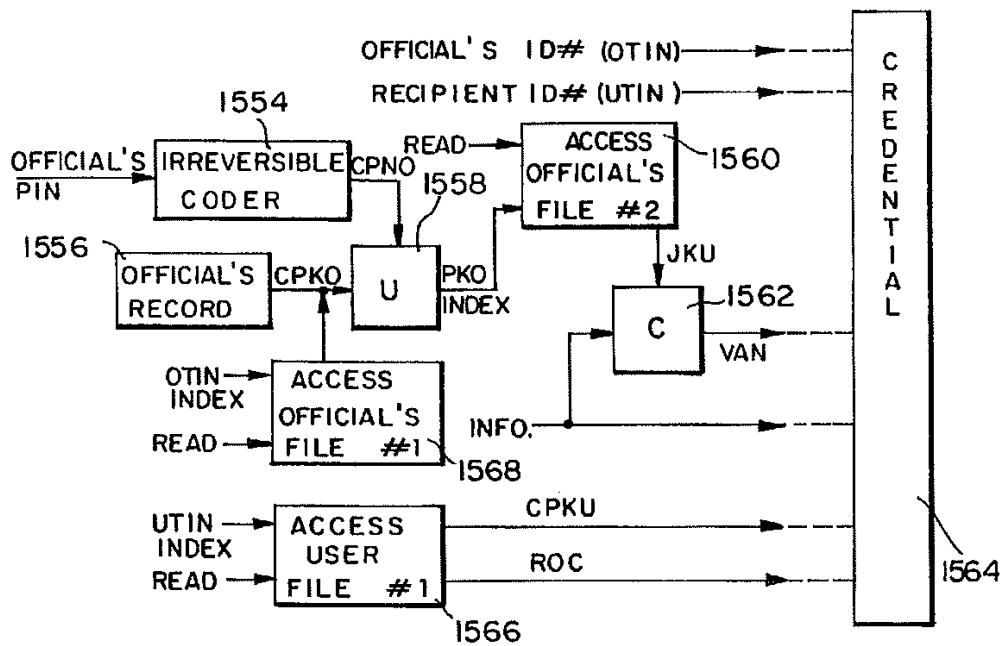


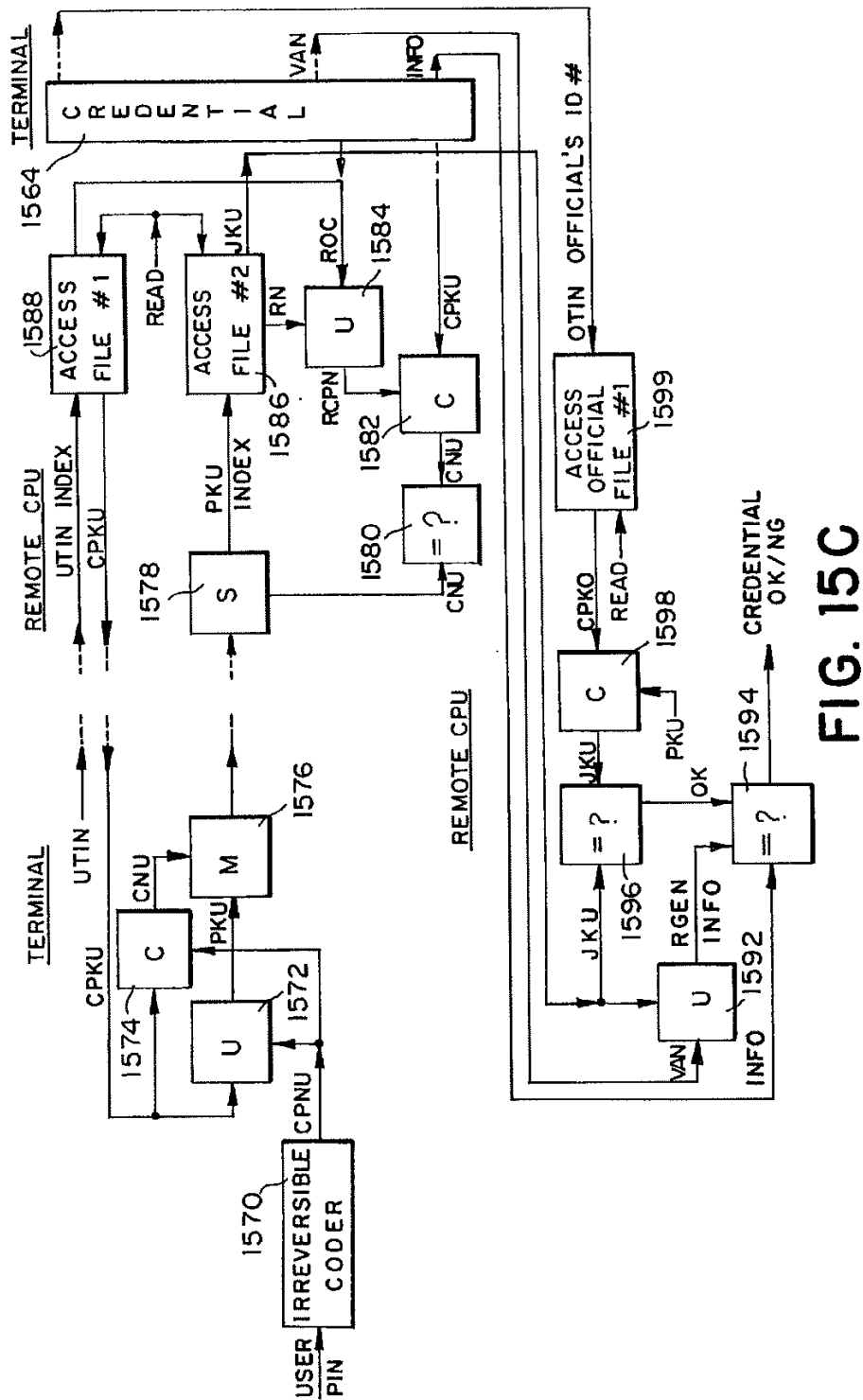
FIG. 15B

U.S. Patent

Oct. 26, 1999

Sheet 14 of 15

5,974,148



U.S. Patent

Oct. 26, 1999

Sheet 15 of 15

5,974,148

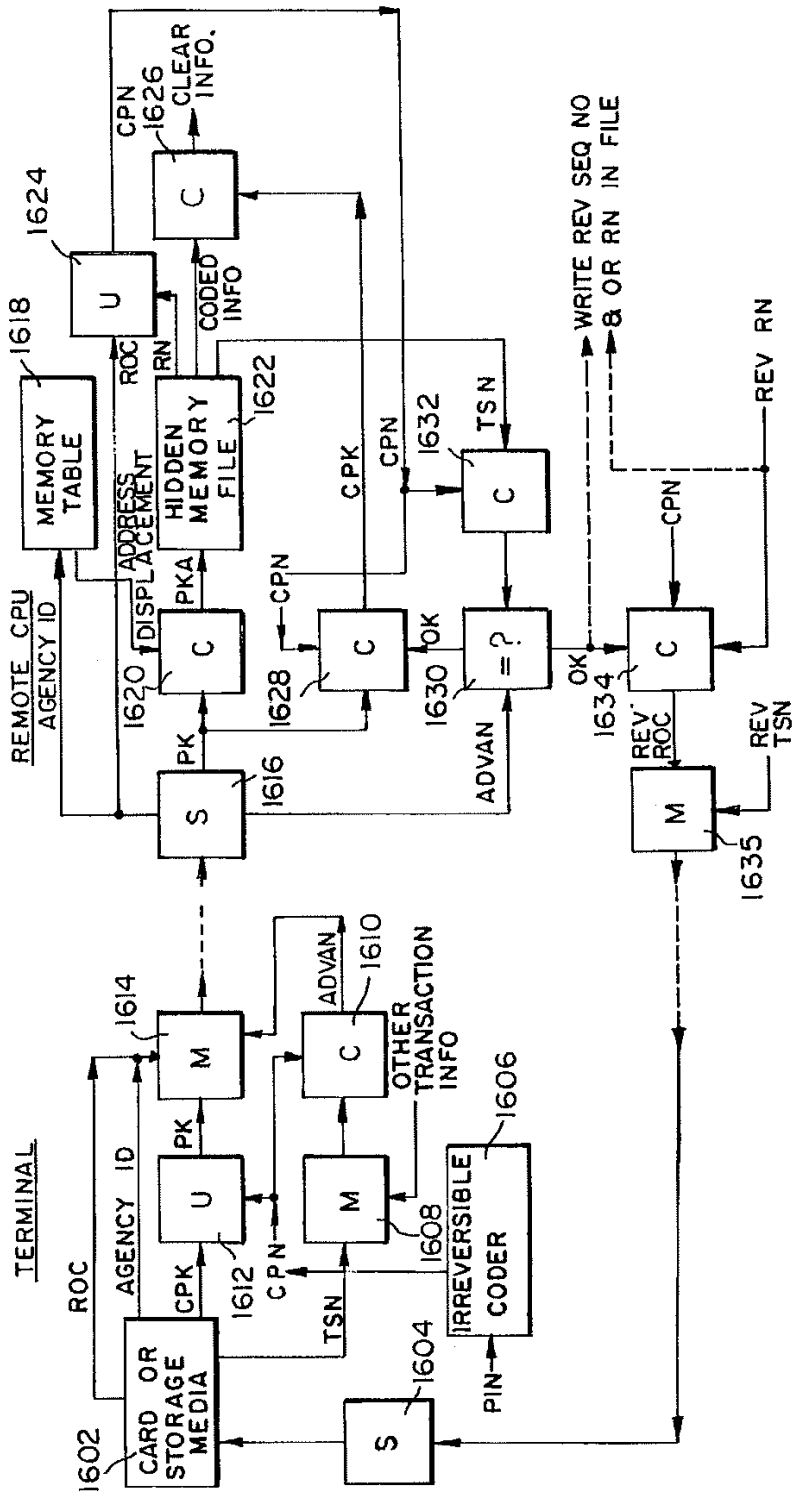


FIG. 16

5,974,148

1

METHOD FOR SECURING INFORMATION RELEVANT TO A TRANSACTION

This is a division of application Ser. No. 08/747,174, filed Nov. 12, 1996, now U.S. Pat. No. 5,793,302 which in turn is a continuation of application Ser. No. 08/446,369, filed May 22, 1995, now abandoned 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. 08/455,477, filed May 22, 1995, and application Ser. No. 08/455,612, 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, wager 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

2

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;

5,974,148

3

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 uncoded 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

4

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 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. 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

5,974,148

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) RNX 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 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 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 CRNX and RNX, 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 CRNX and RNX, with CRNX being applied to a comparison 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 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 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 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

5,974,148

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-

5,974,148

9

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, 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.

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.

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 the present embodiment offers an additional level of security in that, not

10

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 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 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 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 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

5,974,148

11

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. Alternatively, 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 CPKU 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,

12

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. 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. 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

5,974,148

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, RCPTIN, and the recipient'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 RCPTIN, 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,

5,974,148

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 RNK and CRNK produced by coder 220. Uncoder 236 therefore 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 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 RNK as a data input. The data output of coder 244 is therefore the true CRNK.

At block 246, this true CRNK is compared to the CRNK 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 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 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).

5,974,148

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 1540, 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

5,974,148

19

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 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

20

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 1504 (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 revisable 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 (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

5,974,148

21

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.

22

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

5,974,148

23

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

24

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.

What is claimed is:

1. A method of transferring funds from a first party to a second party, the method comprising:

creating a variable authentication number (VAN) on a computer using first information and a secret key of the first party, the first information including an amount and information for identifying the first party or the second party, the VAN attesting to the authenticity of the first party and the first information;

creating an instrument by the first party for transferring funds to the second party, the instrument including the first information and the variable authentication number (VAN) and attaching the VAN to the instrument.

2. The method of claim 1 wherein a credential, including a second VAN and a non-secret key of the first party, was previously issued to the first party by an entity authorized to issue a credential, the credential and the second VAN being used by the second party, or a third party, to attest to the non-secret key belonging to the first party, the non-secret key from the credential being disseminated to the second party, or the third party, by joining the credential to the instrument.

3. The method of claim 2 wherein a non-secret key of the credential issuing entity is appended to the credential and is disseminated to the second party, or the third party, the second or third party using the non-secret key of the credential issuing entity, and the second VAN to determine whether the non-secret key of the first party belongs to the first party.

4. The method of claim 1 wherein the secret key is obtained by the first party using a PIN, or using descriptive details, of the first party.

5. The method of claim 1 wherein the VAN is created by the first party using an error detection code (EDC), and the

5,974,148

25

first information is subsequently authenticated by the second party, or by a third party, the method further comprising:

creating the EDC1 by coding the first information;
creating the VAN by coding the EDC1 using the first party's secret key; the second party, or the third party, subsequently obtaining the instrument and the VAN, and extracting the VAN and first information;

coding the first information to create an error detection code (EDC2);

uncoding the VAN to recover EDC1 using a non-secret key of the first party;

comparing the EDC1 with the EDC2; and
the second party, or the third party, authenticating the first information if EDC1 and EDC2 correspond.

6. The method of claim 1 wherein the form of the instrument is selected from the group comprising paper, plastic and electronic.

7. The method of claim 1 wherein the first information includes information selected from the group comprising the first party's name, the first party's account number, the first party's bank name, the first party's bank identification number, the first party's routing transit number, the first party's error detection code EDC1, the first party's variable authentication number (VAN),

the second party's name, the second party's non-secret key,

an amount, a date, a check control number, a check serial number, a payment instruction and a memo.

8. The method of claim 1 wherein the first information includes a redemption VAN (RVAN) or check control number (CCN), the method further comprising:

using the RVAN or CCN to intercept or reject duplicate instruments by maintaining a list of previously redeemed RVANS or CCNs, and first party names in a storage means located where the funds transfer is processed.

9. The method of claim 1 wherein at least one of the first party or the second party is pre-enrolled and pre-authenticated during enrollment, at least a portion of the enrollment information, including the first party's or the second party's non-secret key being stored in escrow, or in trust, during enrollment by the credential issuing entity, wherein the credential issuing entity is selected from the group comprising an official, an agency, a bank, and a pre-authorized party.

10. The method of claim 1 wherein the first party and the second party are the same party.

11. The method of claim 1 wherein the availability and sufficiency of the amount of funds in the first party's account is verified by the first party's bank prior to or after the instrument is issued.

12. The method of claim 1 wherein the first party's accounts payable file and the second party's accounts receivable file are updated as a result of transferring the funds.

13. The method of claim 1 wherein a redemption VAN (RVAN) is attached to the instrument, the RVAN being created by the second party or an authorizing party, the RVAN indicating that the first information has been authenticated by the second party or by the authorizing party.

14. The method of claim 1 wherein the first information is subsequently authenticated by the second party, or by a third party, the method further comprising:

the second or third party subsequently obtaining the instrument and the VAN and extracting the first information and the VAN,

26

uncoding the VAN to recover the first information using a non-secret key of the first party,

comparing the recovered first information with the extracted first information, and

authenticating the first information if the result of the comparison is favorable.

15. The method of claim 1 wherein the instrument is selected from the group comprising a personal check, a paycheck, a travel check, a third party check, a bond, a stock certificate, food stamps, wager receipts, and a bank card.

16. A method for using a payment instrument to make a payment, the payment instrument being originated by a payor and made payable to a payee, the method comprising:

creating a variable authentication number (VAN) on a computer using payment information and a secret key of the payor, the payment information including an amount and information for identifying the payee, the VAN being usable for attesting to the authenticity of the payor and the payment information; and

the payor using the payment information and the VAN to create the payment instrument, the payment instrument being used to make the payment.

17. The method of claim 16 wherein a credential including a VAN was previously issued to the payer by a credential issuing entity, a non-secret key being included in the credential, the credential and VAN being used by the payee or the payer's bank, to attest to the non-secret key belonging to the payer, the non-secret key of the payer being disseminated to the payee or the payer's bank, by joining the credential to the instrument.

18. The method of claim 17 wherein a non-secret key of the credential issuing entity is appended to the credential and is disseminated to the payee or the payer's bank, the non-secret key of the credential issuing entity and the VAN of the credential being used to attest to the payer's non-secret key belonging to the payer.

19. The method of claim 16 wherein the VAN is created by the payer using an error detection code (EDC1), the payment information being subsequently authenticated by the payee or the payer's bank, the method further comprising:

creating the EDC1 by coding the payment information,
creating the VAN by coding the EDC1 using the secret key of the payer,

the payee or the payer's bank subsequently obtaining the instrument and extracting the VAN and payment information,

coding the payment information to create an error detection code (EDC2),

uncoding the VAN to recover EDC1 using a non-secret key of the payer,

comparing the EDC1 with the EDC2, and,

the payee or the payer's bank authenticating the first information if the EDC1 and the EDC2 correspond.

20. The method of claim 16 wherein the form of the instrument is selected from the group comprising paper, plastic and electronic.

21. The method of claim 16 wherein the instrument is selected from the group comprising a personal check, a paycheck, a travel check, a third party check, a bond, a stock certificate, food stamps, wager receipts, and a bank card.

22. The method of claim 16 wherein the instrument information is selected from the group comprising the payer's name, the payer's account number, the payer's bank name, the payer's bank identification number, the payer's

5,974,148

27

routing transit number, the payer's error detection code EDC1, the payer's variable authentication number (VAN), the payee's name, the payee's non-secret key, an amount, a date, a check control number, a check serial number, a payment instruction, and a memo.

23. The method of claim 16 wherein the instrument information includes a redemption VAN (RVAN) or a check control number (CCN), the method further comprising using the RVAN or CCN to intercept or reject duplicate instruments by maintaining a list of previously redeemed RVANs or CCNs, and names of payers in a storage means located where the payment is processed.

24. The method of claim 16 wherein at least one of the payer or the payee is pre-enrolled and pre-authenticated during enrollment, the enrollment information, and at least the payer's or the payee's non-secret key being stored in escrow, or in trust, during enrollment by the credential issuing entity, wherein the credential issuing entity is selected from the group comprising an official, an agency, a bank, and a pre-authorized party.

25. The method of claim 16 wherein the payer and the payee are the same party.

26. The method of claim 16 wherein the availability and sufficiency of the amount of funds in the payer's account is verified by the payer's bank prior to or after the instrument is issued.

27. The method of claim 16 wherein a redemption VAN (RVAN) is attached to the instrument, the RVAN being created by the payee or the payer's bank, the RVAN indicating that the first information has been authenticated by the payee, or by the payer's bank.

28. A payment method, comprising:

a payer obtaining a document containing document information, the document information being associated with a debt incurred by the payer or for goods or for services to be paid for or purchased by the payor; the payer creating a variable authentication number (VAN) on a computer using at least a portion of the document information, and a secret key of the payor, the document information including an amount, and information for identifying the payee, the VAN being used for attesting to the authenticity of the payor and document information; and

the payor creating a payment instrument using the document information and appending the VAN to the payment instrument, the payment instrument being used to pay for the incurred debt or for the purchase of goods or services.

29. The method of claim 28 wherein at least a portion of the document information comprises billing information or purchase information, the billing information or purchase information being attached to the instrument when payment is made.

28

30. The method of claim 29 further comprising:

creating a second variable authentication number (VAN2) by using at least a portion of the billing or purchase information and the secret key of the payer, and

appending the VAN2 to the document information.

31. The method of claim 28 wherein the form of the document is selected from the group comprising paper, plastic and electronic.

32. The method of claim 28 wherein the document information is selected from the group comprising a bill, information associated with a debt,

a non-secret key of the document originator, a variable authentication number (VAN) of the originator,

software, tickets, data, text, a FAX message, recorded audio or video, a drawing, an image, a photo, electronic mail, physical mail, a medical prescription, motor vehicle registrations, social security cards, passports, birth certificates, identification cards and personal storage media.

33. The method of claim 28 wherein the document is selected from the group comprising a bill and a purchase document.

34. A funds transfer method comprising:

a first party creating an instrument for transferring funds to a second party, the adequacy of the funds in the first party's account being verified after the instrument is issued;

using a computer to create a variable authentication number (VAN), the VAN being created using at least a secret key of the first party; and

including the VAN with the instrument for subsequent use in attesting to the authenticity of the instrument.

35. A funds transfer method comprising:

an originator party creating an instrument for transferring funds to a recipient party, the instrument information comprising (i) a variable authentication number (VAN), and (ii) one or more pieces of payment information including an amount, information for identifying the recipient party or the originator party, a date, and a check control or serial number;

creating an error detection code (EDC1) by coding one or more pieces of the payment information; and

creating the VAN on a computer by coding the EDC1 using a secret key of the originator, the originator's VAN being usable to determine the authenticity of the one or more pieces of payment information.

* * * * *

Exhibit “C”

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

LEON STAMBLER	§	
Plaintiff,	§	
	§	
v.	§	CIVIL ACTION NO. 2-08-cv-204-DF-CE
	§	
JPMORGAN CHASE & CO., et al.,	§	
Defendants.	§	
	§	

MEMORANDUM OPINION AND ORDER

The Court held a *Markman* hearing on March 25, 2010. After considering the submissions and the arguments of counsel, the Court issues the following order regarding claim construction:

I. Background of the Technology

Plaintiff Leon Stambler asserts United States Patent Nos. 5,793,302 (“the ‘302 patent”) and 5,974,148 (“the ‘148 patent”) (collectively, “Stambler patents”) against remaining Defendants Compass Bancshares, Inc., Compass Bank, First Horizon National Corporation, and First Tennessee Bank National Association (collectively, “Defendants”). The Stambler patents have a common specification and claim priority to November 17, 1992. Plaintiff asserts claims 7, 41, 43, 46, 47, 48, and 53 of the ‘302 patent and claims 28, 34, and 35 of the ‘148 patent. The Stambler patents are entitled “Method for Securing Information Relevant to a Transaction” and teach improvements to conducting financial transactions thereby minimizing fraud on the parties.

The patents address two types of fraud that can occur in multi-party transactions, especially electronic transactions. First, the patents disclose a system for authenticating that information relating to the financial transaction has not been fraudulently authored, such as the amount on a check. Second, the patents teach authenticating the parties to a transaction. For example, the transaction system of the patents would detect when a person cashing a check is not the intended

recipient.

The invention uses what is called a “variable authentication number (VAN)” to authenticate the transaction information as well as the parties. A VAN (a disputed term), as disclosed in the embodiment, contains an encoded key that contains information about at least one of the parties and at least some of the transaction information. This encoded key is called a joint key. The joint key might, for example, contain the intended recipient’s tax identification number, the check amount, and the payor’s identifying information. When an endorsed check is presented at the recipient’s bank, the recipient’s bank first verifies whether the party presenting the check is in fact the intended recipient. After verifying that the recipient is authentic, the recipient’s bank requests that the payor’s bank transfer the funds in accordance with the check’s instructions. The payor’s bank will then verify whether the document has been altered based upon the document information encoded into the joint key. Additionally, the payor’s bank will be able to verify whether the payor did in fact originate this check based upon the payor information encoded into the joint key. According to the embodiment, only selected parties would be able to decode the VAN to access the joint key, thereby making it nearly impossible for the VAN to be fraudulently created or modified.

Plaintiff previously pursued claims under the asserted patents before the District of Delaware in 2001. *See Stambler v. RSA Sec. Inc.*, No. 01-65-SLR (D. Del.). The Delaware court issued its claim construction order in 2003. A number of the terms that the Delaware court construed are at issue in this litigation: VAN; secret key of the first party/payor/originator; instrument; previously issued; and credential. Defendants argue that Plaintiff should be estopped from pursuing constructions that are different than those it pursued in the Delaware court when the Delaware court adopted Plaintiff’s proposal. Plaintiff argues that the constructions in the

Delaware court are based upon dictionary definitions almost exclusively and that *Phillips* is intervening law regarding claim construction.

II. General Principles Governing Claim Construction

“A claim in a patent provides the metes and bounds of the right which the patent confers on the patentee to exclude others from making, using or selling the protected invention.” *Burke, Inc. v. Bruno Indep. Living Aids, Inc.*, 183 F.3d 1334, 1340 (Fed. Cir. 1999). Claim construction is an issue of law for the court to decide. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 970-71 (Fed. Cir. 1995) (en banc), *aff’d*, 517 U.S. 370 (1996).

To ascertain the meaning of claims, the court looks to three primary sources: the claims, the specification, and the prosecution history. *Markman*, 52 F.3d at 979. Under the patent law, the specification must contain a written description of the invention that enables one of ordinary skill in the art to make and use the invention. A patent’s claims must be read in view of the specification, of which they are a part. *Id.* For claim construction purposes, the description may act as a sort of dictionary, which explains the invention and may define terms used in the claims. *Id.* “One purpose for examining the specification is to determine if the patentee has limited the scope of the claims.” *Watts v. XL Sys., Inc.*, 232 F.3d 877, 882 (Fed. Cir. 2000).

Nonetheless, it is the function of the claims, not the specification, to set forth the limits of the patentee’s claims. Otherwise, there would be no need for claims. *SRI Int’l v. Matsushita Elec. Corp.*, 775 F.2d 1107, 1121 (Fed. Cir. 1985) (en banc). The patentee is free to be his own lexicographer, but any special definition given to a word must be clearly set forth in the specification. *Intellicall, Inc. v. Phonometrics*, 952 F.2d 1384, 1388 (Fed. Cir. 1992). And, although the specification may indicate that certain embodiments are preferred, particular embodiments appearing in the specification will not be read into the claims when the claim

language is broader than the embodiments. *Electro Med. Sys., S.A. v. Cooper Life Sciences, Inc.*, 34 F.3d 1048, 1054 (Fed. Cir. 1994).

This court's claim construction decision must be informed by the Federal Circuit's decision in *Phillips v. AWH Corporation*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). In *Phillips*, the court set forth several guideposts that courts should follow when construing claims. In particular, the court reiterated that "the *claims* of a patent define the invention to which the patentee is entitled the right to exclude." 415 F.3d at 1312 (emphasis added) (*quoting Innova/Pure Water, Inc. v. Safari Water Filtration Systems, Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). To that end, the words used in a claim are generally given their ordinary and customary meaning. *Id.* The ordinary and customary meaning of a claim term "is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application." *Id.* at 1313. This principle of patent law flows naturally from the recognition that inventors are usually persons who are skilled in the field of the invention. The patent is addressed to and intended to be read by others skilled in the particular art. *Id.*

The primacy of claim terms notwithstanding, *Phillips* made clear that "the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification." *Id.* Although the claims themselves may provide guidance as to the meaning of particular terms, those terms are part of "a fully integrated written instrument." *Id.* at 1315 (*quoting Markman*, 52 F.3d at 978). Thus, the *Phillips* court emphasized the specification as being the primary basis for construing the claims. *Id.* at 1314-17. As the Supreme Court stated long ago, "in case of doubt or ambiguity it is proper in all cases to refer back to the descriptive

portions of the specification to aid in solving the doubt or in ascertaining the true intent and meaning of the language employed in the claims.” *Bates v. Coe*, 98 U.S. 31, 38 (1878). In addressing the role of the specification, the *Phillips* court quoted with approval its earlier observations from *Renishaw PLC v. Marposs Societa’ per Azioni*, 158 F.3d 1243, 1250 (Fed. Cir. 1998):

Ultimately, the interpretation to be given a term can only be determined and confirmed with a full understanding of what the inventors actually invented and intended to envelop with the claim. The construction that stays true to the claim language and most naturally aligns with the patent’s description of the invention will be, in the end, the correct construction.

Consequently, *Phillips* emphasized the important role the specification plays in the claim construction process.

The prosecution history also continues to play an important role in claim interpretation. The prosecution history helps to demonstrate how the inventor and the PTO understood the patent. *Phillips*, 415 F.3d at 1317. Because the file history, however, “represents an ongoing negotiation between the PTO and the applicant,” it may lack the clarity of the specification and thus be less useful in claim construction proceedings. *Id.* Nevertheless, the prosecution history is intrinsic evidence. That evidence is relevant to the determination of how the inventor understood the invention and whether the inventor limited the invention during prosecution by narrowing the scope of the claims.

Phillips rejected any claim construction approach that sacrificed the intrinsic record in favor of extrinsic evidence, such as dictionary definitions or expert testimony. The *en banc* court condemned the suggestion made by *Texas Digital Systems, Inc. v. Telegenix, Inc.*, 308 F.3d 1193 (Fed. Cir. 2002), that a court should discern the ordinary meaning of the claim terms (through dictionaries or otherwise) before resorting to the specification for certain limited purposes. *Id.* at

1319-24. The approach suggested by *Texas Digital*—the assignment of a limited role to the specification—was rejected as inconsistent with decisions holding the specification to be the best guide to the meaning of a disputed term. *Id.* at 1320-21. According to *Phillips*, reliance on dictionary definitions at the expense of the specification had the effect of “focus[ing] the inquiry on the abstract meaning of words rather than on the meaning of the claim terms within the context of the patent.” *Id.* at 1321. *Phillips* emphasized that the patent system is based on the proposition that the claims cover only the invented subject matter. *Id.* What is described in the claims flows from the statutory requirement imposed on the patentee to describe and particularly claim what he or she has invented. *Id.* The definitions found in dictionaries, however, often flow from the editors’ objective of assembling all of the possible definitions for a word. *Id.* at 1321-22.

Phillips does not preclude all uses of dictionaries in claim construction proceedings. Instead, the court assigned dictionaries a role subordinate to the intrinsic record. In doing so, the court emphasized that claim construction issues are not resolved by any magic formula. The court did not impose any particular sequence of steps for a court to follow when it considers disputed claim language. *Id.* at 1323-25. Rather, *Phillips* held that a court must attach the appropriate weight to the intrinsic sources offered in support of a proposed claim construction, bearing in mind the general rule that the claims measure the scope of the patent grant.

III. Agreed Terms

The parties have agreed to definitions of the following terms:

Term	Claim number	Agreed Construction
“coding”	‘302, claim 7; ‘148, claim 35	Transforming information by applying a known algorithm
“credential information”	‘302, claims 47, 53	Information stored or contained in a credential
“determining	‘302, claim 53	Determining whether the at least a portion of the received funds

whether the at least a portion of the received funds transfer information is authentic by using the VAN and the credential information”		transfer information is unchanged by using the VAN and the credential information
“payment”	‘302, claims 43, 53; ‘148, claim 28, 35	Compensation in exchange for goods or services or the discharge of a debt
“payer/payor”	‘148, claim 28	Plain meaning. The parties agree that the terms “payer” and “payor” refer to the same entity.
“creating an error detection code (EDC1) by coding”	‘148, claim 35	Creating an error detection code (EDC1) by applying an algorithm to information in such a manner as to permit the detection of changes without complete recovery of the original information.
“Error detection code or EDC”	‘148, claim 35; ‘302, claim 46	The result of applying an algorithm to information in such a manner as to permit detection of changes but without complete recovery of the original information
“VAN being usable to determine the authenticity of the one or more pieces of payment information”	‘148, claim 35	The VAN being usable to determine that the one or more pieces of payment information has not changed

Joint Claim Construction and Prehearing Statement at 1–2. [Dkt. No. 356]

IV. Disputed Terms

A. “a third party for determining”

Term	Plaintiff’s Definition	Defendants’ Definition
“a third party for determining whether the at least a portion of the received funds transfer information is authentic by using the VAN”	A party or system that performs the determining step of the claim.	A party different from the party performing the other steps of the claim, for determining.

This term appears in claim 41 of the ‘302 patent. The parties dispute whether the “third party” is permitted to perform any of the other steps enumerated in Claim 41. Claim 41 is a method with four steps:

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 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 the 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.

Both parties agree that the third party must perform the “determining” step. Plaintiff argues that the plain language of the claim does not prohibit the third party from performing any of the other three steps. As none of the other three steps recite an actor, Plaintiff argues that the language of the claim indicates that the inventor did not intend to restrict those steps to (or from) particular parties. According to Plaintiff, a third party could receive the funds transfer information and use that to generate a VAN.

Plaintiff further argues that Defendant’s construction would read out a disclosed embodiment. In the “paperless/cashless transaction system,” the transaction system is a terminal belonging to the payment recipient, or “second party” as recited in this claim. ‘302 patent, 24:5–10. The terminal receives funds transfer information from the payment originator, or “first party” in this claim, generates a VAN, and authenticates the payment originator using the VAN. ‘302 patent, 14:10–20. Plaintiff argues that the transaction system is the third party of Claim 41, and performs the “receiving,” “generating,” and “determining” steps.

Finally, Plaintiff argues that the prosecution history supports its construction. When the

inventor amended Claim 41, the inventor told the examiner, “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 [41].” Plaintiff’s Brief, Ex. D at 55. This, according to Plaintiff, shows that the third party performs the “determining” step and the “transferring” step.¹

Defendants argue that in the context of Claim 41, the inventor chose to specify the “third party” to differentiate the party that performs the determining step from the party performing the other steps. According to Defendant, a party, which is neither the first nor third parties, receives “funds transfer information” from the payment originator, generates a VAN, and “informs the first party’s bank to transfer the funds.” Def. Brief at 21. Defendants also argue that it would make no sense to have the same party that receives the funds transfer information and then generates the VAN be the party to authenticate the VAN it just created.

Defendants also rely on the prosecution history, wherein the inventor added the term “third party” by amendment. According to Defendants, “If a ‘third party’ is the same party performing the other steps of the claim, the recitation of a ‘third party’ in the claim would not have been necessary.” Def. Brief at 22. Defendants also disagree with Plaintiff’s reading of the office action response in which the amendment appears. Defendants argue that the sentence, “The use of a third party to authenticate a VAN and transfer and transfer of funds is recited in claim [41],” should be read to mean the third party authenticates a VAN and, thereby, authenticates a transfer of funds.

With respect to the embodiments, Defendants argue that Plaintiff’s arguments are misleading. Defendants say that the “system” recited in the prosecution history is not the same

¹ Plaintiff inserted [sic] following “transfer of funds” to suggest the erroneous insertion of the word “of” by the inventor during prosecution of the patent. Pl. Brief at 9.

“paperless/cashless transaction system” described at the end of the preferred embodiment. *See* ‘302 patent, 24:14–24. *See also* Pl. Br., Ex. D at 55 (“the system which approves or disapproves the payment is a third party”). Defendants attempt to refute Plaintiff’s argument that Defendant’s construction does not read on the paperless/cashless embodiment by arguing that Claim 41 is not intended to read upon that particular embodiment.

Plaintiff argues that it is “black letter law” that the construed claims must read on all of the preferred embodiments. Pl. Reply at 4. Here, however, is a case where the embodiments are so varied that a single claim is not expected to read upon all of them. *See* ‘302 patent, 6:12–45 (describing two authenticating parties, one of which does not and cannot generate a VAN: authenticating transfer information at the originator’s bank with a VAN; authenticating the recipient at the recipient’s bank without using a VAN). *See also id* at 24:5–24 (describing a system where the recipient is never authenticated).

Defendant’s argument is not without force. A construction that allows the party that generates a VAN to turn around and authenticate that very VAN would be nonsensical. As urged at oral argument, however, the same party might authenticate the VAN it had previously created when the payee presents the check at the issuing financial institution for payment. Inartfully drafted though the claim may be, using Defendant’s proposed construction would require four parties, which is not mandated by the claim language, specification, or prosecution history. If the third party is not permitted to perform any of the other steps, then it becomes clear that some additional party or parties must perform the receiving and generating steps. The Court rejects this view of the claim and construes this limitation to mean, “a party, other than the first or second parties, that performs the determining step of the claim.”

B. “variable authentication number (VAN)”

Term	Plaintiff’s Definition	Defendants’ Definition
“generating a variable authentication number (VAN) using at least a portion of the received funds transfer information” ‘302 patent, claim 41	A variable number that can be used in verifying the identity of a party or the integrity of information or both, the number generated by coding information relevant to a transaction, document (paper, electronic, or otherwise), or thing with either a joint key or information associated with or related to at least one party involved in the transaction or issuance of the document or thing.	A variable number that can be used in verifying the identity of a party or the integrity of information or both.
“the payer creating a variable authentication number (VAN) on a computer using at least a portion of the document information, and a secret key of the payor” ‘148 patent, claim 28		
“using a computer to create a variable authentication number (VAN) , the VAN being created using at least a secret key of the first party” ‘148 patent, claim 34		

This term appears in the ‘302 patent, claim 41 and the ‘148 patent, claims 28, 34, and 35. The parties dispute whether Plaintiff is collaterally estopped from arguing a different construction than what it previously proposed and that a Delaware court adopted, and whether a variable authentication number (VAN) must be created in a certain way. Defendants propose the District of Delaware’s construction.

Plaintiff argues that the Delaware court’s construction is of little value because, even though the patentee acted as his own lexicographer, the court’s construction “was based entirely on dictionary definitions of the words ‘variable,’ ‘authentication,’ and ‘number.’” Plaintiff’s Brief at 11. After *Phillips*, according to the Plaintiff, Courts are to defer to the patentee when he defines the terms that appear in the claims.

Plaintiff argues that the patentee acted as his own lexicographer when he wrote in the summary of the invention:

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.

‘302 patent, 2:9–17. Plaintiff argues that VAN is further defined in one of the embodiments: “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.” ‘302 patent, 5:9–25. According to Plaintiff, because “every description and embodiment from the specification” shows the VAN “created by coding information associated with or related to a transaction or credential with either a joint key or ‘information associated with at least one of the parties, without the intermediate step of generating the [joint key].”” Plaintiffs Brief at 13 (quoting ‘302 patent, 5:24–25).

Defendants argue that Plaintiff is collaterally estopped from arguing a different definition in this case and that *Philips* is not intervening law. To prevail on the theory of collateral estoppel, a party must show the following: “(1) the issue is identical to one decided in the first action; (2) the issue was actually litigated in the first action; (3) resolution of the issue was essential to a final judgment in the first action; and (4) plaintiff had a full and fair opportunity to litigate the issue in the first action.” *In re Freeman*, 30 F.3d 1459, 1465 (Fed. Cir. 1994); see also *U.S. v. Shanbaum*, 10 F.3d 305, 311 (5th Cir. 1994) (setting forth a similar test). Defendant argues that only the third element is disputed and that the third element is satisfied because the jury in the Delaware court returned a verdict of non-infringement. Defendants also argue that *Phillips* does not represent a change in law but, rather, is a clarification of then-existing law. Defendant’s Brief at 14.

Should the Court reject Defendant’s collateral estoppel argument, the Defendants alternately argue that defining a VAN by the manner in which is generated is unnecessarily

importing a limitation from the preferred embodiment. Defendants point out that “each of the claims in which VAN appears specifically includes a limitation dictating precisely how the VAN in that particular claim must be generated.” Def. Brief at 15. Both parties agree that the manner in which a VAN is used is necessary to the definition and is consistent in all of the claims, Defendants argue, however, that the VAN is not created the same way in each of claims and to include it in the definition would be superfluous in many of the claims.

Plaintiff’s argument that Claim 41, for example, does not tell a person of ordinary skill in the art that the VAN is generated from information relevant to a transaction is not persuasive. The very text of Claim 41 recites, “generating a variable authentication number (VAN) using at least a portion of the received funds transfer information.” Funds transfer information, likewise, is described within Claim 41 as “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.” Furthermore, the Corut does not agree that the patentee acted as his own lexicographer in the passages that Plaintiff cites.

Absent a showing that a previous construction is incorrect, the Court will not alter a prior court’s claim construction. Moreover, where, as here, the Plaintiff obtains the constructions that he advanced previously, the Court is not easily persuaded to depart from those prior constructions. Central to the invention, however, is that the VAN represents an unalterable truth—thereby thwarting fraud. In order to prevent the manipulation or alteration of the VAN, it is encoded and only decodable by selected, trusted parties. The Delaware court’s construction does not reflect that the VAN has been encoded. The Court slightly modifies the Delaware construction to read, “an encoded variable number that can be used in verifying the identity of a party or the integrity of information or both.”

C. “secret key of the first party/payor/originator”

Term	Plaintiff’s Definition	Defendants’ Definition
“the payer creating a variable authentication number (VAN) on a computer using at least a portion of the document information, and a secret key of the payor” ‘148 patent, Claim 28. “creating the VAN on a computer by coding the EDC1 using a secret key of the originator” ‘148 patent, Claim 35.	A private key that is created by the payor, or an entity originating an instrument on the payor’s behalf, by coding information associated with or related to the payor, which is capable of being separately created by a party intended to authenticate the instrument.	A key that is known only to the payor and those intended to know it and that exists beyond the duration of a particular transaction.

This term, found in claims 28, 34, and 35 of the ‘148 patent, does not appear in the specification. The parties dispute whether the disputed term refers to the “PIN” or the “joint key” of the specification. The Delaware court construed this claim term, adopting plaintiff’s proposal in the previous litigation. Defendants propose the Delaware Court’s construction.

Plaintiff argues that the “secret key” refers to the “joint key” because Claim 34 recites, “[a] VAN being created using at least a secret key of the first party.” According the Plaintiff, only the joint key (or joint code) is used to create the VAN. See ‘302 patent, 5:13–15. Plaintiff argues that the secret key cannot be the PIN because the authenticating party must recreate or uncover the secret key, which cannot be done with a PIN.

Concluding that the secret key is the joint key, Plaintiff goes on to define “joint key.” Plaintiff determines that a joint key is “created by coding ‘information associated with at least one of the parties involved in the transaction (in this case, the originator and recipient).’” Pl. Brief at 15. Plaintiff further explains that the key is secret because “only the first party/originator can initially create and use a particular joint key because only the first party/payor/originator can provide the secret PIN that is used to create a joint key.” Pl. Brief at 16.

Defendants argue that the “secret key” is the PIN because, of all the pieces of data used to create a VAN, “[t]he only thing in that process that the patent describes as ‘secret’ and ‘of a party’ is the originator’s PIN.” Def. Brief at 24. Defendants argue that the secret key cannot be a joint key because ‘the joint key can be created by someone other than the party to whom it belongs and is not a ‘secret key of a party.’” See Def. Brief at 24.

Defendants also argue that the secret key must exist beyond the duration of a transaction. According to Defendant, “[t]he PIN exists before a transaction, during enrollment, and after a transaction, so that the PIN remains associated with the first party and can be used to authenticate that party.” Def. Brief at 25. The bank, so it follows, must have a relatively static reference point in order to perform a meaningful authentication.

Contrary to Plaintiff’s interpretation, the Court is of the opinion that the PIN is indeed used to create a VAN, as described in the ‘302 patent, Column 5, Lines 3–18. Notably, “the originator’s PIN is converted to a coded PIN (CPNO), which is applied as the key input to coder 28.” ‘302 patent, 5:5–6. The coded PIN is then used to code the payment recipient’s information into the joint key. Furthermore, it is the coded PIN that is used to authenticate the originator of an instrument, which means it is known by those intended to know. Finally, Plaintiff’s argument that the VAN cannot be created without the joint key applies equally as well to the coded PIN. The Court finds no error and adopts the Delaware court’s construction. This term means “a key that is known only to the payor and those intended to know it.”

D. “the VAN being used for attesting to the authenticity of the payor and document information”

Term	Plaintiff’s Definition	Defendants’ Definition
“the payer creating a variable authentication number (VAN) on a computer using at least a portion of the document information, and a secret key of the payor, the document information including an amount, and information for identifying the payee, <i>the VAN being used for attesting to the authenticity of the payor and document information</i> ”	The VAN being used to evidence that the instrument originated from the payor and that the at least a portion of the document information used to create the VAN has not changed.	The VAN is used to verify the identity of the payor. In addition, the VAN is used to verify that the document information has not changed.

The disputed phrase appears in claim 28 of the ‘148 patent. First, the parties dispute whether “attesting” means that the VAN “verifies” or “evidences.” Second, the parties dispute whether “attesting to the authenticity of a payor” requires confirming the identity of the payor or merely that the document originated with the payor.

