Paper No. 28

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MASTERCARD INTERNATIONAL INCORPORATED
Petitioner

v.

LEON STAMBLER
Patent Owner

Case Number CBM2015-00044
Patent 5,793,302

PETITIONER'S FILING OF DEMONSTRATIVE EXHIBITS

Petitioner MasterCard respectfully submits its demonstrative exhibits pursuant to 37 C.F.R. § 42.70(b) and the Court's Trial Hearing Order dated February 16, 2016.

March 16, 2016

Respectfully submitted,

BAKER BOTTS LLP

/Robert C. Scheinfeld/

Robert C. Scheinfeld
Reg. No. 31,300
30 Rockefeller Plaza, 44th Floor
New York, New York 10112-4498
Phone: (212) 408-2512
Facsimile: (212) 408-2501
robert.scheinfeld@bakerbotts.com

Eliot D. Williams
Reg. No. 50,822
1001 Page Mill Road
Building One, Suite 200
Palo Alto, CA 94304
Phone: (650) 739-7511
Facsimile: (650) 739-7611
eliot.williams@bakerbotts.com

ATTORNEYS FOR PETITIONER MASTERCARD INTERNATIONAL INCORPORATED

CBM2015-00044	**MasterCard International Incorporated v. Leon Stambler**	**U.S. Pat. 5,793,302**

Petitioner's Demonstrative Exhibits

Oral Argument

March 18, 2016

Table of Contents

U.S. Pat. No. 5,793,302

US005793302A

United States Patent [19]
Stambler

[11] **Patent Number: 5,793,302**
[45] **Date of Patent: *Aug. 11, 1998**

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

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

[*] Notice: The term of this patent shall not extend beyond the expiration date of Pat. No. 5,267,314.

[21] Appl. No.: **747,174**

[22] Filed: **Nov. 12, 1996**

Related U.S. Application Data

[60] Continuation of Ser. No. 446,369, May 22, 1995, which is a division of Ser. No. 122,071, Sep. 14, 1993, Pat. No. 5,524,073, which is a division of Ser. No. 977,385, Nov. 17, 1992, Pat. No. 5,267,314.

[51] **Int. Cl.**[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	Halstof .	
4,208,739	6/1980	Lu .	
4,223,403	9/1980	Konheim et al. .	
4,234,932	11/1980	Gorgens .	
4,264,782	4/1981	Konheim .	
4,264,808	4/1981	Owens et al. .	
4,268,715	5/1981	Atalla .	
4,281,215	7/1981	Atalla .	

(List continued on next page.)

OTHER PUBLICATIONS

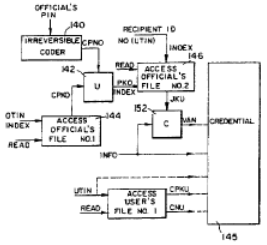
Shipley C., "I threw away my checkbook", PC–Computing, vol. 3, No. 11, pp. 112, 114–115, 118–120, Nov. 1990.
Iida J., "Electronic Presentment Due for N.Y. Test", American Banker, vol. 157, No. 143, p. 3, Jul. 27, 1992.
Torrez A., "Banking Industry Looks at Changing Check Guarantees", The Business Journal–Phoenix & The Valley of the Sun, vol. 9, No. 29, pp. 13–14, May 29, 1989.
Sullivan D., "Bank Technology Trick or Treat?", Bankers Monthly, vol. 109, No. 11, pp. 10, 12–14, 18, 20, Nov. 1992.
Seidenberg, "Bell Companies Now Testing Smart Card Offering Increased Feature Functionality", Card News, vol. 5, No. 10, pp. 5–6, May 21, 1990.
"General Magnaplate Corporation Issues Three–Month Report to Stockholders", PR Newswire, 1 page, Nov. 11, 1992.
Byles T., "More Companies Are Paying Bills 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 uncode the VAN properly in order to re-derive the information. The joint code serves to authenticate the parties, and the comparison of the re-derived information against the information recorded on the document serves to authenticate the accuracy of that information.

91 Claims, 15 Drawing Sheets



- Title: Method for securing information relevant to a transaction
- Issue Date: Aug. 11, 1998
- Priority Date: Nov. 17, 1992

Claim 51 of the ’302 Patent

- 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.

Institution Decision

1. The Board instituted on the following grounds:
   a) Claims 51 and 53 (*anticipated by Davies*)
   b) Claim 55 (*obvious over Davies and Nechvatal*)
   c) Claim 56 (*obvious over Davies, Fischer and Piosenka*)
   d) Claims 51, 53, 55 and 56 (*obvious over Davies and Meyer*)

See Institution Decision (Paper 10), at 27.

Board's Claim Constructions

1. **Variable Authentication Number ("VAN")** – Board construed as "a variable number resulting from a coding operation that can be used in verifying the identity of a party or the integrity of information or both."
2. **Sequence of method steps** – Board construed that at least a portion of the "receiving" step must precede the "generating" step.

See Institution Decision (Paper 10), at 7-8.

Claim Constructions – Issues

1. Claim 51 Is Not Limited to a Single Entity
2. “Information for Identifying the Account of the Second Party”

3. “Credential"
4. “Variable Authentication Number (‘VAN’)”
5. “Error Detection Code” (Claim 55)

Claim Constructions

1. **Claim 51 Is Not Limited to a Single Entity** – This was first raised in Patent Owner's Response.
   - Patent Owner argues that all of the Claim 51's method steps must be performed by a single entity. Paper 16, at 7, 9-14.
     - Patent Owner argues that the '302 Patent describes only a single embodiment, where all steps of the claims are performed by a single entity. Paper 16, at 7, 12.

> Significantly, FIG. 8B illustrates that all of the steps of claim 51 take place at the originator's bank. Ex. 2005, at 18:1-20:15.
>
> * * *
>
> Again, it cannot be stated too strongly that the originator's bank (Figure 8B) performs all of the steps of claim 51, a single entity, and that this supplies the sole Section 112 support for claim 51. Ex. 2004, at ¶¶ 29-34, 61-67; Ex. 2005 at 18:20-19:5. Nowhere does the '302 Patent describe or enable a funds transfer authentication process where the four steps of claim 51 divide up among multiple entities. Ex. 2004, at ¶¶ 61-67.

Paper 16, at 4, 7.

See Paper 16, at 4, 7, 9-14.

Claim Constructions

1. Claim 51 Is Not Limited to a Single Entity

- Patent Owner admits that the Preferred Embodiment disclosed in FIG. 8B contradicts its construction.

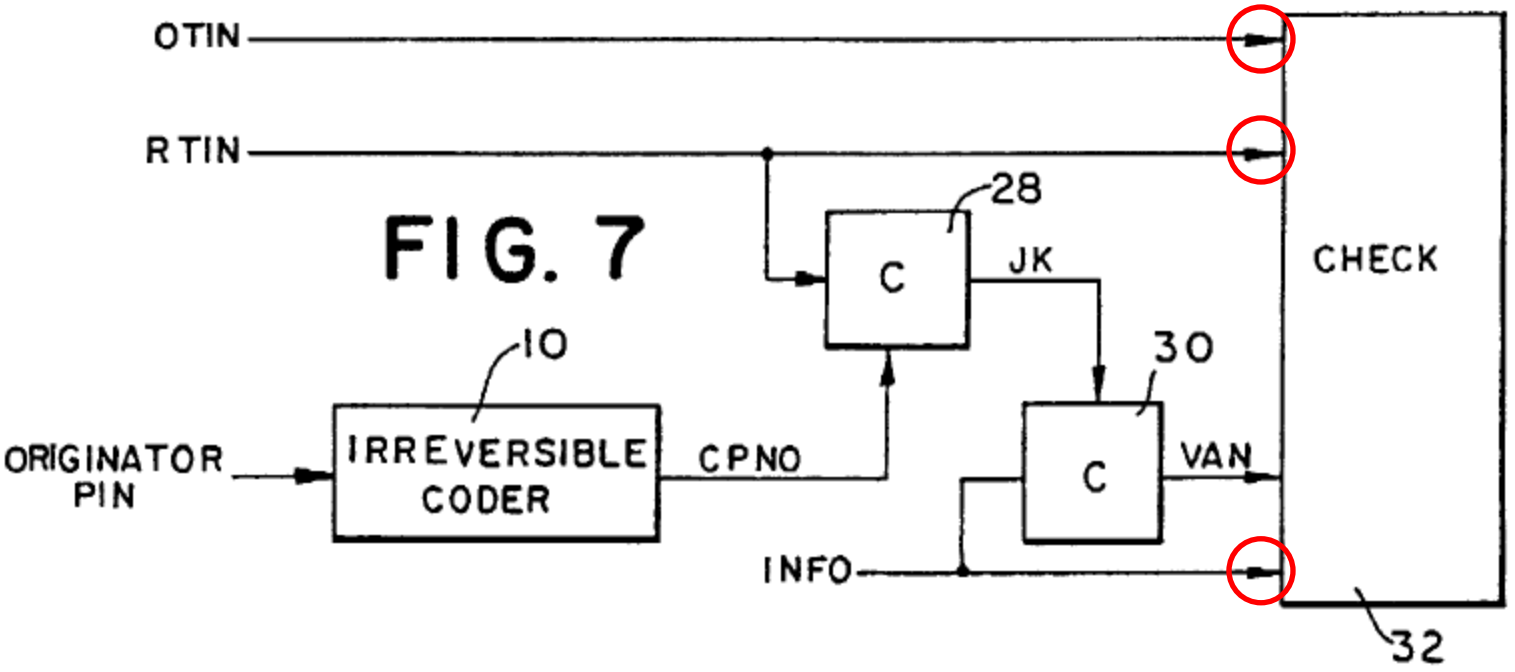
> Up to this point in the discussion, the originator's bank in Figure 8B has not "generated" a VAN (claim 51's "generating" step), since the main embodiment instead "uncodes" (*i.e.*, decrypts) an already-received VAN to verify the funds transfer information. But the written description immediately fills this gap. A fully-

Paper 16 (Patent Owner's Response), at 5.

See Paper 19, at 3-4.

The Embodiment of Claim 51 Illustrated in the Figures

- **The Receiving Step**: "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"

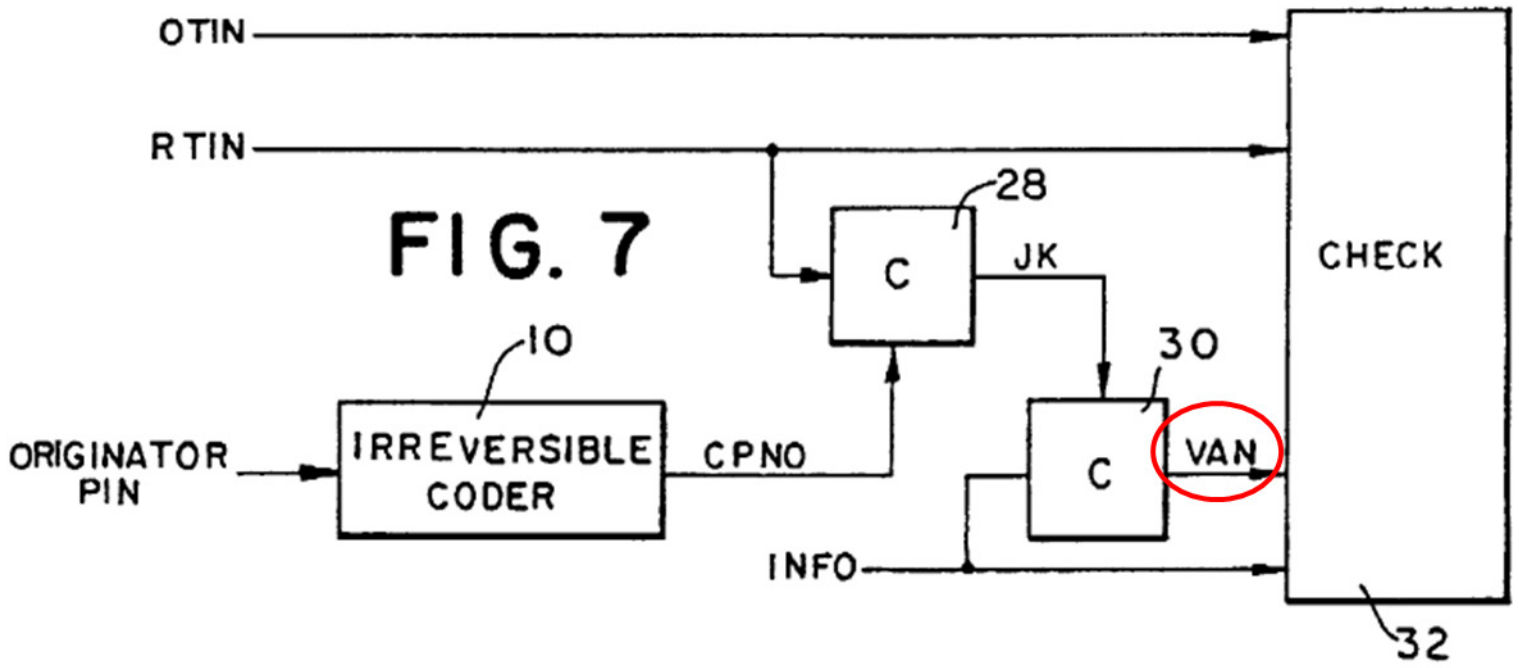


- "This process preferably takes place at the originator's terminal or computer." Ex. 1001, at col. 4 l. 53-54.

See Paper 19, at 7-8; Paper 16, at 3-4.

The Embodiment of Claim 51 Illustrated in the Figures

- **The Generating Step:** "generating a variable authentication number (VAN) using at least a portion of the received funds transfer information"



- "This process preferably takes place at the originator's terminal or computer." Ex. 1001, at col. 4 l. 53-54.

See Paper 19, at 7-8; Paper 16, at 3-4.

