Paper No. 1

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MASTERCARD INTERNATIONAL INCORPORATED
Petitioner

v.

LEON STAMBLER
Patent Owner

Case Number (*to be assigned*)
Patent 5,793,302

PETITION
FOR COVERED BUSINESS METHOD REVIEW

TABLE OF CONTENTS

EXHIBITS

MasterCard Exh. 1001	U.S. Patent No. 5,793,302
MasterCard Exh. 1002	Complaint, *Stambler v. MasterCard Inc. et al.*, 14-cv-60830 (S.D. Fla.)
MasterCard Exh. 1003	Plaintiff's Disclosure of Asserted Claims and Infringement Contentions from *Stambler v. MasterCard Inc. et al.*
MasterCard Exh. 1004	D. W. Davies *et al.*, *Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer* (1989)
MasterCard Exh. 1005	James Nechvatal, Public-key Cryptography (NIST Special Publication 800-2) (April 1991)
MasterCard Exh. 1006	U.S. Patent No. 4,868,877 to Fischer
MasterCard Exh. 1007	U.S. Patent No. 4,200,770 to Hellman et al.
MasterCard Exh. 1008	U.S. Patent No. 4,993,068 to Piosenka et al.
MasterCard Exh. 1009	Prosecution History File Wrapper for 07/977,385
MasterCard Exh. 1010	Prosecution History File Wrapper for 08/122,071
MasterCard Exh. 1011	Prosecution History File Wrapper for 08/747,174
MasterCard Exh. 1012	Memorandum Order dated January 29, 2003 from *Leon Stambler v. RSA Security Inc.*, 01-cv-65 (D. Del.)

MasterCard Exh. 1013	Memorandum Opinion and Order dated April 9, 2010 from *Leon Stambler v. JPMorgan Chase & Co.*, 08-cv-204 (E.D. Tex.)
MasterCard Exh. 1014	Memorandum Opinion and Order dated September 24, 2010 from *Leon Stambler v. Merrill Lynch & Co., Inc.*, 08-cv-462 (E.D. Tex.)
MasterCard Exh. 1015	Claim Construction Order dated December 27, 2010 from *Leon Stambler v. Amazon.com*, 09-cv-310 (E.D. Tex.)
MasterCard Exh. 1016	Memorandum Opinion and Order dated September 28, 2011 from *Leon Stambler v. ING Bank*, FSB., 10-cv-181 (E.D. Tex.)
MasterCard Exh. 1017	Provisional Opinion and Order dated August 29, 2012 from *Leon Stambler v. Atmos Energy Corp.*, 10-cv-594 (E.D. Tex.)
MasterCard Exh. 1018	Previous Constructions of Claim Terms of the ‘302 Patent
MasterCard Exh. 1019	*Intellectual Ventures I LLC v. Capital One Fin. Corp.*, 13-cv-740, 2014 U.S. Dist. LEXIS 53001 (E.D. Va. April 16, 2014)
MasterCard Exh. 1020	Declaration of Professor Whitfield Diffie (“Diffie Declaration”)
MasterCard Exh. 1021	Plaintiff’s Opening Claim Construction Brief from *Leon Stambler v. Amazon.com*, 09-cv-310 (E.D. Tex.) (“Amazon Brief”)
MasterCard Exh. 1022	Carl H. Meyer *et al.*, *Cryptography: A New Dimension in Computer Data Security—A Guide for the Design and Implementation of Secure Systems* (1982)

I. INTRODUCTION

Pursuant to 37 C.F.R. § 42.300, *et. seq*., MasterCard International Incorporated ("MasterCard" or "Petitioner") hereby petitions the Patent Trial and Appeals Board of the United States Patent and Trademark Office (the "Office") to institute a covered business method review of claims 51, 53, 55, and 56 ("the Challenged Claims") of U.S. Patent No. 5,793,302 ("the '302 Patent"). The '302 Patent, a copy of which is provided as MasterCard Exh. 1001, was issued to Leon Stambler ("Patent Owner") and has no record of assignment.

The Challenged Claims recite authentication methods for use in conducting financial transactions. As explained herein, these methods are unpatentable under 35 U.S.C. §§ 102 and 103 and, consequently, it is "more likely than not that at least one of [the Challenged Claims are] unpatentable." 35 U.S.C. § 324(a). Petitioner respectfully submits this petition should be granted on at least the grounds specified herein.

II. MANDATORY NOTICES 37 C.F.R. §42.8(b)

REAL PARTY-IN-INTEREST: The real party-in-interest for Petitioner is MasterCard International Incorporated.

NOTICE OF RELATED MATTERS: Patent Owner has filed numerous lawsuits asserting the '302 Patent dating back to at least 2001. The following cases are still pending as of the date of this petition:

- *Stambler v. Visa, Inc.*, 14-cv-60490 (S.D. Fla)
- *Stambler v. MasterCard, Inc.*, 14-cv-60830 (S.D. Fla)

Furthermore, the '302 Patent has been the subject of two Covered Business Method Review petitions. The only such petition currently pending is in CBM2015-00013, filed by MasterCard.

In addition, the '302 Patent has been the subject of several *inter partes* review petitions. The Board recently entered a decision, discussed in detail below, denying institution of *Inter Partes* Review of the '302 Patent ("IPR Decision"). *See* IPR2014-00694, Paper 10. The other petitions were withdrawn prior to institution due to litigation settlement.

PETITIONER'S LEAD AND BACKUP COUNSEL:

Robert C. Scheinfeld	(lead counsel)	Reg. No. 31,300
Eliot D. Williams	(backup counsel)	Reg. No. 50,822

The necessary powers of attorney are being filed commensurate with this Petition.

SERVICE INFORMATION: Service of all documents may be made to the lead counsel and backup counsel at BAKER BOTTS, LLP, 30 Rockefeller Plaza, New York, NY 10112, with copies to the following email addresses: robert.scheinfeld@bakerbotts.com and eliot.williams@bakerbotts.com. Petitioner's counsel may also be reached via phone at 212-408-2512 and via fax at 212-259-2512.

III. FILING REQUIREMENTS

This Petition is being timely filed pursuant to 37 C.F.R. §42.303 because it is not filed in a period during which a petition for a post-grant review of the patent would satisfy the requirements of 35 U.S.C. § 321(c). Petitioner is submitting a payment in the amount of $30,000 for the fees specified by 37 C.F.R. § 42.15(b). To the extent that any additional fees are required in order for the Board to fully consider this Petition, the Board is hereby authorized by the undersigned to charge Deposit Account 02-4377.

Under 37 C.F.R. § 42.63(e), an Exhibit List including a brief description of each Exhibit is filed herewith. Petitioners have attached a Certificate of Service hereto in accordance with 37 C.F.R. §42.205(a) and 37 C.F.R. § 42.6(e)(4)(iii).

IV. GROUNDS FOR STANDING

Section 18 of the America Invents Act ("AIA") limits review to persons or their privies that have been sued or charged with infringement of a "covered business method patent," which does not include patents for "technological inventions." AIA §§ 18(a)(1)(B), 18(d)(1); *see* 37 C.F.R. §42.302.

A. Petitioners' Eligibility

Pursuant to 37 C.F.R. § 42.302(a), Petitioner is eligible to file this Petition because Patent Owner sued Petitioner for alleged infringement of the '302 Patent. (*See* MasterCard Exh. 1002 (Complaint against MasterCard).) The Challenged

Claims are those same claims that Patent Owner has asserted against Petitioner. (*See* MasterCard Exh. 1003 (Disclosure of Asserted Claims and Infringement Contentions).)[1] Furthermore, Petitioner is not estopped from challenging the claims of the '302 Patent on the grounds identified in this Petition, as required by 37 C.F.R. § 43.302(b).

B. The '302 Patent is a Covered Business Method Patent

A "covered business method patent" is a patent that "claims a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service, except that the term does not include patents for technological inventions." AIA § 18(d)(1); see 37 C.F.R. § 42.301(a). For purposes of determining whether a patent is eligible for a covered business method patent review, the focus is on the claims. *See* Transitional Program for Covered Business Method Patents – Definitions of Covered Business Method Patent and Technological Invention;

[1] Though MasterCard Exh. 1003 is marked "Confidential," Patent Owner sent it to Petitioner without a protective order or agreement as to confidentiality in place and Petitioner does not believe the document contains any confidential information. Accordingly, Petitioner perceives it to be in the public domain.

Final Rule, 77 Fed. Reg. 48,734, 48,736 (Aug. 14, 2012). A patent need have only one claim directed to a covered business method to be eligible for review. *Id*.

In promulgating rules for covered business method patent reviews, the Office considered the legislative intent and history behind the AIA's definition of "covered business method patent." *Id*. at 48,735-36. The "legislative history explains that the definition of covered business method patent was drafted to encompass patents 'claiming activities that are financial in nature, incidental to a financial activity or complementary to a financial activity.'" *Id*. at 48,735 (citing 157 Cong. Rec. S5432 (daily ed. Sept. 8, 2011) (statement of Sen. Schumer)). The legislative history indicates that "financial product or service" should be interpreted broadly. *Id*.

The Challenged Claims squarely meet the definition of a Covered Business Method. In general, the Challenged Claims recite methods of facilitating the exchange of money from one financial account to another. Patent Owner has sued a number of financial institutions. By way of example, Challenged Claims 51, 53, 55 and 56 each recite "a method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party." There can be no question that the process of transferring funds between accounts is "financial in nature," and that authentication of such a transfer is at least "incidental to a financial activity."

C. The '302 Patent is Not Directed to a "Technological Invention"

The definition of "covered business method patent" in AIA §18(d)(1) excludes patents for "technological inventions." To determine whether a patent is for a technological invention, the Board must consider "whether the claimed subject matter as a whole recites a technological feature that is novel and unobvious over the prior art; and solves a technical problem using a technical solution." 37 C.F.R. §42.301(b). "Both prongs must be satisfied in order for the patent to be excluded from review as a technological invention." *Agilysys, Inc. v. Ameranth, Inc.*, CBM2014-00015, Paper No. 20 (Institution Decision) at 11 (PTAB, March 26, 2014). By way of example, (a) reciting the use of known prior art technology to accomplish a process or method, even if that process or method is novel and non-obvious, or (b) combining prior art structures to achieve the normal, expected or predictable result of that combination, will not render a patent a "technological invention." Office Patent Trial Practice Guide, 77 Fed. Reg. 48756, 48763-64 (Aug. 14, 2012). Specifically, a patent is not a technological invention if it merely combines known technology in a new way to perform data processing operations. 157 Cong. Rec. S1364 (daily ed. March 8, 2011) (Sen. Schumer). If even one claim of a patent is not directed to a "technological invention," the exception does not apply. 77 Fed. Reg. 157, p. 48736.

The Challenged Claims do not recite a technological invention. As to the first prong, the '302 Patent makes clear that it utilizes nothing more than conventional elements to perform its authentication task. For example, the patent notes that all of the "functional building blocks utilized in the preferred embodiments" are "*conventional building blocks* for computer or communication systems." (MasterCard Exh. 1001, Col. 3:29-32 (emphasis supplied)). These building blocks (shown in Figs. 1-5) are "a coder, an uncoder, a linker, a mixer, and a sorter." (*Id*., Col. 2:64-67.) The figures also refer to an "irreversible coder," but the patent notes that this "may be any type of conventional coding device which can process the PIN so that the coding is irreversible." (*Id*., Col. 4:21-23.) Even the algorithms used by these coders and uncoders were admittedly "known." (*Id*., Col. 3:37-38.) This alone is sufficient to determine that the Challenged Claims do not recite a technological invention. *See, e.g., eBay Enterprise, Inc. v. Lockwood*, CBM2014-00026, Paper No. 25 (Institution Decision) at 16 (PTAB, May 15, 2014):

> *to the extent that claim 1 recites technology via its mean-plus-function claim limitations, it recites technology that existed before the earliest possible effective filing date of the '951 patent. Accordingly, on the present record, we determine that the subject matter of claim 1, as a whole, does not recite "a technological feature that is novel and*

> *unobvious over the prior art," and, therefore, is not a technological invention.*

Moreover, with respect to the second prong, none of the Challenged Claims recite any of these conventional "building blocks" that could be considered a technical solution to a technical problem. There is no mention of a coder, an uncoder, a linker, a mixer, or a sorter in any of the Challenged Claims. The analysis of whether a patent is for a "technological invention" must focus on the claims, not the specification; for it is axiomatic "that it is the claim that defines the invention." *Warner-Jenkinson Co., Inc. v. Hilton Davis Chem. Co.*, 520 U.S. 17, 24 (1997). In this case, whether viewed "as a whole" or at the limitation level, the Challenged Claims fail to recite a technical feature or suggest a technical solution. Indeed, they would read on steps that could be performed by a human using pen and paper.

For example, with reference to claim 51, a bank teller could: (1) "receiv[e] funds transfer information, including at least information for identifying the account of [a] first party, and information for identifying the account of [a] second party, and a transfer amount" (*e.g.*, by receiving a deposit ticket and paper check from a customer); (2) "generate a variable authentication number (VAN) using [part of that] information" (*e.g.*, by recording numbers from the check in some combination or in a cipher); (3) "determin[e] whether [the] information is authentic

by using the VAN and … credential information" (*e.g.*, by having a supervisor compare the recorded numbers from the check with account information in a bank ledger); and, if so, (4) "transfer[] funds" from an account of the first party to an account of the second party (*e.g.*, by updating the balance of each account in the bank ledger).

No "technology" is needed to practice claim 51. And to the extent terms such as VAN or credential are construed to require some level of encoding beyond that which can be done on paper, it could be done by the admittedly conventional encoder or decoder.

Most of the Challenged Claims depending from claim 51 add essentially nothing, and thus also fail this test. For example, with respect to the second prong, claim 53 requires that the "funds transfer" be a payment from the first party to the second party. Claim 55 requires that the VAN be generated using an error detection code. There is no technological feature recited by these claims, and the claims fail the test based on this ground alone, even when looking at the claims "as a whole."