Plaintiff argues that the invention only gives indications of authenticity and does not exactly “verify” authenticity. Pl. Brief at 18. According the Plaintiff, the invention authenticates that the instrument is not forged and did in fact originate with the payor. The plaintiff also argues that “[i]t is axiomatic that the VAN verifies only the portion of the ‘document information’ that was used to create it.” Pl. Brief at 19. Therefore, as the VAN is only created using “at least a portion of the document information,” the VAN can only attest to that portion of the document information.

With respect to the authenticity of the payor, Plaintiff argues that the VAN does not confirm the originator’s identity. Rather, according to Plaintiff, “the VAN in the funds transfer embodiments is used to confirm that the payor originated, or authorized, the funds transfer

instructions.” Pl. Brief at 19. Under Plaintiff’s construction, the “information extracted from the VAN” needs only match “the information included on the payment instrument.” *Id.* Defendants argue that Plaintiff’s proposal is inconsistent with the definition for VAN and inconsistent with the specification.

Defendants also argue that the invention confirms identities of parties, so the VAN must be used to confirm the identity of the payor in claim 28. *See* Def. Brief at 16–17. Defendants point to the “numerous references to [the invention’s] authentication process involving a verification of a party identity.”

The Court construed VAN such that it “can be used in *verifying* the identity of a party or the integrity of information or both.” Furthermore, as Defendants point out, the specification repeatedly uses the word “verify” and never uses the word “evidences.” The Court is of the opinion that the VAN gives more than just an “indication.” Moreover, while an accurate VAN may be only an indicator that a document is not forged, the claim does not require that the VAN verify the document. Rather, the VAN verifies—not merely indicates—that at least some document information is unchanged and that the payor is authentic.

The Court does not agree that payor authenticity is the same thing as identity verification. The specification does indeed recite that the originator’s bank verifies the originator’s identification, but this is not in connection with a VAN. The bank authenticates the identity of the party at *enrollment*, not as part of a transaction. The party’s identity is presumed to be authentic through the use of the secret PIN, but that identity need not be verified as part of the transaction. The VAN merely confirms that the account holder originated the instrument. The VAN does not confirm that the account holder is who he says that he is. The Court construes the disputed phrase to mean: “The VAN being used to verify that the instrument originated from the

payor and that the at least a portion of the document information used to create the VAN has not changed.”

E. “VAN . . . attesting to the authenticity of the instrument”

Term	Plaintiff’s Definition	Defendants’ Definition
“including the VAN with the instrument for subsequent use in attesting to the authenticity of the instrument”	The VAN evidencing that the instrument has not changed.	The VAN verifies that the information in the instrument as a whole has not changed and verifies the identity of the party who created the instrument.

This phrase appears in claim 34 of the ‘148 patent. The parties again dispute whether the VAN “evidences” or “verifies” authenticity, and whether “authenticity of the instrument” requires verifying the identity of the payor as well as confirming that the instrument has not changed. As discussed above, verifies is the appropriate verb.

Plaintiff argues that this claim requires only that the instrument has not changed and that it does not need to verify the identity of the party. Plaintiff relies upon claim differentiation to explain that the originating party is not required to be authenticated in all claims. Defendants argue that an instrument is authentic if the information has not changed *and* the payor authorized the payment. Defendants further argue that the “instrument as a whole” must be authentic because, “[a]n instrument cannot be authentic . . . if any aspect of the instrument has changed.” Def. Brief at 19.

The Court is of the opinion that an instrument is authentic if it has not been forged. As discussed above, there are two types of forgery: creating an unauthorized check and altering an otherwise authorized check. If the instrument is created fraudulently, even if there are no changes to it, it would not be an authentic instrument. The claim requires authenticating the instrument, not merely the transfer information, as in Claim 28. Therefore, authentication should include verifying on some level that it is an authorized instrument. Plaintiff need not be

concerned that using the word “verifies” would impose greater authenticity restrictions on the claim. The claim recites “for subsequent use in attesting,” which only requires that it be helpful to attesting to authenticity. Therefore, the Court construes the phrase to mean “including the VAN with the instrument for subsequent use in verifying that the information in the instrument has not changed and verifying that the instrument originated from the first party.”

F. “if the at least a portion of the received funds transfer information and the VAN are determined to be authentic”

Term	Plaintiff’s Definition	Defendants’ Definition
“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 <i>if the at least a portion of the received funds transfer information and the VAN are determined to be authentic.</i> ”	If the at least a portion of the received funds transfer information and the VAN are verified or determined to be unchanged.	(1) A verification that the received funds transfer information has not changed or is unaltered; and (2) verifying the identity of the first party.

This limitation appears in claim 41. Continuing with the authentication disputes, the parties dispute whether this limitation requires verifying the identity of the first party. Plaintiff argues that requiring verification of a party’s identity would import a limitation from the specification. Defendants argue that the language “and the VAN” means nothing in this claim if it does not authenticate the party. The Court has construed VAN such that it is “used in verifying the identity of a party or the integrity of information or both.” The claim already recites authenticating the funds transfer information that is included within the VAN. If, in this claim, the first party is not required to be authenticated, this claim would disclose authenticating the funds transfer information twice. Defendants argue that authenticating the VAN means that the identity of the first party is authenticated.

Plaintiff’s argument is convincing. The Court agrees that this claim does not require *party*

authentication. Verifying that the VAN is unchanged, however, as Plaintiff proposes, does little if the VAN was created fraudulently. By requiring the VAN to be authentic, this limitation requires the VAN to represent what it purports to represent. The Court construes this limitation to mean, “if the at least a portion of the received funds transfer information is unchanged and the VAN is not fraudulent.”

G. “instrument” and “payment instrument”

Term	Plaintiff’s Definition	Defendants’ Definition
“an originator party creating an instrument for transferring funds to a recipient party, the instrument information comprising (i) a variable authentication number (VAN), and (ii) one or more pieces of payment information including an amount, information for identifying the recipient party or the originator party, a date, and a check control or serial number” ‘148, Claim 35.	Instrument: document (including paper or electronic) that is used to transfer funds to a recipient party Payment instrument: a document (including paper or electronic) that is used to transfer funds to a recipient party in connection with a payment.	A document, that is an instrument of commerce, used to transfer funds to a recipient party

This term appears in claims 34 and 35 of the ‘148 patent. The parties’ essential dispute is whether the instrument can be mere instructions to pay the recipient party or whether the instrument must be commercial paper. Plaintiff argues that the specification is not limited to checks, but can include a set of instructions. Defendants argue that Plaintiff’s proposal is overbroad. Defendants believe that the scope of the invention is limited to negotiable instruments.

The specification’s inclusion of a cashless system indicates electronic instructions are within the scope of the invention. The Court adopts Plaintiff’s construction.

H. “credential”

Term	Plaintiff’s Definition	Defendants’ Definition
“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.”	A non-secret document or information obtained from a trusted source that is transferred or presented for purposes of determining the identity of a party.	A document or information obtained from a trusted source that is transferred or presented to establish the identity of a party.

This term appears in claims 7, 47, and 53 of the ‘302 patent. The parties primarily dispute whether a credential must conclusively establish the identity of a party and whether it must be non-secret. Defendants offer the Delaware court’s construction of this term.

Plaintiff argues that a credential need not conclusively establish the identity of a party. A credential is only *used* to establish a party’s identity. Pl. Brief at 26. “[A] credential is presented as evidence or proof of identity, and the receiving party or system uses the credential for that purpose.” *Id.* Plaintiff also argues that the credential must be non-secret because it must be “publicly presented for purposes of identifying a party.” A credential, according to Plaintiff, cannot be a password.

In addition to making collateral estoppel arguments, Defendants argue that a credential is not merely *used* to authenticate a party but does authenticate a party. Def. Brief at 31. Defendants point to the specification, which states, “As part of the credential authentication process, the identity of the user is authenticated.” ‘302 patent, 12:27–40. Defendants also argue

that Plaintiff's proposal would make a credential overbroad and would read on a business card. Def. Brief at 32. If the credential were only required to be presented for purposes of determining the identity of a party, according to Defendant a business card would serve as a credential.

Both parties agree that part of the definition of credential includes a requirement that it come from a "trusted source." A mere business card, without more, would not serve as a credential under either proposal. Also, as used in the patent, a credential is intended to be a document or information presented to another for review. As such, it would make sense that the credential cannot be secret. Nonetheless, in the '302 patent, Claim 7, the inventor specifies that the credential has non-secret information. If the Court construes credential to be a non-secret document, this limitation would be meaningless. The Court is therefore of the opinion that "non-secret" should not be part of the definition of credential.

The Court now turns to the issue of whether a credential "establishes" identity. Although a driver's license or a passport is often used to establish identity, social security cards and birth certificates cannot by themselves establish the identity of the bearer. Yet the patent refers to a social security card as a credential. See '302 patent, 8:54–58. This is one of those instances in which the interests of comity yield to this Court's view of its independent obligation to give the correct meaning to claim terms. The Court construes the term to mean, "a document or information obtained from a trusted source that is transferred or presented for purposes of determining the identity of a party."

I. “information for identifying the first/second account of the first/second party”

Term	Plaintiff’s Definition	Defendants’ Definition
“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”	Plain meaning; alternatively, information that is used to identify an account of the first/second party	Information sufficient to uniquely identify a specific account of the first/second party.

These phrases appear in claim 41 of the ‘302 patent. The parties dispute whether the information must “uniquely” identify a specific account. Claim 41 is reproduced below, with the relevant portions emphasized:

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 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 the 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.

Plaintiff argues that the inventor chose to claim the invention broadly such that account numbers or other unique identifiers are not required. Plaintiff also argues that Defendants’ construction excludes the preferred embodiment. In the preferred embodiment, the recipient’s bank identifies the recipient’s bank account information using the recipient’s TIN, which does

not necessarily uniquely identify a specific account. See ‘302 patent, 6:22–30.

Defendants argue that in order to transfer funds from one account to another, as performed in the fourth limitation, information is required to sufficiently identify the originating and target accounts. Relying on claim differentiation, Defendants argue that the inventor chose to specify account identification as opposed to party identification. Where a party has multiple accounts at a single institution, absent specific information, this claim would fail because the transfer would fail.

As Plaintiff points out in his reply, the inventor does not need to “delineate all aspects of a functional, working system.” Pl. Reply at 12 (citing *Rodime PLC v. Seagate Tech., Inc.*, 174 F.3d 1294, 1303 (Fed. Cir. 1999)). The text of this claim does not require specific account identification. Moreover, the information required need only be “*for* identifying,” not “*that* identifies.” The Court construes the term to mean, “information that is used to identify an account of the first/second party.”

J. “previously issued”

Term	Plaintiff’s Definition	Defendants’ Definition
“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” ‘302, Claim 7. “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” ‘302, Claim 47.	“issued before the execution of the steps recited in the claim”	Claim 7: wherein a credential having non-secret information stored therein is previously issued to at least one entity by a trusted entity” is a required step of the claim which occurs prior to “coding the information using second information.” Claim 41: “at least one party being previously issued a credential by a trusted party” is a required step of the claim that occurs before the other steps recited in the claim. Claim 53: the credential referenced in the claim must already be issued before the execution of the steps of the

		claim.
--	--	--------

The phrase “previously issued” appears in claims 7, 47, and 53 of the ‘302 patent. The parties dispute whether “previously issued,” with respect to credentials, denotes a separate step. The parties do not dispute that “previously issued” is not a separate step in Claim 53. The Delaware court construed a related term, “wherein a credential is previously issued,” to mean, “the credential referenced in the claim must already be issued before the execution of the steps of the claim.” Claims 7 and 47 are reproduced below:

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.

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.

Plaintiff argues that, as used in claim 7, “previously issued” is a condition and not a step. In claim 7, the steps are denoted by present participles, according to Plaintiff, whereas “previously issued” is in past tense. In Claim 47, the steps are offset by semicolons and “previously issued” is not offset by a semicolon. Moreover, Plaintiff argues that Stambler’s claims follow the MPEP convention of indenting each step of the claim. *See* MPEP § 608.01 (j) (7th Ed. 1997)(“Where a claim sets forth a plurality of elements or steps, each element or step of the claim should be separated by a line indentation.”).

Defendants argue that, unlike in the Delaware court's construction, "previously issued" in Claims 7 and 47 appear in the body of the claim and are separate steps to be performed in the method. Defendants urge that the inventor could have drafted the claims more clearly if he did not intend "previously issued" to be a separate step.

In claim 7, there are two steps, "coding the first information and then coding the second information." The remainder of the claim merely describes in detail what is being coded. Claim 47, likewise, adds context to the method of claim 41. Claim 47 specifies additional characteristics of the elements of claim 41 and does not add any additional steps to claim 41. The Court adopts Plaintiff's construction.

K. "the adequacy of the funds in the first party's account being verified after the instrument is issued"

Term	Plaintiff's Definition	Defendants' Definition
"a first party creating an instrument for transferring funds to a second party, <i>the adequacy of the funds in the first party's account being verified after the instrument is issued;</i> "	The instrument being created before verifying whether an account of the first party has adequate funds or credit to cover or pay the instrument	after the instrument is released, determining whether or not the first party has sufficient funds in his/her account to pay the amount listed on the instrument

This phrase appears in claim 34 of the '148 patent. The parties dispute whether this phrase is a separate step of claim 34. Claim 34 is reproduced below:

34. A funds transfer method comprising:

a first party creating an instrument for transferring funds to a second party, ***the adequacy of the funds in the first party's account being verified after the instrument is issued;***

using a computer to create a variable authentication number (VAN), the VAN being created using at least a secret key of the first party; and

including the VAN with the instrument for subsequent use in attesting to the authenticity of the instrument.

Plaintiff argues that the disputed phrase merely limits the "creating" step of claim 34.

Plaintiff again explains that the steps of claim 34 are all recited in present participles and offset by semicolons.

Defendants argue that the phrase is a separate step. First, Defendants say that “[t]here is nothing to indicate that the disputed phrase modifies the ‘creating an instrument’ step.” Def. Brief at 27. Second, Defendants argue that the phrase “after the instrument is issued” indicates that verifying the adequacy of the funds is a separate step that occurs, of course, after the instrument is created.

The limitation does not tell a person of ordinary skill in the art to verify the adequacy of the funds. Rather, it tells the person skilled in the art that an instrument is created without knowing whether there are adequate funds in the account. Thus, the phrase limits the step of creating the instrument by imposing a time sequence restriction. Furthermore, Defendants’ argument that nothing indicates that the disputed phrase limits the creating step is incorrect. The words “after the instrument is issued” refers back to the “creating step” and the choice of the gerund “being” as opposed to the verb “is” suggests that the verification of the adequacy of funds is not a separate method step. The Court adopts Plaintiff’s construction.

L. “one or more pieces of payment information including an amount, information for identifying the recipient party or the originator party, a date, and a check control or serial number”

Term	Plaintiff’s Definition	Defendants’ Definition
“an originator party creating an instrument for transferring funds to a recipient party, the instrument information comprising (i) a variable authentication number (VAN), and (ii) <i>one or more pieces of payment information including an amount, information for identifying the recipient party or the originator party, a date, and a check control or serial</i>	One or more pieces of the following payment information: an amount, information for identifying the recipient party or the originator party, a date, and a check control or serial number. If the Court determines that “payment information” should be construed, Stambler proposes “information relevant to a payment.”	Data representing one or more of the following, which is included on an instrument: an amount, information for identifying the recipient party or the originator party, a date, a check control number or a serial number.

<i>number;</i>		
----------------	--	--

This disputed phrase appears in claim 35 of the ‘148 patent. The parties dispute whether the payment information is included on an instrument. The parties appear to agree that payment information is a category of information with the enumerated items as members of that category.

Plaintiff preliminarily argues that “payment information” requires no construction. Thereafter, Plaintiff argues that requiring the payment information to be included on an instrument imports unnecessary limitations and is, in any event, ambiguous. According to Plaintiff, it is not clear whether “an instrument” refers to the instrument recited in the claim or to any generic instrument. Defendants’ sole argument is that the instrument must include the payment information in order to successfully transfer funds.

Defendants’ proposal lacks meaningful support. The Court construes this limitation as proposed by Plaintiff.

M. “associated with”

Term	Plaintiff’s Definition	Defendants’ Definition
“a payer obtaining a document containing document information, the document information being associated with a debt incurred by the payer or for goods or for services to be paid for or purchased by the payer”	Identified with or having a connection to.	Plain meaning; alternatively, identified with or pertaining to.

This term appears in claim 28 of the ‘148 patent and claims 7 and 41 of the ‘302 patent. The parties dispute whether “associated with” can “have some connection to” or can “pertain to.”

Plaintiff argues that its proposal is consistent with “customary definitions” as found in dictionaries. According to Plaintiff, “pertain” is defined as “to belong as an adjunct, part, holding, or quality,” which is narrower than “associated with.” Plaintiff explains that “associated

with” is used to describe the relationships between a party and account or credential information, and between a VAN and a transaction. A VAN has a connection to a transaction, according to Plaintiff, and does not belong as an adjunct. Defendants argue that “having some connection to” is too broad.

Although some portions of the specification support Defendants’ argument, the claim language is broadly written to embrace document information “associated with” the debt. There may be document information that “has a connection to” a debt but does not necessarily “pertain to” a debt. For example, the debtor’s account number pertains to the debtor, but has only a connection to the debt. Plaintiff’s proposal is more consistent with the language of the claim, and the Court adopts it.

V. Conclusion

The court adopts the constructions set forth in this opinion for the disputed terms of the ‘302 and ‘148 patents. The parties are ordered that they may not refer, directly or indirectly, to each other’s claim construction positions in the presence of the jury. Likewise, the parties are ordered to refrain from mentioning any portion of this opinion, other than the actual definitions adopted by the court, in the presence of the jury. Any reference to claim construction proceedings is limited to informing the jury of the definitions adopted by the court.

SIGNED this 9th day of April, 2010.

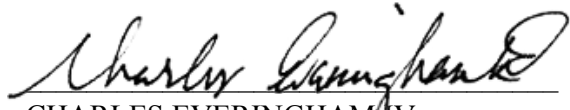

CHARLES EVERINGHAM IV
UNITED STATES MAGISTRATE JUDGE

Exhibit “D”

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

LEON STAMBLER

vs.

MERRILL LYNCH & CO., INC., et al.

§
§
§
§
§
§
§

CASE NO. 2:08-CV-462-DF-CE

MEMORANDUM OPINION AND ORDER

The Court held a Markman hearing on June 29, 2010.¹ After considering the submissions and the arguments of counsel, the Court issues the following order regarding claim construction:

I. Background of the Technology

Plaintiff Leon Stambler asserts United States Patent Nos. 5,793,302 (“the ‘302 patent”) and 5,974,148 (“the ‘148 patent”) (collectively, “Stambler patents”) against remaining Defendants². The Stambler patents have a common specification and claim priority to November 17, 1992. Plaintiff asserts claims 7, 41, 44, 46, 47, 48, and 55 of the ‘302 patent and claims 28, 34, and 35 of the ‘148 patent. The Stambler patents are entitled “Method for Securing Information Relevant to a Transaction” and teach improvements to conducting financial transactions thereby minimizing fraud on the parties. The patents address two types of fraud that can occur in multi-party transactions, especially electronic transactions. First, the patents disclose a system for authenticating that

¹ The Court also held a Markman hearing in a related case, *Stambler v. JP Morgan*, 2:08-cv-204, on March 25, 2010. The claim construction order for that action, Dkt. No. 393, was issued on April 9, 2010. That order is incorporated by reference and referred to as *JP Morgan*.

² Remaining defendants include Jack Henry & Associates, LegacyTexas Bank and associated entities, HSBC USA Inc. and associated entities, and First National Bank and associated entities. The remaining defendants will be referred to herein as “Defendants.”

information relating to the financial transaction has not been fraudulently authored, such as the amount on a check. Second, the patents teach authenticating the parties to a transaction. For example, the transaction system of the patents would detect when a person cashing a check is not the intended recipient.

The invention uses what is called a “variable authentication number (VAN)” to authenticate the transaction information as well as the parties. A VAN (a disputed term), as disclosed in the embodiment, contains an encoded key that contains information about at least one of the parties and at least some of the transaction information. This encoded key is called a joint key. The joint key might, for example, contain the intended recipient’s tax identification number, the check amount, and the payor’s identifying information. When an endorsed check is presented at the recipient’s bank, the recipient’s bank first verifies whether the party presenting the check is in fact the intended recipient. After verifying that the recipient is authentic, the recipient’s bank requests that the payor’s bank transfer the funds in accordance with the check’s instructions. The payor’s bank will then verify whether the document has been altered based upon the document information encoded into the joint key. Additionally, the payor’s bank will be able to verify whether the payor did in fact originate this check based upon the payor information encoded into the joint key. According to the embodiment, only selected parties would be able to decode the VAN to access the joint key, thereby making it nearly impossible for the VAN to be fraudulently created or modified.

Plaintiff previously pursued claims under the asserted patents before the District of Delaware in 2001. *See Stambler v. RSA Sec. Inc.*, No. 01-65-SLR (D. Del.). The Delaware court issued its claim construction order in 2003. A number of the terms that the Delaware court construed are at issue in this litigation: VAN; secret key of the first party/payor/originator; instrument; previously

issued; and credential. Defendants argue that Plaintiff should be estopped from pursuing constructions that are different than those it pursued in the Delaware court when the Delaware court adopted Plaintiff's proposal. Plaintiff argues that the constructions in the Delaware court are based upon dictionary definitions almost exclusively and that *Phillips* is intervening law regarding claim construction.

II. General Principles Governing Claim Construction

"A claim in a patent provides the metes and bounds of the right which the patent confers on the patentee to exclude others from making, using or selling the protected invention." *Burke, Inc. v. Bruno Indep. Living Aids, Inc.*, 183 F.3d 1334, 1340 (Fed. Cir. 1999). Claim construction is an issue of law for the court to decide. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 970-71 (Fed. Cir. 1995) (en banc), *aff'd*, 517 U.S. 370 (1996).

To ascertain the meaning of claims, the court looks to three primary sources: the claims, the specification, and the prosecution history. *Markman*, 52 F.3d at 979. Under the patent law, the specification must contain a written description of the invention that enables one of ordinary skill in the art to make and use the invention. A patent's claims must be read in view of the specification, of which they are a part. *Id.* For claim construction purposes, the description may act as a sort of dictionary, which explains the invention and may define terms used in the claims. *Id.* "One purpose for examining the specification is to determine if the patentee has limited the scope of the claims." *Watts v. XL Sys., Inc.*, 232 F.3d 877, 882 (Fed. Cir. 2000).

Nonetheless, it is the function of the claims, not the specification, to set forth the limits of the patentee's claims. Otherwise, there would be no need for claims. *SRI Int'l v. Matsushita Elec. Corp.*, 775 F.2d 1107, 1121 (Fed. Cir. 1985) (en banc). The patentee is free to be his own

lexicographer, but any special definition given to a word must be clearly set forth in the specification. *Intellicall, Inc. v. Phonometrics*, 952 F.2d 1384, 1388 (Fed. Cir. 1992). And, although the specification may indicate that certain embodiments are preferred, particular embodiments appearing in the specification will not be read into the claims when the claim language is broader than the embodiments. *Electro Med. Sys., S.A. v. Cooper Life Sciences, Inc.*, 34 F.3d 1048, 1054 (Fed. Cir. 1994).

This court's claim construction decision must be informed by the Federal Circuit's decision in *Phillips v. AWH Corporation*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). In *Phillips*, the court set forth several guideposts that courts should follow when construing claims. In particular, the court reiterated that "the *claims* of a patent define the invention to which the patentee is entitled the right to exclude." 415 F.3d at 1312 (emphasis added) (*quoting Innova/Pure Water, Inc. v. Safari Water Filtration Systems, Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). To that end, the words used in a claim are generally given their ordinary and customary meaning. *Id.* The ordinary and customary meaning of a claim term "is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application." *Id.* at 1313. This principle of patent law flows naturally from the recognition that inventors are usually persons who are skilled in the field of the invention. The patent is addressed to and intended to be read by others skilled in the particular art. *Id.*

The primacy of claim terms notwithstanding, *Phillips* made clear that "the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification." *Id.* Although the claims themselves may provide guidance as to the meaning of particular terms,

those terms are part of “a fully integrated written instrument.” *Id.* at 1315 (*quoting Markman*, 52 F.3d at 978). Thus, the *Phillips* court emphasized the specification as being the primary basis for construing the claims. *Id.* at 1314-17. As the Supreme Court stated long ago, “in case of doubt or ambiguity it is proper in all cases to refer back to the descriptive portions of the specification to aid in solving the doubt or in ascertaining the true intent and meaning of the language employed in the claims.” *Bates v. Coe*, 98 U.S. 31, 38 (1878). In addressing the role of the specification, the *Phillips* court quoted with approval its earlier observations from *Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1250 (Fed. Cir. 1998):

Ultimately, the interpretation to be given a term can only be determined and confirmed with a full understanding of what the inventors actually invented and intended to envelop with the claim. The construction that stays true to the claim language and most naturally aligns with the patent’s description of the invention will be, in the end, the correct construction.

Consequently, *Phillips* emphasized the important role the specification plays in the claim construction process.

The prosecution history also continues to play an important role in claim interpretation. The prosecution history helps to demonstrate how the inventor and the PTO understood the patent. *Phillips*, 415 F.3d at 1317. Because the file history, however, “represents an ongoing negotiation between the PTO and the applicant,” it may lack the clarity of the specification and thus be less useful in claim construction proceedings. *Id.* Nevertheless, the prosecution history is intrinsic evidence. That evidence is relevant to the determination of how the inventor understood the invention and whether the inventor limited the invention during prosecution by narrowing the scope of the claims.

Phillips rejected any claim construction approach that sacrificed the intrinsic record in favor of extrinsic evidence, such as dictionary definitions or expert testimony. The *en banc* court condemned the suggestion made by *Texas Digital Systems, Inc. v. Telegenix, Inc.*, 308 F.3d 1193 (Fed. Cir. 2002), that a court should discern the ordinary meaning of the claim terms (through dictionaries or otherwise) before resorting to the specification for certain limited purposes. *Id.* at 1319-24. The approach suggested by *Texas Digital*—the assignment of a limited role to the specification—was rejected as inconsistent with decisions holding the specification to be the best guide to the meaning of a disputed term. *Id.* at 1320-21. According to *Phillips*, reliance on dictionary definitions at the expense of the specification had the effect of “focus[ing] the inquiry on the abstract meaning of words rather than on the meaning of the claim terms within the context of the patent.” *Id.* at 1321. *Phillips* emphasized that the patent system is based on the proposition that the claims cover only the invented subject matter. *Id.* What is described in the claims flows from the statutory requirement imposed on the patentee to describe and particularly claim what he or she has invented. *Id.* The definitions found in dictionaries, however, often flow from the editors’ objective of assembling all of the possible definitions for a word. *Id.* at 1321-22.

Phillips does not preclude all uses of dictionaries in claim construction proceedings. Instead, the court assigned dictionaries a role subordinate to the intrinsic record. In doing so, the court emphasized that claim construction issues are not resolved by any magic formula. The court did not impose any particular sequence of steps for a court to follow when it considers disputed claim language. *Id.* at 1323-25. Rather, *Phillips* held that a court must attach the appropriate weight to the intrinsic sources offered in support of a proposed claim construction, bearing in mind the general rule that the claims measure the scope of the patent grant.

III. Agreed Terms

The parties have agreed to definitions of the following terms:

Term	Claim Number	Agreed Construction
“associated with”	‘302 claims 7, 41, 44, 47, 51 ‘148 claim 28	Identified with or having a connection to
“if the at least a portion of the received funds transfer information and the VAN are determined to be authentic”	‘302 claims 41, 51 ‘148 claim 28	if the at least a portion of the received funds transfer information is unchanged and the VAN is not fraudulent
“payment”	‘302 claim 44 ‘148 claim 28	Compensation in exchange for goods or services or the discharge of a debt
“payment instrument”	‘148 claim 28	A document (including paper or electronic) that is used to transfer funds to a recipient party in connection with a payment
“instrument for transferring funds”	‘148 claims 34, 35	A document (including paper or electronic) that is used to transfer funds to a recipient party
“including the VAN with the instrument for subsequent use in attesting to the authenticity of the instrument”	‘148 claim 34	Including the VAN with the instrument for subsequent use in verifying that the information in the instrument has not changed and verifying that the instrument originated from the first party
“one or more pieces of payment information including an amount, information for identifying the recipient party or the originator party, a date, and a check control or serial number”	‘148 claim 35	One or more pieces of the following payment information: an amount, information for identifying the recipient party or the originator party, a date, and a check control or serial number
“creating an error detection code (EDC1) by coding”	‘148 claim 35	Creating an error detection code (EDC1) by applying an algorithm to

		information in such a manner as to permit detection of changes but without complete recovery of the original information
“the originator’s VAN being usable to determine the authenticity of the one or more pieces of payment information”	‘148 claim 35	The originator’s VAN being usable to verify that the one or more pieces of payment information have not changed and to verify that the one or more pieces of payment information originated from the originator party

Joint Claim Construction Chart, Dkt. No. 393.

IV. Disputed Terms

A. “a third party for determining”

Plaintiff’s Proposed Construction	Defendants’ Proposed Construction	The Court’s Prior Construction
a party, other than the first or second parties, that performs the determining step of the claim	a party different from the party or parties performing the other steps of the claim, for determining	a party, other than the first or second parties, that performs the determining step of the claim

The term “a third party for determining” appears in claim 41 of the ‘302 patent. The parties primarily dispute whether the determining third party of the disputed claim term may perform any other step of the claimed methods. The court previously heard and rejected Defendants’ position in the *JP Morgan* claim construction. Plaintiff has proposed the Court’s construction from *JP Morgan*.

Defendants ask the Court to revisit its prior claim construction and argue that they present a novel justification for their construction. Defendants argue that the plain meaning of the claim requires their construction, but then cite to several embodiments where the “third party” is the financial institution that is also practicing other steps of the claimed method. Defendants pointed

to no evidence requiring the “third party” of claim 41 to be uninvolved in the remaining claim steps. Accordingly, the Court adopts its prior construction and defines “a third party for determining” to be “a party, other than the first or second parties, that performs the determining step of the claim.”

B. “variable authentication number (VAN)”

Plaintiff’s Proposed Construction	Defendants’ Proposed Construction	The Court’s Prior Construction
an encoded variable number that can be used in verifying the identity of a party or the integrity of information or both, the number generated by coding information associated with or related to a transaction, document (paper, electronic, or otherwise), or thing with either a joint key or information associated with or assigned or related to at least one party to the transaction or issuance of the document or thing	a variable number that can be used by a recipient to verify the identity of another who is a party to a transaction and the integrity of information relevant to the transaction either with a joint code produced from information associated with the party or directly with information associated with the party	an encoded variable number that can be used in verifying the identity of a party or the integrity of information or both

The disputed term “variable authentication number” appears in asserted claims 41, 44, 46, 47, 48, and 55 of the ‘302 patent and claims 28, 34, and 35 of the ‘148 patent. The Court’s prior construction makes explicit the requirements for authentication, but does not import any limitations regarding what sort of information may be utilized in synthesizing a VAN.

Plaintiff attempts to import additional limitations from the claims or the preferred embodiments that require some information from the transfer to be used to create the VAN. However, this limitation already appears elsewhere in the asserted claims and, as a result, additional construction of the term beyond the Court’s prior construction is unnecessary. Defendants’ proposed

construction similarly attempts to collapse limitations from elsewhere in the claims into the VAN. Accordingly, the Court adopts its prior construction and defines “variable authentication number” to mean “an encoded variable number that can be used in verifying the identity of a party or the integrity of information or both.”

C. “secret key of the payor/first party/originator”

Plaintiff’s Proposed Construction	Defendants’ Proposed Construction	The Court’s Prior Construction
a private key that is created by the payor/first party/originator, or an entity originating an instrument on the payor’s/first party’s/originator’s behalf, by coding information associated with or related to the payor/first party/originator, which is capable of being separately created by a party intended to authenticate the instrument	key that is generated by coding information associated with and known, prior to any coding, only by the payor/first party/originator party for use in any future transactions	a key that is known only to the payor and those intended to know it

The term “secret key of the payor/first party/originator” appears in claims 28, 34, and 35 of the ‘148 patent. The Court has previously construed the term to mean “a key that is known only to the payor and those intended to know it.” Plaintiffs argue that the only key used in the context of creating a VAN in a fund transfer embodiment is the joint key and thus the joint key must be a “secret key.” However, the joint key is never described as “secret” or “belonging to a party.” Rather, the joint key is derived from the payor/first party/originator’s PIN which is secret and known only to the payor/first party/originator and those intended to know it. Accordingly, the Court adopts its prior construction and defines “secret key of the payor/first party/originator” to mean “a key that

is known only to the payor/first party/originator and those intended to know it.”

D. “credential”

Plaintiff’s Proposed Construction	Defendants’ Proposed Construction	The Court’s Prior Construction
a non-secret document or information obtained from a trusted source that is transferred or presented for purposes of determining the identity of a party	a document or thing obtained from a trusted source that establishes the identity of a party when it is transferred or presented	a document or information obtained from a trusted source that is transferred or presented for purposes of determining the identity of a party

The disputed term “credential” appears in claims 7, 47, and 55 of the ‘302 patent. The Court has previously construed “credential” to mean “a document or information obtained from a trusted source that is transferred or presented for purposes of determining the identity of a party.” Plaintiff seeks to add the limitation “non-secret” while Defendants seek to impose a higher standard on what may serve as a credential. The Court finds that Defendants’ proposed “establishes the identity” language is too restrictive. A credential is evidence of identity, and can aid in determining identity, but need not establish identity. Plaintiff repeats his arguments from *JP Morgan* that the credentials mentioned in the specification are not secret and that the use of the terms in claim 47 and 55 without language specifying that the credential contains non-secret information necessitates their proposed “non-secret” construction. However, if credentials were always non-secret then the requirement that the credential of claim 7 contain “non-secret information” would be superfluous, and the patentee would not have included it in the claims. Further, the distinction between the credential in claim 7 and the credential in claims 47 and 55 would be swallowed by Plaintiff’s proposed construction. Beyond requiring the credential to contain non-secret information, Plaintiff’s construction requires

that the credential contain no secret information. The specification makes no such requirement clear, and reading implicit limitations of the embodiments into broadly drafted claim terms would be improper. Accordingly, the Court adopts its previous construction and defines “credential” to mean “a document or information obtained from a trusted source that is transferred or presented for purposes of determining the identity of a party.”

E. “trusted entity / party”

Plaintiff’s Proposed Construction	Defendants’ Proposed Construction	The Court’s Prior Construction
a party/entity who is trusted or whose integrity is relied upon to issue credentials	agency having officially recognized authority to issue credentials	None

The disputed term “trusted entity / party” appears in claims 7, 47, and 55 of the ‘302 patent. The proposed constructions for “trusted entity/party” define the term based on the entity/party’s authority in issuing credentials, which is circular and adds no clarity to the claims. The trusted entities are relied upon to issue credentials because they are trusted, and they are trusted to do so because they have the authority or ability to establish or confirm a party’s identity. Accordingly, the Court construes “trusted entity / party” to mean “an entity / party that has the authority or ability to establish or confirm a party’s identity.”

F. “information for identifying the first/second account of the first/second party”

Plaintiff’s Proposed Construction	Defendants’ Proposed Construction	The Court’s Prior Construction
information that is used to identify an account of the first/second party	Information for identifying the first account of the first party: information that is used to identify the first account of the first party from which funds are to be transferred to the second account of the second party Information for identifying the second account of the second party: information that is used to identify the second account of the second party into which funds are to be transferred from the first account of the first party	information that is used to identify an account of the first/second party

This disputed term appears in claim 41 of the ‘302 patent. Plaintiff seeks the same construction adopted by the Court in *JP Morgan* while Defendants seek to import limitations from other parts of the claim and elsewhere. Defendants’ proposed construction fails to clarify the disputed term and renders meaningless other limitations of the claim. Accordingly, the Court adopts its prior construction and defines “information for identifying the first/second account of the first/second party” to mean “information that is used to identify an account of the first/second party.”

G. “originator party” / “recipient party”

Plaintiff’s Proposed Construction	Defendants’ Proposed Construction	The Court’s Prior Construction
originator party: plain meaning; alternatively, a party that creates an [instrument for transferring funds] recipient party: plain meaning; alternatively, the intended recipient of a funds transfer	originator party: party whose funds are being transferred recipient party: party who receives the funds transfer from the originator party	None

This term appears in claim 35 of the ‘148 patent. The parties primarily dispute whether the originator party must be the source of the funds or merely the source of an instrument for transferring funds. The plain language of the claim indicates that the originator party creates an instrument for transferring funds but does not require that the funds be transferred from the originator party. The specification supports this position because it indicates that the invention can be used for generating and processing employee paychecks. (3:66-67). Paychecks for the transfer of funds from employers to employees are typically generated by third parties. Additionally, Defendants’ proposed construction requires an actual transfer of funds rather than the generation of an instrument for the transfer of funds. Although the preamble of claim 35 of the ‘148 patent recites a “funds transfer method,” the steps of the method do not require an actual transfer. Reading such a limitation into the claim by redefining the parties would be improper. Also, the Court notes that the constructions advanced by both parties are circular, defining the disputed terms using their interpretations of what the remainder of the claim requires. After reviewing the arguments of the parties, the Court adopts the plain and ordinary meaning for “originator party” and “recipient party.”

H. “first party” / “second party”

Plaintiff’s Proposed Construction	Defendants’ Proposed Construction	The Court’s Prior Construction
First party: plain meaning; alternatively, claim 34 of the ‘148 patent: a party that creates an instrument; claims 41 and 55 of the ‘302 patent: a party identified with a first account Second party: plain meaning; alternatively, claim 34 of the ‘148 patent: a party that is intended to receive funds; claims 41 and 55 of the ‘302 patent: a party identified with a second account	First party: party whose funds are being transferred Second Party: party who receives the funds transferred from the first party	None

“First party” and “second party” appear in claim 34 of the ‘148 patent and claims 41 and 55 of the ‘302 patent. The parties primarily dispute whether these terms have a rigid definition across all claims or their meaning should be supplied by the context of the claims in which they appear. As with “originator party” and “recipient party” above, both Plaintiff and Defendants attempt to construe these terms in a circular fashion, with information about the role of the parties as defined in the claims imported into the term constructions. The court is unpersuaded by these arguments and finds that saddling these terms with information the jury should discern from the context of the claims is unnecessary. Further, Defendants’ proposed definition improperly imports limitations not found in the claims in question by requiring an actual transfer of funds to occur. Accordingly, the Court adopts the plain and ordinary meaning for “first party” and “second party.”

I. “the first/second account information being stored in a first/second storage means”

Plaintiff’s Proposed Construction	Defendants’ Proposed Construction	Prior Construction
This element is not subject to 35 U.S.C. § 112, ¶ 6. information [associated with] the first/second account being stored in a first/second place for storing information Alternatively, if the Court concludes this element is subject to 35 U.S.C. § 112, ¶ 6: Function: storing Structure: document, files, memory, or other computer storage, tables, personal storage media	This term is a means plus function limitation as defined by 35 U.S.C. § 112, ¶ 6: Function: storing the first/second party’s account information Structure: first/second party’s bank’s computer	Delaware: First/second storage means: a first/second place for storing information, which can include a computer file

The disputed term “the first/second account information being stored in a first/second storage means” appears in the preamble of claim 41 of the ‘302 patent. The parties primarily dispute whether this term is subject to 35 U.S.C. § 112, ¶ 6. Assuming the term is subject to § 112, ¶ 6, the parties further dispute both the function and the structure supported by the specification.

Plaintiff argues that the term “storage means” was well defined in the art and that no means plus function construction is necessary. Defendant argues that the use of the word “means” creates a presumption of means plus function and that Plaintiff has failed to rebut that presumption. The Court finds that Plaintiff has established that a means plus function construction is not necessary because the term “storage means” was well defined in the art at the time of the invention. Plaintiff

also argues, and the court agrees, that the claim is not drafted in standard § 112, ¶ 6 format (e.g. “means for [performing a function]”). Accordingly, the Court construes “first/second storage means” to mean “first/second place for storing information, which may include a computer file.”

J. “error detection code”

Plaintiff’s Proposed Construction	Defendants’ Proposed Construction	The Court’s Prior Construction
the result of applying an algorithm to information in such a manner as to permit detection of changes but without complete recovery of the original information	coded information that is compared by the recipient to detect if there are any changes from the information originally encoded into the error detection code	the result of applying an algorithm to information in such a manner as to permit detection of changes but without complete recovery of the original information [by agreement]

The disputed term “error detection code” appears in claims 46 and 55 of the ‘302 patent and claim 35 of the ‘148 patent. When used in the claims, the “error detection code” is used to generate a VAN. Neither party’s construction defines the disputed term such that it can be used to generate a VAN. Plaintiff cited to the record supporting its construction, but failed to define the disputed term in a grammatically sensible way. Defendants’ proposed construction imports limitations absent from the claim while also failing to make grammatical sense. The portion of the specification cited by Plaintiff indicates that an error correcting code must allow for detection of changes in the coded information without complete recovery of the original information. (5:39-44). Accordingly, the Court construes “error detection code” to mean “an algorithm for coding information that, when applied to original information, creates coded information wherein changes to the coded information can be detected without complete recovery of the original information.”

K. “coding”

Plaintiff’s Proposed Construction	Defendants’ Proposed Construction	The Court’s Prior Construction
Transforming information by applying a known algorithm	The meaning of “coding” should be supplied within the context of the phrase in which it is used. “Coding” when used in the context of generating a VAN means: “transforming information into a VAN by applying a known algorithm under which the resulting VAN can either be uncoded by reversing the coding operation or compared to a VAN regenerated by applying the same known algorithm to the information.” “Coding” in the context of “creating an error detection code (EDC1) by coding” is a different contextual use of coding	Transforming information by applying a known algorithm [by agreement; also adopted by Delaware court]

The disputed term “coding” appears in claims 7 and 41 of the ‘302 patent. Plaintiff argues that “coding” should be construed as defined in the specification while Defendant argues that a narrower definition is necessary because various claims of the patent refer to both “coding” and “uncoding.” However, construing “coding” in light of the patentee’s use of “uncoding” does not require the Court to import various limitations from other claims and the specification. The specification defines a coder as a device that “[utilizes] a known algorithm” to code data from one form to another. (3:37-48). The same passage defines an uncoder as a device that reverses the

process performed by the coder to recreate the original data. *Id.* Accordingly, the Court construes “coding” to mean “transforming information by applying a known algorithm” and “uncoding” as “transforming coded information back into its original state.”

L. “payor” / “payer”

Plaintiff’s Proposed Construction	Defendants’ Proposed Construction	The Court’s Prior Construction
A person or entity who pays, or who is to make a payment. The terms refer to the same party.	Payor: party paying for or purchasing goods or services Payer: indefinite	Plain meaning. The terms refer to the same party. [by agreement]

The disputed terms “payor” and “payer” appear in claim 28 of the ‘148 patent. The parties’ primary dispute is whether “payor” and “payer” refer to the same entity. Defendants additionally seek to limit the definition based the underlying purpose of any payment made by the payor. Defendants argue that the term “payer” is insolubly ambiguous and that the Court should invalidate any claims containing the term.