The Embodiment of Claim 51 Illustrated in the Figures

- **The Determining Step:** "determining whether the at least a portion of the received funds transfer information is authentic by using the VAN and the credential information"

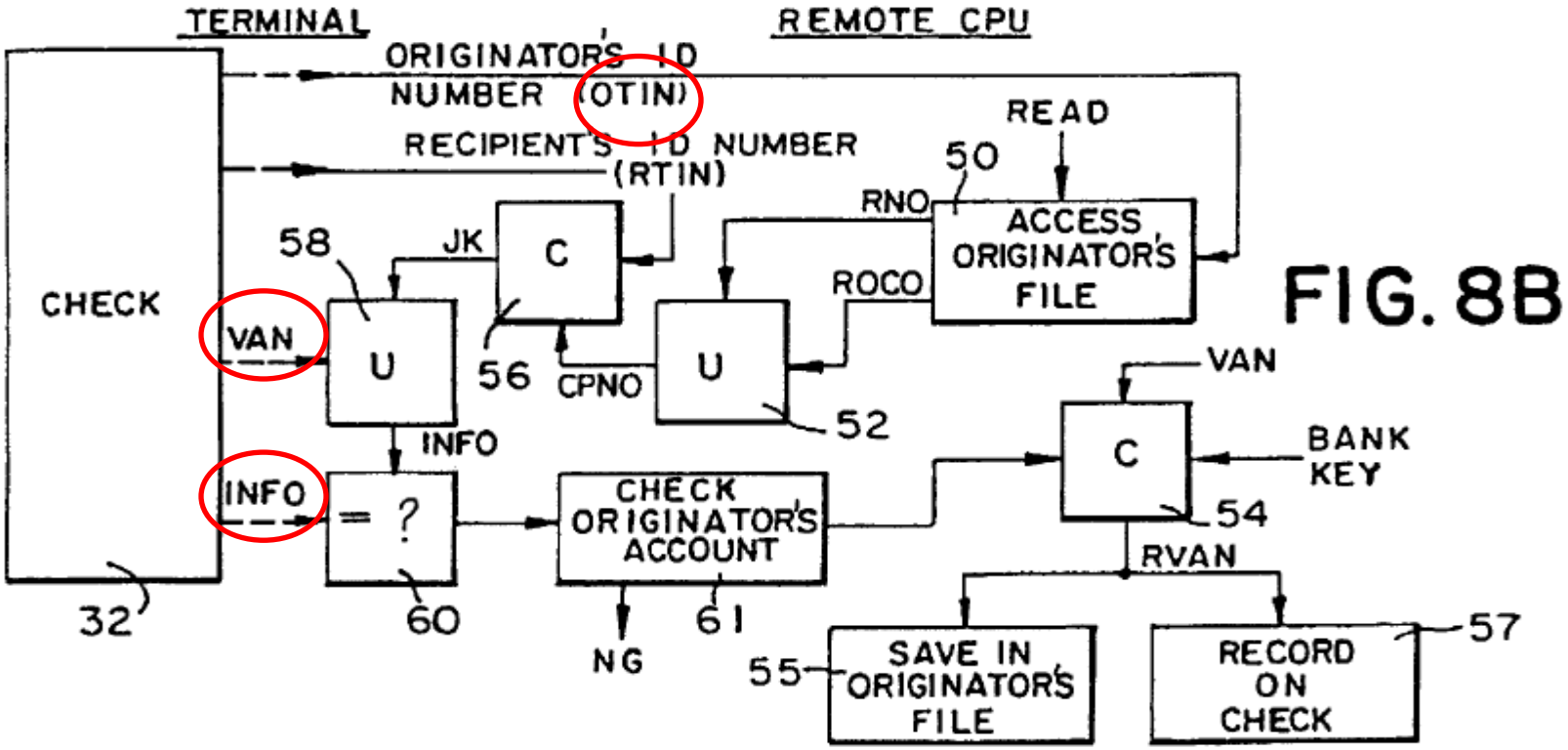


FIG. 8B

- "As shown in FIG. 8B, at the originator's bank…" Ex. 1001, at col. 6 l. 46.

See Paper 19, at 7-8; Paper 16, at 4-5.

The Embodiment of Claim 51 Illustrated in the Figures

- **The Transferring Step:** "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"

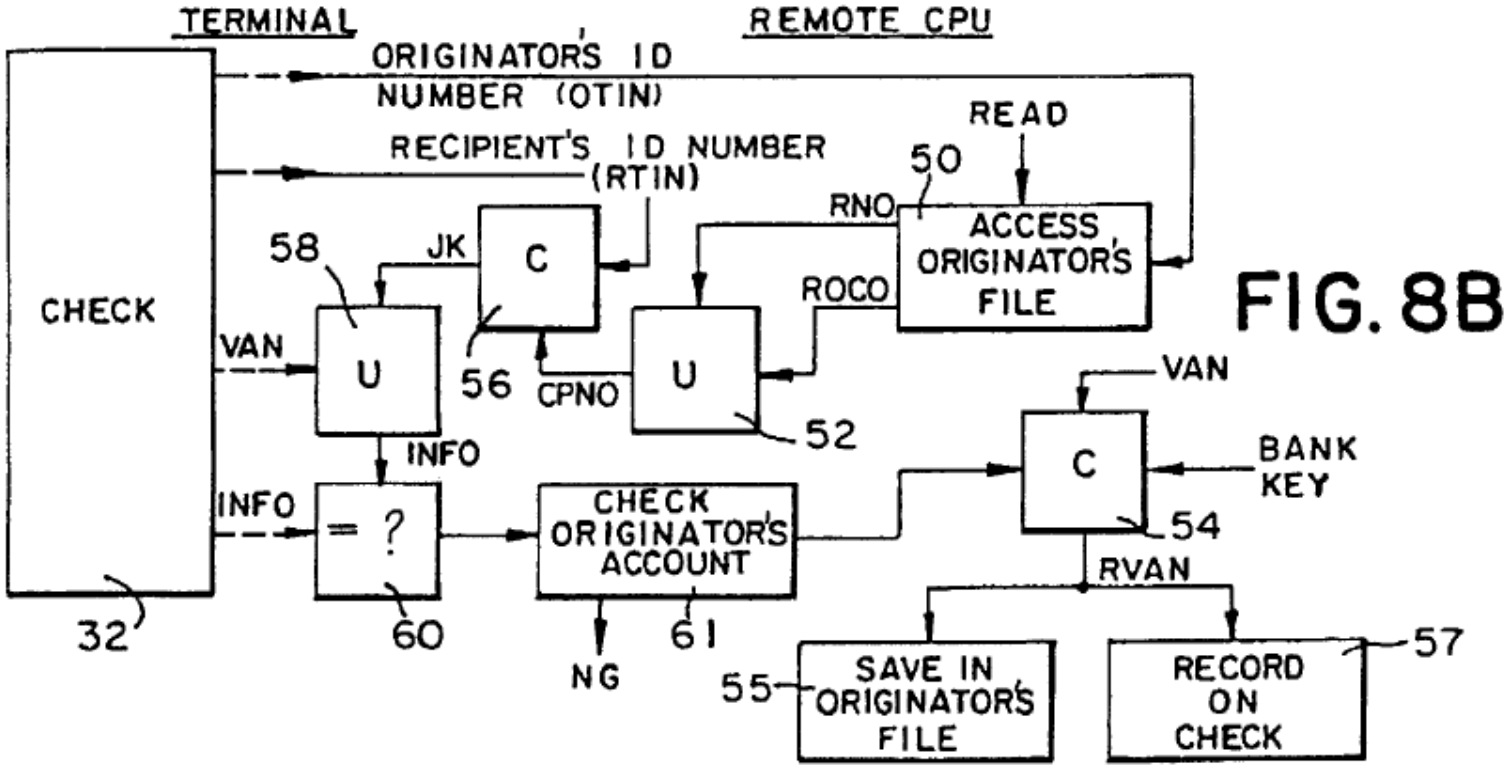


FIG. 8B

- "As shown in FIG. 8B, at the originator's bank…" Ex. 1001, at col. 6 l. 46.

See Paper 19, at 7-8; Paper 16, at 4-5.

Claim Constructions

1. Claim 51 Is Not Limited to a Single Entity

– Patent Owner's Expert Contends Claim 51 Excludes the Preferred Embodiment.

Q. So that embodiment is the one that actually shown in Figure 8B, right? So box 58 8B is the uncoder that you were just referring to, right?

Q. And this is the embodiment that you're saying is not covered by the claims?

A. Yes.

Ex. 1023 (Nielson Depo.), at 44:12-45:3

– Instead, according to Patent Owner's expert, claim 51 covers only the "alternative[]" embodiment described in a mere single sentence in the specification, and not shown in any Figures. Ex. 1023, at 45:4-18.

See Paper 19, at 3-4.

Claim Constructions

1. Claim 51 Is Not Limited to a Single Entity

- Thus, Patent Owner and its expert contend that the claims should be interpreted to *exclude* the preferred embodiment of the figures.
  - This would be legal error. *See MBO Labs, Inc. v. Becton, Dickinson & Co.*, 474 F.3d 1323, 1333 (Fed. Cir. 2007) ("[A] claim interpretation that excludes a preferred embodiment from the scope of the claim is rarely, if ever, correct.").
- Even if the patent only disclosed the "alternative" embodiment, Patent Owner's argument would fail as a matter of law.
  - *McCarty v. Lehigh Valley R.R. Co.*, 160 U.S. 110, 116 (1895)) ("if we once begin to include elements not mentioned in the claim, in order to limit such claim …, we should never know where to stop.")
  - *Kara Tech. Inc. v. Stamps.com Inc.,* 582 F.3d 1341, 1347-48 (Fed. Cir. 2009) ("The claims, not specification embodiments, define the scope of patent protection. The patentee is entitled to the full scope of his claims, and we will not limit him to his preferred embodiment ***or import a limitation from the specification***.") (emphasis supplied).

See Paper 19, at 4-5.

Claim Constructions

1. Claim 51 Is Not Limited to a Single Entity

- Nothing in the language of claim 51 requires that all steps be performed by a single entity.
  - *Tehrani v. Hamilton Med., Inc.*, 331 F.3d 1355, 1362-63 (Fed. Cir. 2003) (holding claimed step of "measuring" need not all be performed by the device performing other claimed steps, because the claim did not "specif[y] that the [device] must do the measuring").
  - *See BMC Res., Inc. v. Paymentech, L.P.*, 498 F.3d 1373, 1379-81 (Fed. Cir. 2007) ("this court will not unilaterally restructure the claim" where the patent owner "could have drafted its claims to focus on one entity").
- When the applicant wanted to restrict steps to a particular entity, he did so explicitly.
  - For example, the preamble to claim 51 requires that the credential be issued "***by a trusted party***." Ex. 1001, at 33:18-19 (emphasis supplied).

See Paper 19, at 5-6.

Claim Constructions

1. Claim 51 Is Not Limited to a Single Entity

- Patent Owner Mischaracterizes Petitioner's Expert's Testimony.
  - Patent Owner argues that Petitioner's expert "conceded that the written description discloses a single entity (the originator's bank) performing all acts of the authentication method." Paper 16, at 10.
  - Mr. Diffie testified only that *Figure 8B* showed steps being performed by the originator's bank. Ex. 2005, at 18:12-19:5 (Q. … in what we've just seen at Figure 8B, would you agree…").
  - As to the proper claim interpretation, Mr. Diffie was unequivocal: "there is no requirement in claim 51 that the steps all be performed by the same entity." Ex. 2005, at 19:7-17.

See Paper 19, at 7-8.

Claim Constructions

2. **"Information for Identifying the Account of the Second Party"** – Board did not construe this term.

- Patent Owner argues that this claim term "does not cover a mere name … of a second party." Paper 16, at 16.
- Patent Owner relies on prior District Court opinions that expressly reject the argument Patent Owner is now making. *Id.* (citing Ex. 1013, at 23-24; Ex. 1014, at 13; and Ex. 1015, at 41-43).

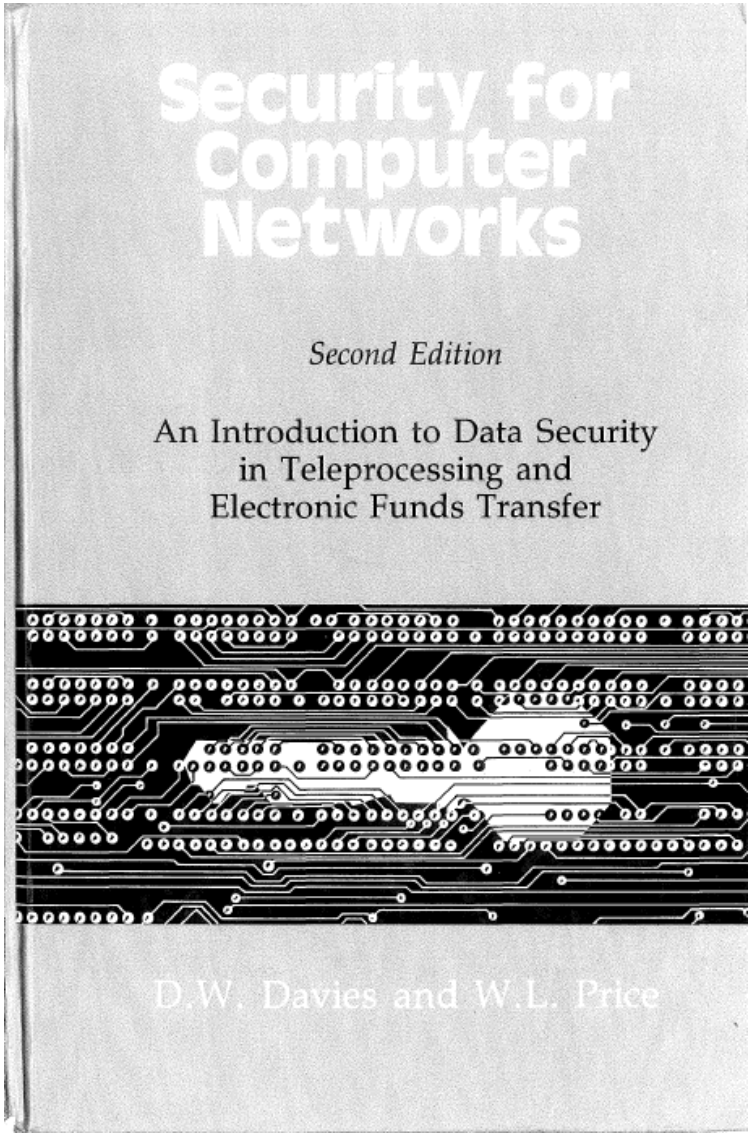
> The text of this claim does not require specific account identification. Moreover, the information required need only be "*for* identifying," not "*that* identifies." The Court construes the term to mean, "information that is used to identify an account of the first/second party."