Indeed, "authenticating the transfer of funds from a first account associated with a first party to a second account associated with a second party" is neither a technical problem, nor is it solved by a technical solution. It simply describes a "business transaction" (MasterCard Exh. 1001, Col. 1:57) that was as

commonplace in 1992 (indeed, well before then) as it is today. No new technology components were required to enable this authentication. Accordingly, based on the language of the Challenged Claims, any purported "problem" did not involve technology, and any perceived "solution" did not involve technology. Thus, a technical problem neither existed nor was it solved by a claimed technical solution.

V. IDENTIFICATION OF CHALLENGE

A. Grounds Asserted

Petitioner requests review of the Challenged Claims on the grounds set forth in the table below, and request that each of the claims be found unpatentable.

Ground	Challenged Claims	Basis for Unpatentability
1	51, 53 and 55	Anticipated under §102(b) by Davies
2	51, 53, 55 and 56	Anticipated under §102(b) by Meyer
3	51, 53, 55 and 56	Obvious under §103(a) by Davies in view of Meyer
4	55	Obvious under §103(a) by Davies or Meyer in view of Nechvatal
5	56	Obvious under §103(a) by Davies in view of Fischer and Piosenka

An explanation of how the claims are unpatentable under the statutory grounds identified above is provided in the form of detailed description and claim charts that follow. The following references ("Cited Art") are relied upon:

- D. W. Davies, *et al., Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer* (1989) (MasterCard Exh. 1004 or "Davies")

- Carl H. Meyer *et al.*, *Cryptography: A New Dimension in Computer Data Security—A Guide for the Design and Implementation of Secure Systems* (1982) (MasterCard Exh. 1022 or "Meyer")
- James Nechvatal, *Public-key Cryptography*, NIST Special Publication 800-2, April, 1991; (MasterCard Exh. 1005 or "Nechvatal")
- U.S. Patent No. 4,868,877 (MasterCard Exh. 1006 or "Fischer")
- U.S. Patent No. 4,993,068 (MasterCard Exh. 1008 or "Piosenka")

The '302 Patent issued from a string of patent applications dating back to an original application filed on November 17, 1992. Accordingly, the Challenged Claims may have, at the earliest, an effective filing date of November 17, 1992.[2] Davies, Nechvatal and Meyer each qualify as prior art under 35 U.S.C. §102(b) because they were published in 1989, April 1991, and 1982, respectively, and thus each was published more than one year prior to the effective filing date of the '302 Patent. Fischer and Piosenka each qualify as prior art under 35 U.S.C. §102(b) because they issued on September 19, 1989 and February 12, 1991, respectively, and thus the disclosure of each was published more than one year prior to the filing

[2] Petitioner does not concede that the claims of the '302 Patent are supported by the parent application. But, the currently cited references are prior art regardless of whether the Challenged Claims are accorded the filing date of the parent.

date of the ‘302 Patent. None of the Cited Art was of record during prosecution of the ‘302 Patent or any of its parent applications.

B. Overview of ‘302 Patent and Prosecution History

Generally, the ‘302 Patent discloses a method for securing information relevant to a transaction, and for authenticating parties or data involved in the transaction. (*See* MasterCard Exh. 1001 at Col. 1:1-23.) In a transaction between two parties, “a variable authentication number (VAN)” is used to authenticate the identity of at least one of the parties (*id.* at Col. 5:19-25) or to authenticate transaction information. (*Id.* at Col. 2:28-30.) The VAN is created by coding the information to be authenticated. (*Id.* at 5:19-21.) In some cases, the VAN is recorded on a “credential” that is previously issued to at least one of the parties by an entity authorized to issue the credential, and the VAN is created by coding credential information with a joint key. (*Id.* at 11:65-12:2.)

The ‘302 Patent resulted from a string of continuation applications beginning with S/N 07/977,385. The ‘385 Application initially included over sixty claims and the Office found it to include four separate inventions. (MasterCard Exh. 1009 (File Wrapper for 07/977,385) at 153-155.) The claims most closely tracking the Challenged Claims of the ‘302 Patent (essentially Group II, involving generation of a VAN) were withdrawn and pursued in a divisional application, S/N 08/122,071. (*See* MasterCard Exh. 1010 (File Wrapper for 08/122,071) at 98-103.)

The Office rejected these claims under §101 in a First Action on October 19, 1994, finding that none of them were directed to patentable subject matter. According to the Office:

> *The claims appear to be directed to the mental processes required for the use of a transaction variable. No automatic electronic signal selections are required and hence, the claims appear to be directed at the actions of individual human intervention with fund transfers and not the statutory classes of invention.*

(MasterCard Exh. 1010 at 145-146.) Patent Owner attempted to argue around the rejection in a response dated January 13, 1995, claiming that "the steps recited are performed using specific devices, such as coders and uncoders, and linkers, mixers and sorters…." (*Id*. at 153.) None of those "devices," however, were recited in the claims, and the Office issued a Final Action on March 23, 1995, again rejecting the claims under §101. (*Id*. at 164-165.)

This time, Patent Owner responded by cancelling most of the rejected claims, and amending the others to be system (rather than method) claims that recited various physical means for performing the functional tasks. (MasterCard Exh. 1010 at 169-178.) This amendment apparently resulted from an interview with the Examiner where "it was agreed that each of the new independent claims which are now in a system or apparatus format are sufficient to overcome the

subject matter rejection under 35 U.S.C. §101…." (*Id*. at 179.) The claims were subsequently allowed in the revised form.

The method-based "VAN generation / authentication" claims turned up again in a later divisional that eventually resulted in the '302 Patent. This time, with a new Examiner, §101 was not raised. Instead, the Examiner rejected the claims of the under 35 U.S.C. §103(a) as being unpatentable over Hellman (U.S. Patent No. 4,200,770) (attached as MasterCard Exh. 1007), and separately as being unpatentable over Maurer (U.S. Patent No. 5,161,244). (MasterCard Exh. 1011 (File Wrapper for 08/747,174) at 242-246.) In the November 7, 1997 response, Patent Owner amended the Challenged Claims significantly, adding a third party authenticator, among other things. (*Id*. at 256, 271-274.) Patent Owner then argued neither Hellman nor Maurer disclosed or taught features such as "[u]se of a third party to authenticate a VAN and transfer of funds, and use of originator, recipient and payment information to derive a VAN." *(Id.* at 305-306.) Without providing any reasons for allowance, the Examiner allowed the claims on January 2, 1998. (*Id.* at 318-320.)

C. Level of Ordinary Skill in the Art

The level of ordinary skill in the art is evidenced by the references relied upon herein. More specifically, one of ordinary skill in the art at the time of the invention would have been someone with at least a bachelor's degree in computer

programming and two years' experience as a programmer or developer in the field of computer science, with a working understanding of cryptographic operations for transforming original input into a coded output using a known algorithm.

D. Claim Construction

The '302 Patent expired in 2012 due to a terminal disclaimer (MasterCard Exh. 1011 at 315-17). In a post-grant proceeding involving claims of an expired patent, claim construction proceeds pursuant to the principle set forth in *Phillips v. AWH Corp*., 415 F.3d 1303 (Fed. Cir. 2005)(*en banc*). *See* M.P.E.P. § 2258(I)(G); *Innolux Corp. v. Semiconductor Energy Lab. Co., Ltd.*, IPR2013-00064, Paper No. 11 (Institution Decision) at 10 (PTAB, April 30, 2013). This is the same standard applied by district courts in litigation. *See In re Rambus, Inc*., 694 F.3d 42, 46 (Fed. Cir. 2012). Under *Phillips*, words of a claim "are generally given their ordinary and customary meaning" as understood by a person of ordinary skill in the art in question at the time of the invention. *Id*. at 1316.

In this case, the Challenged Claims have been construed in litigation by no less than six separate courts, as well as by the Board in the IPR Decision. The associated claim construction orders are included as MasterCard Exhs. 1012-1017. With a few exceptions, the Challenged Claims use straightforward, plain language, and were construed according to their plain and ordinary meaning. For the sake of convenience, Petitioners have included a chart showing the courts' constructions of

certain terms used in the Challenged Claims (MasterCard Exh. 1018). There was very little variability between the constructions, and the version adopted by the Board in its IPR Decision is as follows:

> **1. variable authentication number (VAN)**
>
> *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*

IPR Decision 8.

The above construction was adopted in the *RSA* Decision, and the Board's IPR Decision.

VI. GROUNDS FORMING A REASONABLE LIKELIHOOD THAT THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. The Board's IPR Decision

On October 31, 2014, the Board determined - based on the record before it at the time - that the petitioner there failed "to show a reasonable likelihood [that it] will prevail in showing the unpatentability of any claim." IPR Decision 3. More specifically, the Board determined that "claim 51 requires that at least some portion of the received funds transfer information be utilized in generating the VAN" and that "at least a portion of the receiving step must precede the generating step, because the VAN is generated using a portion of the received funds transfer

information, and it logically follows that the generating must occur after receipt of at least a portion of the funds transfer information in the receiving step." *Id.* at 12.

The Board then concluded that "the portions of the disclosure in Davies *cited by Petitioner* fail to disclose the required 'receiving' and 'generating' steps in the required sequence." *Id*. The Board rejected the petitioner's argument there because the petitioner merely relied "upon the *bank* as performing the 'receiving' step and receiving the funds transfer information" and "upon the *customer*, or the customer aided by a terminal, as performing the 'generating' step and generating the VAN." *Id*. The Petitioner, according to the Board, failed to point to any disclosure in Davies with respect to the required sequence of the "receiving" and "generating" steps in claim 51.

B. The Davies Reference

The Davies reference, however, does disclose exactly what the Board in the IPR Decision stated was missing from that petition's submission. As summarized in the IPR Decision, Davies is a textbook titled "Security for Computer Networks," and it provides in Chapter 10 several disclosures concerning an electronic funds transfer system that uses intelligent tokens. Davies at 282. The Board recognized that Davies, in section 10.6, discloses an implementation of "an electronic cheque by using 'a digital signature facility with a key registry to authenticate public keys." *Id*. at 328. Although the Board cites and discusses Figure 10.22, petitioner

submits that this disclosure, together with Figure 10.23 and accompanying text, provides what the Board stated was missing in the IPR Decision.

More specifically, Figure 10.23, reproduced and annotated below, illustrates a shared ATM network using digital signatures.

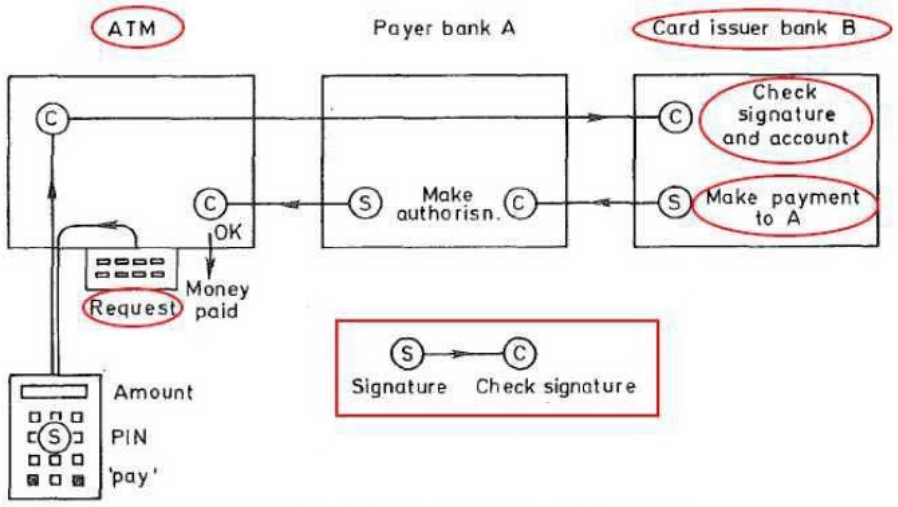


Fig. 10.23 Shared ATM network using digital signatures

As described in Davies:

> Figure 10.23 shows how [a point-of-sale payment by electronic cheque] works in a shared ATM network. The customer's request is formed into a message and presented to the token. Here it is signed and returned to the ATM. The ATM checks the signature, to avoid passing ineffective messages into the system. If it is correct, the 'cheque' passes via the payer bank, A, to the card issuer bank, B. Here the signature is checked and the

> customer's account examined and, if everything is in order, debited. A payment message signed by B is sent to A. The message and its signature are checked and if all is well an authorization goes to the ATM to release the money.

Davies at 331.

Accordingly, this disclosure makes clear—and the arrows illustrating the flow of information make clear—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").

C. The Meyer Reference

Even if the Board finds that Davies does not disclose the sequence required by the Challenged Claims (which Petitioner respectfully submits would be error), the Meyer reference, alone or in combination with Davies, would render the Challenged Claims anticipated and/or obvious to one of ordinary skill in the art.

For example, Meyer discloses techniques for "[a]pplying cryptography to pin-based electronic funds transfer systems." Meyer at 429-73. Meyer describes using a "message authentication code" or "MAC" that is generated by using a

technique "which produces cryptographic check digits which are appended to the message.... These digits...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." *Id.* at 457; *see also id.* at 469. If the same MAC can be generated by the recipient then the message was not modified and the request can be approved ("[s]hould anyone attempt to modify the message between the time the MAC is generated and the time it is checked, he would be detected."). *Id.*

Meyer also discloses, for purposes of authenticating a transfer of funds, the use of digital signatures (DGS) based on public-key algorithms, and specifically, for example, the use of private and public key pairs, the latter of which is shared and used to authenticate transaction request messages signed by a sender with the associated private key. *Id.* at 569-76. Significantly, with reference to Figure 11-44, reproduced and annotated below, Meyer describes that, "[t]o allow the issuer to validate the transaction request message, a DGS ["digital signature" or "VAN"] is generated using [the customer's private key]." *Id.* at 597.

