

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Leon Stambler
U.S. Patent No.: 5,793,302

Issue Date: August 11, 1998
Appl. Serial No.: 08/747,174
Filing Date: November 12, 1996
Title: METHOD FOR SECURING INFORMATION RELEVANT TO A TRANSACTION

**DECLARATION OF PROFESSOR WHITFIELD DIFFIE IN SUPPORT OF
MASTERCARD INTERNATIONAL INCORPORATED'S PETITION FOR COVERED
BUSINESS METHOD REVIEW OF UNITED STATES PATENT NO. 5,793,302**

1. My name is Whitfield Diffie, and I reside in Woodside, California. I understand that I am submitting a declaration offering technical opinions in connection with the Petition for Covered Business Method Review filed herewith in the United States Patent and Trademark Office for U.S. Patent No. 5,793,302 ("the '302 Patent"). I have previously submitted two similar declarations along with petitions for *Inter Partes Review* of the '302 Patent, which I signed on June 10, 2013 and April 25, 2014, respectively, and for the currently pending Petition for Covered Business Method Review, which I signed on October 17, 2014.
2. I have been retained on behalf of MasterCard International Incorporated. My compensation is \$600 hourly and is unaffected by the substance or outcome of my opinions.
3. I have reviewed the content of the '302 Patent, including claims 51, 53, 55, and 56 of the patent. In addition, I have reviewed the following documents: D. W. Davies et al., *Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer*, 254-332 (1989) ("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) ("Meyer"); James Nechvatal, *Public-key Cryptography* (NIST Special Publication 800-2) (April 1991) ("Nechvatal"); U.S. Patent No. 4,868,877 to Fischer ("Fischer"); and U.S. Patent No. 4,993,068 to Piosenka et al. ("Piosenka").

4. I have over forty (40) years of experience in computer science and cryptography. I attended the Massachusetts Institute of Technology from 1961 to 1965, during which, I earned a Bachelor of Science in Mathematics. From 1975 to 1978, I performed graduate studies in Electrical Engineering at Stanford University.
5. In 1965, I joined the Mitre Corporation. At Mitre, I assisted in the development of the MATHLAB symbolic-mathematical-manipulation system, and performed research on interactive debugging and extensible compiling, using the facilities of the MIT Artificial Intelligence Laboratory.
6. In 1969, I joined the Artificial Intelligence Laboratory at Stanford University as a Research Programmer. Over the next three (3) years, I engaged in research on proof of correctness of programs, and on proof checking and extensible compilers, and I assisted in the development of the Lisp 1.6 (now Ilisp) system.
7. I worked at Northern Telecom from 1978 to 1991. As Manager of Secure Systems Research, I was responsible for maintaining a center of expertise in advanced security technologies for BNR, Northern Telecom, and Bell Canada, and I designed the key management architecture for Northern Telecom's PDSO security system for X.25 packet networks.
8. In 1991, I joined Sun Microsystems (Sun) as a Distinguished Engineer. Over the next ten (10) years, I was an advisor on all aspects of computer and communication security within Sun. In 2002, I was given the role of Chief Security Officer and in 2003, I was promoted to Vice President and Fellow. I remained at Sun until 2009.
9. I am currently a Consulting Professor at the Center for International Security and Cooperation at Stanford University and Visiting Professor at Royal Holloway College of the University of London.
10. Over the course of my career, I have authored and co-authored some 40 publications on various aspects of computer security and cryptography, including a November 1976 publication entitled, "New Directions in Cryptography," that introduced the Diffie-

Hellman protocol for key exchange, which is widely recognized as launching the field of public-key cryptography. For this accomplishment, the Swiss Federal Institute of Technology awarded me a Doctorate in Technical Sciences (*Honoris Causa*) in 1992.

11. I am co-inventor of three patents: U.S. Patent No. 4,200,770, entitled “Cryptographic Apparatus and Method,” issued April 29, 1980 (Hellman); U.S. Patent No. 5,371,794, entitled “Method and Apparatus for Privacy and Authentication in Wireless Networks,” issued November 2, 1993; and U.S. Patent No. 7,552,469, entitled “Method for Generating Mnemonic Random Passcodes,” issued June 23, 2009.
12. I am one of the founders of the International Association for Cryptologic Research.
13. For my contributions to the fields of cryptography and computer security, I was inducted into the National Inventors’ Hall of Fame in 2011 and into the Cyber Security Hall of Fame in 2012.
14. I am a Fellow of the Marconi Foundation and a Fellow of the Computer History Museum. In addition to the Levy prize of the Franklin Institute and other awards, I am a recipient of the National Computer Systems Security Award, which is given jointly by the National Institute of Standards and Technology and the National Security Agency.
15. My findings, as explained below, are based on my study, experience, and background in the fields discussed above, informed by my education in mathematics, computer science, and electrical engineering, and my experience in the design and analysis of security systems.
16. My declaration is organized as follows:
 - a. Understanding of claim terms (page 4)
 - b. Brief tutorial on cryptographic concepts discussed in this declaration (page 5)
 - c. Discussion of the Davies reference (page 10)
 - d. Discussion of the Meyer reference (page 22)