See, e.g., Ex. 1013 (*Stambler v. JPMorgan Chase & Co.*, CC Opinion), at 24

- Patent Owner does not explain why a name, if used to identify an account, could not satisfy this claim element.

See Paper 19, at 9-10.

Security for Computer Networks (Davies)



Published in 1989 (§ 102(b))

Board found on the initial record:

- Claims 51 and 53 (*anticipated by Davies*)
- Claims 51, 53, 55 and 56 (*obvious in view of Davies*)

Security for Computer Networks (Davies)

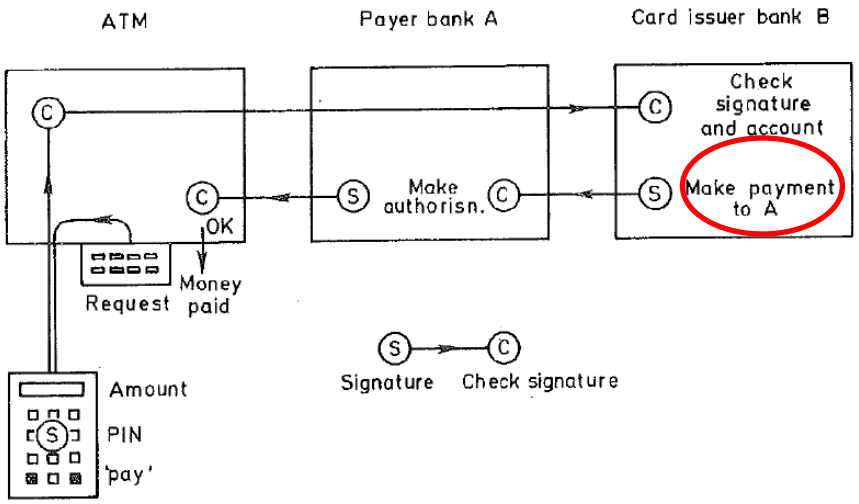


Fig. 10.23 Shared ATM network using digital signatures

- **Preamble [Part A]**: "A method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party"

- "The message and its signature are checked and if all is well an authorization goes to the ATM to release the money." Ex. 1004, Davies p. 331.

See Paper 7, at 24-25.

Security for Computer Networks (Davies)

1 Bank identity	2 Bank public key
3 Expiry date	4 Signature of 1–3 by key registry
5 Customer identity	6 Customer public key
7 Expiry date	8 Signature of 5–7 by Bank
9 Cheque sequence number	10 Transaction type
11 Amount of payment	12 Currency
13 Payee identity	14 Description of payment
15 Date and time	16 Signature of 9–15 by customer

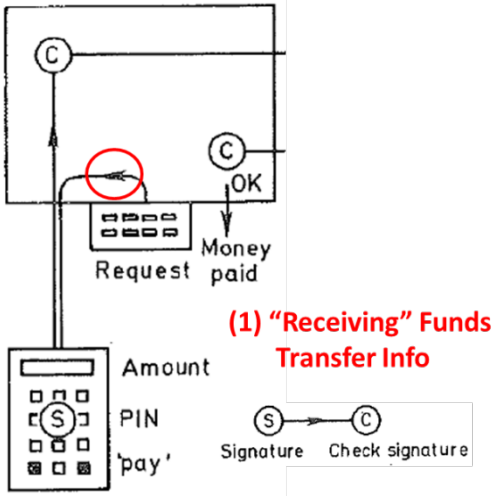
Fig. 10.22 Electronic cheque

- **Preamble [Part B]**: "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 second section of the cheque contains the customer identity and his public key signed by the bank and therefore verifiable using the public key stated in the first section … These first two sections of the cheque are constants which appear on every cheque drawn…" Ex. 1004, Davies p. 328.

See Paper 7, at 25-27; Paper 19, at 16-18.

Security for Computer Networks (Davies)



Davies, FIG. 10.23

- **The Receiving Step**: "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"

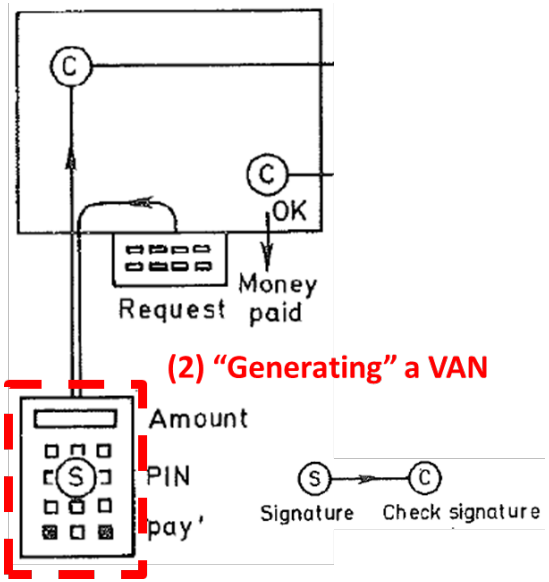
- "The customer's request is formed into a message and presented to the token." Ex. 1004, Davies p. 330 and FIG. 10.23.

1 Bank identity	2 Bank public key
3 Expiry date	4 Signature of 1–3 by key registry
5 Customer identity	6 Customer public key
7 Expiry date	8 Signature of 5–7 by Bank
9 Cheque sequence number	10 Transaction type
11 Amount of payment	12 Currency
13 Payee identity	14 Description of payment
15 Date and time	16 Signature of 9–15 by customer

Fig. 10.22 Electronic cheque

See Paper 7, at 27-29; Paper 19, at 14-16.

Security for Computer Networks (Davies)



Davies, FIG. 10.23

- **The Generating Step:** "generating a variable authentication number (VAN) using at least a portion of the received funds transfer information"
- "The 'customer's request is formed into a message and presented to the token. Here it is signed and returned to the ATM." Ex. 1004, Davies p. 330-31.
- "The final signature, by the customer, covers all the variable information in the cheque." *Id.* at p. 329.

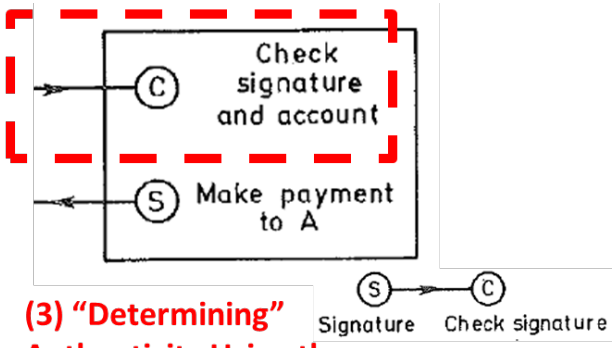
9 Cheque sequence number	10 Transaction type
11 Amount of payment	12 Currency
13 Payee identity	14 Description of payment
15 Date and time	16 Signature of 9–15 by customer

Fig. 10.22 Electronic cheque

Customer's Signature (Item 16) is a "VAN"

See Paper 7, at 29-32.

Security for Computer Networks (Davies)



(3) "Determining" Authenticity Using the VAN and Credential Info

Davies, FIG. 10.23

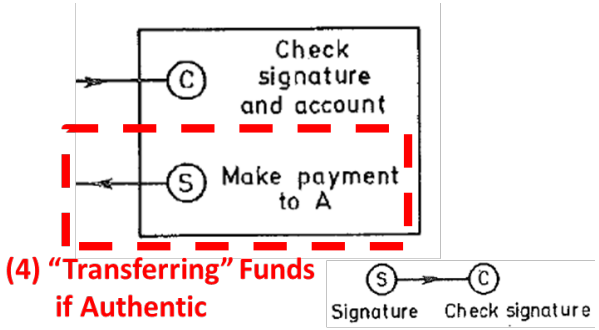
1 Bank identity	2 Bank public key
3 Expiry date	4 Signature of 1–3 by key registry
5 Customer identity	6 Customer public key
7 Expiry date	8 Signature of 5–7 by Bank
9 Cheque sequence number	10 Transaction type
11 Amount of payment	12 Currency
13 Payee identity	14 Description of payment
15 Date and time	16 Signature of 9–15 by customer

Fig. 10.22 Electronic cheque

- **The Determining Step:** "determining whether the at least a portion of the received funds transfer information is authentic by using the VAN and the credential information"
- "[T]he 'cheque' passes via the payer bank, A, to the card issuer bank, B. Here the signature is checked and the customer's account examined…"
  Ex. 1004, Davies p. 331.
- "The second section of the cheque contains the customer identity and his public key, signed by the bank and therefore verifiable…" *Id.* at p. 328
- "At the receiving end, the message is obtained in plaintext form and, in order to check the signature, it is enciphered with A's public key…" *Id.* at p. 260.

See Paper 7, at 30-32.

Security for Computer Networks (Davies)



Davies, FIG. 10.23

- **The Transferring Step:** "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"

- "Here the signature is checked and the customer's account examined and, if everything is in order, debited."
  Ex. 1004, Davies p. 331 and FIG. 10.23.

See Paper 7, at 33-34.

Security for Computer Networks (Davies)

- Patent Owner alleges the following with respect to Davies:
  A. Petition Allegedly Conflates Unrelated Disclosures of Davies
  B. All Steps Allegedly Not Performed by a Single Entity
  C. Davies Allegedly Does Not Disclose "Receiving Funds Transfer Information" and the "Credential Being Previously Issued"
  D. Davies Allegedly Does Not Disclose a "Credential" (as defined by the Patent Owner)
  E. Davies Allegedly Does Not Disclose "Information Identifying the Account of the Second Party"

See Paper 19, at 11-18.

Cited Disclosures of Davies are Explicitly Related

- The disclosures are related, as described by Davies.
  - Davies describes how funds can be transferred between accounts using paper checks, and then explains that the paper checks can be "[c]hanged into a modern form as a message with a digital signature," which can be "regarded as an 'electronic cheque.'" Ex. 1004, Davies pp. 285-86.
  - Davies explicitly states that "the "same intelligent token which provides an electronic cheque between individuals can ... also 'cash a cheque' at an ATM with on-line verification." *Id.* at p. 330.
  - Davies teaches "the cheque…should contain all of the items listed in Figure 10.22." *Id.* at p. 328.

See Paper 19, at 11-12.

Claim 51 is Not Limited to a Single Entity

- Patent Owner argues that "Davies does not anticipate because the four method steps are not performed by a single entity." Paper 16, at 31.

- As previously discussed, however, this is **not a requirement of the claims**. *See* Paper 19, Part II.A.

See Paper 19, at 13.

Davies Discloses a Single Entity Performing All Steps of Claim 51

- Even if Claim 51 were construed to require a single entity performing all method steps, Davies discloses this:
  - The "receiving" steps and "generating" steps are performed by the token issued by the customer's bank. *See, e.g.,* Ex. 2005, at 90:25-91:5.
    - "The token … authenticates a message ***to its 'master' which is the card issuer's computer system***." Ex. 1004, Davies p. 327 (emphasis supplied).
    - Davies also describes additional controls the card issuer can place on the token, *e.g.,* limits on transactions, and notes the token's "intelligence is used on behalf of the customer ***and the card issuer***…." *Id.* at pp. 325, 327 (emphasis supplied).
  - Thus, the customer's bank in Davies performs or directs the performance of all of the claimed steps, therefore satisfying the "directs or controls" standard under *Akamai* (assuming it applies to anticipation).

See Paper 19, at 13-14.

Davies Discloses "Receiving Funds Transfer Information" and a "Previously Issued" Credential

- Contrary to Patent Owner's assertion, Davies does not disclose that the "customer 'receives' funds transfer information from itself." Paper 16, at 34.
- Rather, the token, issued by the card issuing bank, receives funds transfer information from a terminal. Ex. 2005, at 90:3-91:5.
  - As Davies explains, the token contains a microprocessor and memory allowing the use of "intelligence" when the token is inserted into the terminal. Ex. 1004, Davies pp. 324-25, 327.
  - The token receives the transaction data for the check from the terminal, and signs that data. *Id.* at 331 ("The 'cheque' enters the card from the terminal...."); *id.* at 329 ("A terminal is needed to generate a cheque, sign it with the aid of the token and send it….").
  - The token (more precisely, the microprocessor in the token) receives the electronic check data structure (Fig. 10.22) during a transaction. *Id.* at 330-31 and Fig. 10.23 ("The customer's request is formed into a message and presented to the token.").

See Paper 19, at 14.

Davies Discloses "Receiving Funds Transfer Information" and a "Previously Issued" Credential

- Patent Owner asserts that the "customer identity" information in the electronic check cannot be both "received" by the token during the receiving step and be part of a "credential" that is "previously issued." Paper 16, at 36-38.

- Patent Owner never explains the basis for its premise.
  - The "previously issued" credential mentioned in the preamble does not appear in the claim until the "determining" step.
  - Accordingly, the claim requires only that the credential be issued before the "determining" step takes place.
  - Patent Owner does not dispute that the determining step in Davies occurs after the credential is issued.

See Paper 19, at 14-15.

Davies Discloses "Receiving Funds Transfer Information" and a "Previously Issued" Credential

- Even if the credential must be issued before the "receiving" step, Davies discloses this:
  - As admitted by the Patent Owner, the information found in items 1-8 of the electronic check (including item 5, "Customer identity") are stored in the memory of the token.

> MasterCard also ignores that Items 1-8 on Davies the electronic check are not variable. Ex. 1004, at 328 ("These first two sections of the cheque are constants which appear on every cheque…"). As such, they are already contained on the intelligent token before it is every received by the customer, much like many of the fields on a conventional paper check. Notably, among these pre-set fields is field 5, customer identity. This is significant because "customer identity" is what

Paper 16 (Patent Owner's Response), at 36.