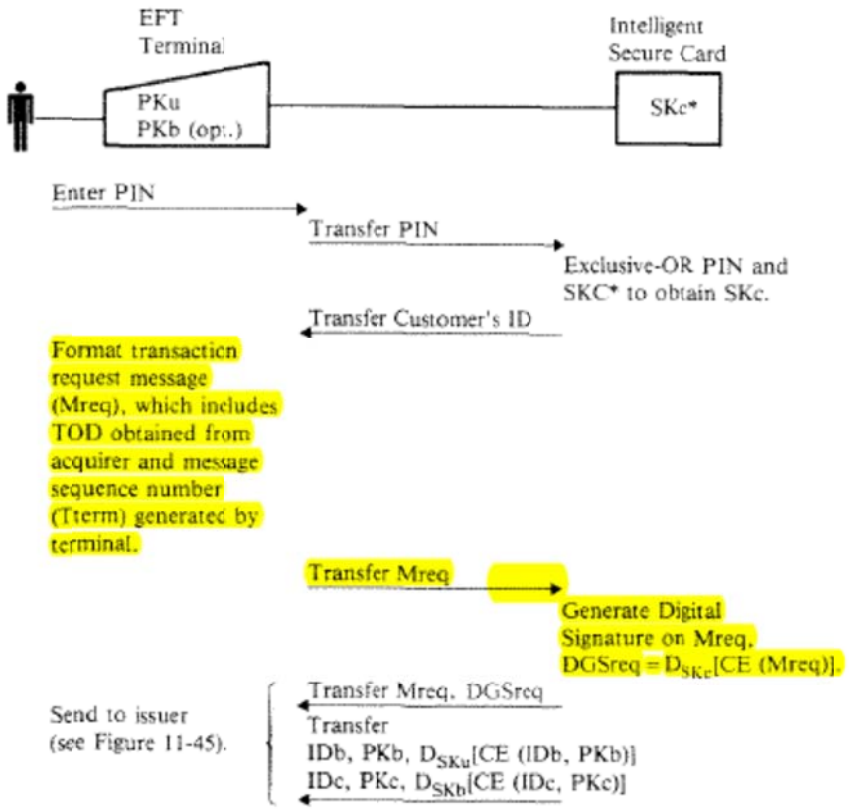


Figure 11-44. On-Line Use—EFT Terminal

Meyer further discloses the sequencing the Board ruled is required by the claims. Meyer makes clear that in order for the "originator" to generate the MAC [or equivalently, in the case of public-key algorithms, the digital signature] for a transaction request message, the originator must, at "a minimum," include (and necessarily have received) at least "[t]ransaction identification information (that information which uniquely identifies a specific transaction from a particular terminal)." *See id.* at 457-58 and 589-90. Additionally, at least Figure 11-44 of Meyer shows receipt by an "Intelligent Secure Card" of the transaction request message (Mreq), e.g., the required transaction information, before it generates the

"digital signature" (or VAN). Accordingly, Meyer discloses what the Board in the IPR Decision considered to be missing from the Davies reference, namely that "at least a portion of the receiving step must precede the generating step."

D. Davies and Meyer Combined Render the Challenged Claims Obvious

In assessing invalidity under Section 103, the "rationale to support a conclusion that the claim would have been obvious is that all the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination yielded nothing more than predictable results to one of ordinary skill in the art." M.P.E.P. § 2143, *see also KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). Such is the case here – combining 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. Davies' method uses "a digital signature facility with a key registry to authenticate public keys," and to approve transactions. Davies at 328-331. 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. Meyer at 457-58, 469 and 590. Applying the Meyer process of having an originator generate

MACs after receiving transaction information to Davies would have yielded predicable results: using the Davies token to first receive the funds transfer information to then generate the VAN. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007) ("The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results."). Thus, these references in their similar purpose of dealing with financial transactions and services, and overlapping teachings, confirm a motivation to combine Davies and Meyer and, as demonstrated in more detail below, should render these claims invalid. *See* Diffie Declaration at ¶¶ 112-18.

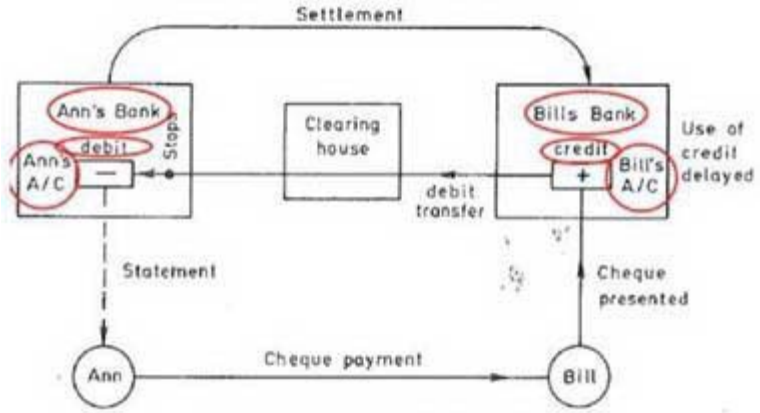
E. The Challenged Claims Are Unpatentable

Petitioners submit that the Challenged Claims should be held unpatentable based on the following reasons.

There are many ways to practice the Challenged Claims (including, for example, with pen and paper). The prior art discussed below should not be read to suggest that any perceived complexity or structure is necessary to practice the Challenged Claims. They simply show documented examples of where the claims were practiced, or where motivation existed to practice them in an obvious fashion, in the past.

1. Claims 51, 53 and 55 are anticipated under 35 U.S.C. §102 by Davies

As shown in the following claim chart, Davies teaches each and every limitation of claims 51, 53 and 55 of the '302 Patent, rendering those claims unpatentable under 35 U.S.C. § 102(b) as being anticipated by Davies.

Claims	Davies
Claim 51 [51preA] A method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party,	**Example I** Davies describes that "Bill, presents the cheque for payment to his own bank which sends the cheque to the payer's bank...The payer's bank debits Ann's account and the payee's bank credits Bill's." Davies at 10.2, p. 285; Fig. 10.1 (reproduced and annotated below). *See also id.* at 10.2, pp. 286-287 and Fig. 10.2.  *Fig. 10.1 Cheque payment mechanism* **Example II** Davies describes that "[t]he second section of the cheque contains the customer identity and his public key... followed by the payment information which forms the third section of the cheque data...The amount and currency of the payment and identity of payee describe the payment to be made... The final signature, by the customer, covers all the variable information in the cheque." Davies at 10.6, pp. 328-329; see also Fig. 10.22 (reproduced and annotated below).

Claims	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* ”Private customers of the bank can carry...an intelligent token or ‘smart card’... Functioning as an electronic chequebook...The smart card used for point-of-sale payment has been called an ‘electronic wallet’... the electronic cheque is transmitted...to the card issuer bank where the signature is checked...and drawer’s account examined...the accounts of the customer and merchant can be updated.” *Id.* at 10.6, pp. 329-331. *See also* Fig. 10.23 and accompanying text (e.g., “The message and its signature are checked and if all is well an authorization goes to the ATM to release the money.”)
[51preB] 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:	**Example I** Davies describes that “[s]ignatures can use the same public keys... A key registry is the source of authentic public keys.” Davies at 9.6, p. 276. “[A] person P wishes to register a new key with the registry R... P must send to the registry the public key [and] ... receive in response the certificate containing the identity and the public key value signed by R. This is the effective certificate.” *Id.* at 9.6, pp. 276-277. Davies also discloses “registering new public keys...giving the owner of the key in question a certificate signed by the registry which will be accepted by other participants as guaranteeing the genuineness of the public key.” Davies at 9.6, p. 276. “Each entity, when it generates its keys, must register the public key with the key registry...When any of these entities requires an authentic public key it is received in a message from the card registry containing the key, the identifying data and

Claims	Davies
	a digital signature using the registry's key. Before using any public key for the first time, each entity checks its signature in this certificate which it has received." *Id.* at 10.5, p. 322; *see also* Diffie Declaration at ¶57. **Example II** Davies describes that "[the] registry authenticates the bank's public key and the bank authenticates the customer's public key…the cheque… contain[s]…a certificate by the key registry which authenticates the bank's public key…the cheque contains the customer identity and his public key signed by the bank." Davies at 10.6, p. 328; *see also* Figs. 10.22 (reproduced and annotated above), and 10.23 (reproduced below), and accompanying text. Davies describes that "[a]nyone can verify the bank's public key using the signature … the customer identity and his public key [are] verifiable." Davies at 10.6, p. 328-331.

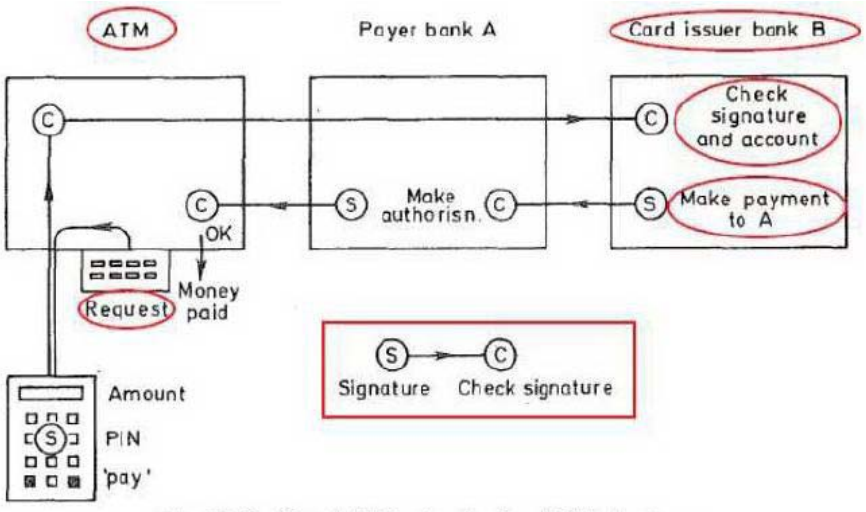
As such, Davies describes funds transfer from Ann's ("first party") bank account to Bill's ("second party") bank account. Diffie Declaration at ¶40 and ¶58. Davies further describes that the public key ("non-secret information") of a sender ("party") is contained in a certificate ("credential") that is issued by a public key registry ("trusted party"). Davies at 9.6, pp. 276-277, 10.5, p. 322.

Davies further describes an electronic check used for funds transfer from a customer ("first party") to a payee ("second party"). Davies at 10.6, pp. 328-329; *see also* Fig. 10.22 (reproduced and annotated above) and 10.23 (reproduced below). Davies teaches that the electronic check serves as a certificate ("credential") for the customer that includes the customer public key signed by the

bank. *Id.* Davies discloses that the information stored in the credential is non-secret in the context of describing that the electronic check ("credential" as construed above) includes public keys ("non-secret" information) and signatures. *Id* at 10.6, p. 328-331. Davies also discloses that the credential is previously issued in the context of describing that a public key is issued in a certificate before the public key is used, as explained above.

As explained in the Diffie Declaration (*see, e.g.*, MasterCard Exh. 1020 at ¶19, ¶26 and ¶37), a public key would be an example of non-secret information, a certificate would qualify as a credential and a key registry would be an example of a trusted entity as described in the '302 Patent. Similarly, as also explained in the Diffie Declaration (*see, e.g.*, MasterCard Exh. 1020 at ¶¶ 29-30), the customer public key included in a certificate would qualify as credential information. *See* Diffie Declaration at ¶¶ 29-30.

Claims	**Davies**
[51a] 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	*See* Davies at 10.6, pp. 328-329 and Fig. 10.22 (reproduced and annotated above); and Fig. 10.23 (reproduced below):

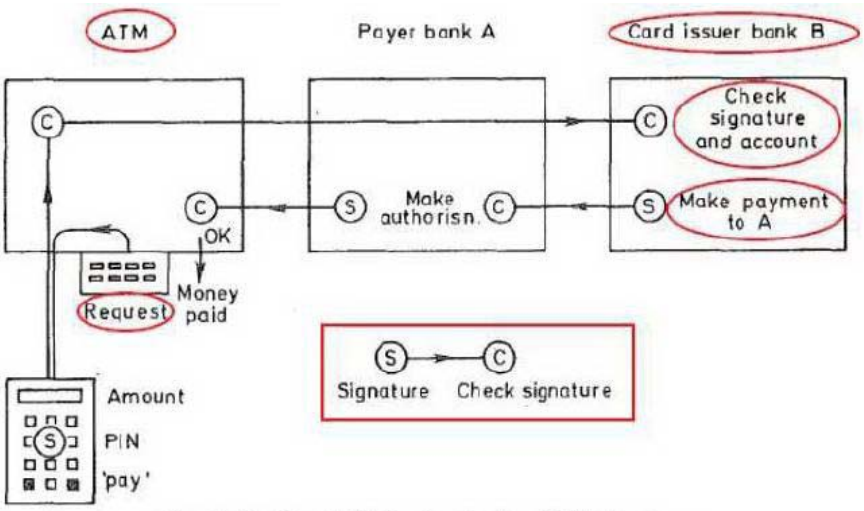
Claims	Davies
transfer amount;	 *Fig. 10.23 Shared ATM network using digital signatures* Fig. 10.23 illustrates processing point-of-sale payments by electronic cheque, including that the "customer's request is formed into a message and presented to the token". *Id.*

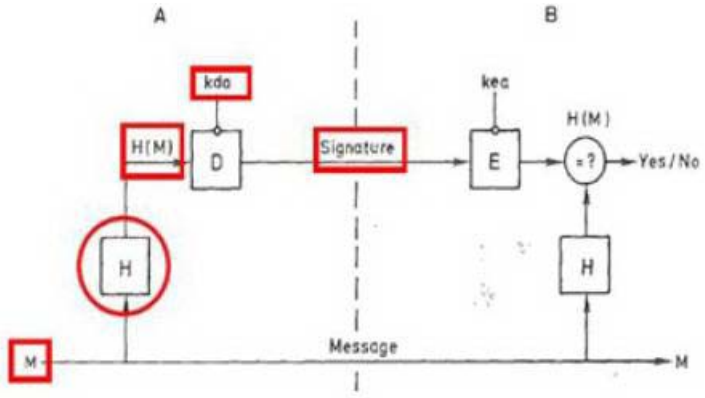
Davies describes the funds transfer transaction using an electronic check that provides the identity of the customer ("information for identifying the account of the first party") and the payee ("information for identifying the account of the second party"), and the payment amount ("transfer amount"). Davies at 10.6, pp. 328-329; Fig. 10.22 and Fig. 10.23 (each reproduced above).