“Payer” and “payor” are alternate spellings of the same word, and in the context of claim 28 the two clearly refer to the same entity. Furthermore, the defendants in *JP Morgan* did not find the term to be ambiguous and did not even seek construction by the court. In order to find the term indefinite, the Court must determine that it is insolubly ambiguous or otherwise not amenable to construction. That is clearly not the case. Accordingly, the Court construes “payor” and “payer” to refer to the same entity and defines that entity to be “a person or entity who pays, or who is to make a payment.”

M. “previously issued”

Plaintiff’s Proposed Construction	Defendants’ Proposed Construction	The Court’s Prior Construction
issued before the execution of the steps recited in the claim; the “previously issued” limitation is not a separate step in the claimed methods	issued before the execution of the other steps recited in the claim; the “previously issued” limitation is a separate step	issued before the execution of the steps recited in the claim; the “previously issued” limitation is not a separate step in the claimed methods

The phrase “previously issued” appears in claims 7, 47, and 55 of the ‘302 patent. Plaintiff argues that “previously issued” describes “credential” in the asserted claims and is not a separate step that must be performed to practice the method. Defendants argue that “previously issued” requires a separate step.

As explained in the *JP Morgan* claim construction order, using “previously issued” to describe “credential” does not require the credential to be issued as part of the claimed method. Accordingly, the Court construes “previously issued” to mean “issued before the execution of the steps recited in the claim” and finds that the “previously issued” limitations are not separate steps of the claimed methods.

N. “determining whether the at least a portion of the received funds transfer information is authentic by using the VAN”

Plaintiff’s Proposed Construction	Defendants’ Proposed Construction	The Court’s Prior Construction
using the VAN to determine that the at least a portion of the funds transfer information has not changed and to determine the origin of the at least a portion of the received funds transfer information	using the VAN to determine that the received funds transfer information has not changed and that the received funds transfer information originated from the first party to the funds transfer	None

The disputed term appears in claim 41 of the ‘302 patent. The parties agree that the VAN

must be used to determine that at least a portion of the funds transfer information has not changed and to determine the origin of the funds transfer information. Defendants’ construction attempts to read out “the at least a portion of” from the disputed term, however, and this is improper. Further, Defendants’ construction attempts to require the first party to be the origin of the funds transfer, which is not required by the claims or the specification. The Court adopts Plaintiff’s proposed construction because it specifies what is required to authenticate the funds transfer information while maintaining the scope of the disputed claim term.

O. “determining whether the at least a portion of the received funds transfer information is authentic by using the VAN and the credential information”

Plaintiff’s Proposed Construction	Defendants’ Proposed Construction	The Court’s Prior Construction
using the VAN and the credential information to determine that the at least a portion of the funds transfer information has not changed and to determine the origin of the at least a portion of the received funds transfer information	using the VAN and the credential information to determine that the received funds transfer information has not changed and to determine that the received funds transfer information originated from a party to the funds transfer.	None

The disputed term appears in claim 51 of the ‘302 patent and is required for infringement of asserted dependent claim 55. As with the disputed “determining” term from claim 41, the parties agree that in this step an infringer must verify that a portion of the payment information has not changed and to determine the origin of the transfer information. As above, Defendants attempt to import additional limitations such as requiring the origin of the funds transfer information to be a party to the transaction while also reading “the at least a portion of” out of the claim. As above,

Defendants' construction is improper. The Court adopts Plaintiff's proposed construction because it specifies what is required to authenticate the funds transfer information while maintaining the scope of the disputed claim term.

V. Conclusion

The court adopts the constructions set forth in this opinion for the disputed terms of the '302 and '148 patents. The parties are ordered that they may not refer, directly or indirectly, to each other's claim construction positions in the presence of the jury. Likewise, the parties are ordered to refrain from mentioning any portion of this opinion, other than the actual definitions adopted by the court, in the presence of the jury. Any reference to claim construction proceedings is limited to informing the jury of the definitions adopted by the court.

SIGNED this 24th day of September, 2010.

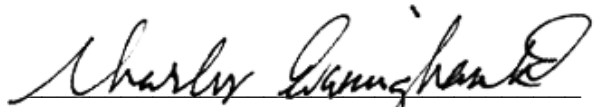

CHARLES EVERINGHAM IV
UNITED STATES MAGISTRATE JUDGE

Exhibit “E”

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

LEON STAMBLER,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Civil Action No. 01-065-SLR
	)	
RSA SECURITY, INC.,	)	
VERISIGN, INC.,	)	
OMNISKY CORPORATION,	)	
	)	
Defendants.	)	

MEMORANDUM ORDER

At Wilmington this 29th day of January, 2003, having heard oral argument and having reviewed papers submitted in connection therewith;

IT IS ORDERED that the disputed claim language in United States Patent Nos. 5,793,302; 5,936,541 and 5,974,148 as identified by the above referenced parties, shall be construed as follows, consistent with the tenets of claim construction set forth by the United States Court of Appeals for the Federal Circuit:

STAM0095415

A. "Variable Authentication Number (VAN)"

Defendants argue that the VAN must be limited to a number created by applying a symmetric key algorithm. Neither the claims, specification, nor prosecution history impose such a limitation. While nearly all of the embodiments apply symmetric key algorithms to create the VAN, the patent does contemplate creating the VAN using asymmetric algorithms. ('148 patent, col. 5, ll. 34-44) In addition, the patent provides examples of VAN's created using asymmetric algorithms, such as the RVAN. ('148 patent, col. 7, ll. 33-38) Thus, "variable authentication number (VAN)" shall be construed to mean "a variable number that can be used in verifying the identity of a party or the integrity of information or both."

B. "Secret Key of the First Party"

The court shall apply the ordinary definition of the word "secret" - "kept from the knowledge of any but the initiated or privileged."¹ The disputed phrase contemplates the initiated being the first party. Thus, the term "secret key of the first party" shall be construed to mean "a key that is known only to the first party and those intended to know it and that exists beyond the duration of a particular transaction."

¹The Random House College Dictionary, 1189 (revised ed. 1980)

C. "Instrument" or "Payment Instrument"

The claims in the '148 patent state that an instrument is "for transferring funds." ('148 patent, col. 24, ll. 43-44; col. 28, ll. 37-38) Similarly, a payment instrument is "to make a payment." ('148 patent, col. 26, ll. 12-13) Accordingly, the term "instrument" or "payment instrument" shall be construed to mean "a document used to transfer funds to a recipient party."

D. "Secret Key of the Payor"

The court shall apply the ordinary definition of the word "secret" - "kept from the knowledge of any but the initiated or privileged."² The phrase contemplates the initiated being the payor. Thus, the term "secret key of the payor" shall be construed to mean "a key that is known only to the payor and those intended to know it and that exists beyond the duration of a particular transaction."

E. "Creating an Error Detection Code (EDC1) by Coding"

The patent defines error detection coding as coding "in such a manner as to permit detection of changes." ('148 patent, col. 5, ll. 41-43) Thus, the term "creating an error detection code (EDC1) by coding" shall be construed to mean "creating an error detection code (EDC1) by applying an algorithm to information in

²The Random House College Dictionary, 1189 (revised ed. 1980)

such a manner as to permit detection of changes but without complete recovery of the original information."

F. "Secret Key of the Originator"

The court shall apply the ordinary definition of the word "secret" - "kept from the knowledge of any but the initiated or privileged."³ The phrase contemplates the initiated being the originator. Thus, the term "secret key of the originator" shall be construed to mean "a key that is known only to the originator and those intended to know it and that exists beyond the duration of a particular transaction."

G. "Coding"

Both parties request unsupportable constructions of this term. Plaintiff's construction is exceedingly broad. Defendants' construction imports limitations not found in the claims. The patent specification does not define the term "code," however, the specification does state that a "coder . . . may be any form of such device utilizing a known algorithm[.]" ('148 patent, col. 3, ll. 37-39) Thus, the term "coding" shall be construed to mean "transforming information by applying a known algorithm."

³The Random House College Dictionary, 1189 (revised ed. 1980)

H. "Wherein a Credential is Previously Issued"

The court shall apply the ordinary definition this term. Thus, the term "previously issued" shall be construed to mean "existing or occurring prior to something else in time or order."⁴ The preamble of claim 20 (from which claim 27 depends) of the '541 patent states that "a credential is previously issued to at least one of the parties." Thus, the credential must be issued prior to the steps of the claim.⁵ The term "wherein a credential is previously issued" shall be construed to mean "the credential referenced in the claim must already be issued before the execution of the steps recited in the claim."

I. "Credential"

Defendants attempt to import limitations from examples in the specification. Defendants' construction would require a physical credential and thus, the physical presence of the parties. The specification, however, recites that "until the present invention, it has not been possible to verify the

⁴The American Heritage Dictionary 982, (2d ed. 1982).

⁵Plaintiff argues that the credential cannot be issued before step one of claim 20 because step one creates the VAN which is included on the credential. Step one of the claim does not state, however, that this is the first time the VAN is created. The patent specifically discusses re-creating the VAN to compare with the VAN from the credential to authenticate the credential. ('541 patent, col. 13, ll. 24-28) This is consistent with the claim language describing a method for securing information.

identity and to secure the interests of . . . absent parties to a transaction." ('148 patent, col. 2, ll. 2-5) Importing defendants' limitation would be improper. Thus, the term "credential" shall be construed to mean "a document or information obtained from a trusted source that is transferred or presented to establish the identity of a party."

J. "Secret Key of the Credential Issuing Entity"

The court shall apply the ordinary definition of the word "secret" - "kept from the knowledge of any but the initiated or privileged."⁶ The phrase contemplates the initiated being the credential issuing entity. Thus, the term "secret key of the credential issuing entity" shall be construed to mean "a key that is known only to the credential issuing entity and those intended to know it and that exists beyond the duration of a particular transaction."

K. "Authenticating At Least One of the Parties by Using the VAN"

These terms shall be construed with their ordinary meaning; no further construction is necessary.

⁶The Random House College Dictionary, 1189 (revised ed. 1980).

L. "Information Associated with the At Least Two Parties"

These terms shall be construed with their ordinary meaning; no further construction is necessary.

M. "The First Party Has a First Personal Identification Number (PIN1)"

This term was defined by the patentee in both the specification and the prosecution history. Accordingly, the term "the first party has a first personal identification number (PIN1)" shall be construed to mean "at the time the method steps are executed, the first party has a number for identification that is secret, is selected by the first party at the time of enrollment, cannot exist in uncoded form, and cannot be recovered from other information anywhere in the system." ('148 patent, col. 2, ll. 31-36; D.I. 293 at 383)

N. "First Storage Means" and "Second Storage Means"

The claims do not support defendants' limitation that the storage means may only be computer files. Plaintiff's construction, however, would appear to eliminate the first/second limitation. The court finds that the term "first storage means" and "second storage means" shall be construed to mean "a first place for storing information, which can include a computer file," and "a second place for storing information, which can be a computer file."

O. "Being Accessible Only to a Party With Knowledge of the First PIN1"

These terms shall be construed with their ordinary meaning; no further construction is necessary.

P. "Information Associated with the First Party"

These terms shall be construed with their ordinary meaning; no further construction is necessary.

Q. "Information Associated with the Second Party"

These terms shall be construed with their ordinary meaning; no further construction is necessary.

R. "Storing in Escrow and in Trust"

"In Escrow" is defined as "in the keeping of a third person for delivery to a given party upon the fulfillment of some condition."⁷ The definition is inherently temporary. Thus, the term "storing in escrow and in trust" shall be further construed to mean "temporarily storing information securely."

S. "Subsequently Granting the First Party Access to the First Storage Means by Using the PIN1 or the Credential"

Claim 12 of the '302 patent recites steps for "a method of enrollment and issuing a credential to a first party by a second party, and subsequently granting access to a first storage

⁷The Random House College Dictionary, 450 (revised ed. 1980).

means[.]” (‘302 patent, col. 26, ll. 10-12) The final claim element recites “subsequently granting the first party access to the first storage means by using the PIN1 or the credential.” (‘302 patent, col. 26, ll. 10-29) Defendants argue that the grant of access must occur subsequent to the issuance of the credential. The court agrees. If the first party is to obtain access to the first storage means using the credential, the credential must have been previously issued. Plaintiff does not explain how access could be granted using the credential if the credential has not yet been issued.

Thus, the term “subsequently granting the first party access to the first storage means by using the PIN1 or the credential” shall be construed to mean “the step of subsequently granting the first party access to the first storage means by using the PIN1 or the credential must occur after the previous steps of the method have been performed, including the step of issuing the credential to the first party.”

T. “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)”

Defendants’ construction adds limitations not supported by the claims. The term “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)" shall be construed to mean "verifying the identity of the first party and the integrity of at least a portion of the non-secret information if EDC2 and EDC3 correspond."

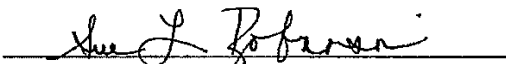
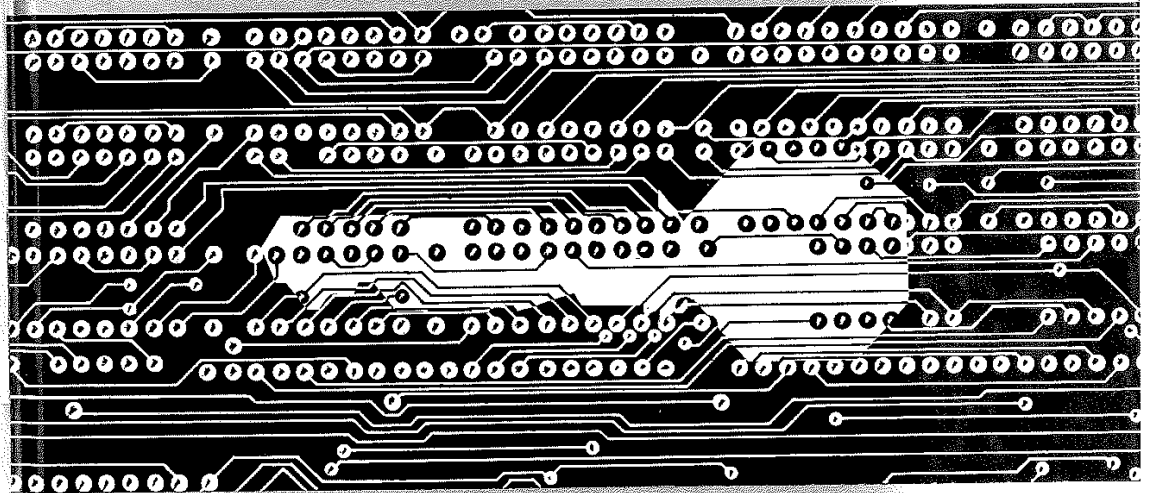

United States District Judge

Exhibit “F”

Security for Computer Networks

Second Edition

An Introduction to Data Security
in Teleprocessing and
Electronic Funds Transfer



D.W. Davies and W.L. Price

SECURITY FOR COMPUTER NETWORKS

An Introduction to Data Security
in Teleprocessing and
Electronic Funds Transfer

Second Edition

D.W. Davies
Data Security Consultant

and

W.L. Price
National Physical Laboratory, Teddington, Middlesex

JOHN WILEY & SONS

Chichester · New York · Brisbane · Toronto · Singapore

Wiley Editorial Offices

John Wiley & Sons Ltd, Baffins Lane, Chichester,
West Sussex PO19 1UD, England

John Wiley & Sons, Inc., 605 Third Avenue,
New York, NY 10158-0012, USA

Jacaranda Wiley Ltd, G.P.O. Box 859, Brisbane,
Queensland 4001, Australia

John Wiley & Sons (Canada) Ltd, 22 Worcester Road,
Rexdale, Ontario M9W 1L1, Canada

John Wiley & Sons (SEA) Pte Ltd, 37 Jalan Pemimpin #05-04,
Block B, Union Industrial Building, Singapore 2057

Copyright © 1984, 1989 by John Wiley & Sons Ltd.

All rights reserved.

No part of this book may be reproduced by any means,
or transmitted, or translated into a machine language
without the written permission of the publisher.

Library of Congress Cataloging-in-Publication Data:

Davies, Donald Watts.

Security for computer networks : an introduction to data security
in teleprocessing and electronic funds transfer / D.W. Davies and
W.L. Price. — 2nd ed.

p. cm. — (Wiley series in communication and distributed
systems)

Includes bibliographies and index.

ISBN 0 471 92137 8

1. Data transmission systems—Security measures. I. Price, W. L.

II. Title. III. Series.

TK5105.D43 1989

005.8—dc20

89-14760
CIP

British Library Cataloguing in Publication Data:

Davies, D. W. (Donald Watts, 1924—)

Security for computer networks : an introduction to
data security in teleprocessing and electronic funds
transfer. — 2nd ed — (Wiley series in communications
and distributed systems)

1. Computer systems. Security measures. Cryptograms

I. Title II. Price, W. L.

005.8'2

ISBN 0 471 92137 8

Typeset by MHL Typesetting Ltd, Coventry

Printed and bound in Great Britain by Courier International, Tiptree, Essex

GLOSSARY

Active card

Thin plastic card of credit-card size containing a store, processor or both, and capable of interaction with a terminal, for example in a point-of-sale transaction. Also called a 'smart card'.

Active line-tap (or wire-tap)

Deliberate interference with a communication system to alter the signals, data or messages it carries. This includes introducing new data or messages, repeating those that were sent earlier, delaying or deleting messages. *See also* passive line-tap.

Algorithm

A precise statement of a method of calculation. It can sometimes be expressed conveniently in a programming language.

Alphabet

The range of values which may be taken by a particular unit of communication, such as a character. When a cipher employs one or more permutations of a character code, each of these is known as an alphabet.

ANSI

American National Standards Institute.

Arbitration

Settling a dispute by referring it to a third party. This arbitrator may take part in a procedure which enables disputes to be settled, as in the production and checking of an 'arbitrated signature'.

ASCII

American Standard Code for Information Interchange. Its full title is USASCII. This code is a national version of the ISO 7-bit coded character set and is mainly compatible with CCITT alphabet No. 5.

ATM

See automatic teller machine.

Authentication

1. Ensuring that a message is genuine, has arrived exactly as it was sent and came from the stated source.

2. Verifying the identity of an individual, such as a person at a remote terminal or the sender of a message.

See also: Data origin authentication and peer-entity authentication.

Authenticator

A number which is sent with a message to enable the receiver to detect alterations made to the message since it left the sender. The number is a function of the whole message and a secret key.

Automatic teller machine (ATM)

A machine at which customers can do business with their bank. Withdrawal of cash is a main part of the service, but the ATM is typically more than a 'cash dispenser' and allows, for example, presenting cheques for payment into an account and enquiry for the account's balance.

Bijection

A mapping from one set of entities $\{x\}$ onto another $\{y\}$ having the same number of elements, such that each x maps onto a unique y and each y is the mapping of a unique x , i.e. it is a one-to-one mapping.

Birthday paradox

How many people must there be in a group to make it likely that at least two of them have the same birthdate? The answer, twenty-three, appears paradoxical. This type of problem is significant for the understanding of security in some systems (see page 279).

Block

A block of data is an array or sequence of bits that are usually stored or transmitted together. Many such arrays have specialized names such as 'character', 'field' or 'packet' which suggest their function. Block is a neutral term and often signifies a fixed-length array of bits.

Block cipher

A cipher method which acts on a fixed-length block of data to produce a result which depends only on that block.

BSI

British Standards Institution.

By-pass mode

A mode of operation of data encipherment equipment in which plaintext passes through unchanged. Federal Telecommunications Standard 1027 requires by-pass mode to be controlled with a lock.

CCITT

International Telephone and Telegraph Consultative Committee. The letters come from the title in French. With the CCIR (radio) it forms the International Telecommunications Union (UIT).

Cryptography

The technique of concealing the content of a message either by a code or a cipher.

Cryptology

The science which includes all aspects of cryptography and cryptanalysis.

Cyclic redundancy check (CRC)

A kind of check field used to guard against errors. This is used in some CCITT recommendations and ISO standards.

DAC

Data Authentication Code. A name used for an authenticator in the proposed Federal Information Processing Standard on Computer Data Integrity. The word 'code' is misused in this term.

Data link layer

The layer of Open Systems Interconnection immediately above the physical layer. At this layer of procedure, error and flow control are introduced.

Data origin authentication

Corroboration that the source of data received is as claimed.

DCE

Data circuit terminating equipment. Data communication local lines typically end at an equipment on the subscriber's premises which belongs to the network and provides the 'customer interface'. This outermost part of the network is the DCE.

DEE

Data encipherment (or encryption) equipment.

DID

Data Identifier; synonymous with 'chain identifier'. A term used in the proposed Federal Information Processing Standard on Computer Data Integrity.

Digital signature

A number depending on all the bits of a message and also on a secret key. Its correctness can be verified by using a public key (unlike an authenticator which needs a secret key for its verification).

DTE

Data terminal equipment. The equipment which is connected to a data communication network in order to communicate. The DTE may be anything that communicates, for example a computer system.

EFT

Electronic Funds Transfer. A term used for various payment methods that employ communication or electronic storage. The most usual context is in point-of-sale transactions.

Hamming distance

Given fixed-length blocks of binary data, the Hamming distance between two such blocks is the number of bits in which their values are different.

Example: 1 0 1 1 0 1 0 1 1 1
 0 1 1 1 0 0 0 1 1 0
 * * * * * Hamming distance = 4

Hash function

A well-defined function of a message or block of data which appears to generate a random number. Care is needed in selecting hash functions because they are used for several different purposes.

Index of coincidence

Two texts can be placed together and corresponding characters compared for equality (coincidence). The proportion of coincidences among the characters is a very useful statistic. Friedman defined the index of coincidence as 'coincidences minus non-coincidences divided by total number of letters compared'.

Initializing value (or variable), IV

For the encipherment or decipherment of a chain it may be necessary, or desirable, to use a value (e.g. a block of bits or set of characters) which starts off the process. This is the initializing value or IV and is known to both sender and receiver.

Integrity (of data)

The property that data have not been altered or destroyed in an unauthorized manner.

Intelligent token

A small device incorporating a processor and store which can be carried by someone for identification and to make transactions with special terminals. One form of this token is the active card or 'smart card'.

ISO

International Organization for Standardization. The international forum at which representatives from national standards bodies (such as ANSI) meet to agree standards for world-wide use.

Key block

In the context of the Data Encryption Standard it is the 64-bit block of data which contains the 56-bit key. It is also known as the 'key variable'.

Key space

The range of all the values which a cryptographic key may take. A large key space is important for security.

Key variable

See key block.

One-time tape or pad

A tape containing random numbers or bits. Only the original and one copy are made so that one station can use it to encipher and another to decipher messages under the strict rule that each portion of the tape may be used only once. Another version is the one-time pad, where the numbers are written down on two identical pads; used pages are destroyed.

One-way function

A function $y=f(x)$ which is relatively easy to compute but much more difficult to compute the inverse. That is, given x it is easy to find y , but given a value y it is (except in a few cases) difficult to find *any* solution x of $y=f(x)$. The exception allows for the fact that, with luck, the x,y pair may already be known.

Open Systems Interconnection (OSI)

A system of standards which should make useful communication possible between any systems attached to a communications network.

Padding

When a message (or a record of arbitrary length) is divided into fixed-length blocks for any purpose, the last block may not be completely filled. The information used to fill the remaining part of the last block is padding.

Passive line-tap (or wire-tap)

Unauthorized reading of signals, data or messages from a communication system, without changing the signals. *See also* active line-tap.

Peer-entity authentication

Corroboration that a peer entity in an association is the one claimed.

Permutation

Changing the order (or sequence) of a set of data elements. The elements can be bits, characters, bytes, etc. Permutation can be used as one operation in a process of encipherment. *See also* transposition cipher.

Physical layer

The lowest layer of Open Systems Interconnection, in which physical phenomena (voltage, current, light waves) are interpreted as a sequence of bits or other units (such as start/stop characters).

PIC

Personal Identification Code. A sequence of symbols (letters and numbers) used to verify the identity of the holder of a bank card. It is different from a PIN in allowing letters to be used. The word 'code' is misused here.

PIN

Personal Identification Number. A sequence of decimal digits (usually four, five or six) used to verify the identity of the holder of a bank card. A kind of 'password'.

Exhibit “G”

INFORMATION SECURITY

DICTIONARY OF CONCEPTS,
STANDARDS AND TERMS

Dennis Longley
Michael Shain
William Caelli

M
stockton
press

© Macmillan Publishers Ltd, 1992

All rights reserved. No part of this publication may be reproduced or transmitted, in any form or by any means, without permission.

Published in the United States and Canada by
STOCKTON PRESS, 1992
257 Park Avenue South, New York, N.Y. 10010, USA

ISBN 1-56159-069-X

First published in the United Kingdom by
MACMILLAN PUBLISHERS LTD, 1992
Distributed by Globe Book Services Ltd
Brunel Road, Houndmills,
Basingstoke, Hants RG21 2XS, England

ISBN 0-333-54698-9

A catalogue record for this book
is available from The British Library.

Typeset and printed in Great Britain

30 audit trail analysis

mated method for tracing the transactions affecting the contents of a record. *See* AUDIT, AUDIT TRAIL ANALYSIS, RECORD. (4) In banking, the ability to view what the system has completed in the past.

audit trail analysis. In access control, the examination of an audit trail, either manually or automatically, possibly in real time. *See* AUDIT TRAIL.

authenticate. To establish the validity of a claimed identity. (DOD). *See* AUTHENTICATION.

authentication. (1) In data security, the act of determining that a message has not been changed since leaving its point of origin. The identity of the originator is implicitly verified. (ANSI). (2) In data security, a process used, between a sender and a receiver, to ensure data integrity and to provide data origin authentication. (ISO). *See* DATA INTEGRITY, DATA ORIGIN AUTHENTICATION. (3) In data security, to establish the validity of a claimed identity (TNI). (4) In computer security, the act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information. (FIPS) *See* ACCESS. (5) In data security, a measure designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, message, station or originator. (FIPS). (6) In data security, processes that ensure everything about a teleprocessing transaction is genuine and that the message has not been altered or corrupted in transmission. The parties to the transaction must identify each other reliably, know that each message they receive comes from the other party and has not been modified, or stored earlier and replayed, by a third party. A check field can be added to the message such that the calculation of the check field depends upon the contents of the whole message, and the calculation involves a secret key. Additional information is required in the message to guard against replay of earlier messages;

time/date fields are sometimes employed for this purpose. Authentication using a secret key, shared by the sender and receiver, cannot assist in the resolution of disputes in which a receiver claims that a forged message was transmitted by the sender, or the sender disowns a messages that was actually sent, claiming that it was forged by the receiver. *See* ANSI X9.9 - 1986, CRYPTOGRAPHY, DIGITAL SIGNATURE, MAC, MESSAGE AUTHENTICATION, REPLAY, WIRETAP. (7) In computer security, the process that verifies the identity of an individual as established by an identification process. (ANSI). (8) In data security and data communications, a term that is used both to mean the prevention of undetected alteration to data and peer entity authentication. The latter meaning is commonly used in data communications where communicating parties seek mutual verification of each other's identities. The term integrity is now preferred for the process of preventing undetected alteration of data. *See* INTEGRITY, PEER ENTITY AUTHENTICATION.

authentication algorithm. In authentication, the act of determining that a message comes from a source authorized to originate messages of that type and that the message is as authorized. (ANSI). *See* MESSAGE AUTHENTICATION.

authentication element. In authentication, a contiguous group of characters which are to be protected by being processed by the authentication algorithm. *See* AUTHENTICATION ALGORITHM.

authentication equipment. In access control, equipment employed to check the authentication of a transmitted message, originator, originating system or telecommunications system, or to provide protection against fraudulent transmissions or masquerading systems.

authentication exchange. In authentication, a mechanism intended to ensure the

140 data independence

data independence. In databases, pertaining to the structure of data that removes the close coupling with user programs, so that the logical or physical structure of the database may be changed without affecting the application programmer's view of the data. *See* LOGICAL DATA INDEPENDENCE, PHYSICAL DATA INDEPENDENCE.

data input voice answerback. In data communications, a system in which a user sends input to a computer using a terminal, e.g. a touchtone telephone, and receives a voice answerback from the computer that may be either actual recorded or synthesized human voice. *See* SPEECH SYNTHESIZER.

data integrity. (1) In data security, the property that data has not been altered or destroyed in an unauthorized manner. (ISO). *Compare* DATA CONFIDENTIALITY. (2) In data security, the state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction. (FIPS). *Compare* DATA CONFIDENTIALITY.

data in voice. In data communications, the type of transmission in which digital data displaces voice circuits in a microwave channel. *Compare* DATA UNDER VOICE, DATA ABOVE VOICE.

data item. In databases, the smallest unit of data that has independent meaning, e.g. an employee's name in a personnel record. *See* FIELD, RECORD. *Synonymous with* DATA ELEMENT.

data keeper. In legislation, a person with a responsibility for ensuring that regular checks are performed on the accuracy and relevance of personal data. *See* DATA PROTECTION.

data key. In key management, a key used to encrypt and decrypt, or to au-

thenticate data. (ANSI). *Compare* KEY ENCRYPTING KEY. *See* CRYPTOGRAPHIC KEY.

data leakage. In data security, the accidental flow of privileged information otherwise presumed to be secure to a person or persons. *Synonymous with* SEEPAGE.

data level. In data security, (a) Level I. Classified data. (b) Level II. Unclassified data requiring special protection; for example Privacy Act, For Official Use Only, technical documents restricted to limited distribution. (c) Level III. All other unclassified data. (OPNAVINST).

data link. (1) In data communications, a physical means of connecting two locations, e.g. a telephone wire. (2) In data communications, the physical medium of transmission, the protocol and the associated devices and programs that together enables data to be transferred from a data source to a data sink. *See* DATA LINK LAYER, DATA SOURCE, DATA SINK.

data link control. *See* PROTOCOL.

data link control standard. In data communications, a set of conventions for sending and receiving data to and from a data network.

data link encryption. In data security, encryption of data over the physical circuit. With this form of encryption the data enters the intermediate and final nodes in plaintext. *Compare* END-TO-END ENCRYPTION, NODE ENCRYPTION. *See* OSI SECURITY, PLAINTEXT. *Synonymous with* LINK ENCRYPTION, LINK TO LINK ENCRYPTION.

data link layer. In data communications, a layer in the ISO open systems interconnection model. The function of this layer is to convert an unreliable transmission channel into a reliable one

data protection 141

for use by the layer above it, i.e. the network layer. The raw data bit stream is organized into frames each containing a checksum for detecting errors. *Compare* APPLICATION LAYER, NETWORK LAYER, PHYSICAL LAYER, PRESENTATION LAYER, SESSION LAYER, TRANSPORT LAYER. *See* BIT STREAM, CHECKSUM, FRAME, OPEN SYSTEMS INTERCONNECTION.

DataLock. In computer security, a virus that terminates and stays resident, infects COMMAND.COM, COM, EXE and OVL files, affects run time operation, corrupts program and OVL files. *See* VIRUS NAMES.

data management. In databases, pertaining to the organization and performance of functions that provide for the creation of stored data, access to it, regulation of input output devices and the enforcement of data storage conventions.

data manipulation language. In databases, a language used by a programmer to manipulate the transfer of data between the database and the application program.

data mining. In legislation, searching databases for personal data that may be used for marketing activities, etc. *See* DATA PROTECTION.

data modelling. In databases, pertaining to the identification of the fundamental groups of data and their interrelationships.

data modification. In data security, altering data in an unauthorized and undetectable manner. (ANSI).

data origination. In computing, the translation of information from its original form into machine readable form or directly into electrical signals.

data origin authentication. (1) In authentication, the corroboration that the source of data received is as claimed. (ISO). (2) In authentication, the positive identification of the source or sender of data received.

data owner. In data security, the statutory authority responsible for a particular type or category of information. Or, the individual or organization responsible for the actual data contained therein. (DODD). *See* OWNERSHIP.

dataplex. In data communications, a generic term used in the U.K. for services that involve multiplexing. *See* MULTIPLEXING.

dataplug. In communications, a proprietary name for a device that enables both telephone conversations and data to be multiplexed on a twisted pair cable connected to PABX. *See* MULTIPLEXING.

data processing. In applications, the systematic performance of operations on data to achieve a desired objective. These operations can include the handling, merging, sorting and computing of data. *See* AUTOMATIC DATA PROCESSING SYSTEM.

data protection. In legislation, procedures adopted to minimize the misuse of personal data. Concerns surrounding the protection of personal data have been an active area of debate since the 1960's.

It was soon recognized that computer systems, storing personal data, represented a potential threat to the individual. Whilst the legislation or constitution of individual states may not recognize the right of privacy per se, the ability to store and process vast amounts of data, concerning individual members of the population, has presented considerable dangers for a significant part of this century.

196 error correction code

that results from an attempt to execute invalid instructions or operate on invalid data. *See* INSTRUCTION.

error correction code. In codes, a code designed to detect an error, in a word or character, identify the incorrect bit or bits and replace them with the correct ones. The number of incorrect bits that can be corrected depends upon the number of redundant bits used in the code. *Compare* ERROR DETECTION CODE. *See* HAMMING CODE, REDUNDANCY. *Synonymous with* SELF CORRECTING CODE.

error detection code. In codes, a code designed to detect, but not correct, an error in a word or character. The number of incorrect bits that can be detected depends upon the number of redundant bits in the code. *Compare* ERROR CORRECTION CODE. *See* PARITY CHECKING.

error extension. In cryptography, an effect that arises when noisy communication channels produce errors, or an attacker introduces changes, in transmitted ciphertext, and such errors result in even lengthier errors in the subsequent received plaintext. For example, in cipher block chaining a single bit error in the ciphertext will produce a garbled 64 bit plaintext block and a single one bit error on the succeeding plaintext block. *See* CIPHER BLOCK CHAIN-ING, CIPHER FEEDBACK. *Synonymous with* ERROR PROPAGATION, GARBLE EXTENSION.

error message. In computing, a statement indicating that the computer has detected an error in the translation or execution phase of a program.

error propagation. *Synonymous with* ERROR EXTENSION, GARBLE EXTENSION.

error rate. In data communications, the frequency of occurrence of errors, defined as the ratio of the number of bits incorrectly received to the total number of bits received.

error recovery service message. *See* ANSI X9.17 - 1985.

error service message. In key management, a message sent to report an error in a cryptographic service message. *See* ANSI X9.17 - 1985, CRYPTOGRAPHIC SERVICE MESSAGE.

error source statistics. In auditing, an accumulation of information on the type and origin of errors, used to assist in the formulation of remedial measures to reduce such errors.

ERS. *See* ERROR RECOVERY SERVICE MESSAGE.

ESC. *See* ESCAPE CODE.

escape character. *See* ESCAPE CODE.

escape code. In codes, a code combination that causes a device to recognize all subsequent code combinations as having an alternate meaning to their normal representation. Escape codes are used for indicating a sequence of control messages in ASCII. *See* ASCII. *Synonymous with* FLAG CODE.

escorts. In physical security, duly designated personnel who have appropriate clearances and access authorizations for the material contained in the system and are sufficiently knowledgeable to understand the security implications of and to control the activities and access of the individual being escorted. (OPNAVINST).

escrow agent. In software protection, an honest broker who is used to resolve disagreements between a software supplier and a licensee. A supplier deposits the source code with the agent for safekeeping, and a licensee will have rights to use it in the event of liquidation of the supplier or failure to give adequate support. *See* SOURCE CODE.

IPSS. See INTERNATIONAL PACKET SWITCHED SERVICE.

IR. See INFORMATION RETRIEVAL.

Iraqi Warrior. In computer security, a virus that infects COMMAND.COM and COM files, affects run-time operation, corrupts program, OVL and data files and file linkage. See VIRUS NAMES.

IRE. U.S. Institute of Radio Engineers.

irreversible encryption. (1) In cryptography, a DEA transformation of cleartext in such a way that the encrypted text cannot be decrypted back to the original cleartext by other than exhaustive procedures. (ANSI). Compare REVERSIBLE ENCRYPTION. See CLEARTEXT, EXHAUSTIVE ATTACK, DEA, PIN MANAGEMENT AND SECURITY. (2) In cryptography, a cryptographic transformation of plaintext such that there is no corresponding decryption operation. This technique can be employed, for example, to store passwords in a secure manner. The password, subsequently entered by a user, is subject to the same encryption process and the result compared with the stored encrypted password.

isarithmic control. In data communications, the control of flow in a packet switched network so as to maintain the total number of packets in transit below a certain limit. See FLOW CONTROL, PACKET SWITCHING.

ISC². See INTERNATIONAL INFORMATION SYSTEMS SECURITY CERTIFICATION CONSORTIUM.

ISDN. See INTEGRATED SERVICES DIGITAL NETWORK.

ISN. In banking, Input Sequence Number, a consecutive sequence number that allows for input message control

between the sending bank and the service. (ANSI). Compare OSN.

ISO. See INTERNATIONAL STANDARDS ORGANIZATION.

ISO-7. In codes, a 7 bit code with 128 characters that is identical with ASCII, that is the U.S. version of this code, with the exception that certain bit patterns can be optionally allocated to national characters. See ASCII, INTERNATIONAL ALPHABET NUMBER 5.

ISO 7498. In standards, an International Standards Organization standard for Open Systems Interconnection. See OPEN SYSTEMS INTERCONNECTION.

ISO 7810. In standards, an International Standards Organization standard for the physical characteristics of identification cards.

ISO 7811. In standards, an International Standards Organization standard for the recording techniques of identification cards. See MAGNETIC STRIPE CARD.

ISO 7816. In standards, an International Standards Organization standard for smart cards. See SMART CARD.

ISO 7982-1. In standards, an International Standards Organization standard, bank telecommunications - Funds transfer messages - Part 1: Vocabulary and data elements.

ISO 8372. In standards, an International Standards Organization standard, information processing- modes of operation for a 64 bit block cipher algorithm. See DATA ENCRYPTION STANDARD.

ISO - 8583. In standards, an International Standards Organization

ify the number of times
should be transmitted in
ansmission errors, and the
etwween each attempt.

In banking, the date on
ds are to be available to
for withdrawal in cash.
pare VALUE DATE. *See*

computer security, a virus
s and stays resident, in-
XE and OVL files, cor-
and OVL files. *See* VIRUS

In banking, a transfer of
orm between two parties.

le. *Synonymous with*
E.

essage. *See* TRANS-
INT MESSAGE.

r. In banking, an instruc-
cifies a funds transfer.

ice. In banking, a service
essages among subscribers
cts settlement for those
constitute funds transfer
(ANSI). *See* FUNDS TRANS-
ION.

ryptography, permutation
onent of an encryption
ch applies a transposition
input signal. *Compare* S
A ENCRYPTION STANDARD,
CIPHER.

ONAL COMPUTER.

complexity theory, a class
at can be solved in poly-
Compare NP CLASS. *See*
CE REQUIREMENTS.

PCM. *See* PULSE CODE MODULATION.

PCS. *See* PHYSICAL CONTROL SPACE.

PDC. *See* PERMANENT DATA CALL.

PDM. *See* PULSE DURATION MODULA-
TION.

PDN. *See* PUBLIC DATA NETWORK.

PDS. *See* PROTECTED DISTRIBUTION
SYSTEM.

PDU. *See* PROTOCOL DATA UNIT.

peer entity. In data communications,
an entity in a corresponding layer of the
OSI seven layer model. *See* OPEN SYS-
TEMS INTERCONNECTION.

peer entity authentication. (1) In auth-
entification, the corroboration that a peer
entity in an association is the one
claimed. (ISO). *See* PEER ENTITY. (2) In
communications security, pertaining to
the action of communicating parties
seeking to verify each others identities.
See AUTHENTICATION, MASQUERADING.

PEM. *See* PRIVACY ENHANCED MAIL.

penetration. (1) In computer security,
a successful unauthorized access to an
ADP system. (FIPS). *See* ACCESS. (2) In
data security, an attack on the security
of a computer system, undertaken to test
the effectiveness of the security and to
highlight any areas of weakness. *See*
PENETRATION TESTING, THREAT TEAM.
(3) In data security, the successful viola-
tion of a protected system (TNI).

penetration profile. In computer se-
curity, a delineation of the activities
required to effect a penetration. (FIPS).
See PENETRATION.

penetration signature. (1) In computer
security, the description of a situation or
set of conditions in which a penetration

could occur. (FIPS). (2) The description
of usual and unusual system events
which in conjunction can indicate the
occurrence of a penetration in progress.
(FIPS). *See* PENETRATION.

penetration study. In computer securi-
ty, a technique of static evaluation in
which individuals are challenged to find
unknown weaknesses in security con-
trols. *Compare* CODE REVIEW, SOURCE
CODE ANALYZER. *See* STATIC EVALU-
ATION.

penetration testing. (1) In computer
security, the portion of security testing
in which the penetrators attempt to
circumvent the security features of a
system. The penetrators may be assumed
to use all system design and implementa-
tion documentation, which may include
listings of system source code, manuals,
and circuit diagrams. The penetrators
work under no constraints other than
those that would be applied to ordinary
users. (DOD). *See* TIGER TEAM. (2) In
computer security, the employment of
special programmer/analyst teams that
attempt to penetrate a system for the
purpose of identifying any security
weaknesses. (FIPS). *See* PENETRATION,
TIGER TEAM.

Pentagon. In computer security, a
virus that infects floppy disk boot sector
and corrupts boot sector. *See* VIRUS
NAMES.

percentage supervision. In physical
security, the ratio of the change in re-
sistance or current to the normal operat-
ing resistance or current in a supervised
line required to produce an alarm signal.
See ALARM SIGNAL, SUPERVISED LINE.

percent denial. In communications, the
average percentage of attempted calls, in
the busy hour, that are blocked due to
network loading. A measure of the
grade of service in a dial access circuit
group. *See* DIAL ACCESS.

information). Specific 'U time, terminal count of directly addressable space, number of I/O units etc. (DOD). See computer security, in any function, device, or at may be allocated to (FIPS).

g. (1) In computer n ADP system, the f a resource by more b or program. (FIPS). (2) In computer net-use of resources available or network, by users g. microcomputer users twork can share a hard nter. See HARD DISK, WORK, SERVER.

computer system. A that uses its resources, output (I/O) devices, processor (arithmetic, control units, and sing capabilities, to re users to manipulate coresident programs in ultaneous manner. The ems with one or more commonly referred to multiprogramming, ultiprocessing or con- (DODD).

communications, a de- cally transmits a pre- when activated by a Compare TRAN-

message. In key man- ge providing an auth- e to a key service SI X9.17 - 1985, KEY

) The time taken by a a specified state or

produce a specified output, after receiv- ing an input. (2) In computing, the time between the generation of the last char- acter at the terminal and receipt of the first character of the reply.

response to request service message. In key management, a message used in response to an RFS, ERS or RSI. See ANSI X9.17 - 1985, ERS, RFS, RSI.

restricted area. In physical security, any area to which access is subject to special restrictions or controls for rea- sons of security or safeguarding of property or material. (AR).

result-based perturbation. In database security, a form of perturbation in which the correct statistic is computed and the result itself is perturbed, typically by some form of rounding. Compare RE- CORD BASED PERTURBATION. See INFER- ENCE, PERTURBATION, STATISTICAL DATABASE.

retailer. In banking, the card acceptor in a retail EFTPOS system. (SAA). See CARD ACCEPTOR.

retention period. In data security, the length of time for which a file is to be kept before it is overwritten. The reten- tion period and the date on which the file was written are used to calculate the earliest date on which the file expires. The date the file was written and the retention period or the expiry date will be written as part of the file label and will be used as a security precaution against the accidental destruction of a file.

retro target. In physical security, a transceiver sensor that employs a re- flector to return the beam back to the receiver section of the transceiver. See TRANSCEIVER.

reusability. In computing, the extent to which a program can be used in other

applications and is related to the pack- aging and scope of functions that the program performs.

reverse engineering. A process by which the design of a product is deter- mined by a detailed study of the product itself, e.g. the software on a ROM can be determined by a microscopic study of the ROM chip. Such techniques have implications for manufacturers protect- ing product design. See ROM.

reverse funds transfer. In banking, a debit transfer in which the credit party is the sender. (ANSI). See DEBIT PARTY.

reverse interrupt. In data communica- tions, a control character sequence sent by the receiving station, in a binary synchronous communications system, to request a premature termination of the transmission in progress. See BINARY SYNCHRONOUS COMMUNICATIONS.

reversible encryption. In cryptogra- phy, a DEA transformation of cleartext in such a way that the encrypted text can be decrypted back to the original clear- text. (ANSI). Compare IRREVERSIBLE ENCRYPTION. See DEA.

review and approval. In computer security, the process whereby information pertaining to the security and integrity of an ADP activity or net- work is collected, analyzed, and submit- ted to the appropriate DAA for accredi- tation of the activity or network. (OPNAVINST) See DAA.