See Paper 19, at 14-15.

Davies Discloses "Receiving Funds Transfer Information" and a "Previously Issued" Credential

- Even if the credential must be issued before the "receiving" step, Davies discloses this:
  - "In order to allow the content of the cheque to be validated with minimum of data beyond the cheque itself it should contain all the items listed in Figure 10.22." *Id.* at p. 328.
  - "The 'cheque' enters the card from the terminal...." Ex. 1004, Davies p. 331.
  - "A terminal is needed to generate a cheque, sign it with the aid of the token and send it…." *Id.* at p. 329.
  - "The customer's request is formed into a message and presented to the token." *Id.* at p. 330.

- Davies thus describes how (1) the information for identifying the account of the first party and (2) the second party, and (3) a transfer amount are received by the token from the terminal as part of the signing process.

See Paper 19, at 14-16.

Davies Discloses a "Credential" (even using the Patent Owner's Proffered Definition)

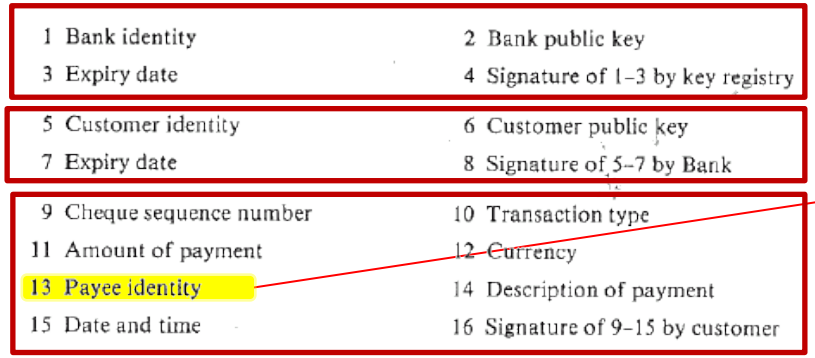
- The customer's certificate in Davies meets the limitations of a "credential."
  - The customer's public key in the certificate is ***public*** (i.e., non-secret). Ex. 1020, at ¶¶ 19, 26, 37.
  - This non-secret credential information is used to "determine whether the at least a portion of the received funds transfer information is authentic" in the "determining" step. Ex. 1004, Davies pp. 328-29.
  - If the signature is verified, the received funds transfer information is determined to be authentic. Paper 7, at 30-32 (citing Davies).
  - Thus, the "credential" is used to determine the identity of the signor of the electronic check message (*i.e.,* the party requesting a transfer of funds from his account). Ex. 1004, Davies pp. 328, 331.

See Paper 7, at 25-27;
Paper 19, at 17-18.

Davies Discloses "Information for Identifying the Account of the Second Party"

- Patent Owner's counter-argument is based on the assertion that in the Davies ATM disclosure, "no 'payee' field is needed or used." Paper 16, at 26.

- Patent Owner's argument fails to address Davies's disclosure of an electronic check at a non-ATM point of sale, which Patent Owner does not dispute includes an identification of the party being paid. Ex. 1004, Davies p. 328 and Fig. 10.22, Item 13 ("Payee identity").



1 Bank identity	2 Bank public key
3 Expiry date	4 Signature of 1–3 by key registry
5 Customer identity	6 Customer public key
7 Expiry date	8 Signature of 5–7 by Bank
9 Cheque sequence number	10 Transaction type
11 Amount of payment	12 Currency
13 Payee identity	14 Description of payment
15 Date and time	16 Signature of 9–15 by customer

Fig. 10.22 Electronic cheque

"Payee Identity" = "Information for Identifying the Account of the Second Party"

See Paper 19, at 18-19.

Davies Discloses "Information for Identifying the Account of the Second Party"

- Patent Owner is wrong to assert that no payee identity is used in the ATM example of Davies.
  - Davies teaches that the structure of the electronic check message is the same when cashing a check at an ATM.
    - Check "should contain all the items listed in Figure 10.22." Ex. 1004, Davies p. 328.
    - "The same intelligent token which provides an electronic cheque between individuals … can also 'cash a cheque' at an ATM with on-line verification." *Id.* at p. 330.

See Paper 19, at 19.

Davies Discloses "Information for Identifying the Account of the Second Party"

- Patent Owner is wrong to assert that no payee identity is used in the ATM example of Davies.
  - Petitioner's expert confirmed that the payee field would be necessary to complete an ATM transaction. Ex. 2005, at 71:16-72:13.
  - Even Patent Owner's expert admitted that the ATM owner must be identified during the transaction. Ex. 1023, at 100:7-102:23.

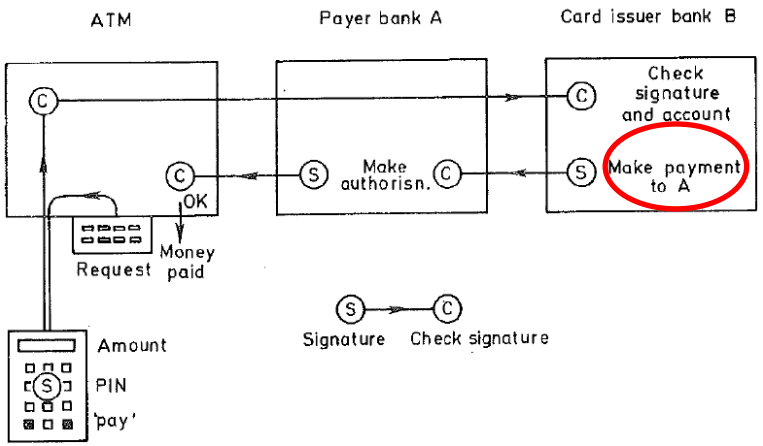
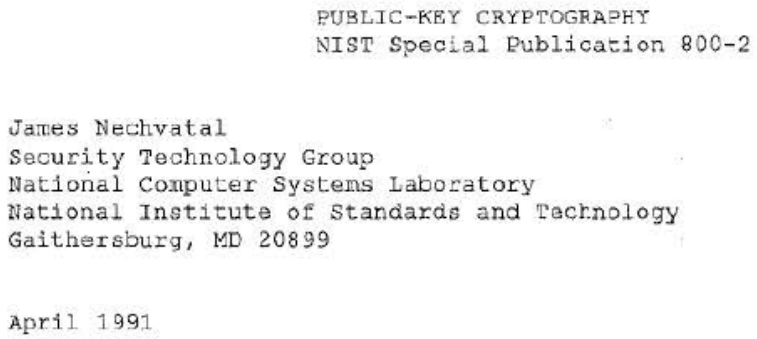


Fig. 10.23 Shared ATM network using digital signatures

See Paper 19, at 19.

Public-Key Cryptography (Nechvatal)



PUBLIC-KEY CRYPTOGRAPHY
NIST Special Publication 800-2

James Nechvatal
Security Technology Group
National Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

April 1991

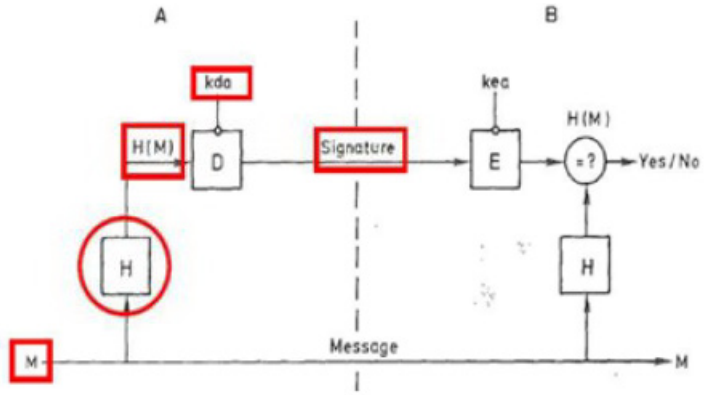
- Published in April 1991 (§ 102(b))

- Board found on the initial record:
  - Claim 55 (*obvious over Davies and Nechvatal*)

Claim 55 is Obvious over Davies and Nechvatal

- Davies teaches that a hash function "**H(M)**" should be used to create the digital signature.

- **Claim 55**: "the VAN is generated by using an error detection code derived by using at least a portion of the funds transfer information"



The construction of the signature is shown by the upper line in the figure. A one-way function $H(M)$ is formed using all the bits of the message and then this quantity is transformed by the public key signature method, to form the signature of the whole message.

Ex. 1004, Davies p. 260 and FIG. 9.5

See Paper 7, at 34- 35; Paper 19, at 22-23.

Claim 55 is Obvious over Davies and Nechvatal

- Nechvatal teaches that a hash function is an error detection code.

- **Claim 55**: "the VAN is generated by using an error detection code derived by using at least a portion of the funds transfer information"

> As we note below, hash functions are useful auxiliaries in this context, i.e., in validating the identity of a sender. They can also serve as cryptographic checksums (i.e., error-detecting codes), thereby validating the contents of a message. Use of signatures and hash functions can thus provide authentication and verification of message integrity at the same time.

Ex. 1005, Nechvatal p. 32

See Paper 7, at 34- 35; Paper 19, at 22-23.

Claim 55 is Obvious over Davies and Nechvatal

- Digital signatures themselves are also known in the art to be error detection codes.

- **Claim 55**: "the VAN is generated by using an error detection code derived by using at least a portion of the funds transfer information"

In principle the signature provides error checking, since any change to the message or signature (whether enciphered or not) would be recognized when the signature is checked. But sometimes signatures are not checked until someone is ready to

Ex. 1004, Davies p. 261

different. But I'm saying that this is a very, very good definition of error detection code.

Q. Would this definition cover a digital signature?

A. Yes.

Q. And why do you say that?

A. Well, the definition here, it says "the result of applying an algorithm for coding information that when applied to original information creates coded information." Let's go that far.

So most of the time when you have a digital signature, it operates on the original information and produces some kind of code or extra information. "Wherein changes to the original information can be detected without complete recovery of the original information."

If somebody changes a message that has a digital signature, then you will be able to tell that it's changed but you can't necessarily recover what the original message was.

Ex. 1023 (Nielson Depo.), at 60:23-61:19

See Paper 7, at 34- 35; Paper 19, at 22-23.

Patent Owner's Case Law Regarding Obviousness is Distinguishable

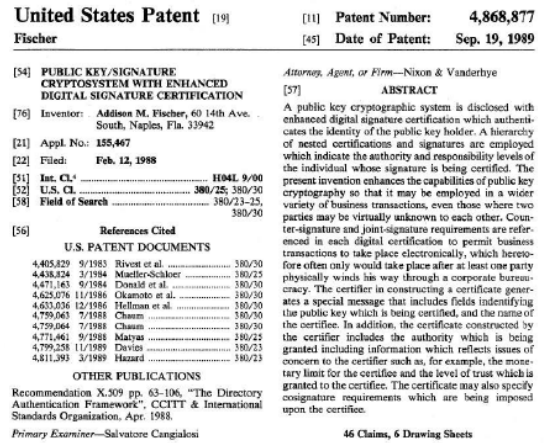
- In *Kinetic* (1) there was no evidence explaining why the references would be combined, (2) none of the prior art taught one of the essential claim elements (treating a wound), and (3) the references taught away from the claimed invention. 688 F.3d at 1369.
  - *See Boston Scientific Scimed v. Cordis Corp.*, Appeal No. 2014-008135, 2015 WL 883933, at *7 (P.T.A.B. Feb. 27, 2015) (distinguishing *Kinetic*).
- *Broadcom* involved a single-reference obviousness argument, based on a reference directed to a "different problem" from the one the patent addressed, and there was no evidence explaining why the reference should be modified. 732 F.3d at 1334.
- *Compare KSR Int'l Co. v. Teleflex Inc.,* 550 U.S. 398, 418 (2007) ("Often, it will be necessary for a court to look to interrelated teachings of multiple patents…").

See Paper 19, at 21-22.

Fischer and Piosenka

U.S. Pat No. 4,868,877

Issued Sep. 19, 1989 (§ 102(b))



United States Patent [19]
Fischer

[11] **Patent Number: 4,868,877**
[45] **Date of Patent: Sep. 19, 1989**

[54] **PUBLIC KEY/SIGNATURE CRYPTOSYSTEM WITH ENHANCED DIGITAL SIGNATURE CERTIFICATION**

[76] Inventor: **Addison M. Fischer**, 60 14th Ave. South, Naples, Fla. 33942

[21] Appl. No.: **155,467**

[22] Filed: **Feb. 12, 1988**

[51] **Int. Cl.**[4] **H04L 9/00**
[52] **U.S. Cl.** **380/25**; 380/30
[58] **Field of Search** 380/23–25, 380/30

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,405,829	9/1983	Rivest et al.	380/30
4,438,824	3/1984	Mueller-Schloer	380/25
4,471,163	9/1984	Donald et al.	380/30
4,625,076	11/1986	Okamoto et al.	380/30
4,633,036	12/1986	Hellman et al.	380/30
4,759,063	7/1988	Chaum	380/30
4,759,064	7/1988	Chaum	380/30
4,771,461	9/1988	Matyas	380/25
4,799,258	11/1989	Davies	380/23
4,811,393	3/1989	Hazard	380/23

OTHER PUBLICATIONS

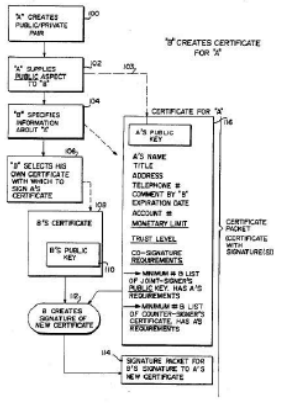
Recommendation X.509 pp. 63–106, "The Directory Authentication Framework", CCITT & International Standards Organization, Apr. 1988.