According to the Board's IPR Decision, "at least a portion of the receiving step must precede the generating step...." IPR Decision 12. As explained in the Diffie Declaration, this is exactly what Davies discloses at Fig. 10-23, and accompanying text: "The customer's request is formed into a message and presented to the token." As described below and with respect to

Fig. 10-22, the customer's request, in the form of an electronic cheque, includes, among other things, "the customer identity and his public key... followed by the payment information which forms the third section of the cheque data...The amount and currency of the payment and identity of payee describe the payment to be made." Davies at 328-29 and Fig. 10-22. Then, after the receipt of such information, the message "is signed and returned to the ATM." As described further below, and supported by the Diffie Declaration (*see,* MasterCard Exh. 1020 at ¶51, ¶81, ¶131 and ¶153) and upon applying the ascribed claim interpretations, a signature would qualify as a VAN.

Claims	**Davies**
[51b] generating a variable authentication number (VAN) using at least a portion of the received funds transfer information;	**Example I** Davies describes that "the payment information…forms the third section of the cheque data…final signature, by the customer, covers all the variable information in the cheque…to form this signature the customer needs a secret key." Davies at 10.6, p. 329; *see also* Figs. 10.22 and 10.23 (reproduced and annotated above) and accompanying text (e.g., "Here it is signed and returned to the ATM"). **Example II**

Claims	Davies
	 *Fig. 10.23 Shared ATM network using digital signatures* Davies describes ""that "[t]he customer's request is formed into a message and presented to the token. Here it is signed and returned to the ATM." Davies at 10.6, pp. 330-331; *see also* Fig. 10.23 (reproduced and annotated below).
[51c] determining whether the at least a portion of the received funds transfer information is authentic by using the VAN and the credential information; and	**Example I** Davies describes that "[t]he second section of the cheque contains the customer identity and his public key, signed by the bank and therefore verifiable using the public key [of the bank]…The final signature, by the customer, covers all the variable information in the cheque." Davies at 10.6, 328-329; *see also* Fig. 10.22 (reproduced and annotated above). "The merchant's terminal can verify the signatures and the merchant is sure that the cheques will be accepted as genuine…the electronic cheque is transmitted…to the card issuer bank where the signature is checked." *Id.* at 10.6, p. 330. **Example II** Davies describes that "[t]he customer's request is…signed…the 'cheque' passes…to the card issuer bank, B. Here the signature is checked." *Id.* at 10.6, p. 330-331; *see also* Fig. 10.23 (reproduced and annotated above). Davies also describes that "[s]ender A is

Claims	Davies
	 transmitting a message *M* and signing it, using his secret key *kda*…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 *kea*." *Id.* at 9.3, p. 260; *see also* Fig. 9.5 (reproduced and annotated below). "[T]he certificate containing the identity and the public key value signed by R. This is the effective certificate and may be used as evidence of the value of the public key." *Id.* at 9.6, pp. 277.

Based on the explanation in the Diffie Declaration (*see* MasterCard Exh. 1020 at ¶51, ¶81, ¶131 and ¶153) and upon applying the ascribed claim interpretations, a signature would qualify as a VAN as described in the '302 Patent.

Davies describes that a customer generates a signature ("VAN") on transaction information included in the electronic check with its secret key. Davies at 10.6, p. 329; *see also* Figs. 10.22 and 10.23 (reproduced above).

Davies further describes a point-of-sale payment using an intelligent token in which the token generates a signature ("VAN") on a payment request. Davies at 10.6, pp. 330-331; *see also* Fig. 10.23 (reproduced above).

Davies further describes funds transfer using an electronic check, which includes a customer certificate ("credential") with the customer identity and the customer public key ("credential information") signed by the bank. Davies at 10.6, 328-329; *see also* Fig. 10.22 (reproduced above). Davies teaches that the payment information in the check ("the funds transfer information") is signed by the customer using his private key. *Id.* at 10.6, 328-329; *see also* Fig. 10.22 (reproduced above). A merchant terminal and an issuer bank verify the customer's signature ("VAN") using the customer public key obtained from the check itself. *Id.* at 10.6, p. 330.

Furthermore, Davies describes a payment transaction in which the signature ("VAN") on a payment request ("funds transfer information") is checked by a bank. *Id.* at 10.6, p. 330-331; *see also* Fig. 10.23 (reproduced above). Davies also describes that the signature ("VAN") on a message ("received funds transfer information") is verified using a public key ("credential information") that is contained in a certificate ("credential"). *Id.* at 9.3, p. 260; *see also* Fig. 9.5 (reproduced above).

As shown above, Davies describes that a message is verified by verifying the signature on the message using the public key of the sender obtained from the sender's certificate, and thus teaches determining whether information is authentic using the VAN and the credential information.

Claims	Davies
[51d] 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.	**Example I** Davies describes that "payment information …forms the third section of the cheque data... final signature, by the customer, covers all the variable information in the cheque…the electronic cheque is transmitted…to the card issuer bank where the signature is checked…and drawer's account examined. If all is well, a payment message…is sent… the accounts of the customer and merchant can be updated." Davies at 10.6, p. 330. **Example II** Davies describes that the "customer's request… is signed…the 'cheque' passes…to the card issuer bank, B. Here the signature is checked and the customer's account examined and, if everything is in order, debited. A payment message signed by B is sent to A…if all is well an authorization goes to the ATM to release the money." *Id.* at 10.6, pp. 330-331; *see also* Fig. 10.23 (reproduced and annotated above).

Hence, Davies describes funds transfer using the electronic check in which the issuer bank authorizes a payment ("transferring funds") if the customer's signature ("VAN") covering the payment information in the check ("funds transfer information") is verified. Davies at 10.6, p. 330.

Davies further describes a payment transaction ("transferring funds") where cash is provided from a customer's bank account ("account of the first party") to the customer ("account of the second party") after the customer's bank checks the signature ("VAN") on the request. *Id.* at 10.6, pp. 330-331; *see also* Fig. 10.23 (reproduced above).

The above description is also consistent with the Patentee's own interpretation of the '302 patent: "the ['302] specification…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.)." MasterCard Exh. 1021 (Amazon Brief) at §II.A.1, pp. 4-5.

Claims	**Davies**
Claim 53 The method of claim 51 wherein the funds transfer comprises a payment made by the first party to the second party.	**Example I** *See* [51pre]. **Example II** *See* [51pre].
Claim 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.	**Example I** *See, e.g.,* [51b]. **Example II** Davies describes that "[s]ender A is transmitting a message *M* and signing it, using his secret key *kda*…A one-way function *H(M)* is formed using…the message and then…transformed by the public key signature method, to form the signature." Davies at 9.3, p. 260; *also* Fig. 9.5 (reproduced and annotated above).

Hence, with respect to Claim 53, Davies describes the transfer of funds where a payment is made by Ann ("first party") to Bill ("second party"), as construed previously with respect to claim 51. Davies further describes funds

transfer from a customer ("first party") to a payee ("second party") using an electronic check, as construed previously with respect to claim 51.

Furthermore, with respect to Claim 55, Davies describes the generation of a signature ("VAN") based on a portion of the transaction information ("funds transfer information"). Davies describes that the signature ("VAN") on a message M is generated by signing H(M) using the sender's secret key, where H(M) is obtained by applying a one-way function H to the message M. Davies discloses that at least one of the second and third information is associated with at least one entity by describing that the secret key *kda* is associated with the sender, as discussed above. Davies at 9.3, p. 260; *also* Fig. 9.5 (reproduced above). Also, as discussed above, Davies discloses that the entity is a person or computer program.

2. Claims 51, 53, 55 and 56 are anticipated by Meyer

As shown in the following claim chart, Meyer teaches each and every limitation of claims 51, 53, 55 and 56 of the '302 Patent, rendering those claims unpatentable under 35 U.S.C. § 102(b).

Claims	**Meyer**
Claim 51 [51preA] A method for authenticating the transfer of funds from an account associated with a first party to an	Meyer describes that "[e]very day EFT systems electronically transfer billions of dollars between institutions and individuals. Such transactions (e.g., deposits and withdrawals) cannot be processed safely unless...the correct, unaltered transmission of messages between network nodes (terminals, computers, etc.) can be assured." Meyer 475. "[T]he process of validating messages is called

Claims	Meyer
account associated with a second party,	*message authentication*." *Id.* "A user is normally provided with an embossed, magnetic stripe identification card (bank card) containing an institution identification number, the card's expiration date, and a *primary account number* (PAN). The institution at which the customer opens his account, and which provides the user with a bank card, is called the *issuer*. At an entry point to the system, information on the user's bank card is read into the system and the user enters a secret quantity called the *personal identification number* (PIN). If the cardholder has supplied the correct PIN and if the balance in the account is sufficient to permit the transaction and if that type of transaction is allowed for that account, the system authorizes the funds transfer." *Id.* "For example, consider a simple transaction in which cryptography is not employed. A customer wishes to use a bank card to pay a grocery bill of $35.00 and to receive an additional $50.00 in cash. Assume that the grocer's account is with institution X and the customer's account is with institution Y. The customer's card is inserted into the EFT terminal, either by the customer or by an employee of the retailer attending the EFT terminal, and the customer enters his PIN via a suitable entry device such as a keyboard or a PIN pad, which looks and operates much like a hand-held calculator. Similarly, the grocer enters a transfer request for $85.00 to be transferred from the customer's account to the grocer's account ($35.00 for the groceries plus the $50.00 to be given to the customer)." *Id.* at 477. "The information entered at the EFT terminal is assembled into a *debit request* message. This message or *transaction request*, which includes the customer's PIN, his account number (PAN), and suitable routing information, is then sent via the acquirer (HPC X) and switch to the issuer (HPC Y)." *Id.*

Claims	Meyer
	"Upon receiving the debit request, HPC Y verifies that the PIN correlates properly with the customer's PAN, and that the customer's account balance is sufficient to cover the $85.00 transfer. If the PIN check fails, the user is normally given at least two more chances to enter the correct PIN. If after the additional trials the PIN is still rejected, HPC Y sends a negative reply to HPC X. If the PIN is correct but the account balance is insufficient to cover the transfer, HPC Y denies the debit request by sending a negative reply or debit refusal (insufficient funds) message to HPC X. A message is then sent via the network to the grocer's EFT terminal indicating to the grocer that the funds transfer has been disapproved." *Id.* "If the debit request is approved, HPC Y records the debit request, reduces the customer's account balance by $85.00, and transmits a positive reply or debit authorization message back to HPC X. Upon receiving the debit authorization HPC X takes two actions. A message is sent to the grocer's EFT terminal, indicating to the grocer that the funds transfer has been approved. Then HPC X credits the grocer's account with $85.00. This completes the transaction. (Although other protocols are possible, the one described above will be assumed throughout the present discussion.)" *Id.*
[51preB] 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:	Meyer describes that "[i]f 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)." Meyer 569. "Consider a digital signature procedure for

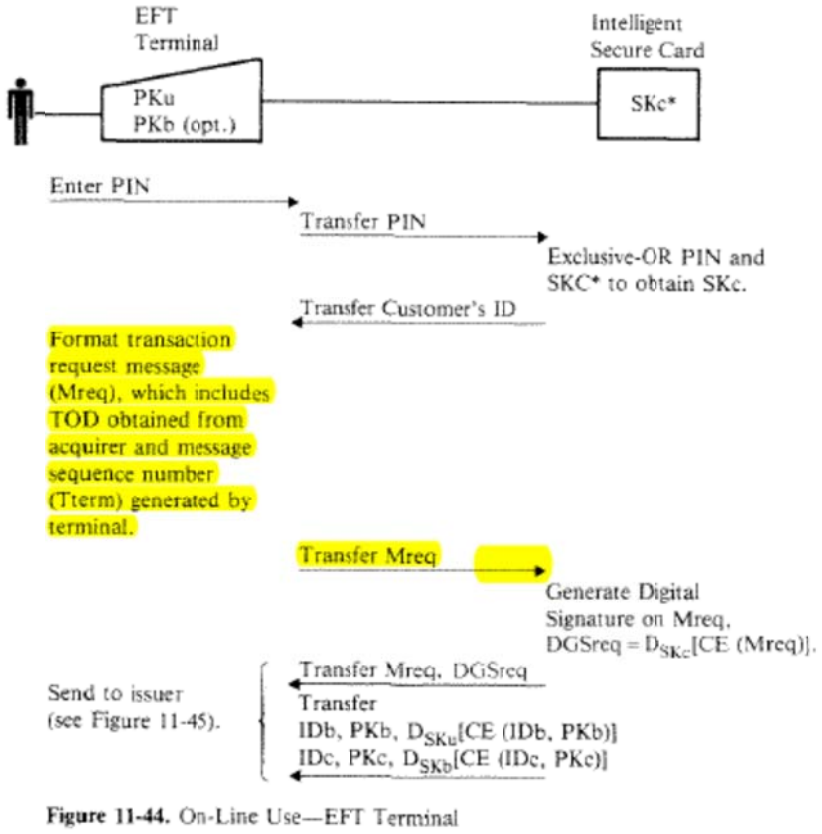
Claims	Meyer
	authenticating transaction response messages which is based on a public key algorithm. Each institution would have a public and private key, PK and SK, respectively. The public key is shared with each other institution and published in a major newspaper to allow each public key to be independently validated." *Id.* "In the asymmetric (e.g., RSA) approach, each user defines his own secret key and corresponding public key. Since the integrity of the public keys must be assured (otherwise authentication is not possible) they will most likely be stored at a system node defined as the key distribution center (KDC). The process of storing public keys requires that users are identified before a public key is accepted by the KDC. (Otherwise an opponent could masquerade as a legitimate system user.) Once this process is completed, the KDC has the added responsibility to route public keys to the appropriate system entry point in such a way that they can be authenticated by the requester. This requires the presence of a secret key belonging to and stored within the KDC. Consequently, a secret key (SKu, or universal secret key) and corresponding public key (PKu) are defined by the KDC." *Id.* at 578. "*Thus the KDC would be the trusted node in the system* and would be called upon to generate and distribute session keys to nodes requesting to communicate with one another....The KDC could also be used with an asymmetric algorithm. In that case the KDC would store all n public keys and route them to the system nodes as required." *Id.* at 583 (emphasis added).