RF. Radio Frequency.

RFE. See RADIO FREQUENCY EMISS- IONS.

RFI. See RADIO FREQUENCY INTER- FERENCE.

rfm. See RE-ENCIPHER FROM MASTER KEY.

Exhibit “H”

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 (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 [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

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.

⁴¹
~~224.~~ (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.

⁴²
~~125.~~ (Amended) The method of claim ~~124~~⁴¹ 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.

⁴⁵
~~127.~~ (Amended) The method of claim ~~124~~⁴¹ wherein the VAN is used to confirm, substantiate, acknowledge, authorize, reference, validate or verify the transfer of funds.

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 -

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

Exhibit “I”

The
AMERICAN
HERITAGE
dic·tion·ar·y
of
THE ENGLISH LANGUAGE



THIRD EDITION

Words are included in this Dictionary on the basis of their usage. Words that are known to have current trademark registrations are shown with an initial capital and are also identified as trademarks. No investigation has been made of common-law trademark rights in any word, because such investigation is impracticable. The inclusion of any word in this Dictionary is not, however, an expression of the Publisher's opinion as to whether or not it is subject to proprietary rights. Indeed, no definition in this Dictionary is to be regarded as affecting the validity of any trademark.

American Heritage and the eagle logo are registered trademarks of Forbes Inc. Their use is pursuant to a license agreement with Forbes Inc.

Houghton Mifflin Company gratefully acknowledges Mead Data Central, Inc., providers of the LEXIS®/NEXIS® services, for its assistance in the preparation of this edition of *The American Heritage Dictionary*.

Copyright © 1992 by Houghton Mifflin Company.
All rights reserved.

No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system without the prior written permission of Houghton Mifflin Company unless such copying is expressly permitted by federal copyright law. Address inquiries to Permissions, Houghton Mifflin Company, 2 Park Street, Boston, MA 02108.

Library of Congress Cataloging-in-Publication Data

The American heritage dictionary of the English language.
—3rd ed.

p. cm.

ISBN 0-395-44895-6

1. English language—Dictionaries.

PE1628.A623 1992

423—dc20

92-851

CIP

Manufactured in the United States of America

(from Latin *complere*, to fill out; see COMPLETE).] — **ac·com·plish·a·ble** *adj.* — **ac·com·plish·er** *n.*

ac·com·plished (ə-kŏm'plisht) *adj.* 1. Skilled; expert: *an accomplished pianist*. 2. Unquestionable; indubitable: *That smoking causes health problems is an accomplished fact*.

ac·com·plish·ment (ə-kŏm'plish-mənt) *n.* 1. The act of accomplishing or the state of being accomplished; completion. 2. Something completed successfully; an achievement. 3. Social poise and grace.

ac·cord (ə-kŏrd') *v.* — **ac·cord·ed**, **ac·cord·ing**, **ac·cords**. — *tr.* 1. To cause to conform or agree; bring into harmony. 2. To grant, especially as being due or appropriate: *accorded the President the proper deference*. See Synonyms at **grant**. 3. To bestow upon: *I accord you my blessing*. — *intr.* To be in agreement, unity, or harmony. See Synonyms at **agree**. — **ac·cord** *n.* 1. Agreement; harmony: *act in accord with university policies*. 2. A settlement or compromise of conflicting opinions. 3. A settlement of points at issue between nations. 4. Spontaneous or voluntary desire to take a certain action: *The children returned on their own accord*. [Middle English *accorden*, from Old French *acorder*, from Vulgar Latin **accordāre*: Latin *ad-*, *ad-* + Latin *cor*, heart; see **kerd-** in Appendix.]

ac·cor·dance (ə-kŏr'dəns) *n.* 1. Agreement; conformity: *in accordance with your instructions*. 2. The act of granting.

ac·cor·dant (ə-kŏr'dənt) *adj.* Being in agreement or harmony; consonant. — **ac·cor·dant·ly** *adv.*

ac·cord·ing (ə-kŏr'ding) *conj.* 1. Corresponding to the way in which; precisely as. 2. Depending on whether; if.

ac·cord·ing·ly (ə-kŏr'ding-lē) *adv.* 1. In accordance; correspondingly. 2. So; consequently.

according to *prep.* 1. As stated or indicated by; on the authority of: *according to historians*. 2. In keeping with; in agreement with: *according to instructions*. 3. As determined by: *a list arranged according to the alphabet*.

ac·cor·di·on (ə-kŏr'dē-ən) *n.* Music. A portable instrument with a small keyboard and free metal reeds that sound when air is forced past them by pleated bellows operated by the player. — **ac·cor·di·on** *adj.* Having folds or bends like the bellows of an accordion: *accordion pleats*; *accordion blinds*. [German *Akkordion*, from *Akkord*, chord, from French *accord*, harmony, from Old French *acorder*, from Medieval Latin *accordāre*, to accord. See **ACCORD**.] — **ac·cor·di·on·ist** *n.*

ac·cost (ə-kŏst', ə-kŏst') *tr.v.* — **ac·cost·ed**, **ac·cost·ing**, **ac·costs**. To approach and speak to in an aggressive, hostile, or sexually suggestive manner. [French *accoster*, from Old French, from Medieval Latin *accostāre*, to adjoin: Latin *ad-*, *ad-* + Latin *costa*, side; see **kost-** in Appendix.]

ac·cou·che·ment (ă-kŏsh-mănt') *n.* A confinement during childbirth; lying-in. [French, from *accoucher*, to assist in childbirth, from Old French: *a-*, to (from Latin *ad-*; see **AD-**) + *coucher*, to lay down; see **COUCH**.]

♦ **ac·count** (ə-kŏunt') *n.* 1. **a.** A narrative or record of events. **b.** A reason given for a particular action. 2. **Abbr. a/c, acct.** **a.** A formal banking, brokerage, or business relationship established to provide for regular services, dealings, and other financial transactions. **b.** A precise list or enumeration of financial transactions. **c.** Money deposited for checking, savings, or brokerage use. **d.** A customer having a business or credit relationship with a firm: *salespeople visiting their accounts*. 3. Worth, standing, or importance: *a landowner of some account*. 4. Profit or advantage: *turned her writing skills to good account*. — **ac·count** *tr.v.* — **ac·count·ed**, **ac·count·ing**, **ac·counts**. To consider as being; deem. See Synonyms at **consider**. See Usage Note at **as**¹. — **phrasal verb. account for**. 1. To constitute the governing or primary factor: *Bad weather accounted for the long delay*. 2. To provide an explanation or justification: *The suspect couldn't account for his time that night*. — **Idioms. call to account**. 1. To challenge or contest. 2. To hold answerable for. **on account**. **On credit. on account of**. 1. Because of; for the sake of: *"We got married on account of the baby"* (Anne Tyler). 2. Chiefly Southern U.S. Because: *"He got picked up by the cops on account of he was walking with his shopping bag and they said there was numbers in it"* (Jimmy Breslin). **on no account**. Under no circumstances. **on (one's) own account**. 1. For oneself. 2. On one's own; by oneself: *He wants to work on his own account*. **take into account**. To take into consideration; allow for. [Middle English, from Old French *acont*, from *aconter*, to reckon: *a-*, to (from Latin *ad-*; see **AD-**) + *cunter*, to count (ultimately from Latin *computāre*, to sum up; see **COMPUTE**).]

ac·count·a·ble (ə-kŏunt'ə-bal) *adj.* 1. Liable to being called to account; answerable. See Synonyms at **responsible**. 2. That can be explained: *an accountable phenomenon*. — **ac·count·a·bil·i·ty**, **ac·count·a·ble·ness** *n.* — **ac·count·a·bly** *adv.*

ac·count·ant (ə-kŏunt'tənt) *n.* **Abbr. acct.** One that keeps, audits, and inspects the financial records of individuals or business concerns and prepares financial and tax reports. — **ac·count·an·cy** (-tən-sē) *n.*

account executive *n.* A person, as in an advertising or a public relations firm, who manages clients' accounts.

ac·count·ing (ə-kŏunt'ing) *n.* The bookkeeping methods involved in making a financial record of business transactions and in the preparation of statements concerning the assets, liabilities, and operating results of a business.

ac·cou·ter or **ac·cou·tre** (ə-kŏt'ər) *tr.v.* — **ac·tered**, **ac·ter·ing**,

ac·ters or **ac·tered**, **ac·ter·ing**, **ac·ters**. To outfit and equip, as for military duty. See Synonyms at **furnish**. [French *accouter*, from Old French *accouter*, arrange, equip: *a-*, to (from Latin *ad-*; see **AD-**) + *couter*, sew; see **COUTURE**.]

ac·cou·ter·ment or **ac·cou·tre·ment** (ə-kŏt'ər-mənt, -trə-) *n.* 1. Often **accouterments** or **accoutrements**. **a.** Ancillary items of equipment or dress. **b.** Military equipment other than uniforms and weapons. 2. **accouterments** or **accoutrements**. Outward forms of recognition; trappings: *the standard accouterments of the historical novel*; *cathedral ceilings, heated swimming pools, and other accoutrements signaling great wealth*. 3. Archaic. The act of accoutering.

Ac·cra (ăk'ra, ə-kŏr'ā). The capital and largest city of Ghana, in the southeast part of the country on the Gulf of Guinea. Originally the capital of an ancient Ga kingdom, it became an important economic center after the completion in 1923 of a railroad to the mining and agricultural hinterland. Population, 859,640.

ac·cred·it (ə-kŏr'dit) *tr.v.* — **ac·cred·it·ed**, **ac·cred·it·ing**, **ac·credits**. 1. To ascribe or attribute to; credit with. 2. **a.** To supply with credentials or authority; authorize. See Synonyms at **authorize**. **b.** To appoint as an ambassador to a foreign government. 3. **a.** To attest to and approve as meeting a prescribed standard. See Synonyms at **approve**. **b.** To recognize (an institution of learning) as maintaining those standards requisite for its graduates to gain admission to other reputable institutions of higher learning or to achieve credentials for professional practice. 4. To believe. [French *accréditer*: *a-*, to (from Latin *ad-*; see **AD-**) + *crédit*, credit (from Old French; see **CREDIT**).]

ac·cred·i·ta·tion (ə-kŏr'di-tā'shan) *n.* The act of accrediting or the state of being accredited, especially the granting of approval to an institution of learning by an official review board after the school has met specific requirements.

ac·cres·cent (ə-kŏr'sənt) *adj.* Botany. Increasing in size after flowering, as the calyx of the ground cherry. [Latin *accrescens*, *accrescent*, present participle of *accrescere*, to grow. See **ACCUE**.]

ac·crete (ə-kŏr'et') *v.* — **ac·cret·ed**, **ac·cret·ing**, **ac·cret·es**. — *tr.* To make larger or greater, as by increased growth. — *intr.* 1. To grow together; fuse. 2. To grow or increase gradually, as by addition. [Back-formation from **ACCRETION**.]

ac·cre·tion (ə-kŏr'ē-shən) *n.* 1. **a.** Growth or increase in size by gradual external addition, fusion, or inclusion. **b.** Something added externally to promote such growth or increase. 2. **Biology.** The growing together or adherence of parts that are normally separate. 3. **Geology.** **a.** Slow addition to land by deposition of water-borne sediment. **b.** An increase of land along the shores of a body of water, as by alluvial deposit. 4. **Astronomy.** An increase in the mass of a celestial object by the collection of surrounding interstellar gases and objects by gravity. [Latin *accrētio*, *accrētio*, from *accrētus*, past participle of *accrescere*, to grow. See **ACCUE**.] — **ac·cre·tion·ar·y** (-shə-nēr'ē), **ac·cre·tive** *adj.*

accretion disk *n.* A disk of interstellar material surrounding a celestial object with an intense gravitational field, such as a black hole.

Ac·cring·ton (ăk'ring-tən). A borough of northwest England north of Manchester. It is the center of a textile-processing area. Population, 79,200.

ac·croi·des gum (ə-kŏr'i-dēz, ə-kŏr'i-) *n.* See **acaroid resin**. [Alteration of New Latin *acaroides*; see **ACAROID RESIN** + **GUM**¹.]

ac·cru·al (ə-kŏr'ŭ-əl) *n.* 1. The act or process of accumulating; an increase. 2. Something that accumulates or increases.

ac·cru·e (ə-kŏr'ŭ) *v.* — **ac·cru·ed**, **ac·cru·ing**, **ac·cru·es**. — *intr.* 1. To come to one as a gain, an addition, or an increment: *interest accruing in my savings account*. 2. To increase, accumulate, or come about as a result of growth: *common sense that accrues with experience*. 3. To come into existence as a claim that is legally enforceable. — *tr.* To accumulate over time: *I have accrued 15 days of sick leave*. [Middle English *accruen*, ultimately from Latin *accrescere*, to grow: *ad-*, *ad-* + *crecere*, to arise; see **ker-**² in Appendix.] — **ac·cru·e·ment** *n.*

acct. *abbr.* 1. Account. 2. Accountant.

ac·cul·tur·ate (ə-kŭl'chə-rāt') *v.* — **ac·cul·tur·at·ed**, **ac·cul·tur·at·ing**, **ac·cul·tur·ates**. — *tr.* To cause (a society, for example) to change by the process of acculturation. — *intr.* To change or be modified by acculturation.

ac·cul·tur·a·tion (ə-kŭl'chə-rā'shan) *n.* 1. The modification of the culture of a group or an individual as a result of contact with a different culture. 2. The process by which the culture of a particular society is instilled in a human being from infancy onward. — **ac·cul·tur·a·tion·al** *adj.* — **ac·cul·tur·a·tive** *adj.*

ac·cum·bent (ə-kŭm'bənt) *adj.* Lying down; reclining. [Latin *accumbens*, *accumbent*, present participle of *accumbere*, to recline at table: *ad-*, *ad-* + *cumbere*, to recline.]

ac·cu·mu·late (ə-kyŏm'yə-lāt') *v.* — **ac·cu·mu·lat·ed**, **ac·cu·mu·lat·ing**, **ac·cu·mu·lates**. — *tr.* To gather or pile up; amass. See Synonyms at **gather**. — *intr.* To mount up; increase. [Latin *accumulāre*, *accumulāt-*: *ad-*, *ad-* + *cumulāre*, to pile up (from *cumulus*, heap; see **keu-** in Appendix).] — **ac·cu·mu·la·ble** (-lə-bal) *adj.*

ac·cu·mu·la·tion (ə-kyŏm'yə-lā'shan) *n.* 1. The act of gathering or amassing, as into a heap or pile: *"Little things grew by continual accumulation"* (Samuel Johnson). 2. The process of



accordion

reillier, to prepare, possibly from Vulgar Latin *appariculāre, from Latin apparāre. See APPARATUS.]

ap·par·ent (ə-pār'ənt, ə-pār'-'-) *adj.* 1. Readily seen; visible. 2. Readily understood; clear or obvious. 3. Appearing as such but not necessarily so; seeming: *an apparent advantage.* [Middle English, from Old French aparant, present participle of aparoir, to appear. See APPEAR.] — **ap·par·ent·ly** *adv.* — **ap·par·ent·ness** *n.*

SYNONYMS: apparent, clear, clear-cut, distinct, evident, manifest, obvious, patent, plain. The central meaning shared by these adjectives is "readily seen, perceived, or understood": *Angry for no apparent reason; a clear danger; clear-cut evidence of tampering; distinct fingerprints; evident hostility; manifest pleasure; obvious errors; patent advantages; making my meaning plain.*

USAGE NOTE: Used before a noun, apparent means "seeming": *For all his apparent wealth, Pat had no money to pay the rent.* Used after a form of the verb *be*, however, apparent can mean either "seeming" (as in *His virtues are only apparent*) or "obvious" (as in *The effects of the drought are apparent to anyone who sees the parched fields*). Writers should take care that the intended meaning is clear from the context.

apparent horizon *n.* See **horizon** (sense 1).

apparent magnitude *n.* Astronomy. See **magnitude** (sense 2).

ap·pa·ri·tion (āp'ə-rish'ən) *n.* 1. A ghostly figure; a specter. 2. A sudden or unusual sight. 3. The act of appearing; appearance. [Middle English apparicioun, from Old French apparition, from Late Latin apparitiō, apparitiō-, an appearance, from Latin apparitus, past participle of apparere, to appear. See APPEAR.] — **ap·pa·ri·tion·al** *adj.*

ap·par·i·tor (ə-pār'i-tər) *n.* An official who was formerly sent to carry out the orders of a civil or ecclesiastical court. [Middle English, from Latin apparitor, from apparere, to appear. See APPEAR.]

ap·peal (ə-pēl') *n.* 1. An earnest or urgent request, entreaty, or supplication. 2. A resort or application to a higher authority, as for sanction, corroboration, or a decision: *an appeal to reason.* 3. Law. a. The transfer of a case from a lower to a higher court for a new hearing. b. A case so transferred. c. A request for a new hearing. 4. The power of attracting or of arousing interest: *a city with appeal for tourists.* — **appeal** *v.* — **pealed, -peal·ing, -peals. — *intr.* 1. To make an earnest or urgent request, as for help. 2. To have recourse, as for corroboration; resort: *I appeal to your sense of justice.* 3. Law. To make or apply for an appeal. 4. To be attractive or interesting. — *tr.* Law. To transfer or apply to transfer (a case) to a higher court for rehearing. [Middle English apel, from Old French, from apeler, to appeal, from Latin appellāre, to entreat. See **pel**-5 in Appendix.] — **ap·peal·a·bil·i·ty** *n.* — **ap·peal·a·ble** *adj.* — **ap·peal·er** *n.***

ap·pear (ə-pīr') *intr.v.* — **peared, -pear·ing, -pears.** 1. To become visible: *a plane appearing in the sky.* 2. To come into existence: *New strains of viruses appear periodically.* 3. To seem or look to be: *appeared unhappy.* 4. To seem likely: *They will be late, as it appears.* 5. To come before the public: *has appeared in two plays; appears on the nightly news.* 6. Law. To present oneself formally before a court as defendant, plaintiff, or counsel. [Middle English aperen, from Old French aparoir, aper-, from Latin apparere: *ad*, *ad* + *pāvere*, to show.]

SYNONYMS: appear, emerge, issue, loom, materialize, show. The central meaning shared by these verbs is "to come into view": *a ship appearing on the horizon; a star that emerged from behind a cloud; a diver issuing from the water; a peak that loomed through the mist; a flash of lightning that seemed to materialize from nowhere; a ruffle showing at the edge of the sleeve.* See also **Synonyms at seem**.

ap·pear·ance (ə-pīr'əns) *n.* 1. The act or an instance of coming into sight. 2. The act or an instance of coming into public view: *The author made a rare personal appearance.* 3. Outward aspect: *an untidy appearance.* 4. Something that appears; a phenomenon. 5. A superficial aspect; a semblance: *keeping up an appearance of wealth.* 6. **appearances.** Outward indications; circumstances: *a cheerful person, to all appearances.*

ap·pease (ə-pēz') *tr.v.* — **peased, -peas·ing, -peas·es.** 1. To bring peace, quiet, or calm to; soothe. 2. To satisfy or relieve: *appease thirst.* 3. To pacify or attempt to pacify (an enemy) by granting concessions, often at the expense of principle. See **Synonyms at pacify**. [Middle English appesen, from Old French apesier: *a*, to (from Latin *ad*; see **AD**-) + *pais*, peace (from Latin *pāx*; see **pag**- in Appendix).] — **ap·peas·a·ble** *adj.* — **ap·peas·a·bly** *adv.* — **ap·peas·er** *n.*

ap·pease·ment (ə-pēz'mənt) *n.* 1. a. An act of appeasing. b. The condition of being appeased. 2. The policy of granting concessions to potential enemies to maintain peace.

ap·pel (ə-pēl') *n.* Sports. A quick stamp of the foot used in fencing as a feint to produce an opening. [French, from apeler, to call, from Old French apeler, to appeal. See APPEAL.]

ap·pel·lant (ə-pēl'ənt) *Law, adj.* Of or relating to an appeal; appellate. — **appellant** *n.* One that appeals a court decision. [Middle English, from Old French apelant, from present participle of apeler, to appeal. See APPEAL.]

ap·pel·late (ə-pēl'it) *adj.* Law. Having the power to hear

appeals and to review court decisions. [Latin appellātus, past participle of appellāre, to entreat. See APPEAL.]

ap·pel·la·tion (āp'ə-lā'shən) *n.* 1. A name, title, or designation. See **Synonyms at name**. 2. The act of naming. [Middle English appellacion, from Old French appellation, from Latin appellātiō, appellātiō-, from appellātus, past participle of appellāre, to entreat. See APPEAL.]

ap·pel·la·tive (ə-pēl'ə-tiv) *adj.* 1. Of or relating to the assignment of names. 2. Grammar. Of or relating to a common noun. — **appellative** *n.* A name or descriptive epithet. [Middle English, common (noun), from Old French appellatif, from Late Latin appellativus, from Latin appellātus, past participle of appellāre, to call upon, entreat. See APPEAL.] — **ap·pel·la·tive·ly** *adv.*

ap·pel·lee (āp'ə-lē') *n.* Law. One against whom an appeal is taken. [French appellé, from Old French apele, from past participle of apeler, to appeal. See APPEAL.]

ap·pend (ə-pēnd') *tr.v.* — **pend·ed, -pend·ing, -pends.** 1. To add as a supplement or an appendix: *appended a list of errors to the report.* 2. To fix to; attach: *append a charm to the bracelet.* [Latin appendere, to hang upon: *ad*, *ad* + *pendere*, to hang; see **(s)pen-** in Appendix.]

ap·pend·age (ə-pēn'dij) *n.* 1. Something added or attached to an entity of greater importance or size; an adjunct. 2. Biology. A part or an organ, such as an arm, a leg, a tail, or a fin, that is joined to the axis or trunk of a body.

SYNONYMS: appendage, appurtenance, adjunct, accessory, attachment. These nouns denote subordinate elements that are added to another entity. An appendage supplements without being essential: "Water jets can be angled to either side, making rudders unnecessary, and the complete absence of appendages at the stern decreases hull resistance" (R.J.L. Dicker). An appurtenance belongs naturally as a subsidiary attribute, part, or member to that with which it is associated: "an internationally known first-class hotel . . . equipped with such appurtenances as computers, word processors, copiers and telex" (Oscar Millard). An adjunct is added as an auxiliary to something else but is often self-sustaining: "Intelligence analysts say they believe that of all the countries of the Middle East, none use terrorism more effectively as an adjunct to diplomacy than Syria" (Elaine Sciolino). An accessory is usually nonessential but desirable and adds to the effect of something already complete in itself: *We bought a car with such accessories as air conditioning, stereo, and a sunroof.* An attachment contributes a supplementary function to the principal thing, to which it can be physically linked: *The food processor has an attachment for making pasta.*

ap·pen·dant (ə-pēn'dənt) *adj.* 1. Affixed as an appendage. 2. Accompanying; attendant: *faith and its appendant hope.* 3. Belonging to a land grant as a subsidiary right in English law. — **ap·pen·dant** *n.*

ap·pen·dec·to·my (āp'an-dēk'tə-mē) *n., pl. -mies.* Surgical removal of the vermiform appendix. [APPEND(IX) + -ECTOMY.]

ap·pen·di·ces (ə-pēn'di-sēz') *n.* A plural of **appendix**. — **ap·pen·di·ci·tis** (ə-pēn'di-si'tis) *n.* Inflammation of the vermiform appendix. [New Latin, from Latin appendix, appendic-, appendage. See APPENDIX.]

WORD HISTORY: Even though the word *appendicitis* was in use in 1885, the year in which the *Oxford English Dictionary* published the section "Anta-Battening" that would have contained the word, the editor, James Murray, omitted this "crack-jaw medical and surgical word" on the advice of Oxford's Regius Professor of Medicine, Sir Henry Wentworth Acland. As K.M. Elisabeth Murray, the granddaughter and biographer of James Murray, points out, "The problem of what scientific words to include was a continuing one, and James Murray was always under pressure—from his advisers . . . who thought the emphasis should be on words from good literature and from those in the [Oxford University] Press who wanted to save cost and time—not to include scientific words of recent origin." In 1902 no less a person than Edward VII had his appendix removed, and his coronation was postponed because of the operation. *Appendicitis* hence came into widespread use and has remained so, thereby pointing up the lexicographer's difficult task of selecting the new words that people will look for in their dictionaries.

ap·pen·dic·u·lar (āp'an-dik'yə-lər) *adj.* Of, relating to, or consisting of an appendage or appendages, especially the limbs: *the appendicular skeleton.* [From Latin *appendicula*, diminutive of *appendix*, *appendic-*, appendix. See APPENDIX.]

ap·pen·dix (ə-pēn'diks) *n., pl. -dix·es or -di·ces* (-dī-sēz'). Abbr. **app.** 1. a. An appendage. b. A collection of supplementary material, usually at the end of a book. 2. The vermiform appendix. 3. **Anatomy.** A supplementary or accessory part of a bodily organ or structure. [Latin, from *appendere*, to hang upon. See APPEND.]

ap·per·ceive (āp'ər-sēv') *tr.v.* — **ceived, -ceiv·ing, -ceives.** Psychology. To perceive in terms of past experiences. [From **APPERCEPTION**.]

ap·per·cep·tion (āp'ər-sēp'shən) *n.* Psychology. 1. Conscious perception with full awareness. 2. The process of understanding by which newly observed qualities of an object are re-

bombardment with atomic weapons. — **at·om·i·za'tion** (-i-zā'shan) *n.*

at·om·iz·er (ăt'a-mī'zər) *n.* A device for converting a substance, especially a perfume or medicine, to a fine spray.

atom smasher *n.* See **accelerator** (sense 3).

at·o·my¹ (ăt'a-mē) *n., pl. -mies.* Archaic. 1. A tiny particle; a mote. 2. A tiny being. [From Latin *atomī*, pl. of *atomus*, atom. See **ATOM**.]

at·o·my² (ăt'a-mē) *n., pl. -mies.* Archaic. A gaunt person; a skeleton. [From an *atomy*, respelling of **ANATOMY**.]

A·ton also **A·ten** (ăt'n) *n.* **Mythology.** An Egyptian god of the sun, regarded during the reign of Akhenaton as the only god.

a·to·nal (ā-tō'nāl) *adj.* **Music.** Lacking a tonal center or key; characterized by atonality. — **a·to·nal·ly** *adv.*

a·to·nal·ism (ā-tō'nāl-iz'm) *n.* **Music.** Atonal composition or the theory of atonal composition. — **a·to·nal·ist** *adj. & n.* — **a·to·nal·is'tic** *adj.*

a·to·nal·i·ty (ā-tō'nāl'i-tē) *n., pl. -ties.* **Music.** The absence of a tonal center and of harmonies derived from a diatonic scale corresponding to such a center; lack of tonality.

a·tone (ā-tōn') *v.* **a·toned, a·ton·ing, a·tones.** — *intr.* 1. To make amends, as for a sin or fault: *These crimes must be atoned for.* 2. Archaic. To agree. — *tr.* 1. To expiate. 2. Archaic. To conciliate; appease: "So heaven, atoned, shall dying Greece restore" (Alexander Pope). 3. Obsolete. To reconcile or harmonize. [Middle English *atonen*, to be reconciled, from *at one*, in agreement: *at*, at; see **AT** + *one*, one; see **ONE**.] — **a·ton·a·ble, a·tone/a·ble** *adj.* — **a·ton·er** *n.*

a·tone·ment (ā-tōn'mənt) *n.* 1. Amends or reparation made for an injury or wrong; expiation. 2. **a. Theology.** Reconciliation or an instance of reconciliation between God and human beings. **b. Atonement.** The redemptive life and death of Jesus. **c. Atonement.** The reconciliation of God and human beings brought about by Jesus. 3. **Christian Science.** The radical obedience and purification, exemplified in the life of Jesus, by which humanity finds oneness with God. 4. Obsolete. Reconciliation; concord.

a·ton·ic (ā-tōn'ik) *adj.* 1. Not accented; an *atonic syllable*. 2. **Pathology.** Relating to, caused by, or exhibiting lack of muscle tone. — **atonic** *n.* A word, syllable, or sound that is unaccented. [From Greek *atōnos*. See **ATONY**.] — **a·to·nic/i·ty** (ăt'a-nis'ti-tē,ăt'n-is-) *n.*

at·o·ny (ăt'a-nē,ăt'n-ē) *n.* 1. Lack of normal muscle tone. 2. Lack of accent or stress. [Late Latin *atonia*, from Greek, from *atōnos*, slack: *a-*, without; see **A-** + *tonos*, stretching, tone; see **TONE**.]

a·top (ā-tōp') *adv.* To, on, or at the top. — **a·top** *prep.* On top of. — **a·top'** *adj.*

a·top·ic (ā-tōp'ik) *adj.* Of, relating to, or caused by a hereditary predisposition toward the development of certain hypersensitivity reactions, such as hay fever, asthma, or chronic urticaria, upon exposure to specific antigens: *atopic dermatitis*. [From Greek *atopia*, unusualness, from *atopos*, out of the way: *a-*, not; see **A-** + *topos*, place.] — **a·to·py** (ăt'a-pē) *n.*

-ator *suff.* One that acts in a specified manner: *radiator*. [Latin *-ātor*: *-ā-*, stem vowel of verbs in *-āre* + *-tor*, agent *n.* suff. (later reanalyzed as *-ātus*, *-ate* + *-or*, *-or*).]

-atory *suff.* 1. **a.** Of or relating to: *perspiratory*. **b.** Tending to: *amendatory*. 2. One that is connected with: *reformatory*. [From Latin *-ātorius* and *-ātorium*, both from *-ātor*, *-ator*.]

a·tox·ic (ā-tōk'sik) *adj.* Not poisonous or toxic.

ATP (ăt'tē'pē) *n.* An adenosine-derived nucleotide, $C_{10}H_{14}N_5O_{13}P_3$, that supplies large amounts of energy to cells for various biochemical processes, including muscle contraction and sugar metabolism, through its hydrolysis to ADP. [A(DENOSINE) T(RI)P(HOSPHATE).]

ATP·ase (ăt'tē-pē'ās, -āz) *n.* An enzyme that catalyzes the hydrolysis of ATP; adenosine triphosphatase.

at·ra·bil·ious (ăt'rā-bil'yəs) also **at·ra·bil·i·ar** (-bil'ē-ər) *adj.* 1. Inclined to melancholy. 2. Having a peevish disposition; surly. [From Latin *ātra bilis*, black bile (translation of Greek *melankhōlia*; see **MELANCHOLY**): *ātra*, black; see **āter-** in Appendix + *bilis*, bile.] — **at·ra·bil·ious·ness** *n.*

a·trem·ble (ā-trēm'bəl) *adj.* Being in a state of shaking or trembling, as from fear or excitement.

a·tre·sia (ā-trē'zhā, -zhē-ā) *n.* 1. The absence or closure of a normal body orifice or tubular passage such as the anus, intestine, or external ear canal. 2. The degeneration and resorption of one or more ovarian follicles before a state of maturity has been reached. [New Latin: Greek *a-*, not, without; see **A-** + *trēsis*, perforation, orifice; see **terə-** in Appendix.] — **a·tre·sic** (-zik, -sik) *adj.*

A·treus (ăt'trōōs,ăt'trē-əs) *n.* **Greek Mythology.** A king of Mycenae, brother of Thyestes and father of Agamemnon and Menelaus.

a·tri·a (ăt'trē-ā) *n.* A plural of **atrium**.

atrial na·tri·u·ret·ic factor (năt'trē-yō-rēt'ik) *n.* **Abbr. ANF** A hormonal substance produced by the right atrium of the heart that stimulates the excretion of sodium and water by the kidneys and helps regulate blood pressure. [ATRIAL + *natrīum*, sodium (from **NATRON**) + *uretīc* + **FACTOR**.]

a·tri·o·ven·tric·u·lar (ăt'trē-ō-vēn-trīk'yə-lər) *adj.* Of, relating to, or involving the atria and the ventricles of the heart.

atrioventricular node *n.* A small mass of specialized cardiac muscle fibers, located in the wall of the right atrium of the heart, that receives heartbeat impulses from the sinoatrial node and directs them to the walls of the ventricles. Also called **AV node**.

a·trip (ə-trīp') *adj.* **Nautical.** Just clear of the bottom. Used of an anchor.

a·tri·um (ăt'trē-əm) *n., pl. a·tri·a* (ăt'trē-ā) or **-ums**. 1. **Architecture.** A rectangular court, as: **a.** A usually skylighted central area, often containing plants, in some modern buildings, especially of a public or commercial nature. **b.** The open area in the center of an ancient Roman house. **c.** The forecourt of a building, such as an early Christian church, enclosed on three or four sides with porticoes. 2. **Anatomy.** A bodily cavity or chamber, especially either of the upper chambers of the heart that receives blood from the veins and forces it into a ventricle. In this sense, also called *auricle*. [Latin *atrium*. See **āter-** in Appendix.] — **a·tri·al** *adj.*

a·tro·cious (ā-trō'shas) *adj.* 1. Extremely evil or cruel; monstrous: *an atrocious crime*. See Synonyms at **outrageous**. 2. Exceptionally bad; abominable: *atrocious decor*; *atrocious behavior*. [From Latin *atrōx*, *atrōc*, frightful, cruel. See **āter-** in Appendix.] — **a·tro·cious·ly** *adv.* — **a·tro·cious·ness** *n.*

a·tro·ci·ty (ā-trōs'i-tē) *n., pl. -ties*. 1. Appalling or atrocious condition, quality, or behavior; monstrosity. 2. **a.** An appalling or atrocious action, situation, or object. **b.** An act of cruelty and violence inflicted by an enemy armed force on civilians or prisoners: *wartime atrocities*.

at·ro·phy (ăt'trā-fē) *n., pl. -phies*. 1. **Pathology.** A wasting or decrease in size of a bodily organ, tissue, or part owing to disease, injury, or lack of use: *muscular atrophy of a person affected with paralysis*. 2. A wasting away, deterioration, or diminution: *intellectual atrophy*. — **atrophy** *v.* — **-phied, -phy·ing, -phies.** — *tr.* To cause to wither or deteriorate; affect with atrophy. — *intr.* To waste away; wither or deteriorate. [Late Latin *atrophia*, from Greek, from *atrophos*, ill-nourished: *a-*, without; see **A-** + *trophē*, food.] — **a·tro·phic** (ăt'trōf'ik) *adj.*

at·ro·pine (ăt'trā-pēn', -pīn) also **at·ro·pin** (-pīn) *n.* A poisonous, bitter, crystalline alkaloid, $C_{17}H_{23}NO_3$, obtained from belladonna and other related plants. It is used to dilate the pupils of the eyes and as an antispasmodic. [From New Latin *Atropa*, genus name of belladonna, from Greek *atropos*, unchangeable. See **ATROPOS**.]

At·ro·pos (ăt'trā-pōs', -pās) *n.* **Greek Mythology.** One of the three Fates, the cutter of the thread of destiny. [Greek, from *atropos*, inexorable: *a-*, not; see **A-** + *tropos*, changeable; see **-TROPOUS**.]

At·si·na (ăt'sē'nā) *n., pl. Atsina* or **-nas**. 1. **a.** A Native American people formerly inhabiting the plains of northern Montana and southern Saskatchewan, with a present-day population in north central Montana. **b.** A member of this people. 2. The Algonquian language of the Atsina, dialectally related to Arapaho. Also called *Gros Ventre*.

att. *abbr.* 1. Attached. 2. Attention. 3. Law. Attorney.

at·tach (ā-tāch') *v.* **-tached, -tach·ing, -tach·es.** — *tr.* 1. To fasten, secure, or join. 2. To connect as an adjunct or associated condition or part: *Many major issues are attached to this legislation. They gained influence by attaching themselves to prominent city institutions.* 3. To affix or append; add: *We attached several riders to the document.* 4. To ascribe or assign: *attached no significance to the threat.* 5. To bind by emotional ties, as of affection or loyalty: *I am attached to my family.* 6. To assign (personnel) to a military unit on a temporary basis. 7. **Law.** To seize (persons or property) by legal writ. — *intr.* To adhere, belong, or relate: *Very little prestige attaches to this position.* [Middle English *attachen*, from Old French *attacher*, alteration of *estacher*, from *estache*, stake, of Germanic origin.] — **at·tach·a·ble** *adj.* — **at·tach·er** *n.*

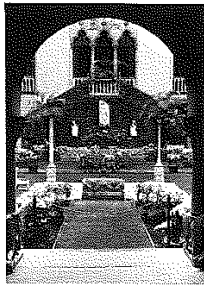
at·ta·ché (ăt'tā-shā',ăt-tā-) *n.* 1. A person officially assigned to the staff of a diplomatic mission to serve in a particular capacity: *a cultural attaché*; *a military attaché*. 2. An attaché case. [French, from past participle of *attacher*, to attach. See **ATTACH**.]

attaché case *n.* A slim briefcase with flat, rigid sides, hinges, and usually a lock.

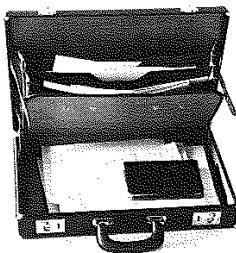
at·tached (ā-tācht') *adj.* 1. **Abbr. att.** **Architecture.** Joined to or by a wall, especially by sharing a wall with another building; not freestanding: *a block of attached houses*. 2. **Biology.** Living in a permanently fixed state in the adult stage, as the barnacle.

at·tach·ment (ā-tāch'mənt) *n.* 1. The act of attaching or the condition of being attached. 2. Something, such as a tie, band, or fastener, that attaches one thing to another. 3. A bond, as of affection or loyalty; fond regard. 4. A supplementary part; an accessory. See Synonyms at **appendage**. 5. **Law.** **a.** Legal seizure of property or a person. **b.** The writ ordering such a seizure.

at·tack (ə-tāk') *v.* **-tacked, -tack·ing, -tacks.** — *tr.* 1. To set upon with violent force. 2. To criticize strongly or in a hostile manner. 3. To start work with purpose and vigor: *attack a problem*. 4. To begin to affect harmfully: *The disease had already attacked the central nervous system.* — *intr.* To make an attack; launch an assault: *The enemy attacked during the night.* — **attack** *n.* 1. The act or an instance of attacking; an assault. 2. An expression of strong criticism; hostile comment: *vicious attacks in all the newspapers*. 3. **Sports.** **a.** An offensive action in a sport or game. **b.** The players executing such an action. 4. The initial



atrium
Isabella Stewart Gardner
Museum, Boston



attaché case

linize

desalt

To remove salts and other chemicals from (sea water or soil, for example). —**de-sal/i-ni-zā/tion** (dē-sāl'ē-nī-zā'shən) *n.*

de-salt (dē-solt') *tr.v.* —**salt-ed**, —**salt-ing**, —**salts**. To desalinate.

Desargues (dā-zārg'), **Gérard**. 1591–1661. French army officer and mathematician regarded as one of the founders of modern geometry.

dis-cant (dēs'kānt') *n.* 1. Also **dis-cant** (dīs'-). *Music. a.* An ornamental melody or counterpoint sung or played above a theme. **b.** The highest part sung in part music. **2.** A discussion or discourse on a theme. —**descant** (dēs'kānt', dē-skānt') *intr.v.* —**-cant-ed**, —**-cant-ing**, —**-cants**. **1.** To comment at length; discourse: "He used to descant critically on the dishes which had been at table" (James Boswell). **2.** Also **dis-cant** (dīs'kānt', dē-skānt'). *Music. a.* To sing or play a descant. **b. To sing melodiously. [Middle English, from Anglo-Norman *descaunt*, from Medieval Latin *discantus*, a refrain: Latin *dis-*, *dis-* + Latin *can-*, song, from past participle of *canere*, to sing. See **can-** in Appendix.] —**des-cant'er** *n.***

Des-cartes (dā-kārt'), **René**. 1596–1650. French mathematician and philosopher. Considered the father of analytic geometry, he formulated the Cartesian system of coordinates. His philosophy is based on the rationalistic premise "I think, therefore I am."

de-scend (dī-sēnd') *v.* —**-scend-ed**, —**-scend-ing**, —**-scends**. —**intr.** **1.** To move from a higher to a lower place; come or go down. **2.** To slope, extend, or incline downward: "A rough path descended like a steep stair into the plain" (J.R.R. Tolkien). **3. a.** To come from an ancestor or ancestry: *She was descended from a pioneer family.* **b.** To come down from a source; derive: *a tradition descending from colonial days.* **c.** To pass by inheritance: *The house has descended through four generations.* **4.** To lower oneself; stoop: "She, the conqueror, had descended to the level of the conquered" (James Bryce). **5.** To proceed or progress downward, as in rank, pitch, or scale: *titles listed in descending order of importance; notes that descended to the lower register.* **6.** To arrive or attack in a sudden or an overwhelming manner: *summer tourists descending on the seashore village.* —**tr.** **1. a.** To move from a higher to a lower part of; go down. **b.** To get down from: "People descended the minibus that shuttled guests to the nearby beach" (Howard Kaplan). **2.** To extend or proceed downward along a road that descended the mountain in sharp curves. [Middle English *descenden*, from Old French *descendre*, from Latin *descendere*: *dē-*, *dē-* + *scandere*, to climb; see **skand-** in Appendix.] —**de-scend/i-ble**, **de-scend/a-ble** *adj.*

de-scen-dant (dī-sēn'dant) *n.* **1.** A person, an animal, or a plant whose descent can be traced to a particular individual or group. **2.** Something derived from a prototype or earlier form: *Today's bicycles are descendants of the earlier velocipede.* —**descendant** *adj.* Variant of **descendent**.

de-scen-dent also **de-scen-dant** (dī-sēn'dant) *adj.* **1.** Moving downward; descending. **2.** Proceeding by descent from an ancestor.

de-scend-er (dī-sēn'dar) *n.* **1.** One that descends. **2. Printing. a.** The part of the lowercase letters, such as *g*, *p*, and *q*, that extends below the other lowercase letters. **b.** A letter with such a part.

de-scent (dī-sēnt') *n.* **1.** The act or an instance of descending. **2.** A way down. **3.** A downward incline or passage; a slope. **4. a.** Hereditary derivation; lineage: *a person of African descent.* **b.** One generation of a specific lineage. **5. a.** The fact or process of coming down or being derived from a source: *a paper tracing the descent of the novel from old picaresque tales.* **b.** Development in form or structure during transmission from an original source. **6.** Law. Transference of property by inheritance. **7.** A lowering or decline, as in status or level: *Her career went into a rapid descent after the charges of misconduct.* **8.** A sudden visit or attack; an onslaught. [Middle English, from Old French, from *descendre*, to descend. See **DESCEND**.]