Primary Examiner—Salvatore Cangialosi
Attorney, Agent, or Firm—Nixon & Vanderhye

[57] **ABSTRACT**

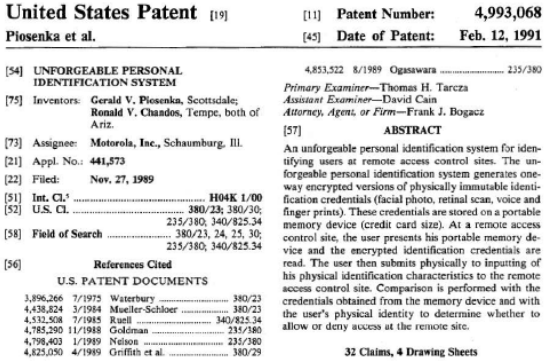
A public key cryptographic system is disclosed with enhanced digital signature certification which authenticates the identity of the public key holder. A hierarchy of nested certifications and signatures are employed which indicate the authority and responsibility levels of the individual whose signature is being certified. The present invention enhances the capabilities of public key cryptography so that it may be employed in a wider variety of business transactions, even those where two parties may be virtually unknown to each other. Counter-signature and joint-signature requirements are referenced in each digital certification to permit business transactions to take place electronically, which heretofore often only would take place after at least one party physically winds his way through a corporate bureaucracy. The certifier in constructing a certificate generates a special message that includes fields indentifying the public key which is being certified, and the name of the certifier. In addition, the certificate constructed by the certifier includes the authority which is being granted including information which reflects issues of concern to the certifier such as, for example, the monetary limit for the certifee and the level of trust which is granted to the certifee. The certificate may also specify cosignature requirements which are being imposed upon the certifee.

46 Claims, 6 Drawing Sheets



U.S. Pat No. 4,993,086

Issued Feb. 12, 1991 (§ 102(b))



United States Patent [19]
Piosenka et al.

[11] **Patent Number: 4,993,068**
[45] **Date of Patent: Feb. 12, 1991**

[54] **UNFORGEABLE PERSONAL IDENTIFICATION SYSTEM**

[75] Inventors: **Gerald V. Piosenka**, Scottsdale; **Ronald V. Chandos**, Tempe, both of Ariz.

[73] Assignee: **Motorola, Inc.**, Schaumburg, Ill.

[21] Appl. No.: **441,573**

[22] Filed: **Nov. 27, 1989**

[51] **Int. Cl.**[5] **H04K 1/00**
[52] **U.S. Cl.** **380/23**; 380/30; 235/380; 340/825.34
[58] **Field of Search** 380/23, 24, 25, 30; 235/380; 340/825.34

[56] **References Cited**

U.S. PATENT DOCUMENTS

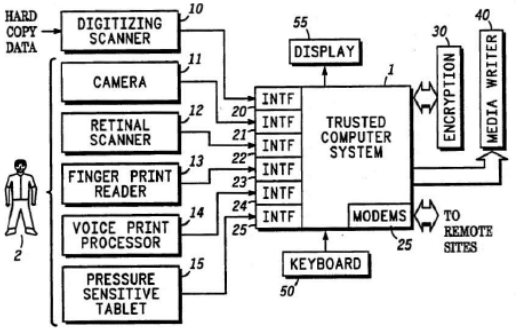
3,896,266	7/1975	Waterbury	380/23
4,438,824	3/1984	Mueller-Schloer	380/23
4,532,508	7/1985	Ruell	340/825.34
4,785,290	11/1988	Goldman	235/380
4,798,403	1/1989	Nelson	235/380
4,825,050	4/1989	Griffith et al.	380/29
4,853,522	8/1989	Ogasawara	235/380

Primary Examiner—Thomas H. Tarcza
Assistant Examiner—David Cain
Attorney, Agent, or Firm—Frank J. Bogacz

[57] **ABSTRACT**

An unforgeable personal identification system for identifying users at remote access control sites. The unforgeable personal identification system generates one-way encrypted versions of physically immutable identification credentials (facial photo, retinal scan, voice and finger prints). These credentials are stored on a portable memory device (credit card size). At a remote access control site, the user presents his portable memory device and the encrypted identification credentials are read. The user then submits physically to inputting of his physical identification characteristics to the remote access control site. Comparison is performed with the credentials obtained from the memory device and with the user's physical identity to determine whether to allow or deny access at the remote site.

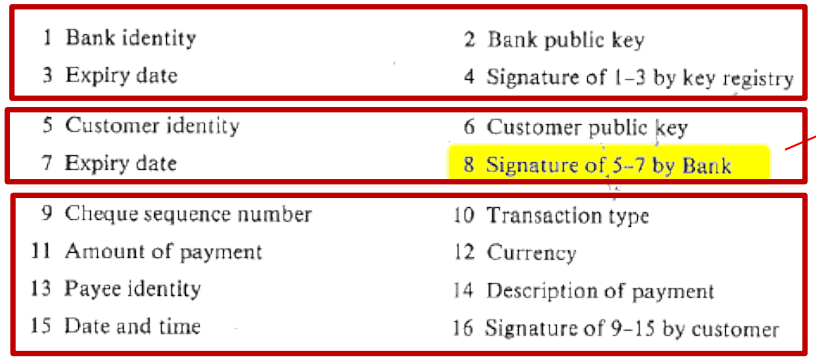
32 Claims, 4 Drawing Sheets



Board found on the initial record:
Claim 56 (*obvious over Davies, Fischer and Piosenka)*

Claim 56 is Obvious over Davies, Fischer and Piosenka

Claim 56: "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…"



1 Bank identity	2 Bank public key
3 Expiry date	4 Signature of 1–3 by key registry
5 Customer identity	6 Customer public key
7 Expiry date	8 Signature of 5–7 by Bank
9 Cheque sequence number	10 Transaction type
11 Amount of payment	12 Currency
13 Payee identity	14 Description of payment
15 Date and time	16 Signature of 9–15 by customer

Fig. 10.22 Electronic cheque

- Davies discloses a Bank's Signature ("VAN1") used to secure the credential information to the customer.

See Paper 7, at 69-76; Paper 19, at 24-25.

Claim 56 is Obvious over Davies, Fischer and Piosenka

Claim 56: "…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."

- Davies teaches sending a certificate chain. Paper 7, at 69-70.
  - "In order to allow the content of the cheque to be validated with minimum of data beyond the cheque itself it should contain all the items listed in Figure 10.22." Ex. 1004, Davies p. 328.
  - "Anyone can verify the bank's public key using the signature and the public key of the key registry…" *Id.*; Ex. 1020, at ¶ 158.
  - "It would be natural for a verified public key issued by the bank to be accepted as a kind of bank reference." Ex. 1004, Davies p. 331.

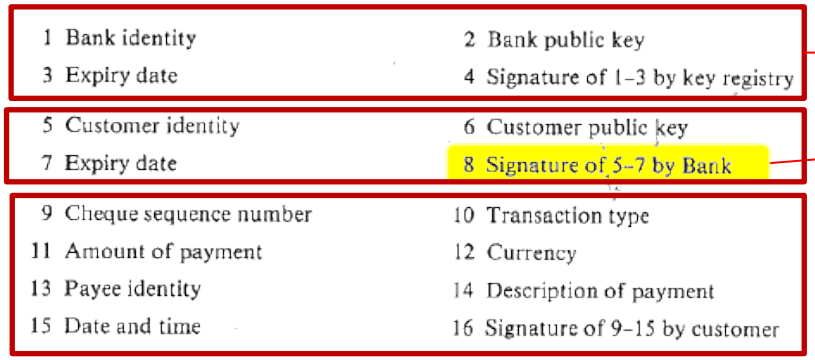


Fig. 10.22 Electronic cheque

The Bank's Certificate

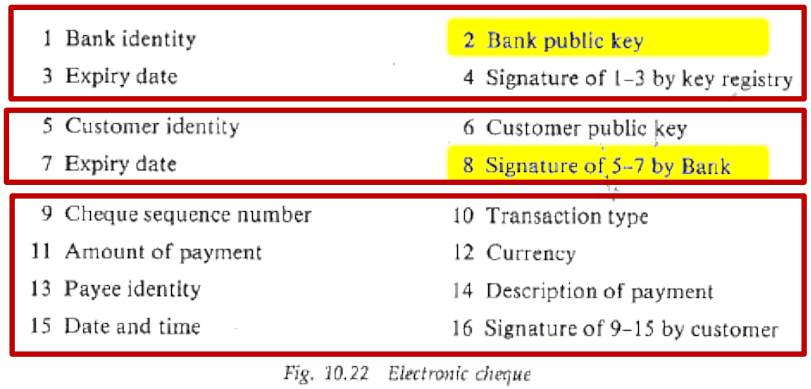
The Bank's Signature (VAN1) on the Customer's Certificate

See Paper 7, at 69-76; Paper 19, at 24-25.

Claim 56 is Obvious over Davies, Fischer and Piosenka

Claim 56: "…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."

- Fischer teaches verifying a certificate chain.



1 Bank identity	2 Bank public key
3 Expiry date	4 Signature of 1–3 by key registry
5 Customer identity	6 Customer public key
7 Expiry date	8 Signature of 5–7 by Bank
9 Cheque sequence number	10 Transaction type
11 Amount of payment	12 Currency
13 Payee identity	14 Description of payment
15 Date and time	16 Signature of 9–15 by customer

Fig. 10.22 Electronic cheque

Ex. 1004, Davies, FIG. 10.22

All certificates must be accompanied by signatures which are themselves authorized by antecedent certificates. Ultimately all the authority can be traced to a set of certificates which have been signed by the holder of the meta-certificate (or possibly a small set of meta-certificates). Each meta-certificate is well known and distributed to all parties "throughout the world".

The recipient examines every signature supplied and verifies that each accurately signs its purported object (whether the object is a primary object, a certificate, or another signature) using the procedure detailed in FIG. 3. The recipient insures that each signature includes a corresponding validated certificate.

If a certificate requires joint signatures, then the recipient insures that the required number of these necessary signatures (to the same object) are present. If the certificate requires counter signatures, then the recipient insures that the required number from the designated subset are present (the counter signatures have signatures as their object).

Ex. 1006, Fischer, at 17:27-46.

See Paper 7, at 69-76; Paper 19, at 24-25.

Claim 56 is Obvious over Davies, Fischer and Piosenka

- Petitioner relies on Piosenka for its explicit teaching to deny a request if the digital signature cannot be authenticated. Paper 7, at 70-71.

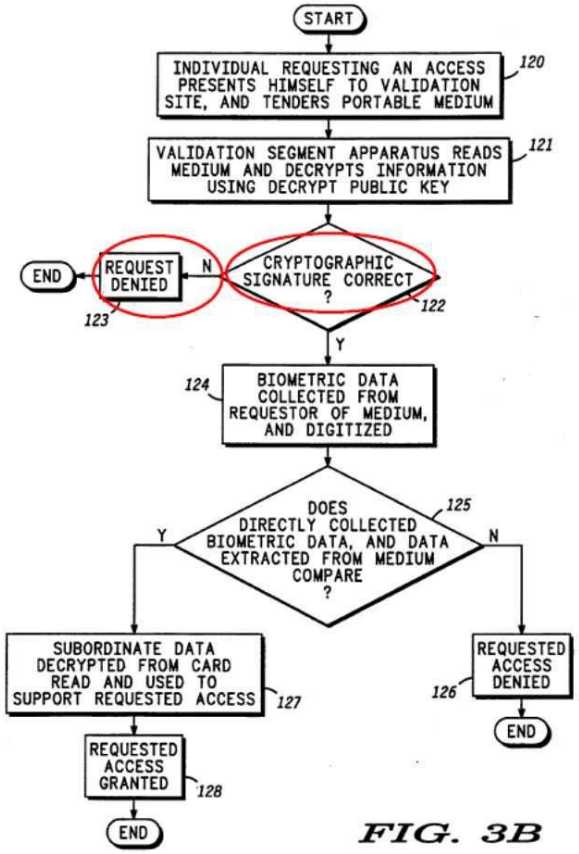


FIG. 3B

See Paper 7, at 69-76; Paper 19, at 24-25.

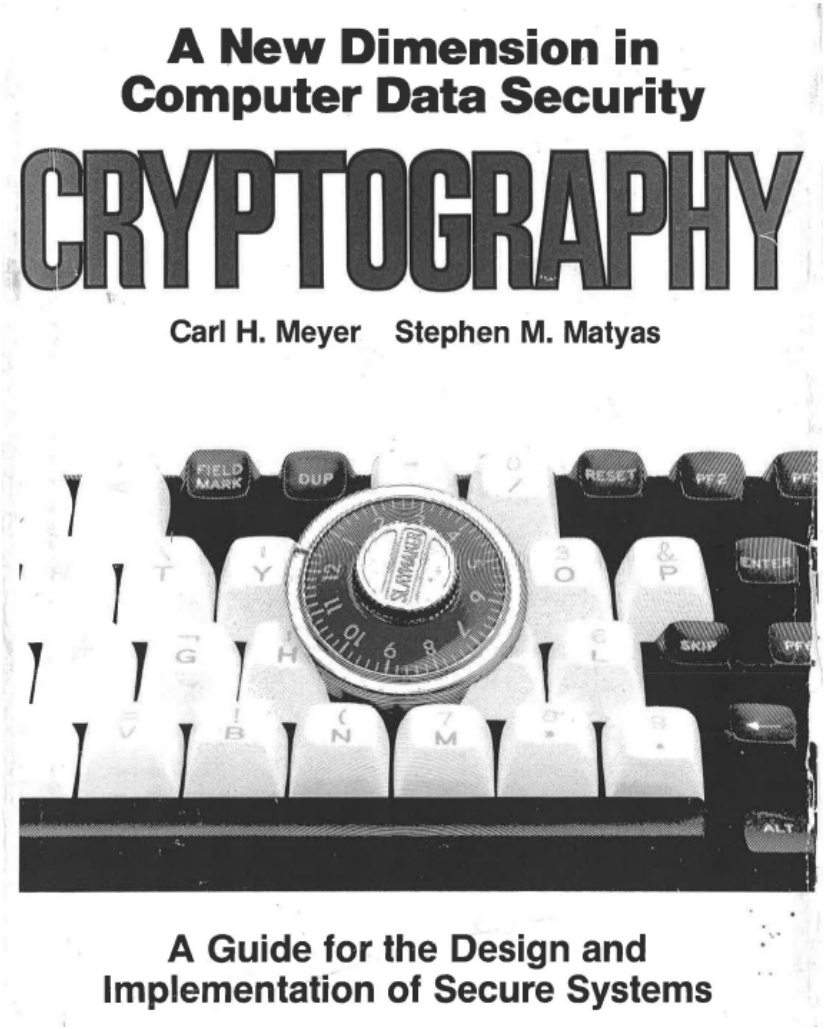
Claim 56 is Obvious over Davies, Fischer and Piosenka

- Patent Owner's only argument is that this teaching is "already there in Davies." Paper 16, at 60.
  - If so, the claim is obvious over Davies and Fischer alone. *Cf. Mobotix v. E-Watch*, Case No. IPR2013-00334, slip op. at 2 (P.T.A.B. Jan. 10, 2014) (Paper 18) ("Within the instituted ground based on Ely, [et al.], Petitioner is free to prove … obviousness … based on Ely alone.").
  - If Patent Owner is wrong, it has failed to rebut Petitioner's showing that Piosenka suggests denying a request signed by a digital signature that cannot be authenticated.