Hence, Meyer describes a transfer request for funds to be transferred from the customer's account **[i.e., "a first party"]** to the grocer's account **[i.e.,**

"a second party"] ($35.00 for the groceries plus the $50.00 to be given to the customer). Meyer at 477 (annotations added). Meyer describes that a public key **[i.e., "a credential"]** is shared with each other institution and published in a major newspaper to allow each public key to be independently validated **[i.e., "the credential is non-secret"]**." *Id.* at 569 (annotations added). The process of storing public keys requires that users are identified before a public key is accepted by the KDC **[i.e., a "trusted party"]**. *Id.* at 578 (annotations added).

As explained in the Diffie Declaration (*see, e.g.*, MasterCard Exh. 1020 at ¶19, ¶26 and ¶37), a public key would be an example of a credential including non-secret information, and a key distribution center (KDC) would be an example of a trusted entity as described in the '302 Patent. Similarly, as also explained in the Diffie Declaration (*see, e.g.*, MasterCard Exh. 1020 at ¶¶ 29-30), the customer public key would qualify as credential information. *See* Diffie Declaration at ¶¶ 29-30.

Claims	Meyer
[51a] receiving funds transfer information including at least information for identifying the account of the first party, and information for identifying the	*See* Fig. 11-44, reproduced below (emphasis added).

Claims	Meyer
account of the second party, and a transfer amount;	 **Figure 11-44.** On-Line Use—EFT Terminal Meyer specifies that "the grocer enters a transfer request for $85.00 to be transferred from the customer's account to the grocer's account ($35.00 for the groceries plus the $50.00 to be given to the customer)." *Id.* at 477. "The information entered at the EFT terminal is assembled into a *debit request* message. This message or *transaction request*, which includes the customer's PIN, his account number (PAN), and suitable routing information, is then sent via the acquirer (HPC X) and switch to the issuer (HPC Y)." *Id.*

Hence, as shown for example in Fig. 11-44, Meyer describes a transaction request message (Mreq) **[i.e., the "funds transfer information"]** from the customer is received by Intelligent Secure Card, via EFT Terminal. Meyer specifies that a transfer request for $85.00 **[i.e., "a transfer amount"]** to

be transferred from the customer's account to the grocer's account is entered. Meyer at 477 (annotations added). Meyer describes that "[t]he information entered at the EFT terminal **[i.e., the "funds transfer information" including the "transfer amount" entered above]** is assembled into a *debit request* message. This message or *transaction request* **[=Mreq]**, which includes the customer's PIN, his account number (PAN) **[i.e., "information for identifying the account of the first party"]**, and suitable routing information **[i.e., "information for identifying the account of the second party"]**, is then sent via the acquirer (HPC X) and switch to the issuer (HPC Y)." *Id* (annotations added).

Claims	**Meyer**
[51b] generating a variable authentication number (VAN) using at least a portion of the received funds transfer information;	*See* Fig. 11-44, reproduced below (emphasis added).

Claims	Meyer

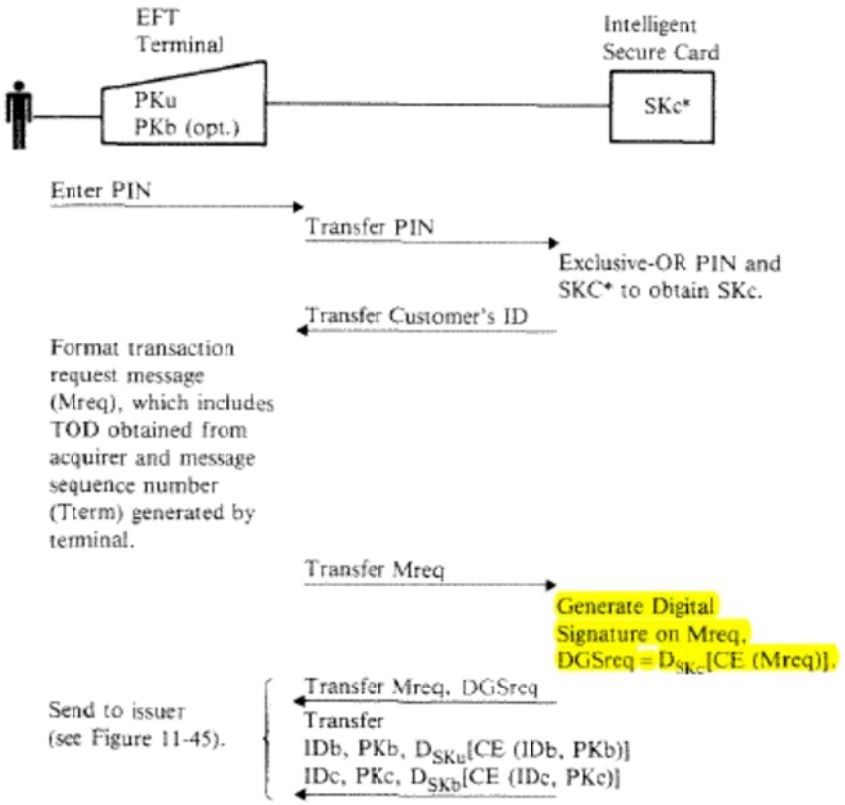


Figure 11-44. On-Line Use—EFT Terminal

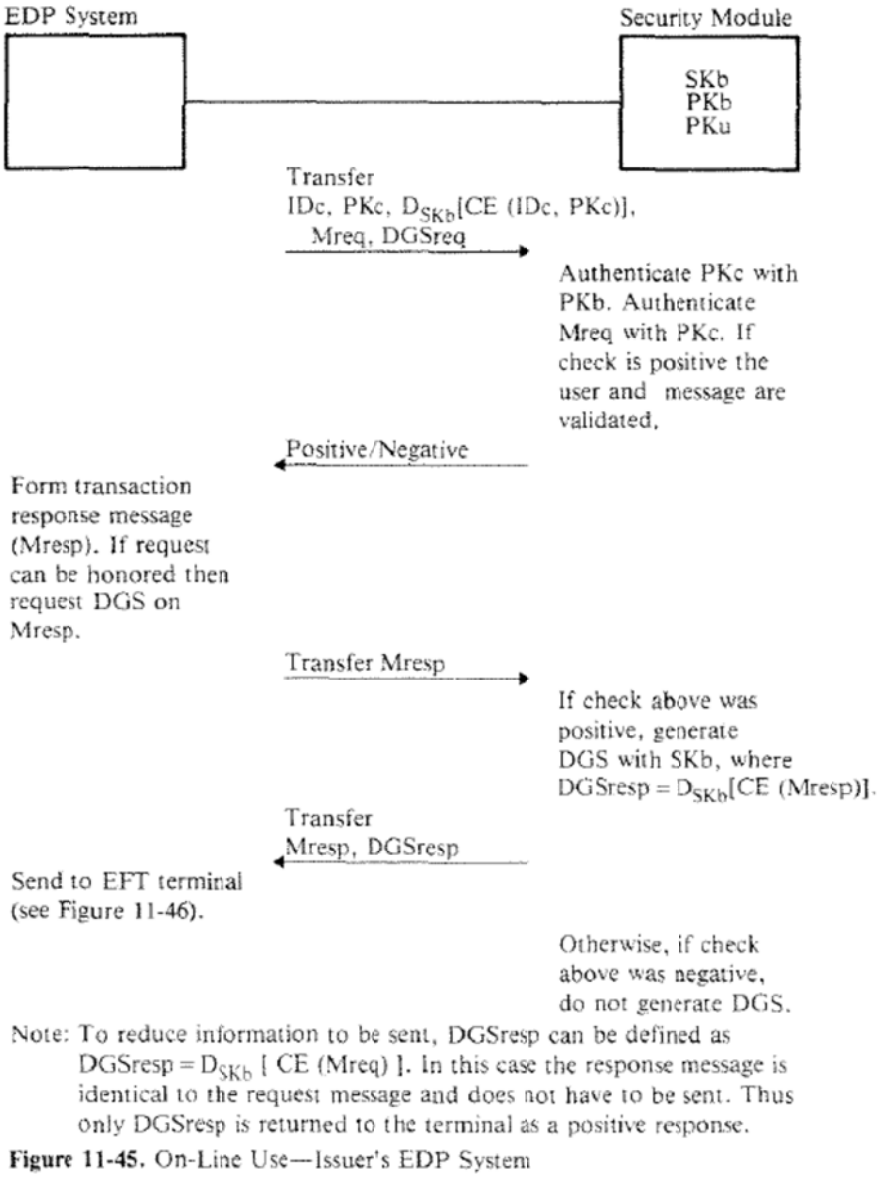
Meyer specifies that "[a] secret user key (SKc, where c stands for customer) is used to generate a quantity (DGSreq) which will enable the issuer to authenticate the transaction request message, Mreq. In the conventional approach this quantity was called a MAC. Since a public-key approach provides a 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 = DsKc [CE(Mreq)]

where CE(Mreq) represents the compressed encoding of Mreq. As discussed in Chapter 9, CE(M) is a one-way function of M and can be generated with publicly known keys for symmetric as well as asymmetric algorithms. In the implementation discussed here it suffices to specify

Claims	Meyer
	one public key for generating CE(M) without, at the same time, specifying the corresponding secret key." Meyer at 590. "Each time the customer initiates a transaction at a terminal, the customer's PIN is entered via a PIN pad or keyboard and transferred to the card. (If the card has its own keyboard, the PIN would not be exposed in the terminal.) On the card, PIN is Exclusive-ORed with the secret card parameter (SKc*) to produce the user's private key, SKc, and *SKc is then used to generate a DGS on the transaction request message via the public-key algorithm*. A time-of-day (TOD) clock obtained from the acquirer via the terminal ... is included in the message to ensure that it is time-variant." *Id.* at 591-92 (emphasis added). "To allow the issuer to validate the transaction request message, a DGS is generated using SKc (i.e., DsKc[CE(Mreq)]). This is accomplished by transferring the assembled message to the card where the compressed encoding of Mreq is generated and in turn deciphered under SKc. The message and signature are returned to the terminal for transmittal to the issuer (identical to the acquirer for a local transaction, different from the acquirer for interchange)." *Id.* at 597
[51c] determining whether the at least a portion of the received funds transfer information is authentic by using the VAN and the credential information; and	*See* Fig. 11-45, reproduced below (emphasis added).

Claims	Meyer



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

"At the issuer (Figure 11-45), the corresponding PKc 'of reference is stored in the EDP system's data base, for example, in the form IDc, PKc, DsKb [CE(IDc, PKc)]. Prior to its use, PKc of reference is authenticated using PKb. The received message is then authenticated by generating its compressed encoding and comparing the result for equality with the received DGSreq encrypted under PKb (i.e., with EPKb(DGSreq) = EPKb IDsKb(CE(Mreq))]). If they are identical, and if the TOD checks, then the issuer concludes that the

Claims	Meyer
	content of the message is correct, the message is not stale, and the secret information supplied by the user, SKc* and PIN, is properly related to the claimed ID." *Id.* at 597.

Hence, as shown for example in Fig. 11-44, Meyer describes a Digital Signature (DGSreq) **[i.e., a "variable authentication number (VAN)"]** is generated by the Intelligent Secure Card after receiving and using the transaction request message (Mreq) **[i.e., including the "received funds transfer information"]**.

As shown for example in Fig. 11-45, Meyer further describes the transaction request message (Mreq) **[i.e., the "received funds transfer information"]** is authenticated using the digital signature (DGSreq) **[i.e., the "VAN"]** and the customer's public key **[i.e., the "credential information"]**. Meyer specifies that the corresponding PKc **[= the customer's public key]** of reference is stored, and prior to its use, PKc of reference is authenticated. The received message is then authenticated by generating its compressed encoding and comparing the result for equality with the received DGSreq encrypted under PKb (i.e., with EPKb(DGSreq) = EPKb IDsKb(CE(Mreq))]). Meyer at 597 (annotations added). If they are identical, and if the TOD checks, then the issuer concludes that the content of the message is correct **[i.e., "the at least a portion**

of the received funds transfer information is authentic"]. *Id.* (annotations added).

Claims	Meyer
[51d] 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.	Meyer specifies "[i]f the requested transaction can be honored, a positive response is sent to the originating terminal. Otherwise, a negative response is sent to the originating terminal." *Id.* "If the debit request is approved, HPC Y records the debit request, reduces the customer's account balance by $85.00, and transmits a positive reply or debit authorization message back to HPC X. Upon receiving the debit authorization HPC X takes two actions. A message is sent to the grocer's EFT terminal, indicating to the grocer that the funds transfer has been approved. Then HPC X credits the grocer's account with $85.00. This completes the transaction." *Id.* at 477.

Hence, Meyer describes 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. Meyer at 477.

Claims	Meyer
Claim 53 The method of claim 51 wherein the funds transfer comprises a payment made by the first party to the second party.	*See* claim 51. Additionally, Meyer specifies that "the grocer enters a transfer request for $85.00 to be transferred from the customer's account to the grocer's account ($35.00 for the groceries plus the $50.00 to be given to the customer)." *Id.* at 477.
Claim 55 The method of claim 51 wherein	*See* claim 51. Additionally, Meyer specifies that "[a] secret user key (SKc, where c stands for customer) is used to

Claims	Meyer
the VAN is generated by using an error detection code derived by using at least a portion of the funds transfer information.	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 = DsKc [CE(Mreq)] where CE(Mreq) represents the compressed encoding of Mreq. As discussed in Chapter 9, CE(M) is a one-way function of M and can be generated with publicly known keys for symmetric as well as asymmetric algorithms. In the implementation discussed here it suffices to specify one public key for generating CE(M) without, at the same time, specifying the corresponding secret key. This is so because the sender and receiver use the same procedure for generating CE(M). To check the signature, the issuer generates the compressed encoding of the received message and compares it with ErKc (DGSreq) (i.e., the received DGSreq encrypted under PKc). If both quantities agree Mreq is accepted; otherwise, not." Meyer at 590.