Des-chutes (dā-shoot', dē-shoots'). A river rising in the Cascade Range of west-central Oregon and flowing about 402 km (250 mi) generally north to the Columbia River near The Dalles.

de-scram-ble (dē-skram'bəl) *tr.v.* —**-bled**, —**-bling**, —**-bles**. To unscramble (a coded message or signal, for example).

de-scram-bler (dē-skram'blər) *n.* An electronic device that decodes a scrambled transmission into a signal that is intelligible to the receiving apparatus.

de-scribe (dī-skrib') *tr.v.* —**-scribed**, —**-scrib-ing**, —**-scribes**. **1.** To give an account of in speech or writing. **2.** To convey an idea or impression of; characterize: *She described her childhood as a time of wonder and discovery.* **3.** To represent pictorially; depict: *Goya's etchings describe the horrors of war in grotesque detail.* **4.** To trace the form or outline of: *describe a circle with a compass.* [Middle English *describen*, from Latin *describere*, to write down: *dē-*, *dē-* + *scribere*, to write; see **skribh-** in Appendix.] —**de-scrib/a-ble** *adj.* —**de-scrib'er** *n.*

SYNONYMS: describe, narrate, recite, recount, rehearse, relate, report. The central meaning shared by these verbs is "to tell the facts, details, or particulars of something verbally or in writing": *described the accident; narrated their experiences in the Far East; an explorer reciting her adventures; a mercenary recounting his exploits; parents rehearsing the dangers the children faced; related the day's events; came back and reported what she had seen.*

de-scrip-tion (dī-skrip'shən) *n.* **1.** The act, process, or technique of describing. **2.** A statement or an account describing something: *published a description of her travels; gave a vivid description of the game.* **3.** A pictorial representation: *Monet's ethereal descriptions of haystacks and water lilies.* **4.** A kind or sort: *cars of every size and description.* [Middle English *descripcioun*, from Anglo-Norman, from Latin *descriptio*, *descriptio*, from *descriptus*, past participle of *describere*, to write down. See **DESCRIBE**.]

de-scrip-tive (dī-skrip'tiv) *adj.* **1.** Involving or characterized by description; serving to describe. **2.** Concerned with classification or description: *a descriptive science.* **3. Grammar. a. Expressing an attribute of the modified noun, as *green in green grass*. Used of an adjective or adjectival clause. **b.** Nonrestrictive. —**de-scrip-tive-ly** *adv.* —**de-scrip-tive-ness** *n.***

descriptive clause *n.* Grammar. A nonrestrictive clause.

descriptive linguistics *n.* The study of a language or languages at a specific stage of development, with emphasis on constructing a complete grammar rather than on historical development or comparison with other languages.

de-scrip-tor (dī-skrip'tər) *n.* Computer Science. A word, a phrase, or an alphanumeric character used to identify an item in an information storage and retrieval system. [Late Latin, *describer*, from Latin *describere*, *descript-*, to describe. See **DESCRIBE**.]

de-scry (dī-skri') *tr.v.* —**-scried**, —**-scry-ing**, —**-scries**. **1.** To catch sight of (something difficult to discern). See **SYNONYMS** at **see**. **2.** To discover by careful observation or scrutiny; detect: *descried a message of hope in her words.* [Middle English *descrien*, from Old French *descrier*, to call, cry out. See **DECRY**.] —**de-scri'er** *n.*

des-e-crate (dēs'ē-krāt') *tr.v.* —**-crat-ed**, —**-crat-ing**, —**-crates**. To violate the sacredness of; profane. [DE- + (CON)SECRATE.] —**des-e-crat'er**, **des-e-cra-tor** *n.* —**des-e-cra-tion** *n.*

de-seg-re-gate (dē-sēg'rē-gāt') *v.* —**-gat-ed**, —**-gat-ing**, —**-gates**. —**tr.** **1.** To abolish or eliminate segregation in. **2.** To open (a school or workplace, for example) to members of all races or ethnic groups, especially by force of law. —**intr.** To become open to members of all races or ethnic groups. —**de-seg're-ga-tion** *n.* —**de-seg're-ga-tion-ist** *n.*

de-sen-si-tize (dē-sēn'sī-tīz') *tr.v.* —**-tized**, —**-tiz-ing**, —**-tiz-es**.

1. To render insensitive or less sensitive. **2. Immunology.** To make (an individual) nonreactive or insensitive to an antigen. **3.** To make emotionally insensitive or unresponsive, as by long exposure or repeated shocks: "The successive assassinations and attempts, not just on Presidential figures but on Martin Luther King Jr. and others, have desensitized us" (Anthony Lewis). **4.** To make (a photographic film or substance) less sensitive to light. —**de-sen'si-ti-zā-tion** (tī-zā'shən) *n.* —**de-sen'si-tiz'er** *n.*

Des-er-et (dēz'ar-ēt'). An area proposed by the Mormons in 1849 as an independent state or a state of the Union. Deseret would have included much of the southwest United States, with a capital at Salt Lake City. Congress refused to recognize the provisional state and created the Utah Territory in 1850.

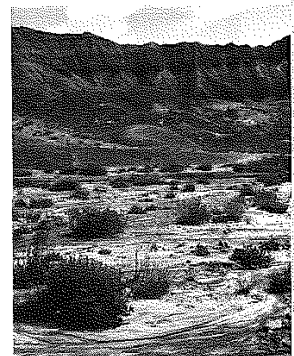
des-ert (dēz'art) *n.* **1.** A barren or desolate area, especially: **a.** A dry, often sandy region of little rainfall, extreme temperatures, and sparse vegetation. **b.** A region of permanent cold that is largely or entirely devoid of life. **c.** An apparently lifeless area of water. **2.** An empty or forsaken place; a wasteland: *a cultural desert.* **3. Archaic.** A wild, uncultivated, and uninhabited region. —**desert** *adj.* **1.** Of, relating to, characteristic of, or inhabiting a desert: *desert fauna.* **2.** Barren and uninhabited; desolate: *a desert island.* [Middle English, from Old French, from Late Latin *desertum*, from neuter past participle of *dēsere*, to desert. See **DESERT**.]

de-sert (dī-zūrt') *n.* **1.** Often **deserts**. Something that is deserved or merited, especially a punishment: *They got their just deserts when the scheme was finally uncovered.* **2.** The state or fact of deserving reward or punishment. [Middle English, from Old French *deserte*, from feminine past participle of *deservir*, to deserve. See **DESERVE**.]

WORD HISTORY: When Shakespeare says in Sonnet 72, "Unless you would devise some virtuous lie, / To do more for me than mine own desert," he is using the word *desert* in the sense of "worthiness; deserving," a word that is perhaps most familiar to us in the plural, meaning "something that is deserved," as in the phrase *just deserts*. This word goes back to the Latin word *dēservire*, "to devote oneself to the service of," which in Vulgar Latin came to mean "to merit by service." *Dēservire* is made up of *dē-*, meaning "thoroughly," and *servire*, "to serve." Knowing this, we can distinguish this *desert* from *desert*, "a wasteland," and *desert*, "to abandon," both of which go back to Latin *dēsere*, "to forsake, leave uninhabited," which is made up of *dē-*, expressing the notion of undoing, and the verb *serere*, "to link together." We can also distinguish all three *deserts* from *dessert*, "a sweet course at the end of a meal," which is from the French word *desservir*, "to clear the table." *Desservir* is made up of *des-*, expressing the notion of reversal, and *servir* (from Latin *servire*, "to serve," hence, "to unserve" or "to clear the table."

de-sert (dī-zūrt') *v.* —**-sert-ed**, —**-sert-ing**, —**-serts**. —**tr.** **1.** To leave empty or alone; abandon. **2.** To withdraw from, especially in spite of a responsibility or duty; forsake: *deserted her friend in a time of need.* **3.** To abandon (a military post, for example) in

ascender
h
q
descender
descender

desert¹

ā pat	oi boy
ā pay	ou out
ār care	ōō took
ā father	ōō boot
ē pet	ū cut
ē be	ūr urge
ī pit	th thin
ī pie	th this
īr pier	hw which
ō pot	zh vision
ō toe	a about, item
ō paw	♦ regionalism

Stress marks: ' (primary); ' (secondary), as in dictionary (dīk'sha-nēr'ē)

dessert wine *n.* A usually sweet wine, such as Sauternes, served with or after dessert.

de-sta-bi-lize (dē-stā'bi-līz') *tr.v.* -lized, -liz-ing, -liz-es.
1. To upset the stability or smooth functioning of: *a policy that threatens to destabilize the economy; a new weapon that threatens to destabilize nuclear deterrence.* 2. To undermine the power of (a government or leader) by subversive or terrorist acts. —**de-sta-bi-li-za-tion** (-lī-zā'shən) *n.*

de-stain (dē-stān') *tr.v.* -stained, -stain-ing, -stains. To remove stain from (a specimen) to aid in microscopic study.

de-sta-lin-i-za-tion (dē-stā'li-nī-zā'shən) *n.* The process of discrediting and eliminating the political policies, methods, and personal image of Joseph Stalin.

de-ster-i-lize (dē-stēr'ē-līz') *tr.v.* -lized, -liz-ing, -liz-es. To release (gold) from an inactive status and return it to use as a backing for credit and new currency.

de Stijl (dā stīl', stāl') *n.* A school of art originating in the Netherlands in 1917 and characterized by the use of rectangular shapes and primary colors. [Dutch: *de*, the + *stijl*, style.]

des-ti-na-tion (dēs'tā-nā'shən) *n.* 1. The place to which one is going or directed. 2. The ultimate purpose for which something is created or intended. 3. *Archaic.* An act of appointing or setting aside for a specific purpose.

des-tine (dēs'tīn) *tr.v.* -tined, -tin-ing, -tines. 1. To determine beforehand; preordain: *a foolish scheme destined to fail; a film destined to become a classic.* 2. To assign for a specific end, use, or purpose: *money destined to pay for their child's education.* 3. To direct toward a given destination: *a flight destined for Tokyo.* [Middle English *destinen*, from Old French *destiner*, from Latin *destinare*, to determine. See **stā-** in Appendix.]

des-ti-ny (dēs'tā-nē) *n., pl. -nies.* 1. The inevitable or necessary fate to which a particular person or thing is destined; one's lot. See Synonyms at **fate**. 2. A predetermined course of events considered as something beyond human power or control: "*Marriage and hanging go by destiny*" (Robert Burton). 3. The power or agency thought to predetermine events; fate: *Destiny brought them together.* [Middle English *destine*, from Old French *destinee*, from feminine past participle of *destiner*, to destine. See **DES-TINE**.]

des-ti-tute (dēs'tī-tōōt', -tyōōt') *adj.* 1. Utterly lacking; devoid: *Young recruits destitute of any experience.* 2. Lacking resources or the means of subsistence; completely impoverished. See Synonyms at **poor**. [Middle English, from Latin *destitutus*, past participle of *destituere*, to abandon: *dē-*, *de-* + *statuere*, to set; see **stā-** in Appendix.] —**des'ti-tute-ness** *n.*

des-ti-tu-tion (dēs'tī-tōō'shən, -tyōō'-) *n.* 1. Extreme want of resources or the means of subsistence; complete poverty. 2. A deprivation or lack; a deficiency.

des-tri-er (dēs'trē-ər, dī-strī'r') *n.* *Archaic.* A war horse. [Middle English *destrer*, from Anglo-Norman, from Vulgar Latin **dextrarius*, right-hand, from Latin *dexter*, right.]

de-destroy (dī-strōi') *v.* -stroyed, -stroy-ing, -stroys. —*tr.* 1. To ruin completely; spoil: *The ancient manuscripts were destroyed by fire.* 2. To tear down or break up; demolish. See Synonyms at **ruin**. 3. To do away with; put an end to: "*In crowded populations, poverty destroys the possibility of cleanliness*" (George Bernard Shaw). 4. To kill: *destroy a rabid dog.* 5. To subdue or defeat completely; crush: *The rebel forces were destroyed in battle.* 6. To render useless or ineffective: *destroyed the testimony of the prosecution's chief witness.* —*intr.* To be destructive; cause destruction: "*Too much money destroys as surely as too little*" (John Simon). [Middle English *destrōien*, from Old French *destruire*, from Vulgar Latin **destruere*, from Latin *destruere*: *dē-*, *de-* + *struere*, to pile up; see **ster-** 2 in Appendix.]

de-destroy-er (dī-strōi'ər) *n.* 1. One that destroys: *a destroyer of family unity; a destroyer of our environment.* 2. A small, fast, highly maneuverable warship armed with guns, torpedoes, depth charges, and guided missiles.

destroyer escort *n.* A warship, usually smaller than a destroyer, used in antisubmarine action.

de-destroy-ing angel (dī-strōi'ɪŋ) *n.* Any of several poisonous mushrooms of the genus *Amanita*.

de-struct (dī-strūkt', dē'strūkt') *n.* The intentional, usually remote-controlled destruction of a space vehicle, rocket, or missile after launching, as for defective performance or reasons of safety. —**destruct** *v.* -struct-ed, -struct-ing, -structs. —*tr.* To destroy intentionally (a rocket or missile) after launch. —*intr.* To self-destruct. [Back-formation from **DESTRUCTION**.]

de-struc-ti-ble (dī-strūkt'ə-bal) *adj.* Breakable or easily destroyed: *destructible glassware.* —**de-struc-ti-bil-i-ty**, **de-struc-ti-ble-ness** *n.*

de-struc-tion (dī-strūkt'shən) *n.* 1. *a.* The act of destroying. *b.* The condition of having been destroyed. 2. The cause or means of destroying: *weapons that could prove to be the destruction of humankind.* [Middle English, from Old French, from Latin *destructio*, *destruction-*, from *destruere*, past participle of *destruere*, to destroy. See **DESTROY**.]

de-struc-tion-ist (dī-strūkt'shə-nīst) *n.* One who believes in or advocates destruction, especially of existing social institutions.

de-struc-tive (dī-strūkt'iv) *adj.* 1. Causing or wreaking destruction; ruinous: *a destructive act; a policy that is destructive to the economy.* 2. Designed or tending to disprove or discredit:

destructive criticism. —**de-struc-tive-ly** *adv.* —**de-struc-tive-ness**, **de-struc-tiv-i-ty** (dē'strūkt'iv'i-tē) *n.*

destructive distillation *n.* A process by which organic substances such as wood, coal, and oil shale are decomposed by heat in the absence of air and distilled to produce useful products such as coke, charcoal, oils, and gases.

de-struc-tor (dī-strūkt'ər) *n.* 1. An incinerator for refuse. 2. An explosive, usually remote-controlled device for effecting a destruct.

des-ue-tude (dēs'wi-tōōd', -tyōōd') *n.* A state of disuse or inactivity. [French *désuétude*, from Latin *désuētudo*, from *dēsuetus*, past participle of *dēsuescere*, to put out of use: *dē-*, *de-* + *suescere*, to become accustomed; see **s(w)e-** in Appendix.]

de-sul-fur-ize (dē-sūl'fā-rīz') *tr.v.* -ized, -iz-ing, -iz-es. To eliminate sulfur from (petroleum, for example). —**de-sul-fur-i-za-tion** (-fār-i-zā'shən) *n.*

des-ul-to-ry (dēs'al-tōr'ē, -tōr'ē, dēz't-) *adj.* 1. Moving or jumping from one thing to another; disconnected: *a desultory speech.* 2. Occurring haphazardly; random. See Synonyms at **chance**. [Latin *dēsultorius*, leaping, from *dēsultor*, a leaper, from *dēsilire*, *dēsult-*, to leap down: *dē-*, *de-* + *salire*, to jump; see **sel-** in Appendix.] —**des'ul-to-ri-ly** *adv.* —**des'ul-to-ri-ness** *n.*

det. *abbr.* 1. Detachment. 2. Detail.

de-tach (dī-tāch') *tr.v.* -tached, -tach-ing, -tach-es. 1. To separate or unfasten; disconnect: *detach a check from the checkbook; detach burs from one's coat.* 2. To remove from association or union with something: *detach a calf from its mother; detached herself from the group.* 3. To send (troops or ships, for example) on a special mission. [French *détacher*, from Old French *destachier*: *dēs-*, *de-* + *attachier*, to attach; see **ATTACH**.] —**de-tach-a-bil-i-ty** *n.* —**de-tach-a-ble** *adj.* —**de-tach-a-bly** *adv.*

de-tached (dī-tāch't) *adj.* 1. Separated; disconnected: *a detached part; a detached plug.* 2. Standing apart from others; separate: *a house with a detached garage.* 3. Marked by an absence of emotional involvement and an aloof, impersonal objectivity. See Synonyms at **cool**, **indifferent**. —**de-tach-ed-ly** (-tāch'id-le, -tāch't/le) *adv.* —**de-tach-ed-ness** *n.*

de-tach-ment (dī-tāch'mənt) *n.* 1. The act or process of disconnecting or detaching; separation. 2. The state of being separate or detached. 3. Indifference to or remoteness from the concerns of others; aloofness: *preserved a chilly detachment in his relations with the family.* 4. Absence of prejudice or bias; disinterest: *strove to maintain her professional detachment in the case.* 5. *a.* The dispatch of a military unit, such as troops or ships, from a larger body for a special duty or mission. *b.* *Abbr. det.* The unit so dispatched. *c.* *Abbr. det.* A permanent unit, usually smaller than a platoon, organized for special duties.

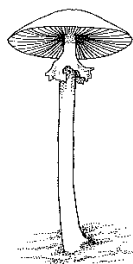
de-tail (dī-tāl', dē'tāl') *n.* *Abbr. det.* 1. An individual part or item; a particular. See Synonyms at **item**. 2. Particulars considered individually and in relation to a whole: *careful attention to detail.* 3. A minor or an inconsequential item or aspect; a minutia: *skipped the details to get to the main point.* 4. A minute or thorough treatment or account: *went into detail about his travels.* 5. *a.* A discrete part or portion of a work, such as a painting, building, or decorative object, especially when considered in isolation. *b.* A representation of such a part or portion: *a detail of a Rembrandt portrait illustrating the technique of chiaroscuro.* 6. *a.* A small elaborated element of a work of art, craft, or design. *b.* Such elements considered together: *the intricate detail of a rococo altarpiece.* *c.* The rendering of artistic detail: *the fine detail of the painter's brushwork.* 7. *a.* The selection of one or more troops for a particular duty, usually a fatigue duty. *b.* The personnel so selected. *c.* The duty assigned: *garbage detail.* —**detail** (dī-tāl') *tr.v.* -tailed, -tail-ing, -tails. 1. To report or relate minutely or in particulars. 2. To name or state explicitly: *tailed the charges against the defendant.* 3. To provide with artistic or decorative detail: *tailed the quilt with colorful appliqué.* 4. To select and dispatch for a particular duty. —*idiom.* *in detail.* With attention to particulars; thoroughly or meticulously: *explained her proposal in detail.* [French *détail*, from Old French *détail*, a piece cut off, from *detaillir*, to cut up: *dē-*, *de-* + *tallier*, to cut; see **TAILOR**.] —**de-tail'er** *n.*

de-tailed (dī-tāld', dē'tāld') *adj.* Characterized by abundant use of detail or thoroughness of treatment: *a detailed report on the state of the economy.*

SYNONYMS: *detailed, circumstantial, minute, particular.* The central meaning shared by these adjectives is "marked by attention to detail": *a detailed account of the trip; a circumstantial narrative; an exact and minute report; a faithful and particular description.*

detail man *n.* A representative of a manufacturer of drugs or medical supplies who calls on doctors, pharmacists, and other professional distributors to promote new drugs and supplies.

de-tain (dī-tān') *tr.v.* -tained, -tain-ing, -tains. 1. To keep from proceeding; delay or retard. See Synonyms at **delay**. 2. To keep in custody or temporary confinement: *The police detained several suspects for questioning. The disruptive students were detained after school until their parents had been notified.* 3. *Obsolete.* To retain or withhold (payment or property, for example). [Middle English *deteinen*, from Old French *deteinir*, from Vulgar Latin **dētēnere*, from Latin *dētēnere*: *dē-*, *de-* + *tenēre*, to hold; see **ten-** in Appendix.] —**de-tain'ment** *n.*



destroying angel

incisor

SYNONYMS: incisive, trenchant, biting, cutting, crisp, clear-cut. These adjectives are synonymous when they refer to keenness and forcefulness of thought, expression, or intellect. *Incisive* and *trenchant* suggest penetration to the heart of a subject and clear, sharp, and vigorous expression: *an incisive and piquant style of writing; trenchant wit*. *Biting* and *cutting* apply to penetration and discernment that often have a sarcastic or sardonic quality capable of wounding or stinging: "*Biting remarks revealed her attitude of contempt*" (D.H. Lawrence). "*He can say the driest, most cutting things in the quietest of tones*" (Charlotte Brontë). *Crisp* suggests clarity, conciseness, and briskness: *a crisp retort; crisp banter*. *Clear-cut* specifies distinctness and sharpness of definition: *The wording of the lease is so clear-cut that no one could possibly misinterpret its meaning*.

in·ci·sor (in-sī'zər) *n.* **Abbrev.** **i.** A tooth adapted for cutting or gnawing, located at the front of the mouth along the apex of the dental arch.

in·ci·ta·tion (in-sī-tā'shən) *n.* **1.** The act or an instance of inciting; stimulation. **2.** Something that incites.

in·cite (in-sīt') *tr.v.* **-cit·ed, -cit·ing, -cites.** To provoke and urge on: *troublemakers who incite riots; inciting workers to strike*. [Middle English *encyten*, from Old French *enciter*, from Latin *incitare*, to urge forward: *in-*, intensive pref.; see *IN-* + *citare*, to stimulate, frequentative of *cire*, to put in motion; see *kei-* in Appendix.] **—in·cite·ment** *n.* **—in·cit·er** *n.*

SYNONYMS: *incite, instigate, foment, abet.* These verbs mean to stir or give support to action. *Incite* is applied primarily to arousing the will and spirit to act: *Their leader tried to incite the dissidents to overthrow the government*. To *instigate* is to conceive and encourage the implementation of a plan of action, usually an evil or illegal one: *instigating a prison riot*. "*Commonly, though not always, we exhort to good actions, we instigate to ill*" (Samuel Johnson). *Foment* usually refers to the systematic fostering of feelings, as of discord or rebellion, that produce violent action: *foment discontent; foment civil insurrection*. To *abet* is to approve, encourage, and support actions, especially those in violation of what is right or proper: *The treasurer, aided and abetted by an assistant, misappropriated company funds*. See also *Synonyms at provoke*.

in·ci·vil·i·ty (in-sī-vil'ī-tē) *n., pl. -ties.* **1.** The quality or condition of being uncivil. **2.** An uncivil or discourteous act.

incl. *abbr.* **1.** Including. **2.** Inclusive.

in·clasp (in-klāsp') *v.* Variant of *endclasp*.

in·dem·ent (in-klem'ənt) *adj.* **1.** Stormy; inclement weather. **2.** Showing no clemency; unmerciful. **—in·dem·en·cy** *n.* **—in·dem·ent·ly** *adv.*

in·clin·a·ble (in-klī'nə-bəl) *adj.* **1.** Having a specified tendency or disposition; inclined: *inclined to laziness*. **2.** Favorably disposed; amenable: *inclined to our urgings*.

in·cli·na·tion (in-klī'nā'shən) *n.* **1.** The act of inclining or the state of being inclined; a bend or tilt: *The inclination of the child's head suggested sleep*. **2.a.** A deviation or the degree of deviation from the horizontal or vertical; a slant: *the steep inclination of a roof*. **b.** An inclined surface; a slope. **3.** A tendency toward a certain condition or character: *the alkaline inclination of the local waters*. **4.** A characteristic disposition to do, prefer, or favor one thing rather than another; a propensity: "*I shall indulge the inclination so natural in old men, to be talking of themselves*" (Benjamin Franklin). See *Synonyms at tendency*.

in·cline (in-klīn') *v.* **-clined, -clin·ing, -clines, -intr.** **1.** To deviate from the horizontal or vertical; slant. **2.** To be disposed to a certain preference, opinion, or course of action. **3.** To lower or bend the head or body, as in a nod or bow. **—tr.** **1.** To cause to lean, slant, or slope. **2.** To influence to have a certain tendency; dispose: *Recent events inclined us to distrust all politicians*. **3.** To bend or lower in a nod or bow: *inclined her head in acquiescence*. **—incline** (in'klīn') *n.* An inclined surface; a slope or gradient. [Middle English *enclinen*, from Old French *encliner*, from Latin *inclinare*: *in-*, into, toward; see *IN-* + *clinare*, to lean; see *klei-* in Appendix.] **—in·clin·er** *n.*

SYNONYMS: *incline, bias, dispose, predispose.* The central meaning shared by these verbs is "to influence or be influenced toward a particular attitude or course of action": *wasn't inclined to believe the excuse; is unjustly biased in her favor; an accomplishment that disposes us to admire him; isn't predisposed to the study of history*. See also *Synonyms at slant*.

ANTONYM: *disincline*.

in·clined (in-klīnd') *adj.* **1.** Sloping, slanting, or leaning. **2.** Having a preference, disposition, or tendency.

Inclined plane *n.* A plane set at an angle to the horizontal, especially a simple machine used to raise or lower a load by rolling or sliding.

in·cli·nom·e·ter (in-klā-nōm'i-tər) *n.* **1.** An instrument used to determine the angle of the earth's magnetic field in respect to the horizontal plane. **2.** An instrument for showing the inclination of an aircraft or a ship relative to the horizontal. **3.** See *clinometer*.

in·close (in-kloz') *v.* Variant of *endose*.

in·clude (in-klūd') *tr.v.* **-clud·ed, -clud·ing, -cludes.** **1.** To take in as a part, an element, or a member. **2.** To contain as a secondary or subordinate element. **3.** To consider with or place into a group, class, or total: *thanked the host for including us*. [Middle English *includen*, from Latin *includere*, to enclose: *in-*, in; see *IN-* + *cludere*, to close.] **—in·clud·a·ble, in·clud·i·ble** *adj.*

SYNONYMS: *include, comprise, comprehend, embrace, involve.* These verbs mean to take in or contain as part of something larger. *Include* and *comprise* both take as their objects things or persons that are constituent parts. *Comprise* usually implies that all of the components are stated: *The book comprises (that is, consists of or is composed of) 15 chapters*. *Include*, like the remaining terms, more often implies an incomplete listing: *included a reference to the accompanist in the review of the concert; will include an amount for postage in my payment*. "*Through the process of amendment, interpretation and court decision I have finally been included in 'We, the people'*" (Barbara C. Jordan). *Comprehend* and *embrace* usually refer to the taking in of subordinate elements as part of something broader: *The study of art comprehends both aesthetic and intellectual considerations*. *No single theory can embrace and explain every facet of human behavior*. *Involve* usually suggests inclusion as a logical consequence or necessary condition: "*Every argument involves some assumptions*" (Brooke F. Westcott).

USAGE NOTE: Some writers have insisted that *include* be used only when it is followed by a partial list of the contents of the referent of the subject. On this account, one may write *New England includes Connecticut and Rhode Island*, but one must use *comprise* or *consist* when a full enumeration is provided: *New England comprises (not includes) Connecticut, Rhode Island, Massachusetts, Vermont, New Hampshire, and Maine*. This restriction is too strong. *Include* does not rule out the possibility of a complete listing. Thus the sentence *The bibliography should include all the journal articles you have used* does not entail that the bibliography must contain something other than journal articles, though it does leave that possibility open. When one wants to make clear that the listing is exhaustive, however, the use of *comprise* or *consist* will avoid ambiguity. Thus the sentence *The task force includes all of the Navy units on active duty in the region* allows for the possibility that Marine and Army units are also taking part, where the same sentence with *comprise* would entail that the task force contained only Navy forces. See *Usage Note at comprise*.

in·clud·ed (in-klūd'dīd) *adj.* **1.** Botany. Not protruding beyond a surrounding part, as stamens that do not project from a corolla. **2.** Mathematics. Formed by and between two intersecting straight lines: *an included angle*.

in·clu·sion (in-klū'zhən) *n.* **1.** The act of including or the state of being included. **2.** Something included. **3.** Geology. A solid, liquid, or gaseous foreign body enclosed in a mineral or rock. **4.** Biology. A nonliving mass, such as a droplet of fat, in the cytoplasm of a cell. **5.** Computer Science. A logical operation that assumes the second statement of a pair is true if the first one is true. [Latin *inclusio*, *inclusiō*, from *inclusus*, past participle of *includere*, to enclose. See *INCLUDE*.] **—in·clu·sion·ar·y** (-zhə-nēr'ē) *adj.*

inclusion body *n.* An abnormal structure in a cell nucleus or cytoplasm having characteristic staining properties and associated especially with certain viral infections, such as rabies and smallpox.

in·clu·sive (in-klū'siv) *adj.* **Abbrev.** **incl.** **1.** Taking a great deal or everything within its scope; comprehensive: *an inclusive survey of world affairs*. **2.** Including the specified extremes or limits as well as the area between them: *the numbers one to ten, inclusive*. **—in·clu·sive·ly** *adv.* **—in·clu·sive·ness** *n.*

inclusive of *prep.* Taking into consideration or account; including.

in·co·er·ci·ble (in'kō-ūr'sə-bal) *adj.* Difficult or impossible to coerce or control forcibly: *incoercible rebel leaders*.

incog. *abbr.* Incognita; incognito.

in·cog·i·tant (in-kōj'ī-tənt) *adj.* Thoughtless; inconsiderate. [Latin *incogitans*, *incogitant*: *in-*, not; see *IN-* + *cogitans*, present participle of *cogitare*, to think; see *COGITATE*.]

in·cog·ni·ta (in'kōg-nē'tə, in-kōg'nī-tə) *adv. & adj.* **Abbrev.** **incog.** With one's identity disguised or concealed. Used of a woman. **—incognita** *n.* A woman or girl whose identity is disguised or concealed. [Italian, feminine of *incognito*, incognito. See *INCOGNITO*.]

in·cog·ni·to (in'kōg-nē'tō, in-kōg'nī-tō) *adv. & adj.* **Abbrev.** **incog.** With one's identity disguised or concealed. **—incognito** *n., pl. -tos.* **1.** One whose identity is disguised or concealed. **2.** The condition of having a disguised or concealed identity. [Italian, from Latin *incognitus*, unknown: *in-*, not; see *IN-* + *cognitus*, past participle of *cognoscere*, to learn, recognize; see *COGNITION*.]

in·cog·ni·zant (in-kōg'nī-zənt) *adj.* Lacking knowledge or awareness; unaware: *incognizant of the new political situation*.

in·co·her·ence (in'kō-hīr'əns) *n.* **1.** The condition or quality of being incoherent. **2.** Something incoherent.

in·co·her·en·cy (in'kō-hīr'an-sē) *n., pl. -cies.* Incoherence.

ā pat	oi boy
ā pay	ou out
ā care	ōō took
ā father	ōō boot
ē pet	ū cut
ē be	ūr urge
ī pit	th thin
ī pie	th this
īr pier	hw which
ō pot	zh vision
ō toe	a about, item
ō paw	♦ regionalism

Stress marks: ' (primary); ' (secondary), as in dictionary (dīk'shə-nēr'ē)

"place of imprisonment." This new sense could have already been developed in Latin and not been recorded, but we have to wait until the 12th century to see it, the sense "captivity" being added in the same century. From Old French as well as the Medieval Latin word *priso*, "prison," derived from Old French, came our Middle English word *prison*, first recorded in a work written before 1121 in the sense "imprisonment." The sense "place of imprisonment" is recorded shortly afterward in a text copied down before 1225 but perhaps actually written in the Old English period before the Norman Conquest.

prison camp *n.* 1. A camp for prisoners of war. 2. A minimum security facility for the internment of prisoners. In this sense, also called *work camp*.

pris-on-er (priz'ə-nər, priz'nər) *n.* 1. A person held in custody, captivity, or a condition of forcible restraint, especially while on trial or serving a prison sentence. 2. One deprived of freedom of expression or action: "He was a prisoner of his own personality—of that given set of traits that . . . predisposed him to see the world in a certain way, to make certain moves, certain choices" (William H. Hallahan).

prisoner of war *n., pl. prisoners of war.* A person taken by or surrendering to enemy forces in wartime.

Prisoner of War Medal *n.* A congressional decoration featuring a bald eagle surrounded by barbed wire and bayonet points, that is awarded to any American prisoner of war held captive by enemy troops after April 5, 1917.

pris-on-er's base (priz'ə-nərz, priz'nərz) *n.* Games. A children's game in which two teams try to capture opposing players by tagging them and bringing them to a base.

prison fever *n.* See *typhus*. [So called because it formerly prevailed in prisons.]

pris-sy (pris'ē) *adj.* -*si-er*, -*si-est*. Excessively or affectedly prim and proper. [Perhaps blend of PR(M)¹ and (S)ISSY.] —*pris'si-ly* *adv.* —*pris'si-ness* *n.*

pris-tine (pris'ten', pri-sten') *adj.* 1. *a.* Remaining in a pure state; uncorrupted by civilization. *b.* Remaining free from dirt or decay; clean: *pristine mountain snow*. 2. *a.* Of, relating to, or typical of the earliest time or condition; primitive or original. [Latin *pristinus*. See *per*¹ in Appendix.] —*pris-tine-ly* *adv.*

Pritch-ett (pritch'it), Sir V(ictor) S(awdon). Born 1900. British writer of novels, literary criticism, and most notably, short stories.

prith-ee (prith'ē, prith'ē) *interj.* Archaic. Used to express a polite request. [Alteration of (*I*) pray thee.]

priv. *abbr.* 1. Private. 2. Grammar. Privative.

priv-a-cy (priv'ə-sē) *n.* 1. *a.* The quality or condition of being secluded from the presence or view of others. *b.* The state of being free from unsanctioned intrusion: *a person's right to privacy*. 2. The state of being concealed; secrecy.

priv-ate (priv'it) *adj.* *Abbr. priv., pvt.* 1. *a.* Secluded from the sight, presence, or intrusion of others: *a private hideaway*. *b.* Designed or intended for one's exclusive use: *a private room*. 2. *a.* Of or confined to the individual; personal: *a private joke; private opinions*. *b.* Undertaken on an individual basis: *private studies; private research*. *c.* Of, relating to, or receiving special hospital services and privileges: *a private patient*. 3. Not available for public use, control, or participation: *a private club; a private party*. 4. *a.* Belonging to a particular person or persons, as opposed to the public or the government: *private property*. *b.* Conducted and supported primarily by private individuals or by a nongovernmental agency or corporation: *a private college; a private sanatorium*. *c.* Of, relating to, or derived from nongovernment sources: *private funding*. 5. Not holding an official or public position: *a former President who is now a private citizen*. 6. *a.* Not for public knowledge or disclosure; secret: *private papers; a private communication*. *b.* Not appropriate for use or display in public; intimate: *private behavior; a private tragedy*. *c.* Placing a high value on personal privacy: *a retiring, private individual*. —*private* *n.* 1. *Abbr. PVT, Pvt* *a.* A noncommissioned rank in the U.S. Army or Marine Corps that is below private first class. *b.* One who holds this rank or a similar rank in a military or paramilitary organization. 2. *privates*. Private parts. Often used with *the*. —*idioms. go private*. To take a publicly owned company into private ownership, as by a leveraged buyout. *in private*. Not in public; secretly or confidentially. [Middle English *privat*, from Latin *privātus*, not in public life, past participle of *privāre*, to release, deprive, from *privus*, single, alone. See *per*¹ in Appendix.] —*priv-ate-ly* *adv.* —*priv-ate-ness* *n.*

private detective *n.* A privately employed detective. Also called *private eye*, *private investigator*.

private enterprise *n.* 1. Business activities unregulated by state ownership or control; privately owned business. 2. A privately owned business enterprise, especially one operating under a system of free enterprise or laissez-faire capitalism.

priv-a-teeer (priv'ə-tēr') *n.* 1. A ship privately owned and manned but authorized by a government during wartime to attack and capture enemy vessels. 2. The commander or one of the crew of such a ship. —*privateer* *intr.v.* -*teered*, -*teer-ing*, -*teers*. To sail as a privateer.

private eye *n.* See *private detective*.

private first class *n., pl. privates first class.* *Abbr. PFC, Pfc* 1. A noncommissioned rank in the U.S. Army that is above private and below corporal or in the U.S. Marine Corps that is above private and below lance corporal. 2. One who holds this rank.

private investigator *n.* *Abbr. PI* See *private detective*.

private law *n.* The branch of law that deals with the legal rights and relationships of private individuals.

private member *n.* Chiefly British. A member of Parliament who does not hold office in the government or in his or her party.

private parts *pl.n.* The external organs of sex and excretion.

private school *n.* A secondary or elementary school run and supported by private individuals or a corporation rather than by a government or public agency.

priv-a-tion (priv'ə-shən) *n.* 1. *a.* Lack of the basic necessities or comforts of life. *b.* The condition resulting from such lack. 2. An act, condition, or result of deprivation or loss. [Middle English *privacion*, from Old French, from Latin *privātio*, *privātiō*, from *privātus*, past participle of *privāre*, to deprive. See *PRIVATE*.]

priv-at-ism (priv'ə-tiz'am) *n.* The social position of being noncommittal to or uninvolved with anything other than one's own immediate interests and lifestyle. —*priv-at-ist* *adj.* & *n.* —*priv-at-ist-ic* *adj.*

priv-a-tive (priv'ə-tiv) *adj.* 1. Causing deprivation, lack, or loss. 2. *Abbr. priv.* Grammar. Altering the meaning of a term from positive to negative. —*privative* *n.* *Abbr. priv.* Grammar. A privative prefix or suffix, such as *a-*, *non-*, *un-*, or *-less*. [Middle English *privatif*, from Latin *privātivus*, from *privātus*, past participle of *privāre*, to deprive. See *PRIVATE*.] —*priv-a-tive-ly* *adv.*

priv-a-tize (priv'ə-tiz') *tr.v.* -*tized*, -*tiz-ing*, -*tiz-es*. *Usage Problem.* To change (an industry or a business, for example) from governmental or public ownership or control to private enterprise: "The strike . . . was called to protest the . . . government's plans to break up and privatize the deficit-ridden national railway system" (Christian Science Monitor). See *Usage Note* at *-ize*. —*priv-a-ti-za-tion* (-tī-zā'shən) *n.*

priv-et (priv'it) *n.* 1. Any of several shrubs of the genus *Ligustrum*, especially *L. vulgare* or *L. ovalifolium*, having opposite leaves and clusters of white flowers and widely used for hedges. 2. Any of several similar or related plants. [Origin unknown.]

priv-i-lege (priv'ə-līj, priv'lij) *n.* 1. *a.* A special advantage, immunity, permission, right, or benefit granted to or enjoyed by an individual, a class, or a caste. See *Synonyms* at *right*. *b.* Such an advantage, an immunity, or a right held as a prerogative of status or rank, and exercised to the exclusion or detriment of others. 2. The principle of granting and maintaining a special right or immunity: *a society based on privilege*. 3. *Law.* The right to privileged communication in a confidential relationship, as between client and attorney, patient and physician, or communicant and priest. 4. An option to buy or sell a stock, including put, call, spread, and straddle. —*privilege* *tr.v.* -*leged*, -*leg-ing*, -*leg-es*. 1. To grant a privilege to. 2. To free or exempt. [Middle English, from Old French, from Latin *privilegium*, a law affecting one person: *privus*, single, alone; see *per*¹ in Appendix + *lēx*, *lēg-*, law; see *leg-* in Appendix.]

priv-i-legged (priv'ə-līd, priv'lijd) *adj.* 1. Enjoying a privilege or having privileges: *privileged students*. 2. Confined to an exclusive or chosen group of individuals: *privileged information*. —*privileged* *n.* (used with *a sing. or pl. verb*). Those enjoying a privilege or having privileges: *tax laws that favored the privileged at the expense of the disadvantaged*.

privileged communication *n.* *Law.* 1. A confidential communication that one cannot be forced to divulge. 2. A communication that is not subject to charges of slander or libel.

priv-i-ly (priv'ə-lē) *adv.* In a privacy manner; privately or secretly.

priv-i-ty (priv'ī-tē) *n., pl. -ties*. 1. Knowledge of something private or secret shared between individuals, especially with the implication of approval or consent. 2. *Law.* *a.* A relation between parties that is held to be sufficiently close and direct to support a legal claim on behalf of or against another person with whom this relation exists. *b.* A successive or mutual interest in or relationship to the same property. [Middle English *privete*, secrecy, privacy, from Old French, from Medieval Latin *privitās*, from Latin *privus*, single, alone. See *per*¹ in Appendix.]

priv-y (priv'ē) *adj.* 1. Made a participant in knowledge of something private or secret: *was privy to government secrets*. 2. Belonging or proper to a person, such as the British sovereign, in a private rather than official capacity. 3. Secret; concealed.

—*privy* *n., pl. -ies*. 1. *a.* An outdoor toilet; an outhouse. *b.* A toilet. 2. *Law.* One of the parties having an interest in the same matter. [Middle English *prive*, from Old French, from Latin *privātus*, private, from *privus*, single, alone. See *per*¹ in Appendix.]

Priv-y Council (priv'ē) *n.* *Abbr. P.C.* 1. A council of the British sovereign that until the 17th century was the supreme legislative body, that now consists of cabinet ministers ex officio and others appointed for life, and that has no important function except through its Judicial Committee, which in certain cases acts as a supreme appellate court in the Commonwealth. 2. *privy council*. An advisory council to an executive. —*privy counselor* *n.*

prix fixe (pre' fiks') *n., pl. prix fixes* (pre' fiks'). 1. A complete meal of several courses, sometimes with choices permitted, offered by a restaurant at a fixed price. 2. A fixed price charged for such a meal. 3. See *table d'hôte* (sense 2). [French: *prix*, price + *fixe*, fixed.]

prize¹ (priz) *n.* 1. Something offered or won as an award for superiority or victory, as in a contest or competition. See *Syn-*

added materials, especially the prevention of metallic ion precipitation from solution by formation of a coordination compound with a phosphate.

se-ques-trum (sĭ-kwĕs'trəm) *n.*, *pl.* **-tra** (-trə). A fragment of dead bone separated from healthy bone as a result of injury or disease. [Latin, deposit, from neuter of *sequester*, depository, trustee. See *sekw-* in Appendix.]

se-quin (sĕ'kwĭn) *n.* 1. A small shiny ornamental disk, often sewn on cloth; a spangle. 2. A gold coin of the Venetian Republic. In this sense, also called *zecchino*. — **sequin** *tr.v.* **-quined**, **-quin-ing**, **-quins**. To affix sequins to (a garment, for example). [French, from Old French, Venetian coin, from Italian *zecchino*, from *zecca*, mint, from Arabic *sikkah*, coin die.]

se-quoi-a (sĭ-kwŏi'ə) *n.* 1. See **redwood** (sense 1). 2. Giant sequoia. [New Latin *Sequoia*, genus name, after SEQUOYA.]