- e. Discussion of Davies in combination with Meyer (page 33)
- f. Discussion of Nechvatal, and its combinations with Davies and/or Meyer (page 35)
- g. Discussion of Fischer, and its combinations with Davies (page 40)
- h. Discussion of Piosenka, and its combinations with Davies and Fischer (page 47)

A. UNDERSTANDING OF CLAIM TERMS

17. I am not a lawyer. However, counsel has advised me that, during *Covered Business Method Review*, claims of an expired patent are generally given their ordinary and customary meaning as understood by a person of ordinary skill in the art in question at the effective filing date of the patent.
18. I have applied the following ordinary and customary meanings, as understood by a person of ordinary skill in the art in question at the effective filing date of the '302 Patent, of the claim terms "error detection code," "credential," and "variable authentication number (VAN)," as follows:
 - "error detection code" means "the result of applying an algorithm for coding information that, when applied to original information, creates coded information wherein changes to the coded information can be detected without complete recovery of the original information";
 - "credential" means "a document or information obtained from a trusted source that is transferred or presented to establish the identity of a party";
 - "variable authentication number (VAN)" means "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"

B. BRIEF TUTORIAL ON CRYPTOGRAPHIC CONCEPTS DISCUSSED IN THIS DECLARATION

19. As shown by the following sections, the references discussed in this declaration, and the '302 Patent, describe cryptographic operations that are used for securing messages exchanged among several parties involved in a transaction. Each party has a private-public key pair, where the private key is a secret known only to the associated party, whereas the public key is a non-secret key that may be widely available to other parties. The private and public keys in a key pair have complementary functions. A sender may code a message using its private key, and the resultant coded message may be revealed by a recipient machine by coding using the sender's public key. Thus, as long as an original coding was performed correctly based on a private key, a complementary public key may be used to reveal the original message.
20. The resultant coded message created by the sender using its private key is an example of a message signature. The message signature has two general uses. Firstly, it is used to authenticate the sender of the message to a remote recipient. Secondly, the signature is used by the recipient to verify that the message has not been modified since the signature was created by the sender.
21. In general, a signature is a coding of some input information through a cryptographic transformation using a private key. The output value of the transformation is different from the input, but is derived from the input information in such a way that any change in the input information will result in a different output value of the transformation, i.e., the signature will be different.
22. The above may be referred to as a primitive signature. In many cases, it is convenient to apply the primitive signature not to the whole message but to a fixed-size value derived from the message. As such, using a hashing technique, the message is input into a secure hash function to obtain a resulting hash value from the message, also called a message digest. The resulting hash value, which is an intermediate step in the signature generation process, may also be referred to as a presignature hash. The sender codes the presignature

hash using its private key to generate the signature. In this case, the same signature may be known as a systematic signature analogous to a systematic error detection code, which adds error-control information to a message without altering the message itself.

23. Typically, a sender sends the signature as an addendum to the non-transformed version of the input information. A recipient may verify that the input information was indeed generated by the purported sender (i.e., verify the authenticity of the message from the sender) by transforming the received signature using the sender's public key that corresponds to the sender's private key used to generate the signature. The result of transforming the signature yields a value that may be compared to the digest of the message, excluding the signature. If the two are identical, then the authenticity of the input information is successfully verified.
24. If the signature is generated by the sender using an intermediate presignature hash, then the receiver may verify the signature by resolving the presignature hash value from the message signature using the sender's public key, computing another presignature hash value on the received copy of the message excluding the signature, and comparing the two to reveal correspondence (and hence, message authentication) or differences, as described above.
25. In the following discussion, the references use different terms that refer to the same operation, and therefore, for the limited purposes of the discussion, the terms are treated alike. The following example illustrates this point: encryption and encipherment are the same cryptographic operation, while decipherment and decryption are the same cryptographic operation. Both cryptographic operations involve transformation of input information into an output value that is different from the input. These operations are examples of coding operations (e.g., encoding or decoding) and referred to interchangeably as such.
26. Other terms that are used interchangeably within the references discussed in paragraphs to follow include a certifying authority, a certificate authority and a key registry, which are interchangeably used; a secret key and private key are interchangeably used; and a

non-secret key and public key are interchangeably used. A digital certificate is sometimes referred to as a credential or simply as a certificate, while a digital signature is sometimes referred to simply as a signature.