Hence, with respect to Claim 53, Meyer specifies that a transfer request for $85.00 to be transferred from the customer's account **[i.e., "a first party"]** to the grocer's account **[i.e., "a second party"]** is entered. Meyer at 477 (annotations added).

With respect to Claim 55, Meyer describes DGSreg **[i.e., the VAN]** is generated by using an error detection code derived by using at least a portion of

the transaction request message (Mreq) **[i.e., the "funds transfer information"]**. Meyer at 590 (annotations added).

Claims	**Meyer**
Claim 56 [56a] 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,	*See* claim 51. Additionally, Meyer specifies that "[t]he issuer will produce (in addition to PIN) a public and private key pair (PKc, SKc) for each customer. The user's private key and PIN are Exclusive-ORed to produce a secret card parameter, SKc* (i.e., SKc* = SKc XOR PIN), which is then written on the user's intelligent secure card." Meyer at 591.
[56b] 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	Meyer further specifies that "[e]ach time the customer initiates a transaction at a terminal, the customer's PIN is entered via a PIN pad or keyboard and transferred to the card. (If the card has its own keyboard, the PIN would not be exposed in the terminal.) On the card, PIN is Exclusive-ORed with the secret card parameter (SKc*) to produce the user's private key, SKc, and SKc is then used to generate a

Claims	Meyer
be secured to the at least one party by using the VAN1.	DGS on the transaction request message via the public-key algorithm. A time-of-day (TOD) clock obtained from the acquirer via the terminal (as described earlier) is included in the message to ensure that it is time-variant." *Id.* at 591-92. "At the issuer, the corresponding PKc of reference, which is filed under the user's identifier is read from the EDP system's data base and used to encrypt the received DGSreq. This result is compared for equality with the compressed encoding calculated on the received message Mreq. Furthermore, the received TOD is checked for currency against a TOD of reference stored in the issuer's EDP system. If both tests succeed, the issuer concludes that the content of the message is correct, the message is not a stale message, and the secret information entered by the customer at the entry point (SKc* and PIN) is properly related to the claimed ID." Meyer at 597. "If the requested transaction can be honored, a positive response is sent to the originating terminal. Otherwise, a negative response is sent to the originating terminal." *Id.*

Hence, Meyer describes that the user's private key and PIN are Exclusive-ORed to produce a secret card parameter, SKc* (i.e., SKc* = SKc XOR PIN) **[i.e., "a second variable authentication number (VAN1)"]**, which is then written on the user's intelligent secure card. Meyer at 591 (annotation added). Meyer further describes that the issuer checks the secret information entered by the customer at the entry point (SKc* and PIN) is properly related to the claimed ID **[i.e., the issuer checks that the secret card parameter SKc* is properly related to the information of the party, e.g., the claimed ID]**." *Id* at

597 (annotations added). Furthermore, if the requested transaction can not be honored, a negative response is sent to the originating terminal **[i.e., the transfer of funds is denied]**." *Id.* (annotation added).

3. Claims 51, 53, 55 and 56 are obvious under 35 U.S.C. §103(a) in light of Davies in view of Meyer

Even if the Board finds that Davies does not disclose the sequence required by the Challenged Claims (which Petitioner respectfully submits would be error), the Meyer reference, alone or in combination with Davies, would render the Challenged Claims anticipated and/or obvious to one of ordinary skill in the art.

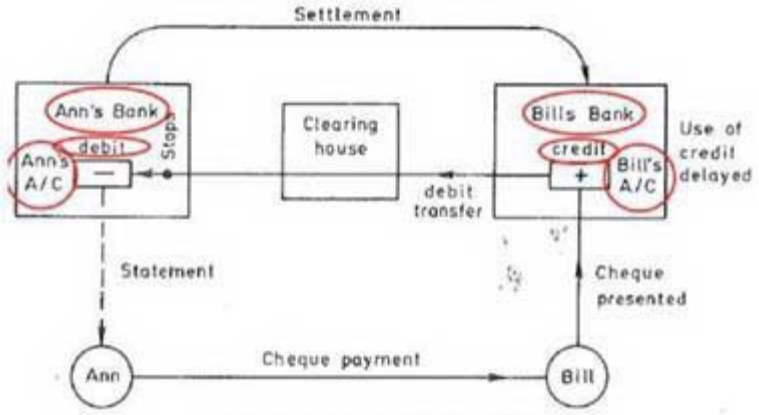
For example, Meyer discloses techniques for "[a]pplying cryptography to pin-based electronic funds transfer systems." Meyer at 429-73. Meyer describes using a "message authentication code" or "MAC" that is generated by using a technique "which produces cryptographic check digits which are appended to the message.... These digits...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." *Id.* at 457; *see also id.* at 469. If the same MAC can be generated by the recipient then the message was not modified and the request can be approved ("[s]hould anyone attempt to modify the message between the time the MAC is generated and the time it is checked, he would be detected."). *Id.*

Meyer makes clear that in order for the "originator" to generate the MAC for a transaction request message, the originator must, at "a minimum," include (and necessarily have received) at least "[t]ransaction identification information (that information which uniquely identifies a specific transaction from a particular terminal)." *Id.* at 457-58. Accordingly, Meyer discloses what the Board in the IPR Decision considered to be missing from the Davies reference, namely that "at least a portion of the receiving step must precede the generating step."

A person of ordinary skill in the art would thus be motivated, at the time of filing the application to which the '302 Patent claims priority, to augment the authentication of message signatures and public keys, as taught by Davies, to perform the "receiving" step prior to the "generating" step, as taught by Meyer.

As noted above [*See* Section VI.D, *supra*] and explained below in the following claim chart in greater detail, the features of claims 51, 53, 55 and 56 of the '302 Patent are obvious over Davies in view of Meyer, rendering these claims unpatentable under 35 U.S.C. § 103(a).

Claims	**Davies in view of Meyer**
Claim 51 [51preA] A method for authenticating the transfer of funds from an account associated with	**Example I** Davies describes that "Bill, presents the cheque for payment to his own bank which sends the cheque to the payer's bank...The payer's bank debits Ann's account and the payee's bank credits Bill's." Davies at 10.2, p. 285; Fig. 10.1 (reproduced and annotated below). *See also id.* at 10.2, pp. 286-287 and Fig. 10.2.

Claims	Davies in view of Meyer
a first party to an account associated with a second party,	 *Fig. 10.1 Cheque payment mechanism* **Example II** Davies describes that "[t]he second section of the cheque contains the customer identity and his public key... followed by the payment information which forms the third section of the cheque data...The amount and currency of the payment and identity of payee describe the payment to be made... The final signature, by the customer, covers all the variable information in the cheque." Davies at 10.6, pp. 328-329; see also Fig. 10.22 (reproduced and annotated below). 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* "Private customers of the bank can carry...an intelligent token or 'smart card'... Functioning as an electronic chequebook...The smart card used for point-of-sale payment has been called an 'electronic wallet'... the electronic cheque is transmitted...to the card issuer bank where the signature is checked...and drawer's account examined...the accounts of the customer and

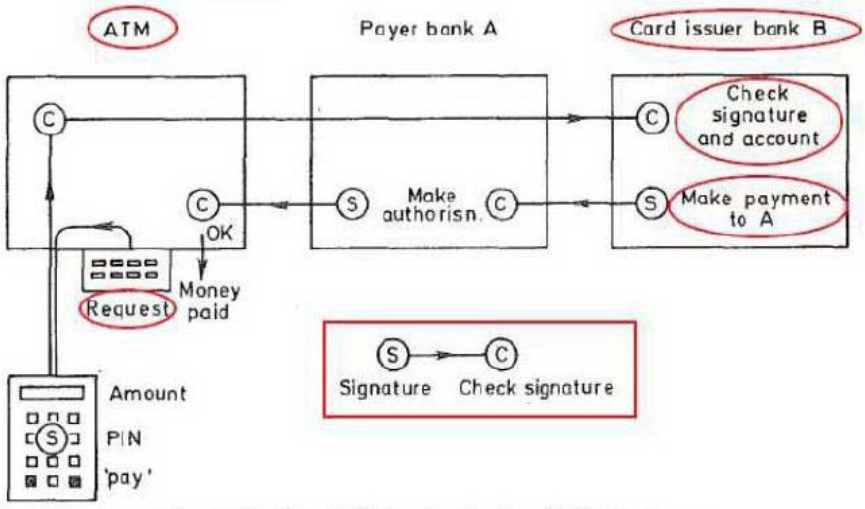
Claims	Davies in view of Meyer
	merchant can be updated." *Id.* at 10.6, pp. 329-331. *See also* Davies, Fig. 10.23 and accompanying text (e.g., "The message and its signature are checked and if all is well an authorization goes to the ATM to release the money.")
[51preB] a credential being previously issued to at least one of the parties by a trusted party, the information stored in the credential being non-secret, the method comprising:	**Example I** Davies describes that "[s]ignatures can use the same public keys... A key registry is the source of authentic public keys." Davies at 9.6, p. 276. "[A] person P wishes to register a new key with the registry R... P must send to the registry the public key [and] ... receive in response the certificate containing the identity and the public key value signed by R. This is the effective certificate." *Id.* at 9.6, pp. 276-277. Davies also describes that "registering new public keys...giving the owner of the key in question a certificate signed by the registry which will be accepted by other participants as guaranteeing the genuineness of the public key." Davies at 9.6, p. 276. "Each entity, when it generates its keys, must register the public key with the key registry...When any of these entities requires an authentic public key it is received in a message from the card registry containing the key, the identifying data and a digital signature using the registry's key. Before using any public key for the first time, each entity checks its signature in this certificate which it has received." *Id.* at 10.5, p. 322; *see also* Diffie Declaration at ¶57. **Example II** Davies describes that "[the] registry authenticates the bank's public key and the bank authenticates the customer's public key…the cheque… contain[s]…a certificate by the key registry which authenticates the bank's public key…the cheque contains the customer identity and his public key signed by the bank." Davies at 10.6, p. 328; *see also* Figs. 10.22 (reproduced and annotated previously at [51preA]), and 10.23 (reproduced below), and accompanying text.

Claims	Davies in view of Meyer
	Davies describes that "[a]nyone can verify the bank's public key using the signature … the customer identity and his public key [are] verifiable." Davies at 10.6, p. 328-331.

As such, Davies describes funds transfer from Ann's ("first party") bank account to Bill's ("second party") bank account. Diffie Declaration at ¶40 and ¶58). Davies further describes that the public key ("non-secret information") of a sender ("party") is contained in a certificate ("credential") that is issued by a public key registry ("trusted party"). Davies at 9.6, pp. 276-277, 10.5, p. 322.

Davies further describes an electronic check used for funds transfer from a customer ("first party") to a payee ("second party"). Davies at 10.6, pp. 328-329; *see also* Fig. 10.22 (reproduced and annotated above) and 10.23 (reproduced below). Davies teaches that the electronic check serves as a certificate ("credential") for the customer that includes the customer public key signed by the bank. *Id.* Davies discloses that the information stored in the credential is non-secret in the context of describing that the electronic check ("credential" as construed above) includes public keys ("non-secret" information) and signatures. *Id* at 10.6, p. 328-331. Davies also discloses that the credential is previously issued in the context of describing that a public key is issued in a certificate before the public key is used, as explained above.

As explained in the Diffie Declaration (*see, e.g.*, MasterCard Exh. 1020 at ¶19, ¶26 and ¶37), a public key would be an example of non-secret information, a certificate would qualify as a credential and a key registry would be an example of a trusted entity as described in the '302 Patent. Similarly, as also explained in the Diffie Declaration (*see, e.g.*, MasterCard Exh. 1020 at ¶¶ 29-30), the customer public key included in a certificate would qualify as credential information. *See* Diffie Declaration at ¶¶ 29-30.

Claims	**Davies in view of Meyer**
[51a] 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;	*See* Davies at 10.6, pp. 328-329 and Fig. 10.22 (reproduced and annotated previously at [51preA]); and Fig. 10.23 reproduced here:  *Fig. 10.23 Shared ATM network using digital signatures* Fig. 10.23 illustrates processing point-of-sale payments by electronic cheque, including that the "customer's request is formed into a message and presented to the token". *Id.*

Hence, Davies describes the funds transfer transaction using an electronic check that provides the identity of the customer ("information for

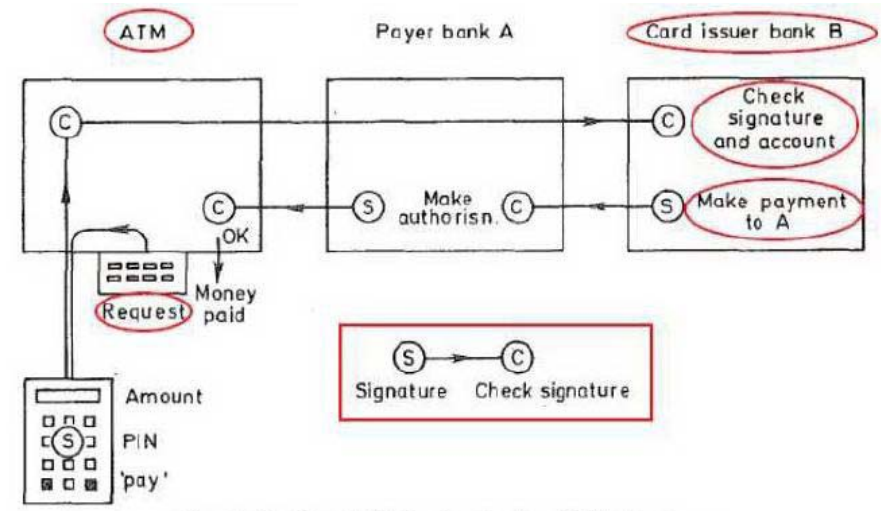
identifying the account of the first party") and the payee ("information for identifying the account of the second party"), and the payment amount ("transfer amount"). Davies at 10.6, pp. 328-329; Fig. 10.22 and Fig. 10.23 (each reproduced above).