Se-quoy-a or **Se-quoy-ah** (sĭ-kwŏi'ə). Also called *George*. Guess. 1770?–1843. Cherokee scholar who developed a system of transcribing the Cherokee language.

ser. *abbr.* 1. Serial. 2. Series. 3. Sermon.

se-ra (sĕr'ə) *n.* A plural of **serum**.

sé-rac (să-răk', sâ-) *n.* A large pointed mass of ice in a glacier isolated by intersecting crevasses. [French, cottage cheese, *sérac*, perhaps from Vulgar Latin **seraceum*, whey, from Latin *serum*.]

se-ra-glio (să-rălyŏ, -răly-) *n.*, *pl.* **-glios**. 1. A large harem. 2. A sultan's palace. [Italian *serraglio*, enclosure, seraglio, probably partly from Vulgar Latin **serraculum*, enclosure (from **servare*, to lace up, from Latin *servare*, from *sera*, door-bar), and partly from Turkish *saray*, palace (from Persian *sarāi*, inn; see CARAVANSARY).]

ser-al (sĕr'al) *adj.* Of or relating to an ecological sere: a *seral stage*; a *seral community*.

se-ra-pe also **sa-ra-pe** (să-ră'pĕ, -răp'ĕ) *n.* A long blanket-like shawl, often brightly colored and fringed at the ends, worn especially by Mexican men. [American Spanish *sarape*.]

ser-aph (sĕr'af) *n.*, *pl.* **-aphim** (-ə-fĭm) or **-aphs**. 1. A celestial being having three pairs of wings. 2. *Theology*. One of the first order of angels. [Back-formation from *pl. seraphim*, from Middle English *seraphim*, from Old English, from Late Latin *seraphim*, from Greek *seraphim*, from Hebrew *serāpîm*, *pl. of sārāp*.] — **se-raph'ic** (să-răf'ĭk), **se-raph'i-cal** (-ĭ-kəl) *adj.* — **se-raph'i-cal-ly** *adv.*

Se-ra-pis (să-ră'pĭs) *n.* *Mythology*. An ancient Egyptian god of the lower world, also worshipped in ancient Greece and Rome.

Serb (sĕrb) *n.* A member of a southern Slavic people that is the principal ethnic group of Serbia and adjacent regions of Yugoslavia. [Serbian *Srb*.]

Ser-bi-a (sĕr'bĕ-ə) *n.* A historical region and former kingdom of eastern Yugoslavia. Serbs settled in the region in the 6th to the 7th century and formed an independent kingdom in the 13th to the 14th century but then fell under Turkish domination, which ended finally in 1878. The new kingdom of Serbia was an important Balkan power until the onset of World War I, precipitated in part by the assassination of Archduke Francis Ferdinand by a Serbian nationalist. Serbia was later a major constituent of the Kingdom of the Serbs, Croats, and Slovenes, which formed the nucleus of modern-day Yugoslavia.

Ser-bi-an (sĕr'bĕ-an) *n.* 1. A native or inhabitant of Serbia; a *Serb*. 2. Serbo-Croatian as spoken in Serbia and adjacent regions of Yugoslavia, written in a Cyrillic alphabet. — **Serbian** *adj.* Of or relating to Serbia or its people, language, or culture.

Ser-bo-Cro-a-tian (sĕr'bŏ-kro-ă'shən) *n.* 1. The Slavic language of the Serbs and the Croats. 2. A native speaker of Serbo-Croatian. — **Serbo-Croatian** *adj.* Of or relating to Serbo-Croatian or those who speak it.

sere¹ also **sear** (sĕr) *adj.* Withered; dry: *sere vegetation at the edge of the desert*. [Middle English, from Old English *sĕar*.]

sere² (sĕr) *n.* The entire sequence of ecological communities successively occupying an area from the initial stage to the climax. [From **SERIES**.]

se-re-nade (sĕr'ə-năd', sĕr'ə-năd') *n.* 1. *Music*. A complimentary performance given to honor or express love for someone. 2. *South Atlantic U.S.* See **shivaree**. See Regional Note at **shivaree**. 3. *Music*. An instrumental composition written for a small ensemble and having characteristics of the suite and the sonata. — **serenade** *v.* **-nad-ed**, **-nad-ing**, **-nades**. *Music*. — *tr.* To perform a serenade for. — *intr.* To perform a serenade. [French *sérénade*, from Italian *serenata*, from *sereno*, calm, clear, the open air, from Latin *serenus*. See **SERENE**.] — **se-re-nad'er** *n.*

ser-en-dip-i-ty (sĕr'ən-dĭp'i-tĕ) *n.* The faculty of making fortunate discoveries by accident. [From the characters in the Persian fairy tale *The Three Princes of Serendip*, who made such discoveries, from Persian *Sarandīb*, Sri Lanka, from Arabic *Sarandīb*.] — **ser'en-dip'i-tous** *adj.* — **ser'en-dip'i-tous-ly** *adv.*

WORD HISTORY: We are indebted to the English author Horace Walpole for coining the word *serendipity*. In one of his 3,000 or more letters, on which his literary reputation primarily rests, and specifically in a letter of January 28, 1754, Walpole says that "this discovery, indeed, is almost of that kind which I call Serendipity, a very expressive word." Perhaps the word itself came to him by serendipity. Walpole formed the word on an old name for Sri Lanka, *Serendip*. He explained that this name was part of the title of

"a silly fairy tale, called *The Three Princes of Serendip*: as their highnesses traveled, they were always making discoveries, by accidents and sagacity, of things which they were not in quest of. . . One of the most remarkable instances of this accidental sagacity (for you must observe that no discovery of a thing you are looking for, comes under this description) was of my Lord Shaftsbury [Anthony Ashley Cooper], who happening to dine at Lord Chancellor Clarendon's [Edward Hyde], found out the marriage of the Duke of York [later James II] and Mrs. Hyde [Anne Hyde, Clarendon's daughter], by the respect with which her mother [Frances Aylesbury Hyde] treated her at table."

se-re-ne (să-rĕn') *adj.* 1. Unaffected by disturbance; calm and unruffled. See Synonyms at **calm**. 2. Unclouded; fair: *serene skies and a bright blue sea*. 3. Often **Serene**. Used as a title and form of address for certain members of royalty: *Her Serene Highness; His Serene Highness*. [Middle English, from Latin *serenus*, serene, clear.] — **se-re-ne'ly** *adv.* — **se-re-ne'ness** *n.*

Ser-en-get-i Plain (sĕr'ən-gĕt'ē). An area of northern Tanzania bordering on Kenya and Lake Victoria. It is noted for its extensive wildlife preserve.

se-ren-i-ty (să-rĕn'i-tĕ) *n.* The state or quality of being serene; tranquillity. See Synonyms at **equanimity**.

serf (sĕrf) *n.* 1. A member of a servile, feudal class of people in Europe, bound to the land and owned by a lord. 2. A person in servitude. [Middle English, from Old French, from Latin *servus*, slave.] — **serf'dom** *n.*

serge (sĕrj) *n.* A twilled cloth of worsted or wool, often used for suits. [Middle English *sarge*, from Old French, from Vulgar Latin **sārica*, from Latin *sērica* (*vestis*), silken (clothing), feminine of *sēricus*, silken, from Greek *sērikos*, of the Seres, silken, from *Sēres*, a people of Eastern Asia.]

ser-geant (săr'jant) *n.* *Abbr.* **Sgt.** 1. *a.* Any of several ranks of noncommissioned officers in the U.S. Army, Air Force, or Marine Corps. *b.* One who holds any of these ranks. 2. *a.* The rank of police officer next below a captain, lieutenant, or inspector. *b.* A police officer holding this rank. 3. See **sergeant at arms**. [Middle English *sergeante*, a common soldier, from Old French *sergent*, from Medieval Latin *serviens*, *servient-*, servant, soldier, from Late Latin, public official, from Latin, present participle of *servire*, to serve, from *servus*, slave.] — **ser'gean-cy**, **ser'geant-ship** *n.*

sergeant at arms *n.*, *pl.* **sergeants at arms**. An officer appointed to keep order within an organization, such as a legislative, judicial, or social body. Also called *sergeant*.

sergeant first class *n.*, *pl.* **sergeants first class**. *Abbr.* **SFC** 1. A noncommissioned rank in the U.S. Army that is above staff sergeant and below master sergeant. 2. One who holds this rank.

sergeant fish *n.* 1. See **cobia**. 2. See **snook**.

sergeant major *n.*, *pl.* **sergeants major** or **sergeant majors**. 1. *Abbr.* **Sgt. Maj.**, **SM** *a.* Used as a title for a noncommissioned officer serving as chief administrative assistant of a headquarters unit of the U.S. Army, Air Force, or Marine Corps. *b.* One who holds this title. 2. *Chiefly British*. A noncommissioned officer of the highest rank. 3. A small damselfish (*Abudefduf saxatilis*) of warm seas, having a flattened body with dark vertical stripes. In this sense, also called *cow pilot*.

se-ri-al (sĕr'i-əl) *adj.* *Abbr.* **ser.** 1. Of, forming, or arranged in a series. 2. *a.* Published or produced in installments, as a novel or television drama. *b.* Relating to such publication or production. 3. *Music*. Relating to or based on a 12-tone row. 4. *Computer Science*. *a.* Of or relating to the sequential transmission of all the bits of a byte over one wire: a *serial port*; a *serial printer*. *b.* Of or relating to the sequential performance of multiple operations: *serial processing*. — **serial** *n.* *Abbr.* **ser.** A literary or dramatic work published or produced in installments. — **se'ri-al-ly** *adv.*

se-ri-al-ism (sĕr'i-ə-lĭz'am) *n.* *Music*. 1. Serial compositions. 2. The theory or composition of serial music. — **se'ri-al-ist** *n.*

se-ri-al-ize (sĕr'i-ə-lĭz') *tr.v.* **-ized**, **-iz-ing**, **-iz-es**. To write or publish in serial form. — **se'ri-al-i-za'tion** (-ə-lĭ-ză'shən) *n.*

serial killer *n.* A person who attacks and slays more than three victims one by one during a relatively short period of time. Also called *serial murderer*. — **serial killing** *n.*

serial number *n.* A number that is one of a series and is used for identification, as of a machine, weapon, or motor vehicle.

se-ri-ate (sĕr'i-ĕ-ăt', -ĭt) *adj.* Arranged or occurring in a series or in rows. — **se-ri-ate-ly** *adv.*

se-ri-a-tim (sĕr'i-ĕ-ăt'im, -ăt'im) *adv.* One after another; in a series. [Medieval Latin *seriatim*, from Latin *series*, series. See **SERIES**.]

se-ri-ceous (sĕ-rĭsh'as) *adj.* 1. Silky. 2. *Botany*. Covered with soft, silky hairs. [Latin *sēricus*, silken, alteration of *sēricus*. See **SERGE**.]

ser-i-cin (sĕr'i-sĭn) *n.* A viscous, gelatinous protein that forms on the surface of raw-silk fibers. [Latin *sēricus*, silken; see **SERGE** + **-IN**.]

ser-ic-te-ri-um (sĕr'ĭk-tĕr'i-əm) *n.*, *pl.* **-te-ri-a** (-tĕr'i-ə). The silk-producing gland or glands of an insect, especially a silkworm. [New Latin *sericterium*, from Greek *sērikon*, silk, from neuter of *sērikos*, silken, from *Sēres*, a people of East Asia.]



Sequoya



serape

ă pat	oi boy
â pay	ou out
ă care	oo took
ă father	oo boot
ê pet	û cut
ê be	ûr urge
î pit	th thin
î pie	th this
ô pier	hw which
ô pot	zh vision
ô toe	ə about, item
ô paw	♦ regionalism

Stress marks: / (primary); ' (secondary), as in dictionary (dĭk'shə-nĕr'ē)

record of business conducted at a meeting; proceedings. — **trans-ac-tion-al** *adj.*

transaccional analysis *n.* *Abbr. TA* A system of psychotherapy that analyzes personal relationships and interactions in terms of conflicting or complementary ego states that correspond to the roles of parent, child, and adult.

trans-ac-ti-vate (tranz-ák'tá-vát', tranz-) *tr.v.* **-vat-ed, -vat-ing, -vates.** To stimulate (a host cell) to replicate the genetic components of a virus. Used of a viral protein. — **trans-ac-ti-va-tion** *n.* — **trans-ac'ti-va'tor** *n.*

Trans A-lai (tranz'á-lí', tranz'). A range of the Pamir Mountains in eastern Tadzhikistan and southern Kirghiz rising to 7,138.5 m (23,405 ft).

trans-al-pine (tranz-ál'pín', tranz-) *adj.* Relating to, living on, or coming from the other side of the Alps, especially as viewed from Italy.

Trans-al-pine Gaul (tranz-ál'pín' gól', tranz-). The part of ancient Gaul northwest of the Alps, including modern France and Belgium.

trans-am-i-nase (tranz-ám'á-nás', -náz', tranz-) *n.* Any of a group of enzymes that catalyze transamination.

trans-am-i-na-tion (tranz-ám'á-ná'shən, tranz-) *n.* 1. Transfer of an amino group from one chemical compound to another. 2. Transposition of an amino group within a chemical compound.

trans-at-lan-tic (tranz'at-lán'tík, tranz'-) *adj.* 1. Situated on or coming from the other side of the Atlantic Ocean. 2. Spanning or crossing the Atlantic Ocean.

trans-ax-le (tranz-ák'səl, tranz-) *n.* An automotive part that combines the transmission and the differential and is used on vehicles with front-wheel drive. [TRANS(MISSION) + AXLE.]

Trans-cau-ca-sia (tranz'kó-ká'zhə, -zhé-ə, tranz'-) *n.* A region of Georgia, Armenia, and Azerbaijan between the Caucasus Mountains and the borders of Turkey and Iran. — **Trans-cau-ca-sian** *adj. & n.*

trans-ceiv-er (tranz-sē'var) *n.* A transmitter and receiver housed together in a single unit and having some circuits in common, often for portable or mobile use. [TRANS(MITTER) + (RE)CEIVER.]

tran-scend (tranz-sēnd') *v.* **-scend-ed, -scend-ing, -scends.** — *tr.* 1. To pass beyond the limits of: *emotions that transcend understanding.* 2. To be greater than, as in intensity or power; surpass: *love that transcends infatuation.* See *Synonyms at excel*. 3. To exist above and independent of (material experience or the universe): *"One never can see the thing in itself, because the mind does not transcend phenomena"* (Hilaire Belloc). — *intr.* To be transcendent; excel. [Middle English *transcenden*, from Old French *transcendre*, from Latin *transcendere*: *trans-* + *scandere*, to climb; see *skand-* in Appendix.]

tran-scen-dent (tranz-sēn'dənt) *adj.* 1. Surpassing others; preeminent or supreme. 2. Lying beyond the ordinary range of perception: *"fails to achieve a transcendent significance in suffering and squalor"* (National Review). 3. Philosophy. *a.* Transcending the Aristotelian categories. *b.* In Kant's theory of knowledge, being beyond the limits of experience and hence unknowable. 4. Being above and independent of the material universe. Used of the Deity. — **tran-scen'dence, tran-scen'den-cy** *n.* — **tran-scen'dent-ly** *adv.*

tran-scen-den-tal (tranz'sēn-dēn'tl) *adj.* 1. Philosophy. *a.* Concerned with the a priori or intuitive basis of knowledge as independent of experience. *b.* Asserting a fundamental irrationality or supernatural element in experience. 2. Surpassing all others; superior. 3. Beyond common thought or experience; mystical or supernatural. 4. Mathematics. *a.* Not capable of being determined by any combination of a finite number of equations with rational integral coefficients. *b.* Not expressible as an integer or as the root or quotient of integers. Used of numbers, especially nonrepeating infinite decimals. — **tran-scen-den'tal-ly** *adv.*

tran-scen-den-tal-ism (tranz'sēn-dēn'tl-iz'm) *n.* 1. A philosophy associated with Kant, holding that one must transcend empiricism or what is experienced in order to ascertain the a priori principles of all knowledge. 2. A literary and philosophical movement, associated with Ralph Waldo Emerson and Margaret Fuller, asserting the existence of an ideal spiritual reality that transcends the empirical and scientific and is knowable through intuition. 3. The quality or state of being transcendental. — **tran-scen-den'tal-ist** *n.*

transcendental meditation *n.* *Abbr. T.M.* A technique of meditation derived from Hindu traditions that promotes deep relaxation through the use of a mantra.

trans-con-ti-nen-tal (tranz'kōn-tá-nēn'tl) *adj.* Spanning or crossing a continent.

trans-cribe (tranz-skrib') *tr.v.* **-scribed, -scrib-ing, -scribes.** 1. To make a full written or typewritten copy of (dictated material, for example). 2. Computer Science. To transfer (information) from one recording and storing system to another. 3. Music. To adapt or arrange (a composition) for a voice or an instrument other than the original. 4. To record, usually on tape, for broadcast at a later date. 5. Linguistics. To represent (speech sounds) by phonetic symbols. 6. To translate or transliterate. 7. Biology. To cause (DNA or RNA) to undergo transcription. [Latin *transscribere*: *trans-* + *scribere*, to write; see *scribh-* in Appendix.] — **tran-scrib'a-ble** *adj.* — **tran-scrib'er** *n.*

tran-script (tranz'skrīpt') *n.* 1. Something transcribed, especially a written, typewritten, or printed copy: *the transcript of court testimony; an academic transcript.* 2. Biology. A sequence of RNA produced by transcription. [Middle English, from Medieval Latin *transcriptum*, from Latin, neuter past participle of *transcribere*, to transcribe. See *TRANSCRIBE*.]

tran-scrip-tase (tranz-skrip'tās, -lās) *n.* 1. A polymerase that catalyzes the formation of RNA from a DNA template in the process of transcription. 2. Reverse transcriptase.

tran-scrip-tion (tranz-skrip'shən) *n.* 1. The act or process of transcribing. 2. Something that has been transcribed, especially: *a. Music.* An adaptation of a composition. *b.* A recorded radio or television program. *c. Linguistics.* A representation of speech sounds in phonetic symbols. 3. Biology. The process by which messenger RNA is synthesized from a DNA template resulting in the transfer of genetic information from the DNA molecule to the messenger RNA. — **tran-scrip-tion-al** *adj.* — **tran-scrip-tion-al-ly** *adv.* — **tran-scrip-tion-ist** *n.*

trans-cul-tu-ra-tion (tranz'kūl-cha-rā'shən) *n.* Cultural change induced by introduction of elements of a foreign culture.

trans-cur-rent (tranz-kūr'ənt, -kūr'-) *adj.* Extending or running transversely.

trans-cu-ta-ne-ous (tranz'kyōō-tā'nē-əs) *adj.* Transdermal.

trans-der-mal (tranz-dūr'mal, tranz-) *n.* Through or by way of the skin: *transdermal inoculation; transdermal medication.*

transdermal patch *n.* A medicated adhesive pad that is placed on the skin to deliver a time-release dose of medication through the skin into the bloodstream. Also called *skin patch*.

trans-duce (tranz-dōs', -dyōs', tranz-) *tr.v.* **-duced, -duc-ing, -duc-es.** 1. To convert (energy) from one form to another. 2. To transfer (genetic material or characteristics) from one bacterial cell to another. Used of a bacteriophage or plasmid. [Back-formation from *TRANS-DUCER*.]

trans-duc-er (tranz-dōō'sər, -dyōō'-, tranz-) *n.* A substance or device, such as a piezoelectric crystal, microphone, or photoelectric cell, that converts input energy of one form into output energy of another. [From Latin *transducere*, to transfer: *trans-* + *ducere*, to lead; see *duk-* in Appendix.]

trans-duc-tant (tranz-dūk'tənt, tranz-) *n.* A bacterial cell into which genetic material has been transduced.

trans-duc-tion (tranz-dūk'shən, tranz-) *n.* Genetics. Transfer of genetic material or characteristics from one bacterial cell to another by a bacteriophage or plasmid. [From Latin *transductus*, past participle of *transducere*, to transfer. See *TRANS-DUCER*.] — **trans-duc-tion-al** *adj.*

tran-sect (tranz-sēkt') *tr.v.* **-sect-ed, -sect-ing, -sects.** To divide by cutting transversely. [TRANS- + -SECT.] — **tran-sec-tion** *n.*

tran-sept (tranz'sēpt') *n.* Architecture. 1. The transverse part of a cruciform church, crossing the nave at right angles. 2. Either of the two lateral arms of such a part. [New Latin *transseptum*: Latin *trans-* + Latin *saepium*, partition; see *SEPTUM*.]

tran-se-unt (tranz'sē-ənt) *adj.* Philosophy. Productive of effects outside the mind. [Latin *transiens, transeunt-*, present participle of *transire*, to go over. See *TRANSIENT*.]

transf. *abbr.* 1. Transfer. 2. Transferred.

trans-fec-tion (tranz-fēk'shən) *n.* Infection of a cell with purified viral nucleic acid, resulting in subsequent replication of the virus in the cell. [TRANS- + (IN)FECTION.] — **trans-fect'** *v.*

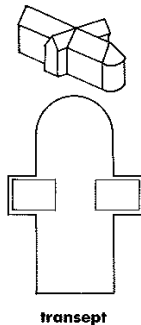
trans-fer (tranz-fēr', tranz'fər) *v.* **-ferred, -fer-ring, -fers.** — *tr.* 1. To convey or cause to pass from one place, person, or thing to another. 2. Law. To make over the possession or legal title of; convey. 3. To convey (a design, for example) from one surface to another, as by impression. — *intr.* 1. To move oneself from one location or job to another. 2. To withdraw from one educational institution or course of study and enroll in another. 3. To change from one public conveyance to another: *transferred to another bus.* — **transfer** (tranz'fər) *n.* *Abbr. trans., transf., tfr.* 1. Also **trans-fer-al** (tranz'fər'al). The conveyance or removal of something from one place, person, or thing to another. 2. One who transfers or is transferred, as to a new school. 3. A design conveyed by contact from one surface to another. 4. *a.* A ticket entitling a passenger to change from one public conveyance to another as part of one trip. *b.* A place where such a change is made. 5. Also **transferral**. Law. A conveyance of title or property from one person to another. [Middle English *transferren*, from Old French *transferer*, from Latin *transfere*: *trans-* + *ferre*, to carry; see *bher-* in Appendix.] — **trans-fer'a-ble** *adj.* — **trans-fer'a-ble-ly** *adv.* — **trans-fer'a-ble** *adj.* — **trans-fer'er** *n.*

trans-fer-al (tranz'fər'al) *n.* 1. Variant of *transfer* (sense 1). 2. Law. Variant of *transfer* (sense 5).

trans-fer-ase (tranz'fə-rās', -rāz') *n.* Any of various enzymes that catalyze the transfer of a chemical group, such as a phosphate or an amine, from one molecule to another.

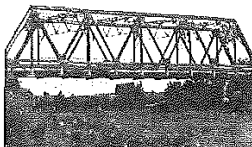
trans-fer-ee (tranz'fə-rē') *n.* 1. Law. One to whom a conveyance of title or property is made. 2. One who is transferred.

trans-fer-ence (tranz'fər-əns, tranz'fər-əns) *n.* 1. *a.* The act or process of transferring. *b.* The fact of being transferred. 2. In psychoanalysis, the process by which emotions and desires originally associated with one person, such as a parent or sibling, are unconsciously shifted to another person, especially to the analyst. — **trans-fer-en-tial** (tranz'fər-ən'shəl) *adj.*





trundle bed
Pulled out from
underneath a canopied bed



truss bridge



Sojourner Truth
Photographed c. 1870

trumpeter swan *n.* A large white swan (*Olor buccinator*) of western North America, having a loud buglelike call.

trumpet honeysuckle *n.* A vine (*Lonicera sempervirens*) of the eastern United States, having tubular reddish flowers.

trumpet vine *n.* See **trumpet creeper**.

trun·cate (trŭng'kāt') *tr.v.* -cat-ed, -cat-ing, -cates. 1. To shorten by or as if by cutting off. See **Synonyms** at **shorten**. 2. To shorten (a number) by dropping one or more digits after the decimal point. 3. To replace (the edge of a crystal) with a plane face. —**truncate** *adj.* 1. Appearing to terminate abruptly, as a leaf of a tulip tree or a coiled gastropod shell that lacks a spire. 2. Truncated. [Latin *truncāre*, *truncāt-*, from *truncus*, trunk. See **tere-** in Appendix.] —**trun'cate'ly** *adv.* —**trun-ca'tion** *n.*

trun·ca·ted (trŭng'kāt'id) *adj.* 1. Having the apex cut off and replaced by a plane, especially one parallel to the base. Used of a cone or pyramid. 2. *a.* Lacking one or more syllables, especially in the final foot; catalectic. *b.* Lacking an initial or final syllable. Used of a line of verse. 3. Truncate.

trun·cheon (trŭn'chan) *n.* 1. A short stick carried by police; a billy club. 2. A staff carried as a symbol of office or authority; a baton. 3. *Obsolete.* *a.* A heavy club; a cudgel. *b.* A thick cutting from a plant, as for grafting. [Middle English *tronchon*, piece broken off, club, from Old North French, from Vulgar Latin **trunciō*, *trunciōn-*, from Latin *truncus*, trunk. See **TRUNK**.] —**trun'cheon** *v.*

trun·dle (trŭn'dl) *n.* 1. A small wheel or roller. 2. The motion or noise of rolling. 3. A trundle bed. 4. A low-wheeled cart; a dolly. —**trundle** *v.* -dled, -dling, -dles. —**tr.** 1. To push or propel on wheels or rollers: "I doubt if Emerson could trundle a wheelbarrow through the streets" (Henry David Thoreau). 2. To spin; twirl. —**intr.** To move along by or as if by rolling or spinning. [Variant of dialectal *trendle*, wheel, from Middle English, from Old English *trendel*, circle.] —**trun'dler** *n.*

trundle bed *n.* A low bed on casters that can be rolled under another bed for storage.

trunk (trŭngk) *n.* 1. *a.* The main woody axis of a tree. *b.* *Architecture.* The shaft of a column. 2. *a.* The body of a human being or an animal excluding the head and limbs. *b.* The thorax of an insect. 3. A proboscis, especially the long prehensile proboscis of an elephant. 4. *a.* A main body, apart from tributaries or appendages. *b.* The main stem of a blood vessel or nerve apart from the branches. 5. A trunk line. 6. A chute or conduit. 7. *Nautical.* *a.* A shaft connecting two or more decks. *b.* The housing for the centerboard of a vessel. 8. *Nautical.* *a.* Any of certain structures projecting above part of a main deck, as: *b.* A covering over the hatches of a ship. *c.* An expansion chamber on a tanker. *d.* A cabin on a small boat. 9. *a.* A covered compartment for luggage and storage, generally at the rear of an automobile. *b.* A large packing case or box that clasps shut, used as luggage or for storage. 10. *trunks.* Shorts worn for swimming or other athletics. [Middle English *trunke*, from Old French *tronc*, from Latin *truncus*. See **tere-** in Appendix.]

trunk·fish (trŭngk'fīsh') *n., pl.* **trunkfish** or **-fish-es.** Any of various colorful tropical marine fishes of the family *Ostraciidae*, having a body enclosed in bony armorlike plates with only the mouth, eyes, fins, and vent exposed. Also called *boxfish*.

trunk hose *pl.n.* Short, ballooning breeches, extending from the waist to mid thigh, worn by men in Europe in the 16th and 17th centuries. [Perhaps from obsolete *trunk*, to cut off, from Latin *truncāre*. See **TRUNCATE**.]

trunk line *n.* 1. A direct line between two telephone switchboards. 2. The main line of a communications or transportation system.

trunk show *n.* A traveling collection of designer clothing or jewelry, displayed in various stores.

trun·nel (trŭn'al) *n.* Variant of **trencil**.

trun·nion (trŭn'yən) *n.* A pin or gudgeon, especially either of two small cylindrical projections on a cannon forming an axis on which it pivots. [French *trognon*, stump.]

truss (trŭs) *n.* 1. *Medicine.* A supportive device, usually consisting of a pad with a belt, worn to prevent enlargement of a hernia or the return of a reduced hernia. 2. *a.* A rigid framework, as of wooden beams or metal bars, designed to support a structure, such as a roof. *b.* *Architecture.* A bracket. 3. Something gathered into a bundle; a pack. 4. *Nautical.* An iron fitting by which a lower yard is secured to a mast. 5. *Botany.* A compact cluster of flowers at the end of a stalk. —**truss** *tr.v.* **trussed**, **truss-ing**, **truss-es.** 1. To tie up or bind tightly. 2. To bind or skewer the wings or legs of (a fowl) before cooking. 3. To support or brace with a truss. [Middle English *trusse*, bundle, from Old French *trousse*, from *torser*, *troussier*, to truss, possibly from Vulgar Latin **torsāre*, from **torsus*, variant of Latin *tortus*, past participle of *torquere*, to twist. See **terk-** in Appendix.]

truss bridge *n.* A bridge supported by trusses.

trust (trŭst) *n.* 1. Firm reliance on the integrity, ability, or character of a person or thing. 2. Custody; care. 3. Something committed into the care of another; charge. 4. *a.* The condition and resulting obligation of having confidence placed in one: *violated a public trust.* *b.* One in which confidence is placed. 5. Reliance on something in the future; hope. 6. Reliance on the intention and ability of a purchaser to pay in the future; credit. 7. *Abb. tr. Law.* *a.* A legal title to property held by one party for the benefit of another. *b.* The confidence reposed in a trustee when giving the trustee legal title to property to administer for another, to-

gether with the trustee's obligation regarding that property and the beneficiary. *c.* The property so held. 8. A combination of firms or corporations for the purpose of reducing competition and controlling prices throughout a business or an industry. —**trust** *v.* **trust-ed**, **trust-ing**, **trusts.** —**intr.** 1. To have or place reliance; depend: *Trust in the Lord. Trust to destiny.* 2. To be confident; hope. 3. To sell on credit. —**tr.** 1. To have or place confidence in; depend on. 2. To expect with assurance; assume: *I trust that you will be on time.* 3. To believe: *I trust what you say.* 4. To place in the care of another; entrust. 5. To grant discretion to confidently: *Can I trust them with the boat?* 6. To extend credit to. —**idiom.** *In trust.* In the possession or care of a trustee. [Middle English *truste*, perhaps from Old Norse *troustr*, confidence. See **deru-** in Appendix.] —**trust'er** *n.*

SYNONYMS: *trust, faith, confidence, reliance, dependence.* These nouns denote a feeling of certainty that a person or thing will not fail. *Trust* implies depth and assurance of feeling that is often based on inconclusive evidence: *The new President said he would try to justify the trust the electorate had placed in him.* *Faith* connotes unquestioning, often emotionally charged belief: *"Faith and knowledge lean largely upon each other in the practice of medicine" (Peter M. Latham).* *"Often enough our faith beforehand in an uncertified result is the only thing that makes the result come true" (William James).* *Confidence*, which suggests less emotional intensity, frequently implies stronger grounds for assurance: *"Confidence is a plant of slow growth in an aged bosom: youth is the season of credulity" (William Pitt).* *Reliance* connotes a confident and trustful commitment to another: *"What reliance could they place on the protection of a prince so recently their enemy?" (William Hickling Prescott).* *Dependence* suggests reliance on the help or support of another to whom one is often subordinate: *"I fared like a distressed Prince who calls in a powerful Neighbor to his Aid . . . when I had once called him in, I could not subsist without Dependence on him" (Richard Steele).* See also **Synonyms** at **care, rely.**

trust·bust·er (trŭst'bŭs'tar) *n.* *Informal.* One that seeks to prosecute or dissolve business trusts. —**trust/bust'ing** *adj. & n.*

trust company *n.* A commercial bank or other corporation that manages trusts.

trust·ee (trŭs'tē) *n.* 1. *Abb. tr. Law.* One, such as a bank, that holds legal title to property in order to administer it for a beneficiary. 2. A member of a board elected or appointed to direct the funds and policy of an institution. 3. A country responsible for supervising a trust territory. See **Usage Note** at **-ee** 1. —**trustee** *tr. & intr.v.* -teed, -tee-ing, -tees. To place (property) in the care of a trustee or to function or serve as a trustee.

trust·ee·ship (trŭs'tē'ship) *n.* 1. The position or function of a trustee. 2. *a.* Administration of a territory by a country or countries so commissioned by the United Nations. *b.* See **trust territory**.

trust·ful (trŭst'fal) *adj.* Inclined to believe or confide readily; full of trust. —**trust/ful·ly** *adv.* —**trust/ful·ness** *n.*

trust fund *n.* Property, especially money and securities, held or settled in trust.

trust territory *n.* *Abb. TT* A colony or territory placed under the administration of a country or countries by commission of the United Nations. Also called *trusteeship*.

trust·wor·thy (trŭst'wŭr'thē) *adj.* -thi-er, -thi-est. Warranting trust; reliable. See **Synonyms** at **reliable.** —**trust/wor'thi·ly** *adv.* —**trust/wor'thi·ness** *n.*

trust·y (trŭs'tē) *adj.* -i-er, -i-est. Meriting trust; trustworthy. See **Synonyms** at **reliable.** —**trusty** *n., pl.* -ies. 1. A convict regarded as worthy of trust and therefore granted special privileges. 2. A trusted person. —**trust/i·ly** *adv.* —**trust/i·ness** *n.*

truth (trŭθ) *n., pl.* **truths** (trŭθz, trŭθs). 1. Conformity to fact or actuality. 2. A statement proven to be or accepted as true. 3. Sincerity; integrity. 4. Fidelity to an original or a standard. 5. Reality; actuality. 6. *Truth.* *Christian Science.* God. [Middle English *trewthe*, loyalty, from Old English *trēowth*. See **deru-** in Appendix.]

SYNONYMS: *truth, veracity, verity, verisimilitude.* These nouns refer to the quality of being in accord with fact or reality. *Truth* is a comprehensive term that in all of its nuances implies accuracy and honesty: *"Every man is fully satisfied that there is such a thing as truth, or he would not ask any questions" (Charles S. Peirce).* *"We seek the truth, and will endure the consequences" (Charles Seymour).* *Veracity* is adherence to the truth: *"Veracity is the heart of morality" (Thomas H. Huxley).* *Verity* often applies to an enduring or repeatedly demonstrated truth: *"beliefs that were accepted as eternal verities" (James Harvey Robinson).* *Verisimilitude* is the quality of having the appearance of truth or reality: *"merely corroborative detail, intended to give artistic verisimilitude to an otherwise bald and unconvincing narrative" (W.S. Gilbert).*

Truth, Sojourner. 1797?–1883. American abolitionist and feminist. Born into slavery, she was freed in 1827 and became a leading preacher against slavery and for the rights of women.

truth·ful (trŭθ'fal) *adj.* 1. Consistently telling the truth; honest. 2. Corresponding to reality; true. —**truth/ful·ly** *adv.* —**truth/ful·ness** *n.*

truth quark *n.* See **top quark**.

Exhibit “J”

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

LEON STAMBLER,

Plaintiff,

v.

RSA SECURITY INC., VERISIGN INC., FIRST
DATA CORPORATION, and OMNISKY
CORPORATION,

Defendants.

Civil Action No. 01-65-SLR

DEFENDANTS' OPENING MARKMAN BRIEF

RICHARDS LAYTON & FINGER, P.A.
Frederick L. Cottrell, III, Esquire
One Rodney Square
P.O. Box 551
Wilmington, DE 19899

HALE AND DORR LLP
William F. Lee
David B. Bassett
Donald R. Steinberg
Mark D. Selwyn
60 State Street
Boston, MA 02109
(617) 526-6000

TESTA, HURWITZ & THIBEAULT, LLP
John D. Lanza
Kia L. Freeman
125 High Street
Boston, MA 02110
(617) 248-7000

Attorneys for RSA Security Inc.

STAM0086530

ASHBY & GEDDES

Steven J. Balick (I.D. # 2114)
John G. Day (I.D. # 2403)
222 Delaware Avenue, 17th Floor
Wilmington, DE 19899-1150
Telephone: (302) 654-1888
Facsimile: (302) 654-2067

Thomas W. Winland
Vincent K. Kovalick
Matthew DelGiorno
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.
1300 I Street, N.W.
Washington, DC 20005-3315
Telephone: (202) 408-4000
Facsimile: (202) 408-4400

Attorneys for Defendant VERISIGN, INC.

FISH & RICHARDSON P.C.
William J. Marsden, Jr. (#2247)
919 N. Market Street, Suite 1100
P.O. Box 1114
Wilmington, DE 19899-1114
(302) 652-5070

HELLER EHRMAN WHITE & McAULIFFE LLP
Robert T. Haslam
Robert D. Fram
333 Bush Street
San Francisco, CA 94104-2878
(415) 772-6000

Attorneys for First Data Corporation

Dated: October 15, 2002

117306.1

STAM0086531

TABLE OF CONTENTS

I.	NATURE AND STAGE OF THE PROCEEDINGS	1
II.	SUMMARY OF THE ARGUMENT	1
III.	STATEMENT OF FACTS	3
	A. The Patent Specification	3
	1. Building Blocks: Symmetric Encryption	4
	2. Stambler's Check Transaction System	5
	3. Issuing and Subsequently Authenticating Credentials	7
	B. Claims 1, 16, 28, and 35 of the '148 Patent	10
	C. Claim 27 of the '541 Patent	11
	D. Claim 34 of the '302 Patent	12
	E. Claim 12 of the '302 Patent	13
IV.	ARGUMENT	14
	A. The Law of Patent Claim Construction	14
	1. The Role of Intrinsic Evidence	14
	2. The Role of Extrinsic Evidence	19
	B. Claim Constructions	20
	1. "VAN"	20
	a. A VAN Is Encrypted Using a Symmetric-Key Algorithm	22
	b. A VAN is Reversible at Least in Part So that Information in the VAN Can Be Recovered	28
	2. "Coding"	32
	a. "Coding" with Two Pieces of Information Means Applying Symmetric Encryption	35

b.	“Coding” Is Sometimes Used to Refer to Creating an Error Detection Code	38
c.	Stambler’s Proposed Construction Is So General that It Deprives the Claims of Clarity	40
3.	“Authenticating at Least One of the Parties by Using the VAN”	41
4.	“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)”	44
5.	“Secret Key”	45
6.	Information “Associated with” a Party	48
7.	“Instrument”	51
8.	“Credential”	53
a.	A “Credential” Is a Physical Item that Vouches for the Holder’s Identity	54
b.	A Credential Vouches for the Holder’s Identity	58
c.	A Credential Can Only Be Authenticated By the Issuing Entity	59
9.	“Previously Issued”	62
C.	Terms Unique to Claim 12 of the ‘302 Patent	66
1.	Background	66
2.	Proper Construction of Claim 12	68
a.	“Subsequently Granting the First Party Access to the First Storage Means”	68
b.	“Wherein The First Party Has A First Personal Identification Number (PIN1)”	71
c.	“First” and “Second” Storage Means	79
d.	“The First Storage Means Being Accessible Only to a Party with Knowledge of the First PIN1”	81

less important information is irreversibly coded and the important information is reversibly coded cannot be interpreted to mean a VAN that is not reversible at all.²⁶

2. “Coding”

“Coding” and various forms of the term (*e.g.*, “coded” and “uncoding”) are used in claim 35 of the ‘148 patent, claim 33 of the ‘302 patent, and claim 20 of the ‘541 patent. The parties have construed the term as follows:

DEFENDANTS

“Coding” has two meanings in the patent and the correct construction of “coding” is dependent on the context in which it is used:

(1) “Coding” with two separate types of information means “applying a reversible, symmetric encryption algorithm.”

(2) “Coding” to create an “error detection code,” without a specified key, means “applying an algorithm to information in such a manner that the result permits detection of changes but without complete recovery of the original information.”

PLAINTIFF

“Transforming information from one form to another”

The term “coding” does not have a uniform meaning in the patents. Stambler uses “coding” (and the variant forms of the term “coded” and “uncoding”) in two distinct ways in the asserted claims. First, he uses “coding” to mean applying a reversible, symmetric encryption algorithm. Second, he uses “coding” to describe the process for creating an “error detection code.” Symmetric encryption and error detection coding are distinct processes with distinct properties. (Tygar Decl., Ex. 2, pp. 53-54.) Applying the correct construction to “coding” is

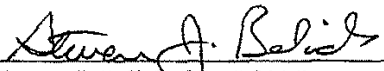
²⁶ Moreover, the definition Stambler now proposes – that any number which is “variable” and used for “authentication” is a VAN – was disclaimed in the prosecution history. During the prosecution of a related application to the patents-in-suit, Stambler expressly argued that his invention was patentable over prior art reference U.S. Patent No. 4,747,050 (Brachtel, et al.) because of the way the VAN was created. The examiner found that the only difference between the Brachtel reference and Stambler’s claimed invention was Stambler’s “use of [the] explicit terms ‘variable authentication number.’” (DelGiorno Decl., Ex. 11 (10/19/94 Office Action), p. 4; *id.*, Ex. 12 (3/23/95 Office Action), pp. 4-5.) Stambler responded by arguing that his VAN was substantively different from the Brachtel MAC because it was created using a PIN. Because the VAN was created differently, “[a]pplicant respectfully asserts that the transaction variable for each transaction [in the Brachtel reference] is not the functional equivalent of the VAN of the present invention...” (DelGiorno Decl., Ex. 8 (1/13/95 Amend.), pp. 6-7.)

V. CONCLUSION

For the reasons set forth above, the Defendants respectfully request that the Court construe the asserted claims as set forth by Defendants in this brief.

ASHBY & GEDDES

Dated: October 15, 2002


Steven J. Balick (I.D. # 2114)
John G. Day (I.D. # 2403)
222 Delaware Avenue, 17th Floor
P.O. Box 1150
Wilmington, DE 19899
302-654-1888

Attorneys for Defendant VeriSign Inc.;
Submitted On Behalf of Defendants
RSA Security Inc., VeriSign Inc., and
First Data Corporation

Exhibit “K”

MICROSOFT PRESS®

COMPUTER DICTIONARY



THE COMPREHENSIVE
STANDARD FOR
BUSINESS, SCHOOL,
LIBRARY, AND HOME

Microsoft
P R E S S

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Copyright © 1991 by Microsoft Press, a division of Microsoft Corporation.

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Library of Congress Cataloging-in-Publication Data
Microsoft Press computer dictionary : the comprehensive standard for business, school, library, and home.

p. cm.

ISBN 1-55615-231-0

1. Computers--Dictionaries. 2. Microcomputers--Dictionaries.

I. Microsoft Press.

QA76.15.M54 1991

004.16'03--dc20

91-9904
CIP

Printed and bound in the United States of America.

4 5 6 7 8 9 MLML 6 5 4 3 2

Distributed to the book trade in Canada by Macmillan of Canada, a division of Canada Publishing Corporation.

Distributed to the book trade outside the United States and Canada by Penguin Books Ltd.

Penguin Books Ltd., Harmondsworth, Middlesex, England

Penguin Books Australia Ltd., Ringwood, Victoria, Australia

Penguin Books N.Z. Ltd., 182-190 Wairau Road, Auckland 10, New Zealand

British Cataloging-in-Publication Data available.

Acquisitions Editor: Marjorie Schlaikjer

Project Editor: Mary Ann Jones

Technical Editors: David Rygmyr, Jeff Hinsch, Mary DeJong, Dail Magee, Jr.