- Either way, the claim is invalid.

See Paper 19, at 24-25.

Cryptography (Meyer)



Published in 1989 (§ 102(b))

Board found on the initial record:

– Claims 51, 53, 55 and 56 (*obvious over Davies and Meyer)*

Meyer is Similar to and Combinable with Davies

- Chapter 10 of Meyer discusses EFT based on shared-key cryptography using "check digits" (MAC) appended to the EFT message.

Message authentication is a technique which produces cryptographic check digits which are appended to the message. These digits are analogous to a parity check or cyclic redundancy check, except that in this case the check digits are cryptographically generated, using DES and a secret key. These digits, called the message authentication code or MAC, are generated by the originator, appended to the transmitted message, and then checked by the recipient, who also holds the same secret key used in the generation process. Should anyone attempt to modify the message between the time the MAC is generated and the time it is checked, he would be detected. Not knowing the secret key, he would be unable to generate the correct MAC for his modified message. Similarly, no one can successfully introduce a spurious message because he could not generate the proper MAC for this message.

* * *

As a minimum, the following fields should be included in the MAC generation for a transaction request message:

1. Transaction type (debit, credit, etc.).
2. Cardholder's account number.
3. Amount.
4. Transaction identification information (that information which uniquely identifies a specific transaction from a particular terminal).

Ex. 1022, Meyer pp. 457-58

- The MAC (*i.e.* VAN) is generated after receiving the funds transfer information.
- The recipient can then check the received MAC to determine the received transaction data was not fraudulently modified or generated.

See Paper 7, at 55-57; Paper 19, at 20-21.

Meyer is Similar to and Combinable with Davies

- Chapter 11 suggests substituting the MAC with "digital signatures" based on a "public-key algorithm."

If institutions do not wish to share secret keys for purposes of authenticating response messages, digital signatures based on either a conventional or public-key algorithm could be used (see Digital Signatures, Chapter 9). A public-key algorithm, however, is more practical, since there are no restrictions on the number of signed messages that can be sent and received using a single pair of keys. With a conventional algorithm, each digital signature must be validated using a separate validation parameter (or pattern of bits).

* * *

A secret user key (SKc, where c stands for customer) is used to generate a quantity (DGSreq) which will enable the issuer to authenticate the transaction request message, Mreq. In the conventional approach this quantity was called a MAC. Since a public-key approach provides a digital signature capability, the term DGS is used instead of MAC. To demonstrate the parallelism between the public-key and conventional algorithm approaches, assume that (Mreq, DGSreq) is routed to the issuer and define DGSreq as

$$DGSreq = D_{SKc}[CE(Mreq)]$$

Ex. 1022, Meyer pp. 569, 589-90

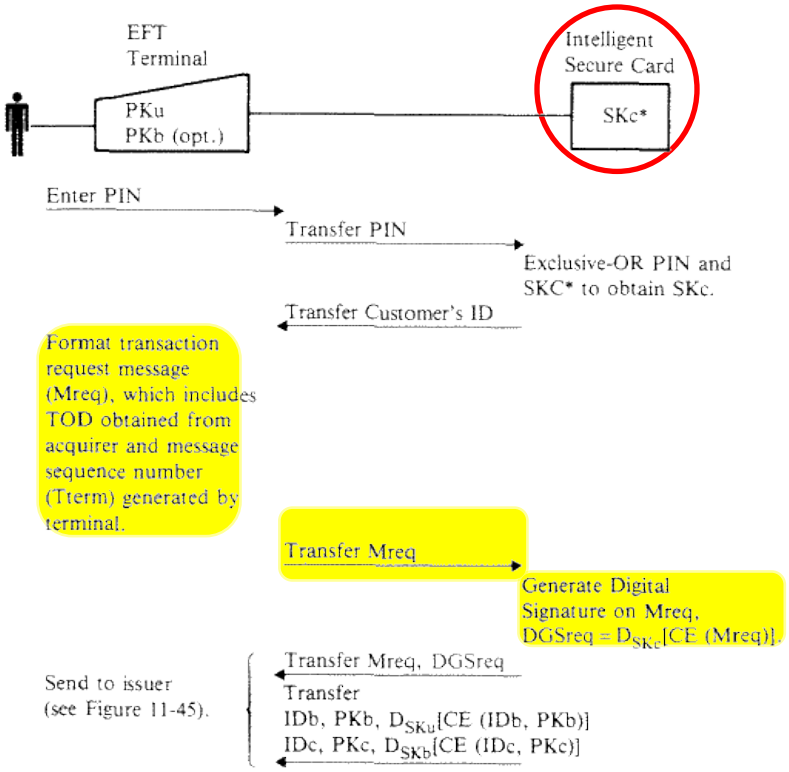


Figure 11-44. On-Line Use—EFT Terminal

  - The cryptographic operations are performed with a token ("intelligent secure card") that interacts with a terminal.

See Paper 19, at 20-21.

Meyer is Similar to and Combinable with Davies

- Both references address methods for facilitating financial transactions and for providing data security for electronic funds transfer.
  - Davies's method uses "a digital signature facility with a key registry to authenticate public keys," and to approve transactions.
    Ex. 1004, Davies pp. 328-31.
  - Meyer similarly discloses using a message authentication code, or equivalently a digital signature in the context of public-key algorithms, to approve or disapprove transaction requests.
    Ex. 1022, Meyer pp. 457-58, 469 and 590.

- These references in their similar purpose of dealing with financial transactions and services, and overlapping teachings, confirm a motivation to combine Davies and Meyer.

See Paper 7, at 22-23.

Claim 55 is Obvious over Davies and Meyer

- Meyer also explains that a digital signature can be considered an authentication (or error detection) code.

A secret user key (SKc, where c stands for customer) is used to generate a quantity (DGSreq) which will enable the issuer to authenticate the transaction request message, Mreq. In the conventional approach this quantity was called a MAC. Since a public-key approach provides a digital signature capability, the term DGS is used instead of MAC. To demonstrate the parallelism between the public-key and conventional algorithm approaches, assume that (Mreq, DGSreq) is routed to the issuer and define DGSreq as

$$DGSreq = D_{SKc}[CE(Mreq)]$$

Ex. 1022, Meyer pp. 589-90

- **Claim 55**: "the VAN is generated by using an error detection code derived by using at least a portion of the funds transfer information"

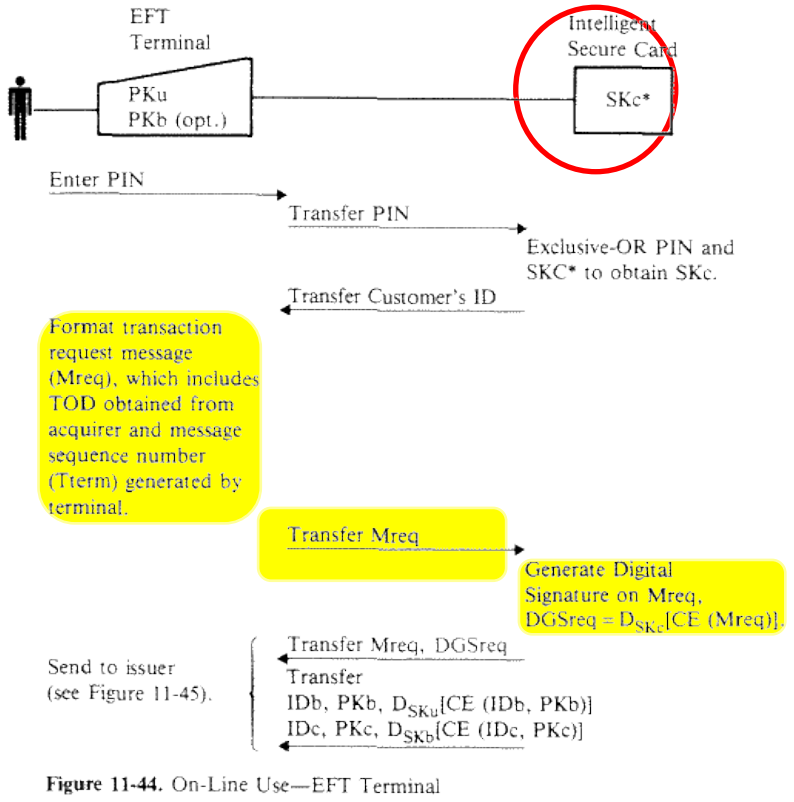
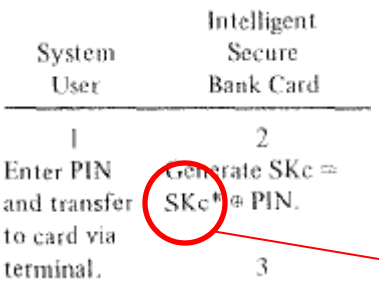


Figure 11-44. On-Line Use—EFT Terminal

See Paper 19, at 22-23.

Claim 56 is Obvious over Davies and Meyer

- There is no requirement that the VAN1 must be "non-secret."
- SKc* secures the non-secret credential information (the customer's public key, PKc) to the customer.
  - SKc* is used to generate the customer's secret key (SKc). Ex. 1022, Meyer p. 596 and Table 11-16.



  - Patent Owner's expert admits that the customer's secret key has a defined mathematical relationship to the customer's public key (PKc). Ex. 1023, at 119:12-120:6.

- **Claim 56**: "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"

See Paper 19, at 25.

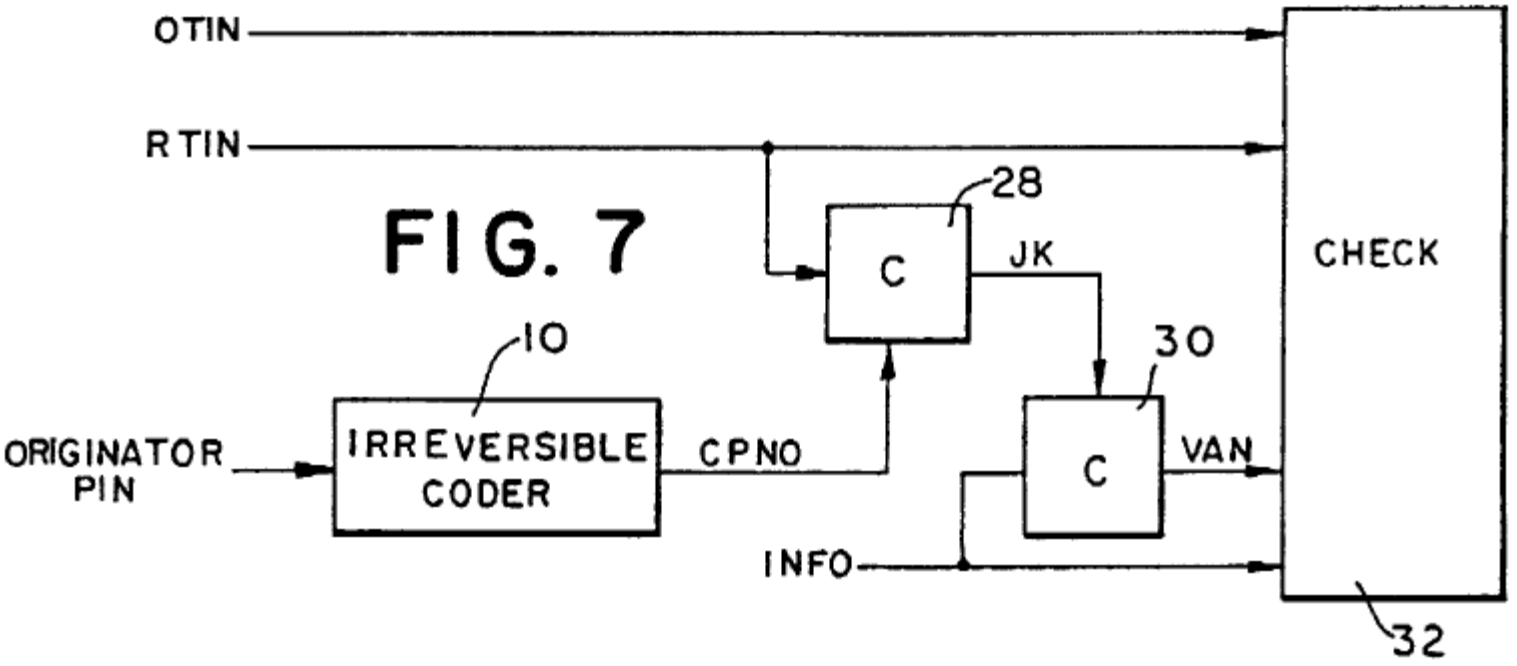
Conclusion

- The Board's findings in the Institution Decision are correct and should be confirmed:
- All the Challenged Claims of the '302 Patent are invalid
  A. Claims 51 and 53 (*anticipated by Davies*)
  B. Claims 51, 53, 55 and 56 (*obvious over Davies and Meyer*)
  C. Claim 55 (*obvious over Davies and Nechvatal*)
  D. Claim 56 (*obvious over Davies, Fischer and Piosenka*)

See Paper 10, at 27.