According to the Board's IPR Decision, "at least a portion of the receiving step must precede the generating step...." IPR Decision 12. As explained in the Diffie Declaration, this is exactly what Davies discloses at Fig. 10-23, and accompanying text: "The customer's request is formed into a message and presented to the token." As described below and with respect to Fig. 10-22, the customer's request, in the form of an electronic cheque, includes, among other things, "the customer identity and his public key... followed by the payment information which forms the third section of the cheque data...The amount and currency of the payment and identity of payee describe the payment to be made." Davies at 328-29 and Fig. 10-22. Then, after the receipt of such information, the message "is signed and returned to the ATM." As described further below, and supported by the Diffie Declaration (*see,* MasterCard Exh. 1020 at ¶51, ¶81, ¶131 and ¶153) and upon applying the ascribed claim interpretations, a signature would qualify as a VAN.

Meyer further discloses the sequencing the Board ruled is required by the claims. Meyer makes clear that in order for the "originator" to generate the MAC

[or equivalently, in the case of public-key algorithms, the digital signature] for a transaction request message, the originator must, at "a minimum," include (and necessarily have received) at least "[t]ransaction identification information (that information which uniquely identifies a specific transaction from a particular terminal)." Meyer at 457-58 and 589-90. Additionally, at least Figure 11-44 of Meyer shows receipt by an "Intelligent Secure Card" of the transaction request message (Mreq), e.g., the required transaction information, before it generates the "digital signature" (or VAN). Accordingly, Meyer discloses what the Board in the IPR Decision considered to be missing from the Davies reference, namely that "at least a portion of the receiving step must precede the generating step."

Claims	**Davies in view of Meyer**
[51b] generating a variable authentication number (VAN) using at least a portion of the received funds transfer information;	**Example I** Davies describes that "the payment information…forms the third section of the cheque data…final signature, by the customer, covers all the variable information in the cheque…to form this signature the customer needs a secret key." Davies at 10.6, p. 329; *see also* Figs. 10.22 and 10.23 (reproduced and annotated above) and accompanying text (e.g., "Here it is signed and returned to the ATM"). **Example II**

Claims	Davies in view of Meyer
	 *Fig. 10.23 Shared ATM network using digital signatures* Davies describes that "[t]he customer's request is formed into a message and presented to the token. Here it is signed and returned to the ATM." Davies at 10.6, pp. 330-331; *see also* Fig. 10.23 (reproduced and annotated below). Meyer, which discloses techniques for "[a]pplying cryptography to pin-based electronic funds transfer systems," Meyer at 429-73, further specifies using a "message authentication code" or "MAC" that is generated by using a technique "which produces cryptographic check digits which are appended to the message.... These digits...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." *Id.* at 457; *see also id.* at 469. ("[s]hould anyone attempt to modify the message between the time the MAC is generated and the time it is checked, he would be detected."). *Id.*

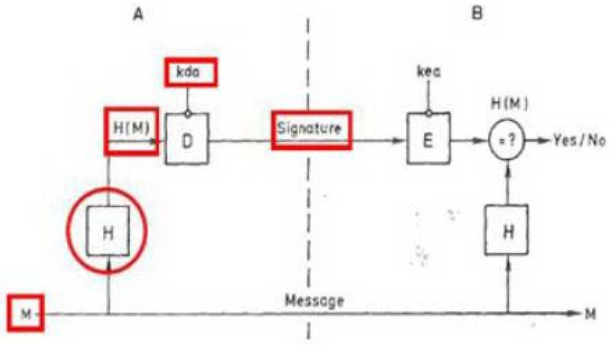
Based on the explanation in the Diffie Declaration (*see* MasterCard Exh. 1020 at ¶51, ¶81, ¶131 and ¶153) and upon applying the ascribed claim interpretations, a signature would qualify as a VAN as described in the '302 Patent.

Davies describes that a customer generates a signature ("VAN") on transaction information included in the electronic check with its secret key. Davies at 10.6, p. 329; *see also* Figs. 10.22 and 10.23 (reproduced above).

Davies further describes a point-of-sale payment using an intelligent token in which the token generates a signature ("VAN") on a payment request. Davies at 10.6, pp. 330-331; *see also* Fig. 10.23 (reproduced above).

Although as discussed above, Davies teaches that the receiving step [51a] is performed before the generating step [51b], Meyer further makes clear that in order for the "originator" to generate the MAC for a transaction request message, the originator must, at "a minimum," include (and necessarily have received) at least "[t]ransaction identification information (that information which uniquely identifies a specific transaction from a particular terminal)." *Id.* at 457-58; *see also* Fig. 11-44 and accompanying text (showing "transfer" of transaction request message to Intelligent Secure Card before the card generates a "digital signature" on the message). Accordingly, Meyer discloses what the Board in the IPR Decision considered to be missing from the Davies reference, namely that "at least a portion of the receiving step must precede the generating step."

Claims	**Davies in view of Meyer**
[51c] determining whether the at least a portion of the received funds	**Example I** Davies describes that "[t]he second section of the cheque contains the customer identity and his public key, signed by the bank and therefore verifiable using

Claims	Davies in view of Meyer
transfer information is authentic by using the VAN and the credential information; and	 the public key [of the bank]…The final signature, by the customer, covers all the variable information in the cheque." Davies at 10.6, 328-329; *see also* Fig. 10.22 (reproduced and annotated above). "The merchant's terminal can verify the signatures and the merchant is sure that the cheques will be accepted as genuine…the electronic cheque is transmitted…to the card issuer bank where the signature is checked." *Id.* at 10.6, p. 330. **Example II** Davies describes that "[t]he customer's request is…signed…the 'cheque' passes…to the card issuer bank, B. Here the signature is checked." *Id.* at 10.6, p. 330-331; *see also* Fig. 10.23 (reproduced and annotated above). Davies also describes that "[s]ender A is transmitting a message *M* and signing it, using his secret key *kda*…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 *kea*." *Id.* at 9.3, p. 260; *see also* Fig. 9.5 (reproduced and annotated below). "[T]he certificate containing the identity and the public key value signed by R. This is the effective certificate and may be used as evidence of the value of the public key." *Id.* at 9.6, pp. 277.'

Davies further describes funds transfer using an electronic check, which includes a customer certificate ("credential") with the customer identity and the customer public key ("credential information") signed by the bank. Davies at 10.6,

328-329; *see also* Fig. 10.22 (reproduced above). Davies teaches that the payment information in the check ("the funds transfer information") is signed by the customer using his private key. *Id.* at 10.6, 328-329; *see also* Fig. 10.22 (reproduced above). A merchant terminal and an issuer bank verify the customer's signature ("VAN") using the customer public key obtained from the check itself. *Id.* at 10.6, p. 330.

Furthermore, Davies describes a payment transaction in which the signature ("VAN") on a payment request ("funds transfer information") is checked by a bank. *Id.* at 10.6, p. 330-331; *see also* Fig. 10.23 (reproduced above). Davies also describes that the signature ("VAN") on a message ("received funds transfer information") is verified using a public key ("credential information") that is contained in a certificate ("credential"). *Id.* at 9.3, p. 260; *see also* Fig. 9.5 (reproduced above).

As shown above, Davies describes that a message is verified by verifying the signature on the message using the public key of the sender obtained from the sender's certificate, and thus teaches determining whether information is authentic using the VAN and the credential information.

Claims	**Davies in view of Meyer**
[51d] transferring funds from the account of the first party to the	**Example I** Davies describes that "payment information …forms the third section of the cheque data... final signature, by the customer, covers all the variable

Claims	Davies in view of Meyer
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.	information in the cheque…the electronic cheque is transmitted…to the card issuer bank where the signature is checked…and drawer's account examined. If all is well, a payment message…is sent… the accounts of the customer and merchant can be updated." Davies at 10.6, p. 330. **Example II** Davies describes that the "customer's request… is signed…the 'cheque' passes…to the card issuer bank, B. Here the signature is checked and the customer's account examined and, if everything is in order, debited. A payment message signed by B is sent to A…if all is well an authorization goes to the ATM to release the money." *Id.* at 10.6, pp. 330-331; *see also* Fig. 10.23 (reproduced and annotated above).

Hence, Davies describes funds transfer using the electronic check in which the issuer bank authorizes a payment ("transferring funds") if the customer's signature ("VAN") covering the payment information in the check ("funds transfer information") is verified. Davies at 10.6, p. 330.

Davies further describes a payment transaction ("transferring funds") where cash is provided from a customer's bank account ("account of the first party") to the customer ("account of the second party") after the customer's bank checks the signature ("VAN") on the request. *Id.* at 10.6, pp. 330-331; *see also* Fig. 10.23 (reproduced above).

The above description is also consistent with the Patentee's own interpretation of the '302 patent: "the ['302] specification…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.)." MasterCard Exh. 1021 (Amazon Brief) at §II.A.1, pp. 4-5.

Claims	**Davies in view of Meyer**
Claim 53 The method of claim 51 wherein the funds transfer comprises a payment made by the first party to the second party.	**Example I** *See* [51pre]. **Example II** *See* [51pre].
Claim 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.	**Example I** *See, e.g.,* [51b]. **Example II** Davies describes that "[s]ender A is transmitting a message *M* and signing it, using his secret key *kda*…A one-way function *H(M)* is formed using…the message and then…transformed by the public key signature method, to form the signature." Davies at 9.3, p. 260; *also* Fig. 9.5 (reproduced and annotated above).

Hence, with respect to Claim 53, Davies describes the transfer of funds where a payment is made by Ann ("first party") to Bill ("second party"), as construed previously with respect to claim 51. Davies further describes funds transfer from a customer ("first party") to a payee ("second party") using an electronic check, as construed previously with respect to claim 51.

Furthermore, with respect to Claim 55, Davies describes the generation of a signature ("VAN") based on a portion of the transaction information ("funds transfer information"). Davies describes that the signature ("VAN") on a message M is generated by signing H(M) using the sender's secret key, where H(M) is obtained by applying a one-way function H to the message M. Davies discloses that at least one of the second and third information is associated with at least one entity by describing that the secret key *kda* is associated with the sender, as discussed above. Davies at 9.3, p. 260; *also* Fig. 9.5 (reproduced above). Also, as discussed above, Davies discloses that the entity is a person or computer program.

Claims	**Davies in view of Meyer**
Claim 56 [56a] 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),	Meyer specifies that "[t]he issuer will produce (in addition to PIN) a public and private key pair (PKc, SKc) for each customer. The user's private key and PIN are Exclusive-ORed to produce a secret card parameter, SKc* (i.e., SKc* = SKc XOR PIN), which is then written on the user's intelligent secure card." Meyer at 591.

Claims	Davies in view of Meyer
the VAN1 being used to secure at least a portion of the credential information to the at least one party,	
[56b] 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.	Meyer further specifies that "[e]ach time the customer initiates a transaction at a terminal, the customer's PIN is entered via a PIN pad or keyboard and transferred to the card. (If the card has its own keyboard, the PIN would not be exposed in the terminal.) On the card, PIN is Exclusive-ORed with the secret card parameter (SKc*) to produce the user's private key, SKc, and SKc is then used to generate a DGS on the transaction request message via the public-key algorithm. A time-of-day (TOD) clock obtained from the acquirer via the terminal (as described earlier) is included in the message to ensure that it is time-variant." *Id.* at 591-92. "At the issuer, the corresponding PKc of reference, which is filed under the user's identifier is read from the EDP system's data base and used to encrypt the received DGSreq. This result is compared for equality with the compressed encoding calculated on the received message Mreq. Furthermore, the received TOD is checked for currency against a TOD of reference stored in the issuer's EDP system. If both tests succeed. the issuer concludes that the content of the message is correct, the message is not a stale message, and the secret information entered by the customer at the entry point (SKc* and PIN) is properly related to the claimed ID." Meyer at 597. "If the requested transaction can be honored, a positive response is sent to the originating terminal. Otherwise, a negative response is sent to the originating terminal." *Id.*

Hence, Meyer describes that the user's private key and PIN are Exclusive-ORed to produce a secret card parameter, SKc* (i.e., SKc* = SKc

XOR PIN) **[i.e., "a second variable authentication number (VAN1)"]**, which is then written on the user's intelligent secure card. Meyer at 591 (annotation added). Meyer further describes that the issuer checks the secret information entered by the customer at the entry point (SKc* and PIN) is properly related to the claimed ID **[i.e., the issuer checks that the secret card parameter SKc* is properly related to the information of the party, e.g., the claimed ID]**." *Id.* at 597 (annotations added). Furthermore, if the requested transaction can not be honored, a negative response is sent to the originating terminal **[i.e., the transfer of funds is denied]**." *Id.* (annotation added).

4. Claim 55 is obvious under 35 U.S.C. §103(a) in light of Davies or Meyer in view of Nechvatal

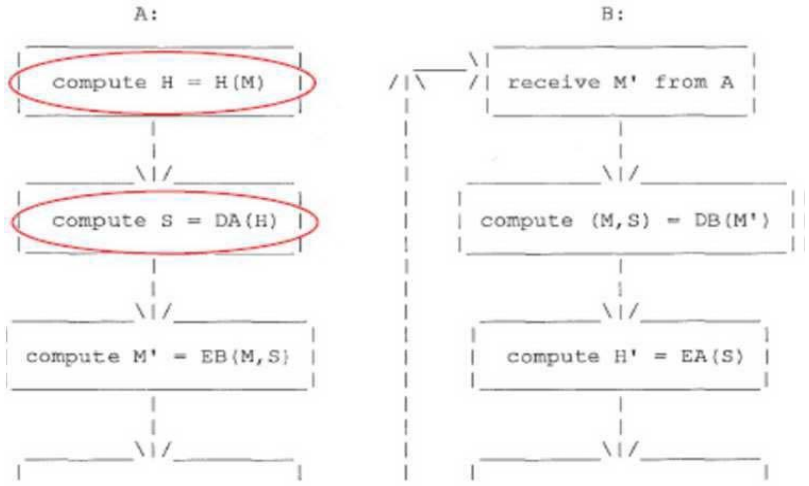
Davies teaches that the signatures may be generated by computing hash values on the transaction information as an intermediate step. *See, e.g.,* Davies at 267. Similarly, Meyer teaches that the digital signature is formed as a compressed encoding of the transaction request message using a one-way function. *See, e.g.*, Meyer at 590.