Manuscript Editor: Pamela Beason

Copy Editor: Alice Copp Smith



automatically; recording and executing login procedures; and repeatedly dialing busy lines. Once a connection is made, communications programs can also be instructed to save incoming messages on disk or to find and transmit disk files. During communication, communications programs perform the major, and usually invisible, tasks of encoding data, coordinating transmissions to and from the distant computer, and checking incoming data for transmission errors.

communications protocol A set of rules or standards designed to enable computers to connect with one another and to exchange information with as little error as possible. The protocol generally accepted for standardizing overall computer communications is a seven-layer set of hardware and software guidelines known as the OSI (Open Systems Interconnection) model. A somewhat different standard, widely used before the OSI model was developed, is IBM's SNA (Systems Network Architecture). However, protocols exist within protocols, all affecting different aspects of communication. Thus, the word *protocol* is used, sometimes confusingly, in reference to a multitude of standards affecting different aspects of communication. Some, such as the RS-232-C standard, affect hardware connections. Other standards govern data transmission; among these are the parameters and handshaking signals (such as XON/XOFF) used in asynchronous (typically, modem) communications, as well as such data-coding methods as bit-oriented and byte-oriented protocols. Still other protocols, such as the widely used XMODEM, govern file transfer, and others yet, such as CSMA/CD, define the methods by which messages are passed around the stations on a local area network. Taken as a whole, these various and sometimes conflicting protocols represent attempts to ease the complex process of enabling computers of different makes and models to communicate.

communications satellite A satellite stationed in geosynchronous orbit (seemingly stationary in relation to the earth) that acts as a microwave relay station, receiving signals sent from a ground-based station (earth station), amplifying them, and retransmitting on a different frequency to another

ground-based station. Transmission to the satellite is called the uplink; transmission to the ground is the downlink. Communications satellites are capable of handling immense volumes of information. Initially used for telephone and television signals, communications satellites can also be used for high-speed transmission of computer data. Two factors affecting the use of satellites with computers, however, are propagation delay (the time lag caused by the distance traveled by the signal) and security concerns.

communications server A type of gateway that translates packets on a local area network (LAN) into asynchronous signals, such as those used on telephone lines or in RS-232-C serial communications, and allows all nodes on the LAN access to its modems or RS-232-C connections. *See also* gateway.

communications system The combination of hardware, software, and data-transfer links that make up a communications facility.

compact disc Abbreviated CD. Also called an optical disc. A nonmagnetic, polished metal disk used to store digital information. The disk is read by an optical scanning mechanism that uses a high-intensity light source, such as a laser, and mirrors. *See also* CD-ROM.

compact disc-interactive *See* CD-I.

compact disc player Also called a CD player. A device that reads the information stored on a compact disc. A CD player contains the optical equipment to read the disc's contents and the electronic circuitry for interpreting the data as it is read.

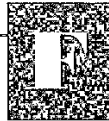
compaction A process that gathers and packs the currently allocated regions of memory or auxiliary storage into as small a space as possible, so as to create as much continuous free space as possible. *Compare* dispersion, file fragmentation.

compact model A memory model of the Intel 80x86 processor family. The compact model allows only 64 kilobytes (KB) for the code of a program but up to 1 megabyte (MB) for the program's data. *See also* memory model.

comparator A device for comparing two items to determine whether they are equal. In electronics, a comparator is a circuit that compares two input

lator

flip-flop



floppy-disk drive

archi-
have
direc-
), an
stem,
stem
ul file

rect-
g the
cur-
pare
ech-

flow
the
ally
flat-
play,

age,
oc-
in-
re a
ter-
the
ter-
ron
dd-
red
ted
be
r to
nes

ion
ght
ars
cy
es
er-
tic
in

flip-flop Also called bistable multivibrator. A circuit that changes between two possible states when a pulse is received at the input. For example, the output of a flip-flop might be high until a pulse is received at the input, at which time it "flips" to low. A second input pulse "flops" the output back to high, and so on.

flippy-floppy A type of floppy disk, such as that used in the Apple II, that uses both sides for storage but that must be physically removed from the drive and "flipped" over because the drive can read only one side at a time. The user can turn a double-sided disk into a flippy-floppy by cutting an extra write-protect notch on the side opposite the original one. This practice is not generally approved of by disk and disk-drive manufacturers, however, because the felt pad that rides on the disk surface opposite the single read/write head can damage data on that side of the disk.

floating-point arithmetic Arithmetic performed on floating-point numbers.

floating-point constant A constant representing a real, or floating-point, value. *See also* constant, floating-point notation.

floating-point notation Also called exponential notation. A numeric format that can be used to represent very large numbers and very small numbers. Floating-point numbers are stored in two parts, a mantissa and an exponent. The mantissa specifies the digits in the number, and the exponent specifies the magnitude of the number (the position of the decimal point). For example, the numbers 314600000 and .0000451 are expressed respectively as 3146E5 and 451E-7 in floating-point notation. Most microprocessors don't directly support floating-point arithmetic; consequently, floating-point calculations are performed either by using software or with a special floating-point processor. *See also* fixed-point notation, integer.

floating-point operation Abbreviated FLOP. An operation that performs arithmetic on data formatted as a normalized signed decimal number followed by a signed exponent. For example, the number 2,147,483 is formatted as 2.147483+E6. Floating-point calculations are commonly used in spreadsheet and computer-aided design (CAD)

operations. The term is also used as a measurement of computer performance: Computers are commonly rated in terms of how many megaflops (millions of floating-point operations per second, or MFLOPS) they are capable of performing. The presence of a "floating-point processor" chip in a system (such as the 80287 for machines based on the 80286 microprocessor, or the 68881 for machines based on the 68030 microprocessor) dramatically increases the number of floating-point operations a machine can perform in a given unit of time. *See also* floating-point notation, MFLOPS.

floating-point processor Also called a numeric coprocessor, a math coprocessor, and a floating-point unit. A coprocessor (processor additional to the main system microprocessor) that performs calculations using floating-point numbers, as opposed to integers (whole numbers). Adding a floating-point processor to a system can speed up math and graphics functions (graphics work is generally math-intensive) dramatically with programs that are designed to recognize and use it. Except for the Intel 80486 and the Motorola 68040, both the Intel 80x86 and the Motorola 680x0 families of microprocessors have companion floating-point processors.

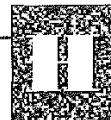
FLOP *See* floating-point operation.

floppy disk A round, flat piece of Mylar coated with ferric oxide, a rustlike substance containing tiny particles capable of holding a magnetic field, and encased in a protective plastic cover, the disk jacket. Data is stored on a floppy disk by the disk drive's read/write head, which alters the magnetic orientation of the particles. Orientation in one direction represents binary 1; orientation in the other, binary 0. Typically, a floppy disk is 5.25 inches in diameter, with a large hole in the center that fits around the spindle in the disk drive. Depending on its capacity, such a disk can hold from a few hundred thousand to over one million bytes of data. A 3.5-inch disk encased in rigid plastic is usually called a microfloppy disk but can also be called a floppy disk. *See also* microfloppy disk.

floppy-disk controller *See* disk controller.

floppy-disk drive An electromechanical device that reads data from and writes data to floppy or microfloppy disks. *See also* floppy disk.

handler



hard disk

to move or reshape the image.

handler A routine that manages a common and relatively simple condition or operation, such as error recovery or data movement. In certain object-oriented programming languages that support messages (such as HyperTalk), *handler* is the name for what is normally called a subroutine (a message handler). *See also* message, object-oriented programming.

handshake As in human relations, a signal acknowledging that communication or the transfer of information can take place. Handshakes can be controlled by either hardware or software. A hardware handshake, as between a computer and a printer or a modem, is an exchange of signals, over specific wires, in which each device signals its readiness to send or receive data. A software handshake, usually exchanged during modem-to-modem types of communication, consists of actual information transmitted between the sending and receiving devices. A software handshake establishes agreement between devices on the protocols that both will use in communicating. A hardware handshake is thus similar to two people physically clasping hands; a software handshake is more akin to those parties agreeing to converse in a particular language.

hands-on An adjective describing practical experience as opposed to theoretical knowledge. In computer terminology, the term refers to interactive work with a computer or computer program. For example, a hands-on tutorial might teach a program or a skill by means of practice sessions and question-and-answer dialogues.

handwriting recognition The ability of a computer to recognize handwriting, especially a signature, as a means of identifying the user; also, the ability to translate handwritten text—from paper or a special tablet—into data for processing and storage. Because of variations in even a single individual's handwriting, few computer applications using handwriting recognition are available at the present time.

hang An unexpected halt of a computer system, usually while running an application program. A hung machine is characterized by a total lack of re-

sponse from any input device, and the user can almost never effect a recovery except by turning the computer off and restarting it. The difference between a hang and a crash is mostly visual: In a hung system, the screen looks as if it is functioning properly, whereas in a crashed system, the screen might be blank or display erratic characters or an error message. A hung machine is also referred to as *locked up*.

hanging indent Sometimes called an outdent; a format in which the first line of a paragraph or block of text is placed farther to the left than the subsequent lines. *Compare* indent.

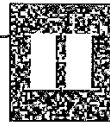
hard In computing, an adjective meaning permanent, fixed, or physically defined—for example, hard copy, which is printed output; a hard error, which is a recurrent problem, often associated with equipment malfunction that usually allows no recovery; a hard-sectored disk, on which storage units (sectors) are defined by holes punched into the disk or nonerasable magnetic marks; and a hard return, which is a permanent end-of-line character inserted by pressing the Enter or Return key. *Hard* is the opposite of *soft*, which is used in reference to things that are transient or changeable.

In electronics, an adjective referring to magnetic materials that retain their magnetism even when removed from a magnetic field.

hard-coded An adjective describing a routine or program that is designed for a specific situation or that uses embedded constants in place of more general user input. In some senses, *hard-coded* is the opposite of *generalized*.

hard copy Printed output on paper, film, or other permanent media. Its opposite is *soft copy*, the electronic version of information on a floppy disk, hard disk, CD-ROM disk, tape, display, or other ephemeral medium.

hard disk One or more inflexible platters coated with material that allows the magnetic recording of computer data. A typical hard disk rotates at 3600 RPM (revolutions per minute), and the read/write heads ride over the surface of the disk on a cushion of air 10 to 25 millionths of an inch deep. A hard disk is sealed to prevent contaminants from interfering with the close head-to-disk tolerances. Hard



user can
turning
fference
ual: In a
ctioning
e screen
ers or an
ferred to

ident; a
graph or
than the

; perma-
example,
rd error,
ated with
lows no
a storage
hed into
nd a hard
character
ey. *Hard*
reference

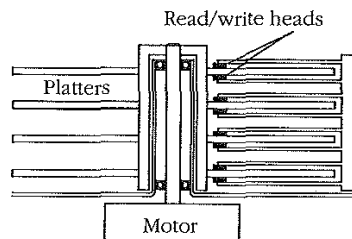
magnetic
en when

outline or
uation or
of more
!-coded is

, or other
copy, the
ppy disk,
or other

rs coated
cording of
es at 3600
ead/write
a cushion
p. A hard
rom inter-
nces. Hard

disks provide faster access to data than floppy disks and are capable of storing much more information. Because platters are rigid, they can be stacked so that one hard-disk drive can access more than one platter. Most hard disks have from two to eight platters. See the illustration.



Hard disk.

The interior of a hard-disk drive.

hard error An error caused by a hardware failure or by accessing incompatible hardware; also, any error that prevents a program from continuing an operation. *Compare* soft error; *see also* fatal error, hard failure.

hard failure Also called hardware failure. A cessation of function from which there is no recovery. Correcting a hard failure usually requires a call to a repairperson.

hard hyphen *See* hyphen.

hard return A signal to a program that the cursor (or printer) is to move to the beginning of a new line. In word-processing programs, which automatically break lines within the margins of a page, hard returns are used to end paragraphs. In text-entry programs that lack wordwrap, a hard return is required to end each line. Because they can have slightly different meanings to different programs, hard returns can cause unusual line breaks or extra line spacing in documents transferred from one program to another. *Compare* soft return; *see also* wordwrap.

hard-sectored disk A floppy disk whose data sectors have been physically marked with punched holes. The holes are detected by sensors when the disk drive is in operation, enabling the drive to locate the beginning of each sector. Hard-sectored

disks, the product of an older technology, are less commonly used than soft-sectored disks. *Compare* soft-sectored disk.

hardware The physical components of a computer system, including any peripheral equipment such as printers, modems, and mice. *Compare* firmware, software.

hardware check An automatic check performed by hardware to detect internal errors or problems—for example, in transferring data from one point to another.

hardware-dependent An adjective describing programs, languages, or computer components and devices that are tied to a particular computer system or configuration. Assembly language, for example, is hardware-dependent because it is created for and works only with a particular make or model of microprocessor.

hardware failure *See* hard failure.

hardware interrupt A type of interrupt (request for service) generated either externally by hardware devices such as the keyboard, disk drive, and input/output ports or internally by the microprocessor. External hardware interrupts are used by devices to request attention from a computer's microprocessor. Internal hardware interrupts are generated by microprocessors, such as those in IBM and compatible computers, to control events (for example, to report a program's attempt to divide by zero—an illegal action). Hardware interrupts can occur at random, as when characters are received from the keyboard, or they can occur predictably, as is the case with the computer's timer. Because the microprocessor must have some means of distinguishing between urgent and nonurgent requests, hardware interrupts are assigned levels of priority. The highest priority is given to a type of interrupt called a nonmaskable interrupt—one that indicates a serious error, such as a memory failure, that must be serviced immediately. *See also* external interrupt, interrupt.

hardware key A physical device used to secure a computer system from unauthorized use. For example, the key on the front of the IBM PC/AT computer not only prevents the computer's cover from being removed but also disables the computer's

etic disk

magnetic domain



main loop

e value of

r can then
,b" in the
nbling, the
the state-
lues of the

ibstitution.
fined equi-
) results in
cro, macro

to manage
ember that
t of macro
recognize
dm, for ex-
ize the in-
age.
cro instruc-
cessor. For
nstructions
also macro

orms macro
nacros have
these differ
macro lan-
or is (among
or. See also
ction.

er.
ls and stores

sion.
emory tech-
lacement for
long access
ecialized ap-
also bubble

sed in a pro-
py disk) and
permits flux
; (magnetic

domains) of the disk surface. Flux changes are changes in magnetic polarity and are used to encode information in binary form (one polarity equals 1, the opposite equals 0). The changes are produced at high speed by the read/write head of the disk drive as it passes over the surface of the disk. Because of its properties, a computer disk should be protected from exposure to sources of magnetism, which can damage or destroy the information it holds.

magnetic domain Also called ferromagnetic domain. A region of a ferromagnetic material in which the individual atomic or molecular magnetic particles are aligned in the same direction.

magnetic field The space around a magnetic object in which magnetic force acts. A magnetic field is conceived of as consisting of flux lines that originate at the north magnetic pole and terminate at the south magnetic pole. A magnetic field can be made visible by putting a sheet of paper over a magnet and sprinkling iron filings on the paper—the filings will line up along the flux lines.

magnetic head See head.

magnetic-ink character recognition Commonly abbreviated MICR, pronounced "mike-er." A form of character recognition that reads text printed with magnetically charged ink, determining the shapes of characters by sensing the magnetic charge in the ink. Once the shapes have been determined, character recognition methods—pattern matching with stored sets of characters—are used to translate the shapes into computer text. The numbers at the bottom of bank checks are usually printed with magnetic ink. *Compare* optical character recognition; *see also* character recognition.

magnetic oxide See ferric oxide.

magnetic storage A generic term for non-internal-memory computer data storage involving a magnetic medium, such as disk or tape.

magnetic tape See tape.

magneto-optical recording A type of recording technology used with optical discs in which a laser beam heats a small portion of the magnetic material covering the disc. The heating enables a weak magnetic field to change the orientation of the portion, thus recording onto the disc. This technique

can be used to erase the disc, making the disc rewritable.

magneto-optic disc An erasable or semi-erasable storage disc, similar to a CD-ROM disc and of very high capacity, in which a laser beam is used to heat the recording surface to a point at which tiny regions on the surface can be magnetically aligned to store bits of data. *See also* CD-ROM.

magnitude The size of a number, regardless of its sign (+ or -). For example, 16 and -16 have the same magnitude. *See also* absolute value.

mailbox A disk storage area assigned to a network user for receipt of electronic mail messages.

mail merge A mass-mail facility that takes names, addresses, and (sometimes) pertinent facts about recipients and merges the information into a form letter or another such basic document.

main body The set of statements in a computer program at which execution of the program begins and from which execution branches to the subroutines of the program. Most programming languages require programs to have a main body. Execution begins with the first statement in the main body; it usually ends when the last statement in the main body has finished executing, although it can end earlier.

mainframe computer A high-level computer designed for the most intensive computational tasks. Mainframe computers are often shared by multiple users connected to the computer via terminals. The most powerful mainframes, called supercomputers, perform highly complex and time-consuming computations and are used heavily in both pure and applied research by scientists, large businesses, and the military. *See also* computer.

main function The main body of a program written in a computer language that uses sets of functions to create an entire program. For example, the C language requires each program to contain a function called *main*, which C uses as the starting point of execution. *See also* main body.

main loop A loop in the main body of a program that performs the principal function of the program over and over until termination is somehow signaled. In event-driven programs, this loop checks for events received from the operating system and

ragged left/right



raster display

and other documents are commonly left-justified, with ragged-right margins (as in the example on the left). Ragged-left text is used infrequently—typically, in advertisements—for visual effect.

ragged left/right See rag.

RAM Pronounced “ram.” Acronym for random access memory. Semiconductor-based memory that can be read and written by the microprocessor or other hardware devices. The storage locations can be accessed in any order. Note that the various types of ROM memory are capable of random access. The term *RAM*, however, is generally understood to refer to volatile memory, which can be written as well as read. Compare core, EPROM, PROM, ROM.

RAM card An add-in circuit board containing RAM memory and the interface logic necessary to decode memory addresses.

RAM cartridge See memory cartridge.

RAM chip A semiconductor storage device. RAM chips can be either dynamic or static memory. See also dynamic RAM, static RAM.

RAM disk A simulated disk drive whose data is actually stored in RAM memory. A special program fools the operating system into believing that an additional disk drive is present. The operating system reads and writes to the simulated device, and the program stores and retrieves data from memory. RAM disks are extremely fast, but they require that system memory be given up for their use. Also, RAM disks usually use volatile memory, so the data stored on them disappears when power is turned off. Many portables offer RAM disks that use battery-backed CMOS RAM to avoid this problem. Compare disk cache; see also CMOS RAM.

RAM refresh See refresh.

RAM-resident program See terminate-and-stay-resident program.

random access Also called direct access. The ability of a computer to find and go directly to a particular storage location without having to search sequentially from the beginning location. With microcomputers, the term is often encountered in reference to a computer's memory, in which certain general locations are reserved for different types of information (applications, operating system, and so

on) but specific items can be located directly through the use of numbers (addresses) that identify individual locations in memory. The term is also used to describe access to files stored on disk. This type of access is best used for files in which each set of information has no intrinsic relationship to what comes before or after it, such as in databases of client records, inventories, and so on. The human equivalent of random access would be the ability to find a desired address in an address book without having to proceed sequentially through all the addresses. Compare indexed sequential access method, sequential access.

random access memory See RAM.

random noise A signal in which there is no relationship between amplitude and time and in which many frequencies occur randomly, without pattern or predictability.

random number generation The creation of a number or sequence of numbers characterized by unpredictability so that no number is any more likely to occur at a given time or place in the sequence than any other. Because truly random number generation is generally viewed as impossible, the process would be more properly called “pseudorandom number generation.”

range In a spreadsheet, a block of cells selected for similar treatment. A range of cells can extend across a row, down a column, or over a combination of the two, but all cells in the range must be contiguous, sharing at least one common border. Ranges allow the user to affect many cells with a single command—for example, to format them similarly, enter the same data into all of them, give them a name in common and treat them as a unit, or select and incorporate them into a formula.

In more general usage, *range* refers to the spread between specified low and high values. Range checking is an important method of validating data entered into an application.

raster A rectangular pattern of lines; on a video display, the horizontal scan lines from which the term *raster scan* is derived.

raster display A video monitor (generally a CRT) that displays an image on the screen from top to bottom as a series of horizontal scan lines. The scan



computers. *See also* robotics.

robotics The branch of engineering devoted to the creation and training of robots. Roboticians work within a wide range of fields, such as mechanical and electronic engineering, cybernetics, bionics, and artificial intelligence, all toward the end of endowing their creations with as much sensitivity, independence, and flexibility as possible. *See also* artificial intelligence, bionics, cybernetics.

robustness Soundness; the ability of a program to function, or to continue functioning well, in unexpected situations.

rollback A return to a previous stable condition, as when the contents of a hard disk are restored from a backup after a destructive hard-disk error.

ROM Rhymes with "bomb"; acronym for read-only memory. Semiconductor-based memory that contains instructions or data that can be read but not modified. To create a ROM chip, the designer supplies a semiconductor manufacturer with the instructions or data to be stored; the manufacturer then produces one or more chips containing those instructions or data. Because creating ROM chips involves a manufacturing process, it is economically viable only if the ROM chips are produced in large quantities; experimental designs or small volumes are best handled using PROM or EPROM. In general usage, the term *ROM* often means any read-only device, including PROM and EPROM. *See also* EEPROM, EPROM, PROM.

roman An adjective describing a typeface or type style in which the characters are upright. *Compare* italic; *see also* font family.

ROM BASIC A version of interpreted BASIC stored in ROM (read-only memory). Many early home computers from companies such as Apple, Atari, Commodore, and Texas Instruments contained versions of BASIC in ROM so that the user could start programming by simply turning on the machine (versus having to load BASIC from a disk or cassette tape first).

ROM BIOS Acronym for read-only memory basic input/output system. A set of software routines shipped with IBM and compatible computers, providing low-level routines for performing simple input/output operations. In the IBM PC, the BIOS

takes up 64 kilobytes (KB) of address space, beginning at location 0F0000H. In the PS/2 series, the BIOS is expanded to 128 KB, beginning at location 0E0000H. For both the IBM PC and PS/2, the ROM BIOS also includes that portion of the BASIC interpreter—commonly called cassette BASIC—that does not provide disk support or support for advanced graphics. *Compare* Toolbox; *see also* BIOS.

ROM card A plug-in module that contains one or more printer fonts, programs, or games or other information stored in ROM (read-only memory). A typical ROM card is about the size of a credit card and about three times as thick. It stores information directly on integrated circuit boards. *See also* ROM, ROM cartridge.

ROM cartridge A plug-in module that contains one or more printer fonts, programs, games, or other information stored in ROM (read-only memory). The ROM is in the form of one or more computer chips mounted on a printed circuit board. The board is enclosed in a plastic case with a connector exposed at one end so that it can easily plug into a printer, computer, game system, or other device. For example, a cartridge that plugs into a Nintendo or similar game system is a ROM cartridge. *See also* ROM, ROM card.

ROM emulator Also called ROM simulator. A special circuit containing RAM memory that is connected to a target computer where the target computer's ROM chips would normally be installed. The contents of the RAM memory are supplied by a separate computer; after the RAM chips are programmed, they are used as ROM in the target computer. Before the advent of EPROMs, using a ROM emulator was the only economical way to debug ROM-resident software owing to the high cost of creating ROM chips. Today, an EPROM can be used in the prototype circuit and replaced with a ROM when the software is completed. Because a ROM emulator's memory contents can be changed much more quickly than those of an EPROM, developers often prefer using a ROM emulator even though doing this is more expensive than programming an EPROM. *See also* EEPROM, EPROM, ROM.

root The main or uppermost level in a hier-

stochastic



strikethrough

actuator arm from one track to the next. The term derives from the use of a stepper motor to move the actuator arm. *See also* stepper motor.

stochastic Based on chance (random) occurrences. For example, a stochastic model attempts to describe a system by taking into account random events as well as planned events.

stop bit In asynchronous transmission, a bit that signals the end of a character. Depending on the conventions used, the data bits composing the character can be followed by 1, 1.5, or 2 stop bits.

storage In computing terms, any physical device in or on which computer information can be kept. A microcomputer has two main types of storage. Its random access memory (RAM) represents temporary storage that the microprocessor uses for programs, work in progress, and various types of internal work-control information. The computer's disk drives and other external storage media represent facilities for holding information on a more permanent basis, available but out of the way until it is needed by the microprocessor. A computer has other types of storage as well. Its read-only memory (ROM) is a permanent, nonerasable medium for holding necessary information, including startup instructions and input/output procedures. In addition, a computer uses various buffers—reserved areas of memory—as temporary holding areas designated for specific information, such as characters to be sent to the printer or characters being read from the keyboard.

storage device Any apparatus for recording computer data in permanent or semipermanent form. A disk drive, along with the disks it records on, is a storage device.

Sometimes a computer is said to have primary (or main) and secondary (or auxiliary) storage devices. When this distinction is made, the primary storage device is the computer's random access memory (RAM)—impermanent, but a storage device nevertheless, however temporary its contents. The secondary storage includes the computer's more permanent storage devices, such as disk and tape drives.

storage location The position at which a particular item can be found. A storage location can be an

addressed (uniquely numbered) location in memory or it can be a uniquely identified location on disk, tape, or a similar medium—for example, a particular side, track, and sector on a disk.

storage media The various types of physical material on which data bits are written and stored. Common storage media for computer data are floppy disks, hard disks, tape, optical discs, and (for output only) paper.

storage tube *See* direct view storage tube.

store-and-forward A message-passing technique used on communications networks in which a message is held temporarily at a “collecting” station between the sender and receiver before being forwarded to its intended destination. Store-and-forward message routing can take longer than communication via direct, physical connections, but it offers several advantages, especially over large networks separated by long distances: It minimizes or eliminates “traffic jams” and thus contributes to effective use of communications lines; it allows messages to be sent to machines or networks even when they are not on line; and it enables transmission during off hours, when traffic or costs are lowest.

stored program concept The underlying concept of most system architectures today, credited largely (although not exclusively) to John von Neumann. The concept is that both programs and data are in direct access storage (random access memory, or RAM), allowing code and data to be treated interchangeably (including modifications to both) and avoiding the timing problems involved when code is located on a sequential storage medium (as was the case in many early computers). *See also* von Neumann architecture.

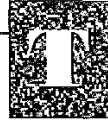
straight-line code Program code that follows a direct sequence of statements, rather than skipping ahead or jumping back via transfer statements such as GOTO, JUMP, and so on. *Compare* spaghetti code; *see also* GOTO statement.

streaming tape *See* tape.

stream-oriented file A file used to store a more-or-less-continuous series of bits, bytes, or other small, structurally uniform units.

strikethrough One or more lines drawn through a

tandem processors



teleprocessing

one or several key fields for the purpose of establishing the order of their associated records.

tandem processors Multiple processors wired so that the failure of one processor transfers CPU operation to another processor. Using tandem processors is part of the strategy for implementing fault-tolerant computer systems.

tape A thin strip of Mylar coated with magnetic material that permits the recording of data. To use a tape, a machine must have two reels between which the tape can pass, with a read/write head located somewhere between the reels. Because tape is a continuous length of data storage material and because the read/write head cannot "jump" to a desired point on the tape without the tape first being advanced to that point, tape must be read or written sequentially, not randomly (as is a floppy or a hard disk).

tape cartridge A module, somewhat resembling an audio cassette, that contains magnetic tape that can be written on and read from by a tape drive. Tape cartridges are primarily used to back up hard disks.

tape drive A device for reading and writing tapes. *See also* tape.

target Loosely, the objective of a computer command or operation. Examples are a computer that is to run a program translated for its use; a "foreign" language (for another computer) into which a program is to be translated; or a group of people for whom a particular product is designed. In specific usage, as often seen by users of MS-DOS, the target is the disk referred to by prompts displayed by the operating system in a copy operation (for example, "insert TARGET diskette"). In terms of the SCSI (small computer system interface) connection, the target is the device that receives commands; the device that issues commands is the initiator.

target computer The computer that receives data from a communications device, a hardware add-in, or a software package.

target disk Usually, the disk that is the destination of a copy operation. When disks are being copied, one disk is the source disk and the other is the target disk. The term can also refer to a disk to which data is to be written. *Compare* source disk.

target language The language into which source

code is compiled or assembled. *See also* assembler, compiler, cross-compiler.

task A stand-alone application or a subprogram that is run as an independent entity.

task management The operating-system process of tracking the progress of and providing necessary resources for separate tasks running on a computer, especially in a multitasking environment.

TB *See* terabyte.

TCM *See* trellis-coded modulation.

TCP/IP Acronym for Transport Control Protocol/Interface Program, a software protocol developed by the Department of Defense for communications between computers.

TDM *See* time-division multiplexing.

technology The application of science and engineering to the development of machines and procedures in order to enhance or improve human conditions, or at least to improve human efficiency in some respect. *See also* high tech.

telecommunications A general term for the electronic transmission of information of any type, including data, television pictures, sound, facsimiles, and so on.

telecommuting Also called electronic commuting. The practice of working in one location (often, at home) and communicating with a main office in a different location through a personal computer equipped with a modem and communications software.

teleconferencing The use of audio, video, or computer equipment linked through a communications system to enable geographically separated individuals to participate in a meeting or discussion.

telecopying *See* fax.

telematics From the French *télématique*; a term used in communications for the combination of computers and telecommunications.

telephony Telephone technology; the conversion of sound into electrical signals, its transmission to another location, and its reconversion to sound, with or without the use of connecting wires.

teleprocessing A term originated by IBM; the use of a terminal or computer and communications equipment to access computers and computer files located elsewhere.

Exhibit “L”

THE CHICAGO MANUAL OF STYLE

*The Essential Guide for
Writers, Editors, and
Publishers*

15th edition

The University of Chicago Press, Chicago 60637
The University of Chicago Press, Ltd., London
© 1982, 1993, 2003 by The University of Chicago
All rights reserved. Published 2003
First edition published 1906. Thirteenth edition 1982. Fourteenth edition 1993. Fifteenth
edition 2003.
Printed in the United States of America

12 11 10 09 08 07 06 05 04 03 1 2 3 4 5

ISBN: 0-226-10403-6 (CLOTH)

Library of Congress Cataloging-in-Publication Data

The Chicago manual of style. — 15th ed.
p. cm.

Includes bibliographical references and index.

ISBN 0-226-10403-6 (alk. paper)

1. Printing—Style manuals. 2. Authorship—Style manuals.

Z253 .U69 2003

808'.027'0973—dc21

2003001860

© The paper used in this publication meets the minimum requirements of the American
National Standard for Information Sciences—Permanence of Paper for Printed Library
Materials, ANSI Z39.48-1992.

www.chicagomanualofstyle.org

5.108 | GRAMMAR AND USAGE

Participles and Gerunds

5.108 *Forming participles.* Two participles are formed from the verb stem: the present participle invariably ends in *ing*, and the past participle usually ends in *ed*. The present participle denotes the verb's action as in progress or incomplete at the time expressed by the sentence's principal verb {watching intently for a mouse, the cat settled in to wait} {hearing his name, Jon turned to answer}. The past participle denotes the verb's action as completed {planted in the spring} {written last year}.

5.109 *Participial phrases.* A participial phrase is made up of a participle plus any closely associated word or words, such as modifiers or complements. It can be used (1) as an adjective to modify a noun or pronoun {nailed to the roof, the slate will stop the leaks}, or (2) as an adverb to modify the predicate, or any adverb or adjective in the predicate {she will succeed, persevering despite discouragement} {she pointed to the chef drooping behind the counter}. For more on participial adjectives, see 5.68, 5.84.

5.110 *Gerunds.* A gerund is a present participle used as a noun. Being a noun, the gerund can be used as (1) the subject of a verb {complaining about it won't help}; (2) the object of a verb {I don't like your cooking}; (3) a predicate nominative or complement {his favorite hobby is sleeping}; or (4) the object of a preposition {reduce erosion by terracing the fields}.

Properties of Verbs

5.111 *Five properties.* A verb has five properties: voice, mood, tense, person, and number.

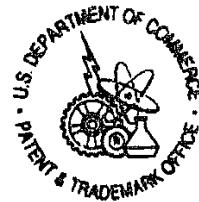
5.112 *Active and passive voice.* Voice shows whether the subject acts (active voice) or is acted on (passive voice)—that is, whether the subject performs or receives the action of the verb. Only transitive verbs are said to have voice. The clause *the judge levied a \$50 fine* is in the active voice because the subject (*judge*) is acting. But *the tree's branch was broken by the storm* is in the passive voice because the subject (*branch*) does not break itself—it is acted on by the object (*storm*). The passive voice is always formed by joining an inflected form of *to be* (or, in colloquial usage, *to get*) with the verb's past participle. Compare *the ox pulls the cart* (active voice) with *the cart is pulled by the ox* (passive voice). A passive-voice verb in a subordinate clause often has an implied *be*: in *the advice given by the novelist*, the implied (or understood) words *that was* come before *given*; so the passive construction is *was given*. Although the inflected form of *to be* is sometimes implicit, the past participle must always appear. Sometimes the agent remains unnamed

Exhibit “M”

Manual of PATENT EXAMINING PROCEDURE

Original Sixth Edition, January 1995

Latest Revision July 1997



U.S. DEPARTMENT OF COMMERCE
Patent and Trademark Office

Rev. 3, July 1997

U.S. DEPARTMENT OF COMMERCE
Patent and Trademark Office
Washington, D.C. 20231

MANUAL OF PATENT EXAMINING PROCEDURE
Sixth Edition

Instructions Regarding Revision No. 3

This revision consists of replacement pages for the **Title Page, the Forward, and the Introduction** in the front of the Manual; **entire Chapters 100 through 1000, 1200 through 1400, 1600 through 1900, 2100, 2200, 2400 and 2500, Appendices I - Partial List of Trademarks, II- List of Decisions Cited, L- Patent Laws, and R - Patent Rules, and entire Index.**

Pages which have been printed in this revision are labeled as "**Rev. 3**" on the bottom. Sections of the Manual which have been changed by this revision are indicated by "**[R-3]**" after the section title.

Additions to the text of the Manual are indicated by arrows (><) inserted in the text. Deletions are indicated by a single asterisk (*) where a single word was deleted and by two asterisks (**) where more than one word was deleted. The use of three or five asterisks in the body of the laws and rules indicates a portion of the law or rule which was not reproduced.

Magdalen Y. C. Greenlief, Editor
Manual of Patent Examining Procedure

Rev. 3, July 1997

Chapter 600 Parts, Form, and Content of Application

601	Content of Provisional and Nonprovisional Applications	605.04(f)	Signature on Joint Applications — Order of Names
601.01	Complete Application	605.04(g)	Correction of Inventorship
>601.01(a)	Nonprovisional Applications Filed Under 35 U.S.C. 111(a)	605.05	Administrator, Executor, or Other Legal Representative
601.01(b)	Provisional Applications Filed Under 35 U.S.C. 111(b)	605.07	Joint Inventors
601.01(c)	Conversion to a Provisional Application	606	Title of Invention
601.01(d)	Application Filed Without All Pages of Specification	606.01	Examiner May Require Change in Title
601.01(e)	Nonprovisional Application Filed Without at Least One Claim	607	Filing Fee
601.01(f)	Applications Filed Without Drawings	607.02	Returnability of Fees
601.01(g)	Applications Filed Without All Figures of Drawings	608	Disclosure
601.01(h)	Forms	608.01	Specification
601.02	Power of Attorney or Authorization of Agent	608.01(a)	Arrangement of Application
601.03	Change of Correspondence Address	608.01(b)	Abstract of the Disclosure
601.04	National Stage Requirements of the United States as a Designated Office	608.01(c)	Background of the Invention
602	Original Oath or Declaration	608.01(d)	Brief Summary of Invention
602.01	Oath Cannot Be Amended	608.01(e)	Reservation Clauses Not Permitted
602.02	New Oath or Substitute for Original	608.01(f)	Brief Description of Drawings
602.03	Defective Oath or Declaration	608.01(g)	Detailed Description of Invention
602.04	Foreign Executed Oath	608.01(h)	Mode of Operation of Invention
602.04(a)	Foreign Executed Oath Is Ribbioned to Other Application Papers	608.01(i)	Claims
602.05	Oath or Declaration — Date of Execution	608.01(j)	Numbering of Claims
602.05(a)	Oath or Declaration in Division and Continuation Cases	608.01(k)	Statutory Requirement of Claims
602.06	Non-English Oath or Declaration	608.01(l)	Original Claims
602.07	Oath or Declaration Filed in United States as a Designated Office	608.01(m)	Form of Claims
603	Supplemental Oath or Declaration	608.01(n)	Dependent Claims
603.01	Supplemental Oath or Declaration Filed After Allowance	608.01(o)	Basis for Claim Terminology in Description
604	Administration or Execution of Oath	608.01(p)	Completeness
604.01	Seal	608.01(q)	Substitute or Rewritten Specification
604.02	Venue	608.01(r)	Derogatory Remarks About Prior Art in Specification
**		608.01(s)	Restoration of Cancelled Matter
604.03(a)	Notarial Powers of Some Military Officers	608.01(t)	Use in Subsequent Application
604.04	Consul	608.01(u)	Use of Formerly Filed Incomplete Application
604.04(a)	Consul — Omission of Certificate	608.01(v)	Trademarks and Names Used in Trade
604.06	By Attorney in Case	608.02	Drawing
605	Applicant	608.02(a)	New Drawing — When Required
605.01	Applicant's Citizenship	608.02(b)	Informal Drawings
605.02	Applicant's Residence	608.02(c)	Drawing Print Kept in File Wrapper
605.03	Applicant's Post Office Address	608.02(d)	Complete Illustration in Drawings
605.04(a)	Applicant's Signature and Name	608.02(e)	Examiner Determines Completeness of Drawings
605.04(b)	One Full Given Name Required	608.02(f)	Modifications in Drawings
605.04(c)	Inventor Changes Name	608.02(g)	Illustration of Prior Art
605.04(d)	Applicant Unable to Write	608.02(h)	Additional, Duplicate, or Substitute Drawings
605.04(e)	May Use Title With Signature	608.02(i)	Transfer of Drawings From Prior Applications
		608.02(m)	Drawing Prints
		608.02(n)	Duplicate Prints in Patentability Report Cases
		608.02(o)	Dates Entered on Drawing
		608.02(p)	Correction of Drawings
		608.02(q)	Conditions Precedent to Amendment of Drawing
		608.02(r)	Separate Letter to Draftsman
		608.02(t)	Cancellation of Figures
		608.02(v)	Drawing Changes Which Require Sketches

PARTS, FORM, AND CONTENT OF APPLICATION

608.01(j)

applicant's best mode disclosure is so poor as to effectively result in concealment; *In re Sherwood*, 204 USPQ 537 (CCPA 1980).

The question of whether an inventor has or has not disclosed what he or she feels is his or her best mode is a question separate and distinct from the question of sufficiency of the disclosure, *In re Gay*, 135 USPQ 311 (CCPA 1962); *In re Glass*, 181 USPQ 31 (CCPA 1974). See 35 U.S.C. 112 and 37 CFR 1.71(b). *Sylgab Steel & Wire Corp. v. Imoco-Gateway Corp.*, 357 F. Supp. 657, 178 USPQ 22 (N.D. Ill. 1973); *H. K. Porter Co., Inc. v. Gates Rubber Co.*, 187 USPQ 692, 708, (D. Colo. 1975).

If the best mode contemplated by the inventor at the time of filing the application is not disclosed, such defect cannot be cured by submitting an amendment seeking to put into the specification something required to be there when the application was originally filed, *In re Hay*, 534 F.2d 917, 189 USPQ 790 (CCPA 1976). Any proposed amendment of this type should be treated as new matter.

Patents have been held invalid in cases where the patentee did not disclose the best mode known to him. See *Flick-Reedy Corp. v. Hydro-Line Manufacturing Co.*, 351 F.2d 546, 146 USPQ 694 (CA 7 1965), cert. denied, 383 U.S. 958, 148 USPQ 771 (1966); *Indiana General Corp. v. Krystinel Corp.*, 297 F. Supp. 427 161 USPQ 82 (S.D. N.Y. 1969), affirmed, 421 F.2d 1033, 164 USPQ 321 (CA 2 1970); *Dale Electronics, Inc. v. R.C.L. Electronics, Inc.*, 488 F.2d 382, 180 USPQ 235 (CA 1 1973); *Union Carbide Corp. v. Borg-Warner Corp.*, 550 F.2d 355, 193 USPQ 1 (CA 6 1977); *Reynolds Metals Co. v. Acorn Building Components Inc.*, 548 F.2d 155, 163, 192 USPQ 737 (CA 6 1977).

NOTE. — Completeness, >see< MPEP § 608.01(p) >and § 2165 to § 2165.04<.

608.01(i) Claims [R-3]**37 CFR 1.75. Claims**

(a) The specification must conclude with a claim particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention or discovery.

(b) More than one claim may be presented provided they differ substantially from each other and are not unduly multiplied.

(c) One or more claims may be presented in dependent form, referring back to and further limiting another claim or claims in the same application. Any dependent claim which refers to more than one other claim ("multiple dependent claim") shall refer to such other claims in the alternative only. A multiple dependent claim shall not serve as a basis for any other multiple dependent claim. For fee calculation purposes under § 1.16, a multiple dependent claim will be considered to be that number of claims to which direct reference is made therein. For fee calculation

purposes, also, any claim depending from a multiple dependent claim will be considered to be that number of claims to which direct reference is made in that multiple dependent claim. In addition to the other filing fees, any original application which is filed with, or is amended to include, multiple dependent claims must have paid therein the fee set forth in § 1.16(d). Claims in dependent form shall be construed to include all the limitations of the claim incorporated by reference into the dependent claim. A multiple dependent claim shall be construed to incorporate by reference all the limitations of each of the particular claims in relation to which it is being considered.

(d)(1) The claim or claims must conform to the invention as set forth in the remainder of the specification and the terms and phrases used in the claims must find clear support or antecedent basis in the description so that the meaning of the terms in the claims may be ascertainable by reference to the description (See § 1.58(a).)

(2) See §§ 1.141 to 1.146 as to claiming different inventions in one application.

(e) Where the nature of the case admits, as in the case of an improvement, any independent claim should contain in the following order, (1) a preamble comprising a general description of all the elements or steps of the claimed combination which are conventional or known, (2) a phrase such as "wherein the improvement comprises," and (3) those elements, steps and/or relationships which constitute that portion of the claimed combination which the applicant considers as the new or improved portion.

(f) If there are several claims, they shall be numbered consecutively in Arabic numerals.

** >(g) The least restrictive claim should be presented as claim number 1, and all dependent claims should be grouped together with the claim or claims to which they refer to the extent practicable.

(h) The claim or claims must commence on a separate sheet.

(i) Where a claim sets forth a plurality of elements or steps, each element or step of the claim should be separated by a line indentation <

NOTE

Numbering of Claims, MPEP § 608.01(j).

Form of Claims, MPEP § 608.01(m).

Dependent claims, MPEP § 608.01(n).

Examination of claims, MPEP § 706.

Claims in excess of fee, MPEP § 714.10.

608.01(j) Numbering of Claims [R-1]**37 CFR 1.126. Numbering of claims.**

The original numbering of the claims must be preserved throughout the prosecution. When claims are canceled the remaining claims must not be renumbered. When claims are added, except when presented in accordance with § 1.121(b), they must be numbered by the applicant consecutively beginning with the number next following the highest numbered claim previously presented (whether entered or not). When the application is ready for allowance, the examiner, if necessary, will renumber the claims consecutively in the order in which they appear or in such order as may have been requested by applicant.

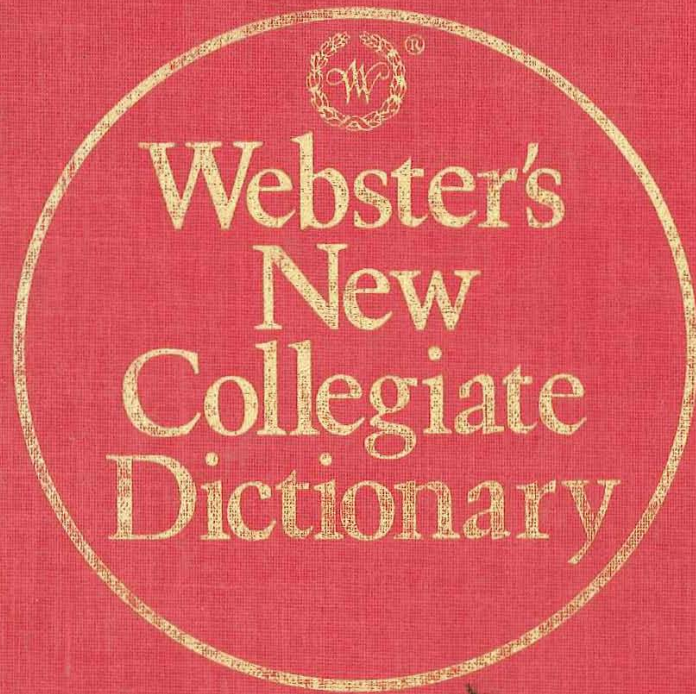
In a single claim case, the claim is not numbered.