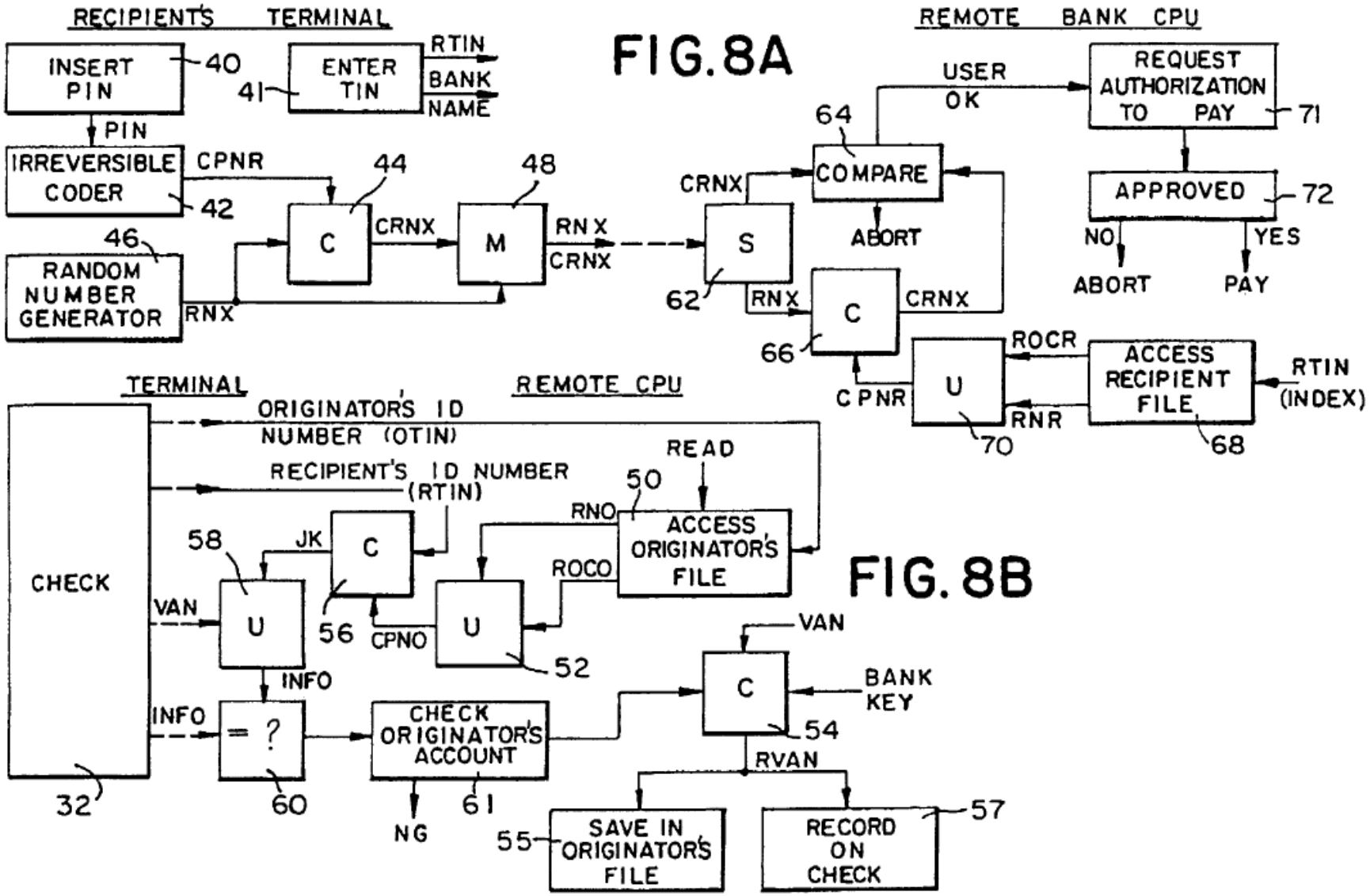
BACKUP SLIDES

FIG. 7 of ‘302 Patent



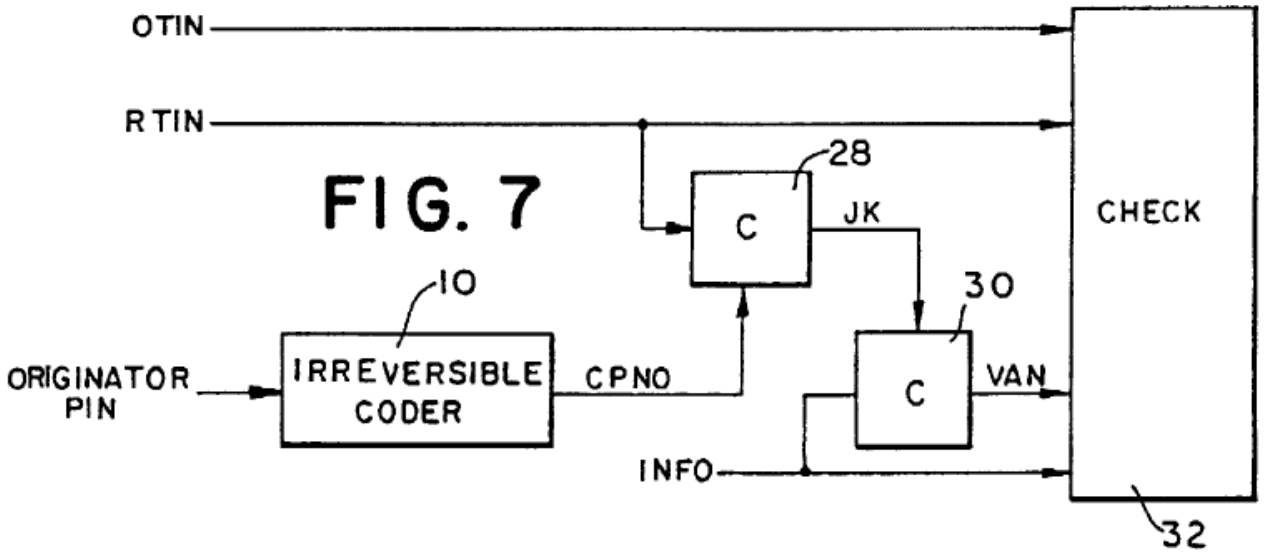
See Paper 19, at 7-8.

FIGS. 8A-8B of '302 Patent



See Paper 19, at 7-8.

Claims Not Limited to a Single Entity



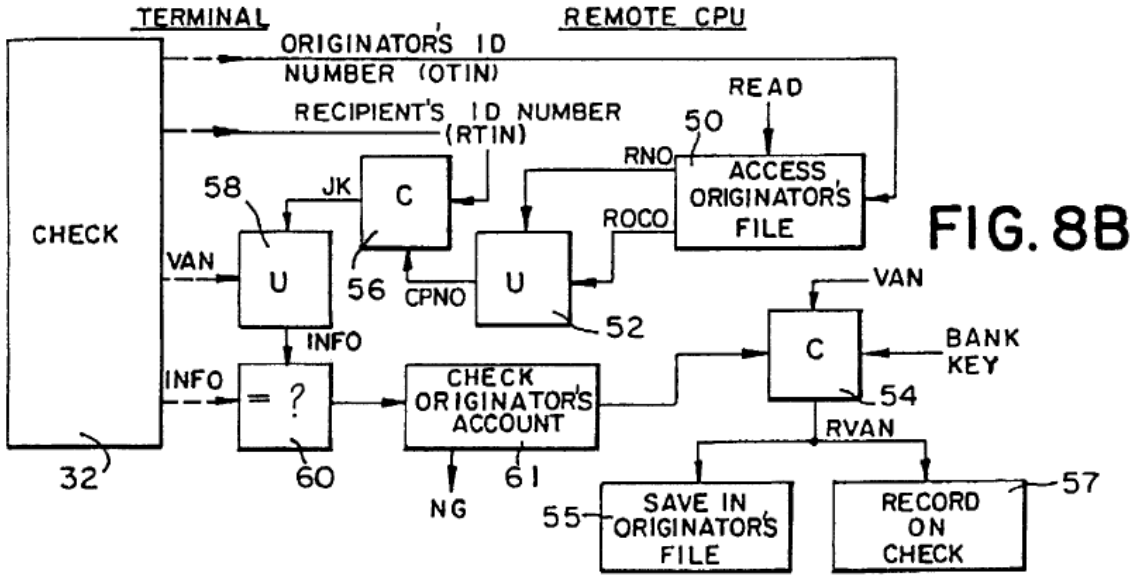


FIG. 8B

See Paper 19, at 7-8.

FIGS. 10.22 (annotated) of Davies

1 Bank identity	2 Bank public key
3 Expiry date	4 Signature of 1–3 by key registry
5 Customer identity	6 Customer public key
7 Expiry date	8 Signature of 5–7 by Bank
9 Cheque sequence number	10 Transaction type
11 Amount of payment	12 Currency
13 Payee identity	14 Description of payment
15 Date and time	16 Signature of 9–15 by customer

Fig. 10.22 Electronic cheque

FIGS. 10.23 (annotated) of Davies

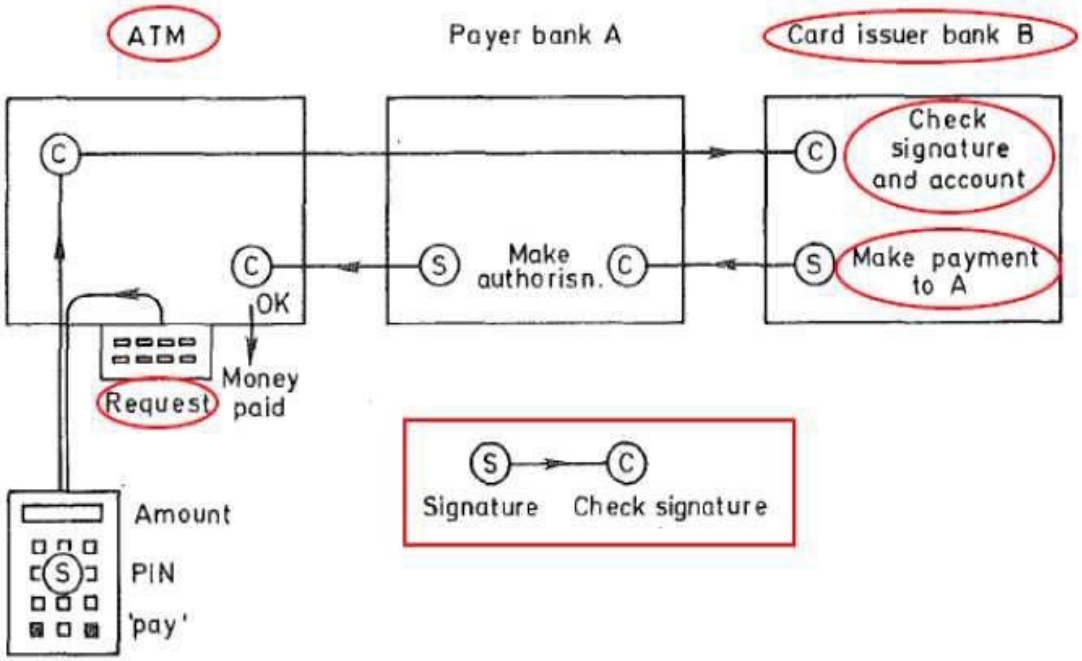


Fig. 10.23 Shared ATM network using digital signatures

FIGS. 11-44 and 11-45 (annotated) of Meyer

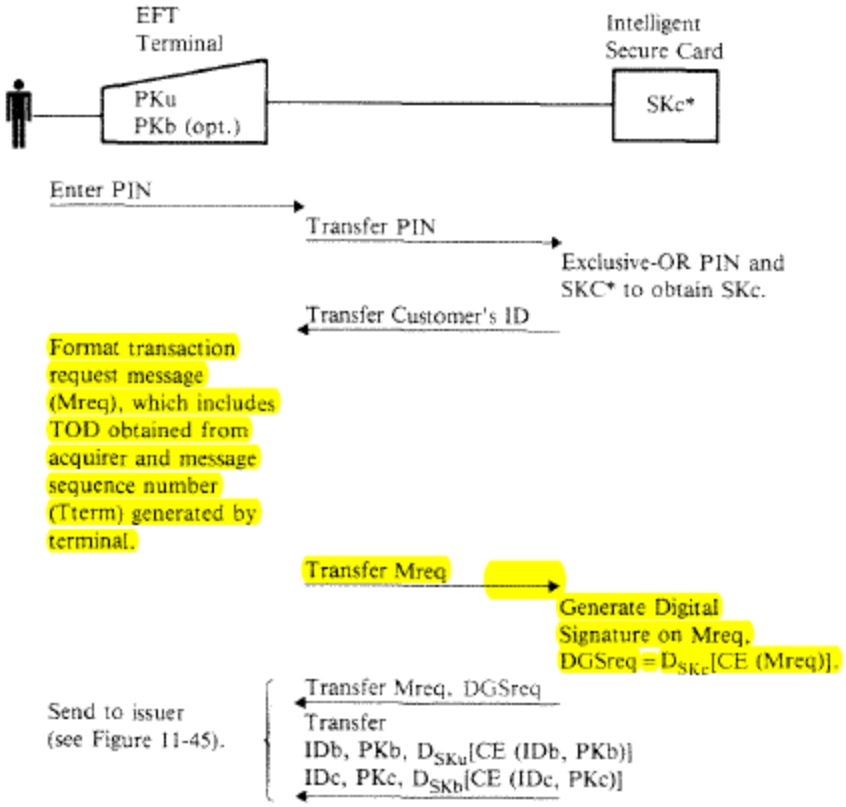
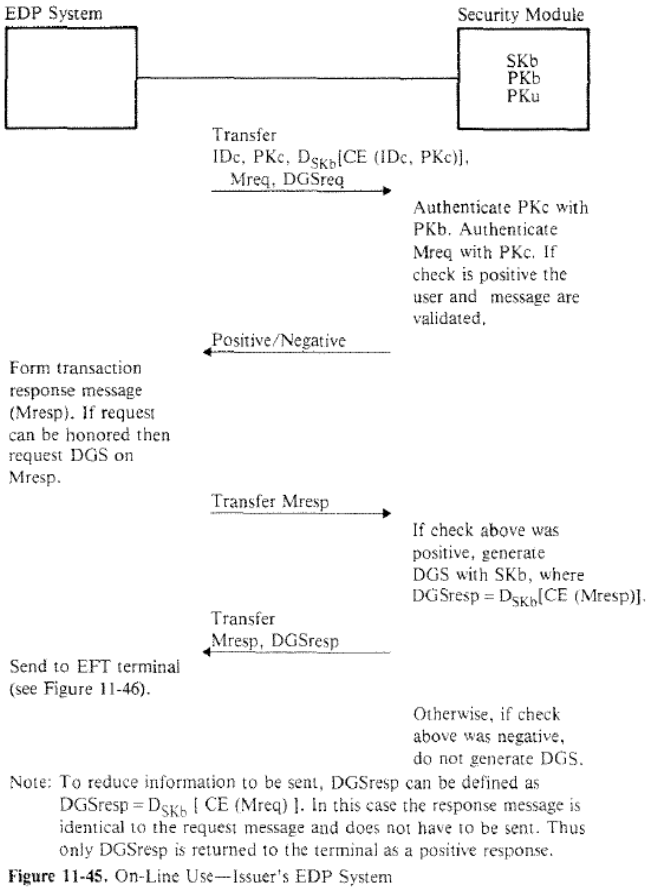


Figure 11-44. On-Line Use—EFT Terminal



Note: To reduce information to be sent, DGSresp can be defined as $DGSresp = D_{SKb}[CE(Mreq)]$. In this case the response message is identical to the request message and does not have to be sent. Thus only DGSresp is returned to the terminal as a positive response.