Nechvatal provides rationale for using one-way functions or hash functions in this manner, which include, among others, an explanation that hash functions mitigate the effects of data expansion and lower bandwidth transmission that result from generating digital signatures. Nechvatal at 32-33. Hash functions therefore

allow the signing entity in each of Davies and Meyer to condense the information *M* included in a certificate into a fixed size representation *H(M)* that is of smaller size than *M*, and sign *H(M)* in a relatively quick fashion, which would improve signing efficiency, as taught by Nechvatal. It would be obvious for a person of ordinary skill in the art, at the time of the effective filing date of the '302 Patent, to combine the teachings of Davies or Meyer with Nechvatal to implement an electronic funds transfer system in which the transactions are authenticated by digital signatures, as taught by Davies and Meyer. *See* Diffie Declaration at ¶135.

As noted above and explained below in the claim chart in greater detail, claim 55 of the '302 Patent is rendered obvious over Davies or Meyer in view of Nechvatal, rendering claim 55 unpatentable under 35 U.S.C. § 103(a).

Claims	**Davies or Meyer in view of Nechvatal**
Claim 55 The method of claim 51	*See* Sections VI.E.1-VI.E.3, *supra*
wherein the VAN is generated by using an error detection code derived by using at least a portion of the funds transfer information.	*See, e.g.,* VI.E.1, [51b]. Furthermore, Davies describes that "[s]ender A is transmitting a message *M* and signing it, using his secret key *kda*…A one-way function *H(M)* is formed using…the message and then…transformed by the public key signature method, to form the signature." Davies at 9.3, p. 260; Fig. 9.5 (reproduced and annotated above). Meyer specifies that "CE(M) is a one-way function of M and can be generated with publicly known keys for symmetric as well as asymmetric algorithms. Meyer at 590. Nechvatal specifies that "[i]f a hash function H is used, A computes [signature] s = DA(H(M)) and sends both M [message] and s to B." Nechvatal at 3.1.1; *see also* Figure

Claims	Davies or Meyer in view of Nechvatal
	5 (partially reproduced and annotated below). "[H]ash functions…serve as cryptographic checksums (i.e., error-detecting codes), thereby validating the contents of a message." *Id.* at 3.  **Nechvatal, Fig. 5**

Hence, Davies describes the generation of a signature ("VAN") based on a portion of the transaction information ("funds transfer information"). Davies describes that the signature ("VAN") on a message M is generated by signing H(M) using the sender's secret key, where H(M) is obtained by applying a one-way function H to the message M. Davies discloses that at least one of the second and third information is associated with at least one entity by describing that the secret key *kda* is associated with the sender, as discussed above. Davies at 9.3, p. 260; *also* Fig. 9.5 (reproduced above). Also, as discussed above, Davies discloses that the entity is a person or computer program.

Meyer describes DGSreg **[i.e., the VAN]** is generated by using an error detection code derived by using at least a portion of the transaction request message (Mreq) **[i.e., the "funds transfer information"]**. Meyer at 590 (annotations added).

While Davies and Meyer each suggests that the signature, i.e., VAN, is based on a one-way function, Nechvatal explicitly mentions that the one-way function is an error detection code, i.e., the VAN is generated using an error detection code. Indeed, Nechvatal discloses that a signature ("VAN") is generated using a hash function, which is an error detection code. Nechvatal at 3.1.1; *see also* Figure 5 (reproduced in part above).

5. Claim 56 is obvious under 35 U.S.C. §103(a) in light of Davies in view of Fischer and Piosenka

Claim 56 depends from independent claim 51 and additionally requires the use of a second VAN to secure credential information and a transfer of funds to be denied if the credential information in the second VAN is not validated.

A person of ordinary skill in the art would be motivated, at the time of the effective filing date of the '302 Patent, to combine the teachings of Davies with the teachings of Fischer for securing messages, end-to-end. *See* Diffie Declaration at ¶158. In greater detail, Davies teaches generation/application of a signature on a message that is sent by a sender to a recipient. Along with the message, the sender

may send a certificate that includes the sender's public key. Using a sender's public key that is obtained from the received certificate, the recipient is able to verify the message signature.

Fischer, in describing the signature verification procedure, explicitly discloses that the recipient may authenticate the sender's public key itself before using the public key to verify the message signature. Specifically, according to Fischer's signature verification procedure, the sender's certificate includes a hierarchy of all certificates and signatures by higher authorities that validate the sender's certificate. The receiver preliminarily validates the sender's public key by verifying the signature on the sender's certificate using a higher authority's certificate that is included in the sender's certificate. Fischer at 17:34-47.

It would also be obvious for a person of ordinary skill in the art to augment the authenticated electronic funds transfer mechanisms using digital signatures, which is taught by Davies, with the counter signature of Fischer, as this would allow for the electronic funds transfer transaction using a chain of authority, where each higher level approves any commitment/signature made at a lower level. *See* Diffie Declaration at ¶159-60.

Although the combination of Davies and Fischer discloses the verification of message signatures along with the authentication of the public key that is used for generating the message signature, the two references do not explicitly describe

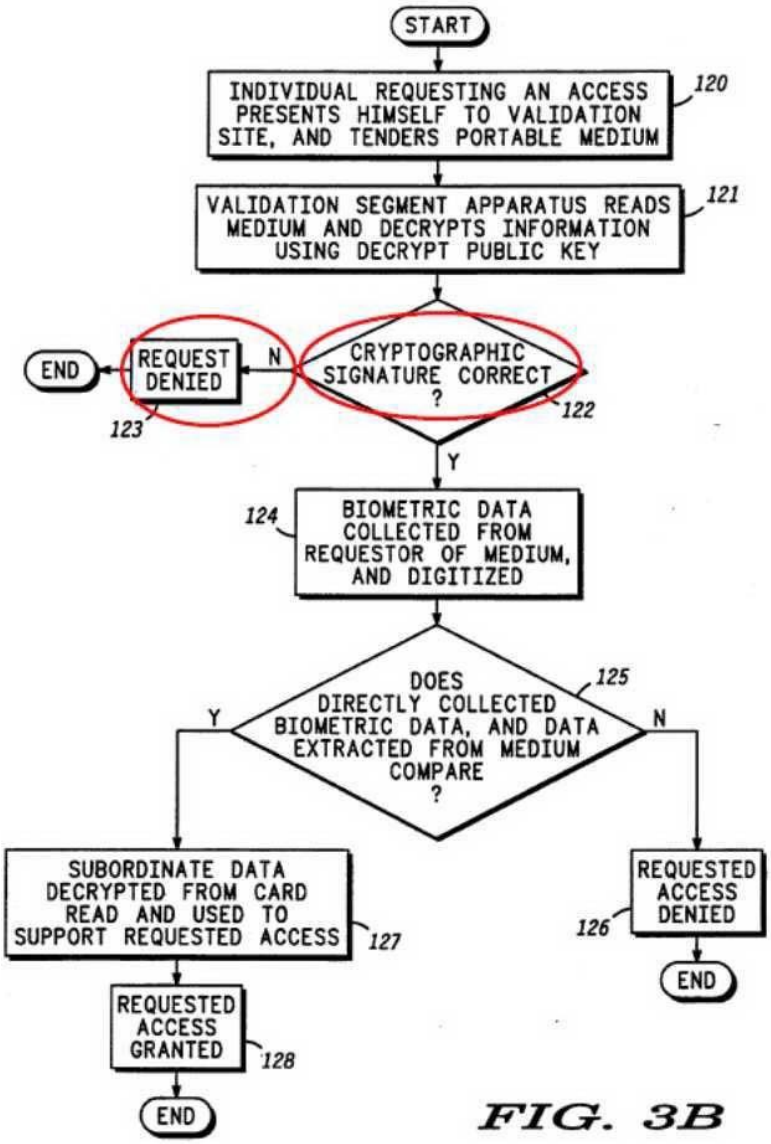
what happens if an authentication is unsuccessful[3]. It would be common sense to one of ordinary skill in the art as of the priority date of the '302 Patent to have the system reject a transaction if the authentication was unsuccessful. Nevertheless, this rejection is explicitly disclosed by Piosenka, who describes that a user's request for access is denied if the signature on the user's credential cannot be validated. A person of ordinary skill in the art would be motivated, at the time of filing the application to which the '302 Patent claims priority, to augment the verification 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. Diffie Declaration at ¶174. A recipient of a message, *e.g.*, an electronic funds transfer message, verifies the message based on authenticating the sender's public key certificate and the message signature. If either the certificate signature or the message signature does not verify successfully, the recipient denies the transaction. *See*, *e.g.*, *id.* at ¶¶ 171-74.

As noted above and explained below in the following claim chart in greater detail, the features of claim 56 of the '302 Patent are obvious over Davies in view

[3] Davies explicitly says that "if everything is in order" the customer's account is "debited," meaning that if everything is not is order the transaction fails. Davies 331. As such, whether or not denial from an unsuccessful authentication is explicit there, it certainly is implied and obvious.

of Fischer and further in view of Piosenka, rendering claim 56 unpatentable under 35 U.S.C. § 103(a).

Claims	Davies in view of Fischer and Piosenka
Claim 56 [56pre] The method of claim 51 for further securing the transfer of funds,	*See* claim 51.
[56a] 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,	*See* [51preB]. **Example I** *See* Davies at 10.6, p. 328; *see also* [51preB]. '**Example II** *See* Davies at 10.6, p. 328; *see also* [51preB].
[56b] authentication and the transfer of funds being denied to the at least one party if the at least a	Davies states that "[t]he recipient examines every signature supplied and verifies that each accurately signs its purported object (...a certificate or another signature). The recipient insures that each signature includes a corresponding validated certificate...All certificates are then examined." Fischer at 17:34-47. Piosenka specifies that "user's credentials...written on

Claims	Davies in view of Fischer and Piosenka
portion of the credential information cannot be secured to the at least one party by using the VAN1.	to...card having memory." Piosenka at 6:41-42. "[D]etermines whether the cryptographic signature it calculates matches the cryptographic signature recorded on the memory medium. If the two cryptographic signatures do not match...The request is denied and the process ended." *Id.*, 11:15-23; Fig. 3B (reproduced and annotated below).
	 FIG. 3B

Hence, Davies describes that an electronic check ("credential") includes a signature ("VAN1"—*see* [51b]) by the bank that binds the customer ("one party") identity to the customer public key. The bank's signature may be verified using the bank's public key, which is signed by the trusted key registry ("trusted party"—*see* [51preB]) and thus the bank itself may be a trusted party. Davies at 10.6, p. 328; *see also* [51preB].

Based on the Diffie Declaration at ¶40 and ¶62-69, an electronic check would qualify as a credential per the '302 Patent. *See* MasterCard Exh. 1020 at ¶¶ 40, 62-69.

Davies further describes that a customer ("one party") uses an electronic check that includes a customer certificate ("issued a credential"), where a bank ("trusted party") generates a signature ("VAN1") verifying the customer's identity and public key included in the electronic check ("secure at least a portion of the credential information to the at least one party"). *Id.* at 10.6, p. 328; [51preB].

Davies discloses that authentication and the transfer of funds is 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 in the context of describing that a payment message ("transfer of funds") based on the electronic check is approved only if the signatures ("VAN1") on the check are verified. *Id*. at 10.6, pp. 328-330 and Fig. 10.22 (reproduced above); *also* [51preB].

As discussed in [51preB], in Davies, the signature of the bank ("VAN1") in the second section of the electronic check ("credential") serves to verify ("authentication") the identity and public key of the customer ("the credential information... secured to the at least one party by using the VAN1"). The merchant's terminal and the bank verify the signatures before a payment is made. *Id*. at 10.6, pp. 328-330 and Fig. 10.22 (reproduced above); [51preB].

Davies states that the payment is approved if the signature is verified, and thus it is obvious that the payment would be denied if the signature of the bank ("VAN1") in the second section of the electronic check ("credential") cannot verify the identity and public key of the customer, or if the customer signature ("VAN1") in the third section of the check does not verify the payment information. Therefore, Davies teaches that authentication and the transfer of funds are denied if the credential information cannot be secured to the one party by using the VAN1.

While Davies suggests checking the bank's signature to verify the customer's public key, Fischer specifies that certificate information is verified based on the signature in the certificate. Fischer at 17:34-47.

While Davies in view of Fischer suggests that authentication and funds transfer are denied to the at least one party if the credential information cannot be verified by the one party by using the VAN1, Piosenka clearly states that a request

("authentication and funds transfer") is denied if the signature with the user's credentials stored in memory medium cannot be verified. Piosenka at 6:41-42, 11:15-23; *see also* Fig. 3B (reproduced above).

CONCLUSION

For the foregoing reasons, Petitioner respectfully requests that CBM review of the '302 Patent be instituted, and that trial be instituted on each of the Challenged Claims based on each of the separate and distinct grounds set forth above.

Respectfully Submitted,

Date: January 21, 2015

/Robert C. Scheinfeld/

Robert C. Scheinfeld
BAKER BOTTS L.L.P.
30 Rockefeller Plaza
New York, NY 10112

Eliot D. Williams
BAKER BOTTS L.L.P.
1001 Page Mill Road
Building One, Suite 200
Palo Alto, CA 94304

Counsel *for* MASTERCARD INTERNATIONAL INCORPORATED

CERTIFICATE OF SERVICE

The undersigned hereby certifies that, on January 21, 2015, a true copy of the foregoing **Petition for Covered Business Method Review**, was served via overnight Fedex upon the following:

Lawrence R. Youst
Lawrence Youst PLLC
46 Wooded Park Pl
The Woodlands TX 77380-2490

that being the address on file with the Office for the patent at issue.

Respectfully Submitted,

Date: January 21, 2015

/Robert C. Scheinfeld
Robert C. Scheinfeld