Form Paragraph 6.17 may be used to notify applicant.

¶ 6.17 Numbering of Claims, 37 CFR 1.126

The numbering of claims is not in accordance with 37 CFR 1.126. The original numbering of the claims must be preserved

Exhibit “N”



Copyright © 1981 by G. & C. Merriam Co.

Philippines Copyright 1981 by G. & C. Merriam Co.

Library of Congress Cataloging in Publication Data
Main entry under title:

Webster's new collegiate dictionary.

Editions for 1898-1948 have title: Webster's collegiate dictionary.
Includes index.

1. English language—Dictionaries.

PE1628.W4M4 1981 423 80-25144

ISBN 0-87779-408-1

ISBN 0-87779-409-x (indexed)

ISBN 0-87779-410-3 (deluxe)

Webster's New Collegiate Dictionary principal copyright 1973

COLLEGIATE trademark Reg. U.S. Pat. Off.

All rights reserved. No part of this work covered by the copyrights hereon may be reproduced or copied in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems—without written permission of the publisher.

Made in the United States of America

50494847 RMcN8281

incitement • inconceivable

576

: stir up : spur on : urge on — *in-cit-ent* \-'sit-'nt/ *n* — *in-cite-ment* \-'ment/ *n* — *in-citer* *n*

syn INCITE, INSTIGATE, ABET, FOMENT *shared meaning element* : to spur to action or excite into activity *ant* restrain

in-civil-i-ty \in-(t)-s-'vil-at-ē/ *n* [MF *incivilité*, fr. LL *incivilitas*, *incivilitas*, fr. *incivilis*, fr. L *in-* + *civilis* civil] 1 : the quality or state of being uncivil 2 : a rude or discourteous act

incl *abbr* including; inclusive

in-clem-en-cy \in-'klem-ən-sē/ *n* : the quality or state of being inclement

in-clem-ent \in-'klem-ənt/ *adj* [L *inclement*, *inclemens*, fr. *in-* + *clement*, *clemens* clement] : lacking clemency; as *a* : physically severe : STORMY (~ weather) *b* *archaic* : severe in temper or action : UNMERCIFUL — *in-clem-ent-ly* *adv*

in-clin-able \in-'kli-nə-bəl/ *adj* : having a tendency or inclination; also : disposed to favor or think well of

in-clin-a-tion \in-'kli-nə-shən, -jē/ *n* 1 : an act or the action of bending or inclining; as *a* : BOW, NOD *b* : a tilting of something 2 *a* *obs* : natural disposition : CHARACTER *b* : a particular disposition of mind or character : PROPENSITY; *esp* : LIKING (had little ~ for housekeeping) 3 *a* : a deviation from the true vertical or horizontal : SLANT; also : the degree of such deviation *b* : an inclined surface : SLOPE *c* (1) : the angle determined by two lines or planes (2) : the angle made by a line with the *x*-axis measured counterclockwise from the positive direction of that axis 4 : a tendency to a particular aspect, state, character, or action (the clutch has an ~ to slip) — *in-clin-a-tion-al* \-shən-, -shən-'l/ *adj*

in-cline \in-'klin/ *vb* *in-clined*; *in-clin-ing* [ME *inclinen*, fr. MF *incliner*, fr. L *inclinare*, fr. *in-* + *clinare* to lean — more at LEAN] *vi* 1 : to bend the head or body forward : BOW 2 : to lean, tend, or become drawn toward an opinion or course of conduct 3 : to deviate from a line, direction, or course; *specif* : to deviate from the vertical or horizontal ~ *vi* 1 : to cause to stoop or bow : BEND 2 : to have influence on : PERSUADE (his love of books inclined him toward a literary career) 3 : to give a bend or slant to — *in-clin-er* *n*

syn 1 *see* SLANT
2 *INCLINE*, BIAS, DISPOSE, PREDISPOSE *shared meaning element* : to influence one to have or take an attitude toward something *ant* disincline

in-cline \in-'klin/ *n* : an inclined plane : GRADE, SLOPE
in-clined \in-'kli-nd, 2 *also* in-'/ *adj* 1 : having inclination, disposition, or tendency 2 *a* : having a leaning or slope *b* : making an angle with a line or plane

inclined plane *n* : a plane surface that makes an oblique angle with the plane of the horizon

in-clin-ing \in-'kli-niŋ/ *n* 1 : INCLINATION 2 *archaic* : PARTY, FOLLOWING

in-clin-om-e-ter \in-'kli-nəm-ət-ər, -jē-, -jē-, -kli-/ *n* 1 : an apparatus for determining the direction of the earth's magnetic field with reference to the plane of the horizon 2 : a machinist's clinometer 3 : an instrument for indicating the inclination to the horizontal of an axis of a ship or an airplane

in-clip \in-'kli-p/ *vt*, *archaic* : CLASP, ENCLOSE

in-close, *inclosure* *var* of ENCLOSE, ENCLOSURE
in-clude \in-'klüd/ *vt* *in-clud-ed*; *in-clud-ing* [ME *includen*, fr. L *includere*, fr. *in-* + *cludere* to close — more at CLOSE] 1 : to shut up : ENCLOSE 2 : to take in or comprise as a part of a larger aggregate or principle — *in-clud-able* or *in-clud-ible* \-'klüd-ə-bəl/ *adj*

syn INCLUDE, COMPREHEND, EMBRACE, INVOLVE *shared meaning element* : to contain within as part of a whole *ant* exclude

in-clud-ed *adj* : that is enclosed or embraced; *esp* : not projecting beyond the mouth of the corolla — used of a stamen or pistil

in-clusion \in-'klü-zhən/ *n* [L *inclusion*, *inclusio*, fr. *inclusus*, pp. of *includere*] 1 : the act of including : the state of being included 2 : something that is included; as *a* : a gaseous, liquid, or solid foreign body enclosed in a mass (as of a mineral) *b* : a passive product of cell activity (as a starch grain) within the protoplasm 3 : a relation between two classes that obtains when all members of the first are also members of the second — compare MEMBERSHIP

inclusion body *n* : a rounded or oval intracellular body that consists of elementary bodies in a matrix, is characteristic of some virus diseases, and is believed to represent a stage in the multiplication of the virus

in-clu-sive \in-'klü-siv-, -ziv/ *adj* 1 *a* : broad in orientation or scope *b* : covering or intended to cover all items, costs, or services 2 : comprehending the stated limits or extremes (from Monday to Friday ~) — *in-clu-sive-ly* *adv* — *in-clu-sive-ness* *n*

inclusive disjunction *n* : a statement of a logical proposition expressing alternatives that usu. takes the form *p* v *q* meaning *p* or *q* or both — *see* TRUTH TABLE

inclusive of prep : taking into account (the cost of building *in-clusive* of materials)

in-co-er-ci-ble \in-'kō-'ər-sə-bəl/ *adj* : incapable of being controlled, checked, or confined

incog *abbr* incognito

in-cog-i-tant \in-'kāj-ət-ənt/ *adj* [L *incogitant*, *incogitans*, fr. *in-* + *cogitant*, *cogitans*, pp. of *cogitare* to cogitate] : THOUGHTLESS, INCONSIDERATE

in-cog-ni-ta \in-'käg-'nēt-ə, in-'käg-nət-ə/ *adv* or *adj* [It. fem. of *incognito*] : INCognito — used only of a woman — *incognita* *n*

in-cog-ni-to \in-'käg-'nēt-(ō), in-'käg-ne-, -tō/ *adv* or *adj* [It. fr. L *incognitus* unknown, fr. *in-* + *cognitus*, pp. of *cognoscere* to know — more at COGNITION] : with one's identity concealed

incognito *n*, *pl* -tos 1 : one appearing or living incognito 2 : the state or disguise of an incognito or incognita

in-cog-ni-zant \in-'käg-nə-zənt/ *adj* : lacking awareness or consciousness — *in-cog-ni-zance* \-zəns(ə)/ *n*

in-co-her-ence \in-'kō-'hēr-ən(t)s-, -hēr-/ *n* 1 : the quality or state of being incoherent 2 : something that is incoherent

in-co-her-ent \-ənt/ *adj* : lacking coherence; as *a* : lacking cohesion : LOOSE *b* : lacking orderly continuity, arrangement, or relevance : INCONSISTENT — *in-co-her-ent-ly* *adv*

in-com-bus-ti-ble \in-'kəm-'bas-tə-bəl/ *adj* [ME, prob. fr. MF, fr. *in-* + *combustibile*] : not combustible : incapable of being burned — *in-com-bus-ti-bil-i-ty* \-bəl-sə-'bil-at-ē/ *n* — *incombustible* *n*

in-come \in-'kəm/ *n* 1 : a coming in : ENTRANCE, INFLUX (fluctuations in the nutrient ~ of a body of water) 2 : a gain or recurrent benefit usu. measured in money that derives from capital or labor; also : the amount of such gain received in a period of time (a small yearly ~)

income account *n* : a financial statement of a business showing the details of revenues, costs, expenses, losses, and profits for a given period — called also *income statement*

income bond *n* : a bond that pays interest at a rate based on the issuer's earnings

income tax \in-'kəm-/ *n* : a tax on the net income of an individual or a business

in-com-ing \in-'kəm-iŋ/ *n* 1 : the act of coming in : ARRIVAL 2 : INCOME — *usu.* used in pl.

incom-ing *adj* 1 *a* : coming in : ARRIVING (an ~ ship) *b* : taking a new place or position (the ~ president) *c* : received at a usual, proper, or designated destination (~ mail) 2 : just starting or beginning (the ~ freshman)

in-com-men-su-ra-ble \in-'kə-'men(t)s-(ə)-rə-bəl, -'mench-(ə)-/ *adj* : not commensurable; *broadly* : lacking a common basis of comparison in respect to a quality normally subject to comparison — *in-com-men-su-ra-bil-i-ty* \-men(t)s-(ə)-rə-'bil-at-ē, -'mench-(ə)-/ *n*

incommensurable \in-'kə-'mench-(ə)-/ *adv* — *in-com-men-su-ra-bly* \-men(t)s-(ə)-rə-'bil-, -'mench-(ə)-/ *adv*

in-com-men-su-rate \in-'kə-'mən-(ə)-rət, -'mench-(ə)-/ *adj* : not commensurate; as *a* : INADEQUATE *b* : DISPROPORTIONATE

in-com-mo-de \in-'kə-'mōd-/ *vt* -*mod-ed*; -*mod-ing* [MF *incommoder*, fr. L *incommodare*, fr. *in-* + *commodus* convenient — more at COMMODORE] : to give inconvenience or distress to : DISTURB

in-com-mo-di-ous \in-'kə-'mōd-ē-əs/ *adj* : not commodious : INCONVENIENT — *in-com-mo-di-ous-ly* *adv* — *in-com-mo-di-ous-ness* *n*

in-com-mo-di-ty \-'mād-ət-ē/ *n* : a source of inconvenience : DISADVANTAGE

in-com-mu-ni-ca-ble \in-'kə-'myū-ni-kə-bəl/ *adj* [MF or LL; MF, fr. LL *incommunicabilis*, fr. L *in-* + LL *communicabilis* communicable] : not communicable; as *a* : incapable of being communicated or imparted *b* : UNCOMMUNICATIVE — *in-com-mu-ni-ca-bil-i-ty* \-'myū-ni-kə-'bil-at-ē/ *n* — *in-com-mu-ni-ca-bly* \-'myū-ni-kə-'bil-ē/ *adv*

in-com-mu-ni-ca-do \-'myū-nə-'kād-(ō)/ *adv* or *adj* [Sp *incommunica-do*, fr. pp. of *incomunicar* to deprive of communication, fr. *in-* (fr. L) + *comunicare* to communicate, fr. L *comunicare*] : without means of communication; also : in solitary confinement

in-com-mu-ni-ca-tive \-'myū-nə-'kāt-iv-, -ni-kət-/ *adj* : UNCOMMUNICATIVE

in-com-mut-a-ble \in-'kə-'myūt-ə-bəl/ *adj* [ME, fr. L *incommutabilis*, fr. *in-* + *commutabilis* commutable] : not commutable; as *a* : not interchangeable *b* : UNCHANGEABLE — *in-com-mut-a-bly* \-blē/ *adv*

in-com-pa-ra-ble \in-'kəm-p(ə)-rə-bəl/ *adj* [ME, fr. MF, fr. L *incomparabilis*, fr. *in-* + *comparabilis* comparable] 1 : eminent beyond comparison : MATCHLESS 2 : not suitable for comparison — *in-com-pa-ra-bil-i-ty* \in-'kəm-p(ə)-rə-'bil-at-ē/ *n* — *in-com-pa-ra-bly* \in-'kəm-p(ə)-rə-'bil-ē/ *adv*

in-com-pat-i-bil-i-ty \in-'kəm-pat-ə-'bil-at-ē/ *n*, *pl* -ties 1 *a* : the quality or state of being incompatible *b* : lack of interfertility between two plants 2 *pl* : mutually antagonistic things or qualities

in-com-pat-i-ble \in-'kəm-pat-ə-bəl/ *adj* [MF & ML; MF, fr. ML *incompatibilis*, fr. L *in-* + ML *compatibilis* compatible] 1 : incapable of being held by one person at one time — used of offices that make conflicting demands on the holder 2 *a* : incapable of association because incongruous, discordant, or disagreeing (~ colors) *b* : unsuitable for use together because of undesirable chemical or physiological effects (~ drugs) *c* : not both true (~ propositions) *d* : incapable of blending into a stable homogeneous mixture — *incompatible* *n* — *in-com-pat-i-bly* \-blē/ *adv*

in-com-pe-tence \in-'kəm-pət-ən(t)s/ *n* : the state or fact of being incompetent

in-com-pe-ten-cy \-ən-sē/ *n* : INCOMPETENCE

in-com-pe-ten-t \in-'kəm-pət-ənt/ *adj* [MF *incompétent*, fr. *in-* + *compétent* competent] 1 : lacking the qualities needed for effective action 2 : not legally qualified 3 : inadequate to or unsuitable for a particular purpose — *incompetent* *n* — *in-com-pe-ten-ly* *adv*

in-com-plete \in-'kəm-'plēt-/ *adj* [ME *incomplete*, fr. LL *incompletus*, fr. L *in-* + *completus* complete] : not complete : UNFINISHED; as *a* : lacking a part; *esp* : lacking one or more sets of floral organs *b* of a football pass : not legally caught — *in-complete-ly* *adv* — *in-complete-ness* *n*

in-com-pli-ant \in-'kəm-'pli-ənt/ *adj* : not compliant or pliable : UNYIELDING

in-cog-ni-ta-ble \in-'käm-pri-'hen(t)-sə-bəl/ *adj* [ME, fr. L *incomprehensibilis*, fr. *in-* + *comprehensibilis* comprehensible] 1 : incomprehensible; having or subject to no limits 2 : impossible to comprehend : UNINTELLIGIBLE — *in-cog-ni-ta-bil-i-ty* \-hen(t)-sə-'bil-at-ē/ *n* — *in-cog-ni-ta-ble-ness* *n* — *in-cog-ni-ta-bly* \-hen(t)-sə-'bil-ē/ *adv*

in-com-pre-hen-sion \in-'hen-chen-/ *n* : lack of comprehension or understanding

in-com-pres-si-ble \in-'kəm-'pres-ə-bəl/ *adj* : incapable of or resistant to compression — *in-com-pres-si-bil-i-ty* \-pres-ə-'bil-at-ē/ *n* — *in-com-pres-si-bly* \-blē/ *adv*

in-com-put-a-ble \in-'kəm-'pyūt-ə-bəl/ *adj* : not computable : very great — *in-com-put-a-bly* \-blē/ *adv*

in-con-ceiv-a-ble \in-'kən-'sē-və-bəl/ *adj* : not conceivable; as *a* : impossible to comprehend *b* : UNBELIEVABLE — *in-con-ceiv-*

Exhibit “O”

DICTIONARY OF BUSINESS



FITZROY DEARBORN PUBLISHERS

650.03
C691d
Copyright © 1985, 1994, 1998 by P.H.Collin

First published in Great Britain by
Peter Collin Publishing Ltd
1 Cambridge Road, Teddington, Middlesex, TW11 8DT

This edition published in the United States of America by
Fitzroy Dearborn, Publishers
70 East Walton Street, Chicago, Illinois 60611

Text computer typeset by Barbers Ltd, Kent
Printed and bound by WSOY in Finland

All rights reserved, including the right of reproduction in whole or in part in any form

A Cataloging-in-Publication record for this book is available from the Library of Congress

ISBN 1-57958-077-7

First Published in the USA and UK 1998

Cover: Peter Aristedes, Chicago Advertising and Design

conditional
 at certain
 apply; we
 we have
 the offer;
 all part of
 is good

aptance
 [ənsəʊs]
 (k) which
 ies to pay
 mmediate
 : Bank of
 ltee = the
 ch act as
 tly better
 nd

access to
 or reach
 ounts of
 ken by a
 rb to call
 uter; she
 uter

omething
 (such as
 ident =
 accident
 ay when

1] **noun**
 o reach
 to agree
 n bill =
 ing (the
 ny (the
 to live;
 r hotel
 hey are
 idation;
 sed for
 the real
 al in GB
 have

ines to
 for full

aveller

can let
 tenant
 Times

roomy

Month

with;
 eeting;
 they
 plaint,

accompanied by an invoice for damage
 (NOTE: accompanied by something)

accordance [ə'kɔ:dəns] **noun** in
 accordance with = in agreement with or
 according to; in accordance with your
 instructions we have deposited the money in
 your current account; I am submitting the
 claim for damages in accordance with the
 advice of our legal advisers

◇ **according to** [ə'kɔ:dɪŋtu] **preposition** as
 someone says or writes; the computer was
 installed according to the manufacturer's
 instructions

◇ **accordingly** [ə'kɔ:dɪŋli] **adverb** in
 agreement with what has been decided; we
 have received your letter and have altered the
 contract accordingly

QUOTE: the budget targets for employment and
 growth are within reach according to the latest
 figures

Australian Financial Review

account [ə'kaʊnt] **1 noun** (a) record of
 financial transactions over a period of time,
 such as money paid, received, borrowed or
 owed; please send me your account or a
 detailed or an itemized account; expense
 account = money which a businessman is
 allowed by his company to spend on travelling
 and entertaining clients in connection with his
 business; he charged his hotel bill to his
 expense account (b) (in a shop) arrangement
 which a customer has to buy goods and pay for
 them at a later date (usually the end of the
 month); to have an account or a charge
 account or a credit account with Harrods; put
 it on my account or charge it to my account
 (of a customer) to open an account = to ask a
 shop to supply goods which you will pay for at
 a later date; (of a shop) to open an account or
 to close an account = to start or to stop
 supplying a customer on credit; to settle an
 account = to pay all the money owed on an
 account; to stop an account = to stop
 supplying a customer until he has paid what he
 owes (c) on account = as part of a total bill;
 to pay money on account = to pay to settle
 part of a bill; advance on account = money
 paid as a part payment (d) customer who does
 a large amount of business with a firm and has
 an account; he is one of our largest accounts;
 our salesmen call on their best accounts twice
 a month; account executive = employee who
 is the only person to deal with a certain
 customer or who is the link between a certain
 customer and his company (e) the accounts of
 a business or a company's accounts =
 detailed records of a company's financial
 affairs; to keep the accounts = to write each
 sum of money in the account book; the
 accountant's job is to enter all the money
 received in the accounts; account book =
 book with printed columns ready for accounts

to be entered; annual accounts = accounts
 prepared at the end of a financial year;
 management accounts = financial information
 (sales, expenditure, credit, and profitability)
 prepared for a manager so that he can take
 decisions; profit and loss account (P&L
 account) = statement of company expenditure
 and income over a period of time, almost
 always one calendar year, showing whether
 the company has made a profit or loss (the
 balance sheet shows the state of a company's
 finances at a certain date; the profit and loss
 account shows the movements which have
 taken place since the last balance sheet)
 (NOTE: the US equivalent is the profit and loss
 statement or income statement); accounts
 department = department in a company which
 deals with money paid, received, borrowed or
 owed; accounts manager = manager of an
 accounts department; accounts payable =
 money owed by a company; accounts
 receivable = money owed to a company (f)
 bank account or US banking account =
 arrangement to keep money in a bank;
 building society account; savings bank
 account; Lloyds account; he has an account
 with Lloyds; I have an account with the
 Halifax Building Society; to put money in (to)
 your account; to take money out of your
 account or to withdraw money from your
 account; budget account = bank account
 where you plan income and expenditure to
 allow for periods when expenditure is high;
 current account or cheque account or US
 checking account = account which pays little
 or no interest but from which the customer can
 withdraw money when he wants by writing
 cheques; deposit account = account which
 pays interest but on which notice usually has
 to be given to withdraw money; external
 account = account in a British bank of
 someone who is living in another country;
 frozen account = account where the money
 cannot by used or moved because of a court
 order; joint account = account for two people;
 most married people have joint accounts so
 that they can each take money out when they
 want it; overdrawn account = account where
 you have taken out more money than you have
 put in (i.e. where the bank is lending you
 money); savings account = account where
 you put money in regularly and which pays
 interest, often at a higher rate than a deposit
 account; to open an account = to start an
 account by putting money in; she opened an
 account with the Halifax Building Society; to
 close an account = to take all money out of a
 bank account and stop the account; he closed
 his account with Lloyds (g) (Stock Exchange)
 set period (formerly about ten working days)
 during which shares can be bought and at the
 end of which the purchaser must pay for the
 shares bought; rolling account = system of
 paying for shares bought on the stock
 exchange, where the buyer pays at the end of a

ly

pay

211

payoff

=
ral
is;
of
or
de
rn
erin
ith
to
ct;
he
=
ct
to
aon
of

r's

ey
ay
=
ts;
nd
th
by
id;
by
is
ily
ay
rs
sk,
for
ay
ms
ay
ng
=
of
us
ng
he
al
ce
ht;
if
ey
a
ce
ey
re
ay
m
ve
nts
by
ay

cash = to pay the complete sum in cash; to **pay by cheque** = to pay by giving a cheque, not by using cash or credit card; to **pay by credit card** = to pay, using a credit card and not a cheque or cash (**b**) to give money; to **pay on demand** = to pay money when it is asked for, not after a period of credit; **please pay the sum of £10** = please give £10 in cash or by cheque; to **pay a dividend** = to give shareholders a part of the profits of a company; *these shares pay a dividend of 1.5p*; to **pay interest** = to give money as interest on money borrowed or invested; *building societies pay an interest of 10% (c)* to give a worker money for work done; *the workforce has not been paid for three weeks*; *we pay good wages for skilled workers*; *how much do they pay you per hour?*; to be paid by the hour = to get money for each hour worked; to be paid at piece-work rates = to get money for each piece of work finished (**d**) to give money which is owed or which has to be paid; to **pay a bill**; to **pay an invoice**; to **pay duty on imports**; to **pay tax (e)** to pay a cheque into an account = to deposit money in the form of a cheque (NOTE: **paying - paid**)

◇ **payable** ['peɪəbl] *adjective* which is due to be paid; **payable in advance** = which has to be paid before the goods are delivered; **payable on delivery** = which has to be paid when the goods are delivered; **payable on demand** = which must be paid when payment is asked for; **payable at sixty days** = which has to be paid by sixty days after the date of invoice; **cheque made payable to bearer** = cheque which will be paid to the person who has it, not to any particular name written on it; **shares payable on application** = shares which must be paid for when you apply to buy them; **accounts payable** = money owed by a company; **bills payable** = bills which a debtor will have to pay; **electricity charges are payable by the tenant** = the tenant (and not the landlord) must pay for the electricity

◇ **pay as you earn (PAYE)** ['peɪəzjuːˈɜːn] *GB* tax system, where income tax is deducted from the salary before it is paid to the worker

◇ **pay-as-you-go** ['peɪəzjuːˈɡəʊ] (**a**) *US* = **PAY AS YOU EARN** (**b**) *GB* payment system where the purchaser pays in small instalments as he uses the service

◇ **pay back** ['peɪˈbæk] *verb* to give money back to someone; *to pay back a loan*; *I lent him £50 and he promised to pay me back in a month*; *he has never paid me back the money he borrowed*

◇ **payback** ['peɪbæk] *noun* paying back money which has been borrowed; **payback clause** = clause in a contract which states the terms for repaying a loan; **payback period** = period of time over which a loan is to be repaid or an investment is to pay for itself

◇ **pay-cheque** or *US* **paycheck** ['peɪtʃek] *noun* salary cheque given to an employee

◇ **pay down** ['peɪˈdaʊn] *verb* to pay money down = to make a deposit; *he paid £50 down and the rest in monthly instalments*

◇ **PAYE** ['piːerwaɪː] = **PAY AS YOU EARN**

◇ **payee** ['peɪiː] *noun* person who receives money from someone or person whose name is on a cheque

◇ **payer** ['peɪə] *noun* person who gives money to someone; **slow payer** = person or company which does not pay debts on time; *he is well known as a slow payer*

◇ **paying** ['peɪɪŋ] 1 *adjective* which makes a profit; *it is a paying business*; it is not a **paying proposition** = it is not a business which is going to make a profit 2 *noun* giving money; *paying of a debt*; **paying-in book** = book of forms for paying money into a bank account or building society; **paying-in slip** = form which is filled in when money is being deposited in a bank account or building society

◇ **payload** ['peɪləʊd] *noun* cargo or passengers carried by a ship or train or plane for which payment is made

◇ **payment** ['peɪmənt] *noun* (**a**) giving money; *payment in cash or cash payment*; *payment by cheque*; *payment of interest or interest payment*; **payment on account** = paying part of the money owed; **full payment** or **payment in full** = paying all money owed; **payment on invoice** = paying money as soon as an invoice is received; **payment in kind** = paying by giving goods or food, but not money; **payment by results** = money given which increases with the amount of work done or goods produced (**b**) money paid; **back payment** = paying money which is owed; **deferred payment** = (i) money paid later than the agreed date; (ii) payment for goods by instalments over a period of time; *the company agreed to defer payments for three months*; **down payment** = part of a total payment made in advance; **repayable in easy payments** = repayable with small sums regularly; **incentive payments** = extra pay offered to a worker to make him work better; **balance of payments** = the international financial position of a country including visible and invisible trade

◇ **pay off** ['peɪˈɒf] *verb* (**a**) to finish paying money which is owed; *to pay off a mortgage*; *to pay off a loan* (**b**) to pay all the money owed to someone and terminate his employment; *when the company was taken over the factory was closed and all the workers were paid off*

◇ **payoff** ['peɪɒf] *noun* (**a**) money paid to finish paying something which is owed, such as money paid to a worker when his employment is terminated (**b**) profit or reward;

realizable

244

receiver

◇ **realizable** [riə'laɪzəbl] *adjective*
realizable assets = assets which can be sold for money

◇ **realization** [riə'lai'zeɪʃən] *noun* (a) gradual understanding; *the chairman's realization that he was going to be outvoted* (b) making real; *the realization of a project = putting a project into action; the plan moved a stage nearer realization when the contracts were signed* (c) **realization of assets** = selling of assets for money

realtor ['ri:ltə] *noun* US estate agent, person who sells real estate for customers

◇ **reality** ['ri:lti] *noun* property or real estate

reapply [ri:ə'plai] *verb* to apply again; *when he saw that the job had still not been filled, he reapplied for it*

◇ **reapplication** [ri:ə'pli'keɪʃən] *noun*
 second application

reappoint [ri:ə'pɔɪnt] *verb* to appoint someone again; *he was reappointed chairman for a further three-year period*

◇ **reappointment** [ri:ə'pɔɪntmənt] *noun*
 being reappointed

reason ['ri:zn] *noun* thing which explains why something has happened; *the airline gave no reason for the plane's late arrival; the personnel officer asked him for the reason why he was late again; the chairman was asked for his reasons for closing the factory*

◇ **reasonable** ['ri:znəbl] *adjective* (a) sensible or not annoyed; *the manager of the shop was very reasonable when she tried to explain that she had left her credit cards at home; no reasonable offer refused* = we will accept any offer which is not extremely low (b) moderate or not expensive; *the restaurant offers good food at reasonable prices*

reassess [ri:ə'ses] *verb* to assess again

◇ **reassessment** [ri:ə'sesmənt] *noun* new assessment

reassign [ri:ə'sain] *verb* to assign again

◇ **reassignment** [ri:ə'sainmənt] *noun* new assignment

reassure [ri:ə'sʊə] *verb* (a) to make someone calm or less worried; *the markets were reassured by the government statement on import controls; the manager tried to reassure her that she would not lose her job* (b) to reinsure, to spread the risk of an insurance by asking another insurance company to cover part of it and receive part of the premium

rebate ['ri:bet] *noun* (a) reduction in the amount of money to be paid; *to offer a 10% rebate on selected goods* (b) money returned

to someone because he has paid too much; *he got a tax rebate at the end of the year*

rebound [ri'baʊnd] *verb* to go back up again quickly; *the market rebounded on the news of the government's decision*

recall [ri'kɔl] *verb* (of a manufacturer) to ask for products to be returned because of possible faults; *they recalled 10,000 washing machines because of a faulty electrical connection*

recd = RECEIVED

receipt [ri'si:t] 1 *noun* (a) paper showing that money has been paid or that something has been received; *customs receipt; rent receipt; receipt for items purchased; please produce your receipt if you want to exchange items; receipt book or book of receipts* = book of blank receipts to be filled in when purchases are made (b) act of receiving something; *to acknowledge receipt of a letter* = to write to say that you have received a letter; *we acknowledge receipt of your letter of the 15th; goods will be supplied within thirty days of receipt of order; invoices are payable within thirty days of receipt; on receipt of the notification, the company lodged an appeal* (c) receipts = money taken in sales; *to itemize receipts and expenditure; receipts are down against the same period of last year* 2 *verb* to stamp or to sign a document to show that it has been received or to stamp an invoice to show that it has been paid

QUOTE: the public sector borrowing requirement is kept low by treating the receipts from selling public assets as a reduction in borrowing

Economist

QUOTE: gross wool receipts for the selling season to end June appear likely to top \$2 billion

Australian Financial Review

receive [ri'si:v] *verb* to get something which has been delivered; *we received the payment ten days ago; the workers have not received any salary for six months; the goods were received in good condition; 'received with thanks'* = words put on an invoice to show that a sum has been paid

◇ **receivable** [ri'si:vəbl] *adjective* which can be received; **accounts receivable** = money owed to a company; **bills receivable** = bills which are due to be paid by a company's debtors

◇ **receivables** [ri'si:vəblz] *plural noun* money which is owed to a company

◇ **receiver** [ri'si:və] *noun* (a) person who receives something; *the receiver of the shipment* (b) official receiver = government official who is appointed to run a company which is in financial difficulties, to pay off its debts as far as possible, and to close it down; *the court appointed a receiver for the*

Exhibit “P”

U.S. Pat. No. 5,793,148, Claim 28	Plaintiff's Proposed Construction	Defendant's Proposed Construction	Court's Construction
A payment method, comprising: a <i>payer</i> obtaining a document containing document information, the document information being associated with a debt incurred by the <i>payer</i> or for goods or for services to be paid for or purchased by the <i>payer</i>; the <i>payer</i> creating a <i>variable authentication number (VAN)</i> on a computer using at least a portion of the document information, and a <i>secret key of the payer</i>, the document information including an amount, and information for identifying the payee, the <u>VAN</u> being used for attesting to the authenticity of the payer and document information; and	“payer”; A person or entity who pays, or who is to make a payment. In this claim payor and payer refer to the same person or entity.	“payor”; Party paying for or purchasing goods or services.	
	“payer”; A person or entity who pays, or who is to make a payment. In this claim payor and payer refer to the same person or entity.	“payer”; Indefinite.	
	“payment” [AGREED]	“payment” [AGREED]	Compensation in exchange for goods or services or the discharge of a debt.
	“associated with” [AGREED]	“associated with” [AGREED]	Identified with or having a connection to.

U.S. Pat. No. 5,793,148, Claim 28	Plaintiff's Proposed Construction	Defendant's Proposed Construction	Court's Construction
the payor creating a <u>payment instrument</u> using the document information and appending the VAN to the <u>payment instrument</u>, the <u>payment instrument</u> being used to pay for the incurred debt or for the purchase of goods or services.	“variable authentication number (VAN)”; An encoded variable number that can be used in verifying the identity of a party or the integrity of information or both, the value generated by coding information relevant to a transaction, document, or thing either with a joint key or information associated with or assigned or related to at least one party to the transaction or issuance of the document or thing.	“variable authentication number (VAN)”; A variable number that can be used by a recipient to verify the integrity of information relevant to the transaction and that a party to the transaction originated the transaction information, the value generated by [coding] information relevant to the transaction either with a joint code produced from information associated with the party or directly with information associated with at least one party. The term “coding” means: Transforming information into a VAN by applying a known algorithm under which the resulting VAN can either be uncoded by reversing the coding operation or compared to a VAN regenerated by applying that same known algorithm to the information. “secret key of the payor”; Key that is generated by coding information associated with and known, prior to any coding, only by the payor for use in any future transactions.	
	“secret key of the payor”; A private key that is created by the payor, or an entity originating an instrument on the payor’s behalf, by coding information associated with or related to the payor, which is capable of being separately created by a party intended to authenticate the instrument.		

U.S. Pat. No. 5,793,148, Claim 28	Plaintiff's Proposed Construction	Defendant's Proposed Construction	Court's Construction
	“the VAN being used for attesting to the authenticity of the payor and document information” [AGREED]	“the VAN being used for attesting to the authenticity of the payor and document information” [AGREED]	The VAN being used to verify that the instrument originated from the payor and that the at least a portion of the document information used to create the VAN has not changed.
	“payment instrument” [AGREED]	“payment instrument” [AGREED]	A document (including paper or electronic) that is used to transfer funds to a recipient party in connection with a [payment].

Exhibit “Q”

United States Patent [19][11] **4,404,649****Nunley et al.**[45] **Sep. 13, 1983**

- [54] **DOCUMENT PROCESSING SYSTEM**
- [75] Inventors: **Leonard J. Nunley; Willis D. Simpson**, both of Dallas; **William J. Reid**, Richardson, all of Tex.
- [73] Assignee: **Recognition Equipment Incorporated**, Irving, Tex.
- [21] Appl. No.: **202,970**
- [22] Filed: **Nov. 3, 1980**
- [51] Int. Cl.³ **G06F 15/30**
- [52] U.S. Cl. **364/900; 235/379**
- [58] Field of Search ... **364/200 MS File, 900 MS File, 364/408; 235/379, 425, 449, 493**

4,025,905 5/1977 Gorgens 364/900
 4,027,142 5/1977 Paup et al. 235/379
 4,082,945 4/1978 Van de Goor et al. 235/379
 4,091,448 5/1978 Clausen 364/200
 4,166,945 9/1979 Inoyama et al. 235/379
 4,180,799 12/1979 Smith 340/146.3

Primary Examiner—Raulfe B. Zache*Attorney, Agent, or Firm*—Richards, Harris & Medlock

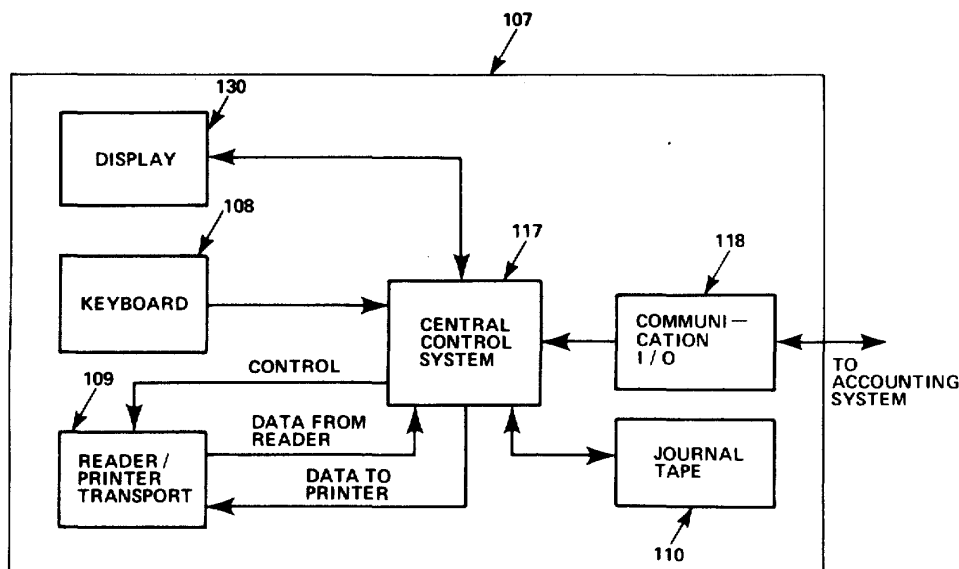
[57]

ABSTRACT

The system described herein provides a capability for automatically processing documents such as bank checks, deposit slips, loan payments, etc., from all points within a banking organization, with exception of the point of receipt, based on the utilization of a Source Item Control Number (SICN), which uniquely identifies a document at all subsequent processing points. Processing at the source point of receipt is semi-automatic in that the first person to handle the document within the organization is generally required to key or otherwise manually enter certain data related to the document.

[56] **References Cited****U.S. PATENT DOCUMENTS**

3,178,690 4/1965 Masters et al. 364/200
 3,228,006 1/1966 Neilson et al. 364/200
 3,277,444 10/1966 Masters 364/200
 3,308,439 3/1967 Tink et al. 364/200
 3,596,256 7/1971 Alpert et al. 364/200
 3,970,992 7/1976 Boothroyd et al. 364/900
 3,998,155 12/1976 Cothran et al. 364/200 X

9 Claims, 9 Drawing Figures

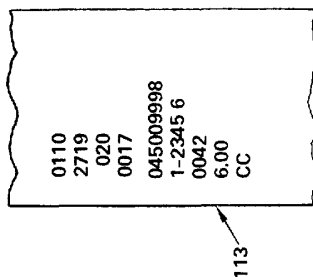
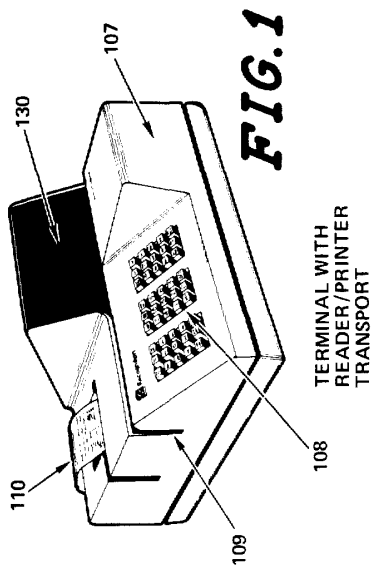
RECORD FOR
CHECK NO. 0042

FIG. 4

3

destination record which includes the SICN. If such a record is present in memory storage, it is retrieved and utilized by the batch oriented document processing system to remove said document from the stream of documents and sort it to the address destination indicated as desired in said exception destination record. Also, during the bookkeeping operations, the accounting system may utilize the data from each record to generate address destination records which are placed in a memory storage. Each of said address destination records contain a source item control number and the address of the destination desired for the documents if they are not determined to be exception items together with any other data deemed appropriate by the processing organization.

Also, in the batch processing of documents to separate them according to destination or account, the SICN can be read from each document to determine if all necessary data concerning each of the documents have already been processed into the system and stored in memory. It may thus be determined if all of the documents entered at a specific time have been received for separation and that none of the documents have been misplaced or lost. If there are any SICN's assigned to documents that have not been run through batch processing at the appropriate state, then the system can be alerted that certain items have not been processed. If a particular document did not contain a SICN, this would also alert the system to the fact that such document has not been completely processed through the system.

Referring to FIG. 1, there is illustrated a terminal system 107 with a keyboard, 108. Such a system might be used to process the check illustrated in FIG. 2. The front of the check 100 has been illustrated comprising three MICR fields 101, 102 and 103. Field 101 is a bank number field. Field 102 is an account number field. Field 103 is a transaction code field which, in the illustration, consists of the check serial number. The amount of the check is indicated in areas 104 and 105. The check 100 thus illustrated (without the SICN 106) represents a typical check which might be submitted to a bank teller for cashing, depositing, etc.

To process this check using the subject invention, the teller would look at the check 100, and using the keyboard 108 of terminal 107, would key the amount 104 or 105 from the face of the check. The teller would also typically key data indicating the type of transaction being performed which in this case is assumed to be "check cash." The teller would then insert the check 100 into a reader/printer transport 109, which is a part of the terminal 107. The reader/printer transport 109 automatically moves the document past a reader device (not shown) which is capable of reading MICR format fields 101-103. The data read from the face of the check together with the keyed amount and the type of transaction become part of the computer record 113 (FIG. 4) created by the terminal 107 for check 100. The terminal 107 then automatically assigns a unique SICN 106 to the check based on data in the terminal central control system which was previously entered by the teller or built into the terminal or both. In the example shown, the first four digits of the SICN might identify that this check was processed by a terminal located in branch number 110. The next four digits of the SICN might represent the teller's employee number or other identification (employee number 2719). The next three digits of the SICN might represent the data (020 the twentieth day of the year) on which this document is processed.

4

The next four digits might represent the sequence number of this item (the seventeenth item processed by this teller on this terminal today). Many other formats of SICN are possible. The SICN might be shorter or longer and might contain other data, but the SICN assigned to a document will not be assigned to any other document for a significant period of time. As an example, not for one year or longer. There are many ways to assure the necessary uniqueness for the SICN.

The terminal 107 also operates to cause the SICN 106 to become a part of the computer record 113 for check 100. The reader/printer transport 109 of the terminal also moves the document past a printer device which prints the SICN 106 on the face of the check, as illustrated in FIG. 2, in a machine readable code which is also, preferably, human readable.

The computer record which is created by the terminal 107 for the check may contain more or less data than the example 113 illustrated in FIG. 4. The exact data and format of such computer records are based upon the processing organizations requirements for proper handling when read into their accounting system. It is important to this invention, however, that the computer record created by terminal 107 contain at least the following data:

All or part of the data read from the document by the reader of terminal 107, all data relative to the document which was keyed manually by the terminal operator using keyboard 108, and a SICN which is sufficiently unique to avoid confusing the associated document with any other document during subsequent processing. These minimum data requirements in the computer record for a given document are essential to assure that all further processing of the document which is required, based on the procedures of the processing organization, may be accomplished by automatic means without the need for any additional manual entries of data obtained from the document.

FIG. 3 illustrates a journal tape record 110 created by the terminal 107. As illustrated, this journal tape record contains all the data 111 and 112 which is contained on the face of the document in areas 104-106. Data from areas 101-103 and other data could also be included. This journal tape record is shown for reference only and is not essential to the invention.

Referring now to FIG. 5. There is illustrated a block diagram of an overall system for processing documents according to the present invention. Terminal 107, which is the same terminal illustrated in FIG. 1, may be operated alone or in conjunction with a terminal control computer 107a to perform the following basic functions for each document processed: (1) Create a computer record which contains a Source Item Control Number and all necessary data from the document, and transmit the computer record over a communication link 114 to the processing organization's accounting system 115, and (2) Print a machine readable Source Item Control Number on the document.

Once these basic functions have been performed by terminal 107, the processing organization has captured all of the data from the document related to the document, and has transferred the data into the accounting system 115, then bookkeeping operations for the organization may be carried out under automated control and in accordance with established and well known principles. Typically, all remaining processing operations performed on the document will relate to distributing the document based on the organization's procedures,