Figure 11-45. On-Line Use—Issuer's EDP System

See Paper 7, at 41-45; Paper 19, at 21.

Table 11-16 of Meyer

602

System Nodes					
System User	Intelligent Secure Bank Card	EFT Terminal	Acquirer's Host	Switch's Host	Issuer's Host
1 Enter PIN and transfer to card via terminal.	2 Generate SKc = SKc* ⊕ PIN.	4 Authenticate PKb with PKu and PKc with PKb.	10 Forward received Mreq and DGSreq to switch.	11 Forward received Mreq and DGSreq to issuer.	12 Check received DGSreq with PKc of reference and TODsw of reference.
	3 Read IDb,PKb, D_{SKu}[CE(IDb,PKb)] IDc, PKc and D_{SKu}[CE(IDc,PKc)] from card and transfer to terminal.	5 Read card information and formulate Mreq which includes TODacq and Tterm.			13 Verify user.
		6 Send Mreq to intelligent secure card.			14 Decide if Mreq is to be honored.
	7 Compute DGSreq with SKc (i.e., D_{SKc}[CE(Mreq)]).	9 Forward received Mreq and DGSreq to acquirer.			15 Formulate Mresp which includes Tterm.
	8 Send Mreq and DGSreq to terminal.				

Note: It is assumed that the acquirer periodically sends time-of-day information (TODacq,term) to the terminals in its domain. The TOD stored at the other network host nodes (TODsw at the switch and TODiss at the issuer) is assumed to be equal to TODacq within an allowable range (ΔTOD). The terminal also generates time-variant information (Tterm) which is transmitted to the issuer.

The integers 1–15 in the table show the sequence of steps in the transaction.

Table 11-16. Information Flow from Card to Issuer—Public Key Approach with Intelligent Secure Card

See Paper 19, at 21.

Board's Analysis of Davies

- '302 Patent: "Patent Owner first appears to assert that Davies does not disclose that a portion of the step of receiving funds transfer information precedes the step of generating a VAN. Prelim. Resp. 40." But:
  - "For purposes of this decision, Petitioner's evidence, namely the disclosure in Figure 10.23 and related text that "**the token both receives the funds transfer information** ('the customer's request is formed into a message and presented to the token')…"
  - "…and then, **after receipt of that information, the token generates a VAN** using at least a portion of that received funds transfer information ('[h]ere it is signed and returned to the ATM')," adequately shows that Davies discloses receipt of funds transfer information prior to generation of a signed message. Pet. 18–19, 27–29; Ex. 1004, Fig. 10.23, 328–331."

See Paper 10, at 16 (emphasis added).

Board's Analysis of Davies

- '302 Patent: "Patent owner further argues that Petitioner 'mixes and matches' separate unrelated disclosures (the 'cheque embodiment' and the 'ATM embodiment') from Davies. Prelim. Resp. 41–43." But:
  - "The two 'embodiments,' however, are related as described by Davies, which states the '**same intelligent token** which provides an electronic cheque between individuals can . . . also 'cash a cheque' at an ATM with on-line verification.' Ex. 1004, 330."
  - "We are persuaded that Petitioner has demonstrated that it is more likely than not that Petitioner would prevail in establishing the unpatentability of claim 51 as anticipated by Davies."

See Paper 10, at 16 (emphasis added).

Board's Analysis of Davies and Meyer

- '302 Patent: "Patent Owner also argues Petitioner has not provided sufficient analysis of a reason to combine Davies with Meyer. Prelim. Resp. 57–58." But:
  - "Petitioner, however, provides articulated reasoning with rational underpinning for the reason to combine, stating that:
    - '[C]ombining Davies with Meyer demonstrates that all the elements at issue were known in the prior art, and their combination yielded nothing but predictable results.'
    - 'Both references address methods for facilitating financial transactions and for providing data security for electronic funds transfer….'
    - '…[T]hese references in their **similar purpose** of dealing with financial transactions and services, and **overlapping teachings**, confirm a motivation to combine Davies and Meyer.'

  Pet. 22–23 (citing to Ex. 1020 ¶¶ 112–18); Pet. 51."

See Paper 10, at 21 (emphasis added).

Board's Analysis of Davies and Nechvatal

- '302 Patent: "Patent Owner argues 'the Petition does not assert a proper 'reason to combine…,'" But:
  - Patent Owner "concedes Davies and Nechvatal 'might **overlap** in certain teachings.' Prelim. Resp. 60."
  - "Petitioner, however, explains that Nechvatal's hash functions improve signing efficiency and that it would be obvious for a person of ordinary skill in the art to combine the teachings of Davies 'with Nechvatal to implement an electronic funds transfer system in which the transactions are authenticated by digital signatures, as taught by Davies.' Pet. 67."

See Paper 10, at 23 (emphasis added).

Board's Analysis of Davies, Fischer and Piosenka

- '302 Patent: "Patent Owner argues 'the asserted 'reason to combine'' is insufficient. Prelim. Resp. 62." But:
  - "Petitioner, however, explains that:
    - 'A person of ordinary skill in the art would be motivated… to combine the teachings of Davies with the teachings of Fischer **for securing messages, end-to-end**….'
    - 'A person of ordinary skill in the art would be motivated… to augment the certification of message signatures and public keys, as taught by the combination of Davies and Fischer, with the **denial of request upon failure to verify the user's credential**, as taught by Piosenka.'

  Pet. 69–71 (citing Ex. 1020 ¶¶ 158–60, 174)."

See Paper 10, at 26 (emphasis added).

Claim Constructions

3. "Credential" – Board did not construe this term.

- Patent Owner argues that the credential must be "transferred or presented *for purposes of determining the identity of a party*." Paper 16, at 14-16.
  - Patent Owner, nonetheless, accepts Petitioner's construction offered in CBM2015-00013.
- Patent Owner, however, may be attempting to import an additional, unstated limitation to this construction that the credential must be "transferred or presented for purposes of determining the identity of *the presenting party.*"
  - Such a construction is improper at least because the specification states that the invention permits verification of the identity of "absent parties to a transaction." Ex. 1001, at 2:1-4, 4:67-5:2.

See Paper 19, at 9.

Claim Constructions

4. **"Variable Authentication Number ('VAN')"** – Board construed as "a variable number resulting from a coding operation that can be used in verifying the identity of a party or the integrity of information or both."
   - Patent Owner argues further construction is necessary for CBM standing purposes. Paper 16, at 16-17.
     - Patent Owner fails to raise an issue of CBM standing, instead purporting to incorporate by reference arguments made in its preliminary response, which is expressly forbidden. 37 C.F.R. § 42.6(a)(3).
   - Even if considered, this should be rejected as an improper attempt to re-write the claims to include a requirement that the VAN be generated "entirely electronic[ally]".
     - *See Tehrani*, 331 F.3d at 1362-63 (method steps need not be performed "automatically" by a hardware device).

See Paper 19, at 10-11.

Claim Constructions

5. **"Error Detection Code" (Claim 55)** – Board did not construe this term.
   - Patent Owner argues this should mean "the result of applying an algorithm for coding information that, when applied to original information, creates coded information wherein changes to the original information can be detected without complete recovery of the original information." Paper 16, at 18.
   - Petitioner's expert adopted a similar construction proposed by Patent Owner in the *Amazon* litigation, which was adopted by that court. *Compare* Ex. 1020, at 4 *with* Ex. 1015, at 51.
     - Patent Owner now proposes the construction that it offered in the subsequent *ING* litigation, which was adopted by that court. *Compare* Paper 16, at 18 *with* Ex. 1016, at 25.
     - Petitioner's expert credibly explained why the *Amazon* construction was more accurate, but concluded that the difference in constructions made no difference to this case. Ex. 2005, at 94:25-97:20.

See Paper 19, at 11.

Patent Owner's Expert Opinions on Claim Construction Should Be Given No Weight

- In paragraphs 46, 48, 51, 55, 57, 60, 62–64, 84, 89, 90, 100, 101, 104, 108 and 113 of his Declaration, Patent Owner's expert opines that certain constructions of the Challenged Claims should be adopted by this Board.

- However, during his deposition, Patent Owner's expert admitted he has no basis for providing such an opinion — as he does not even understand the methodology for determining the meaning of claim terms applicable in this Trial. Ex. 1023, at 56:12–57:17.

See Paper 22, at 4-5.

Patent Owner's Expert Opinions on Claim Construction Should Be Given No Weight

- It is well-established that the opinion of an expert is inadmissible under Rule 702 when that expert fails to understand or properly apply the applicable legal standard.
  - In *Medicines Co. v. Mylan, Inc.*, the court excluded the testimony of an expert as to commercial success where the expert's opinions rested on a legally incorrect understanding of the relevance of commercial success as a secondary consideration of obviousness. 2014 WL 1227214, at *4-6.
  - *See also Pacific Coast Marine Windshields Ltd. v. Malibu Boats, LLC*, No. 6:12-cv-00033, slip. op. at 19–23 (M.D. Fla. Jan. 4, 2013) (Ex. 1024) (excluding expert opinions about a design patent where the expert improperly relied on the "point of novelty" test rejected by the Federal Circuit).
  - *See also Numatics, Inc. v. Balluff, Inc.*, 66 F. Supp. 3d 934, 944–45 (E.D. Mich. 2014). In *Numatics*, the court excluded expert opinion testimony regarding obviousness where the expert later admitted in a deposition "that he had no idea what 'obviousness' means in the context of a patent lawsuit." *Id.*

See Paper 22, at 5-6.

Patent Owner's Expert Opinions on Claim Construction Should Be Given No Weight

- Patent Owner asserts that its expert's unreliable claim construction opinions are "no different" from certain opinions submitted by Petitioner's expert, Mr. Diffie. Paper 25, at 6.
  - This overlooks the striking difference between Dr. Nielson's testimony and Mr. Diffie's: Mr. Diffie explains rather than omits the methodology he used to arrive at his opinions. *See* Ex. 1020, at ¶ 18 ("I have applied the following ordinary and customary meanings, as understood by a person of ordinary skill in the art….").
  - In stark contrast, Dr. Nielson's declaration provides no explanation of the basis for his claim constructions. *Cf.* Ex. 2004, at ¶¶ 41–67. Petitioner learned why this was so at his deposition when Dr. Nielson candidly admitted that he had "no knowledge" of the methodology that is supposed to be used when interpreting claims. Ex. 1023, at 57:12–17.
- While it may be proper for an expert to rely on counsel's claim construction, it is not proper for an expert to do so while giving the false impression that those constructions are his own. *Cf. Butera v. D.C.*, 235 F.3d 637, 661 (D.C. Cir. 2001).

See Paper 26, at 3-4.

Patent Owner's Expert Opinions on Claim Construction Should Be Given No Weight

- Patent Owner cites to various opinions denying motions to exclude expert testimony. *See* Paper 25, at 6-10. These cases are distinguishable:
  - *Teva* does not overrule or call into question the Supreme Court's holding in *Daubert v. Merrell Dow Pharm., Inc.*, that unreliable expert testimony must be excluded. 509 U.S. 579, 597 (1993).
  - In *Silicon Motion*, the expert applied a dictionary definition rather than the Board's construction.
  - In *Aspex Eyewear*, the court concluded the expert's methodology was reasonable and permitted it. 2002 U.S. Dist. LEXIS 14834, at *94.
  - In *Alien Tech*, the challenge related to the expert's application of claim construction law, not his technical reasoning. 2008 U.S. Dist. LEXIS 38212, at *3-4.
- In contrast, Dr. Nielson does not identify *any* methodology or reasoning forming the basis for his claim construction opinions. This is so because, as he subsequently admitted, he has none. Ex. 1023, at 57:12-17.

See Paper 26, at 4-5.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the foregoing PETITIONER'S FILING OF DEMONSTRATIVE EXHIBITS was filed and served electronically via e-mail on March 16, 2016, in its entirety on the following:

Robert P. Greenspoon
Flachsbart & Greenspoon, LLC
333 N. Michigan Ave., Suite 2700
Chicago, IL 60601
Telephone: (312) 551-9500
rpg@fg-law.com

/ Robert C. Scheinfeld/
Robert C. Scheinfeld