27. When using public-key cryptography, i.e., a system in which public-private key pairs are used, it is possible to create a network resource known as a certificate authority (CA), which is able to communicate with all parties and is trusted by all parties. In this context, to be trusted by all parties implies that the CA has the officially recognized authority to establish or confirm the identity of a party in the system. The CA has its own private-public key pair, of which the public key is published and readily available to all parties in a transaction.
28. Each party may generate its own private-public key pair, or the CA may generate the private-public key pair for each party. In either case, the public key of each party is available to the CA during a registration phase, at which time other information identifying the party is also provided to the CA.
29. The CA may verify the identifying information for a party, for example, party A, during that party's registration phase. Upon successful verification, the CA generates a digital document for party A, which is commonly known as a certificate, and sometimes also referred to as a credential. The certificate includes a signature, which is generated by the CA, on the information included in the certificate, such as the public key of party A and the information identifying party A.
30. The signature in the certificate is a transformation of A's public key (and optionally, the information identifying A) using the CA's private key. In addition to the signature, the certificate information also includes A's public key and may include information identifying party A.
31. The certificate provided to A by the CA is available to other parties involved in transactions with A. Because a certificate may be verified by verifying the CA's signature, the authenticity of the certificate does not depend on whether the certificate is obtained from a public directory or from an individual party such as A itself. A party

involved in a transaction with A may thus obtain A's certificate either directly from A or from a public directory. Subsequently, A may enable authentication, i.e., verification, of a message that it sends by signing the message. In some cases, when signing the message, A may include redundant information as part of the message that is coded. A appends the signature to the message and may transmit the message either encrypted or in the clear.

32. A party receiving A's message, for example party B, may authenticate, i.e., verify, the message using A's public key. In this context, verification of a message implies verifying that the signature appended to the message is generated by the party (i.e., A) claimed to be the sender of the message. B performs the verification using A's certificate, which may be obtained either from A (for example, A may send its certificate along with the message, or in a separate message upon a request from B), or from a public directory. B is then able to obtain A's public key from A's certificate and use this public key to verify the signature of A's message. Specifically, B makes use of its knowledge of the CA's public key to verify the certificate signature as a signature by the CA on A's certificate, which contains A's public key.
33. In even greater detail, B verifies the CA's signature by coding the signature using the CA's public key, which is available to B as described above. Coding the CA's signature using the CA's public key reveals the signature contents, which may be either party A's certificate that includes its public key, or a hash of A's certificate, depending on how the signature is generated by the CA. In the case of primitive signatures, A's certificate may itself be the object of the signature, along with an explicit redundancy, which may be a field of known digits, that is added to the object being signed before the signature is generated. Recipient B codes the received signature with sender A's public key to determine whether the field of known digits is present in the result and thus verify the signature. If the signature is a systematic signature, the signature is created using a message digest of the object being signed, i.e., A's certificate. The message digest is revealed upon the recipient B coding the received signature with A's public key. B then compares this message digest with another digest that B computes using A's certificate that is received in the clear – if the two digests match, then the signature, and therefore, the certificate containing A's public key, is verified.

34. Once B has verified A's public key, it uses that public key to verify A's signature of the message received from A. To do this, B codes the received signature using A's public key. Again, if a primitive signature is used, coding of the signature reveals a copy of the message with a known field of redundant digits. If the signature is correct and A's public key that B uses to code the signature matches A's private key that was used to create the signature, the field of digits revealed from the signature should be the same as the known field of digits, thereby verifying the signature. On the other hand, if the signature is fraudulent, or the public key applied to the signature does not match A's corresponding private key, or both, then the transformation of the signature using the public key yields a result in which the known field of digits is not present.
35. In the case of systematic signature, when recipient B codes the received signature with sender A's public key, a copy of the message digest is revealed. B compares this message digest against a digest of the message that B computed to verify whether the message is authentic. If a signature is correct and the public key that is applied to the signature matches A's corresponding private key that was used to create the signature, then the transformation of the signature using the public key yields a message digest that matches the digest of the message computed by B, thereby verifying the signature. On the other hand, if the signature is fraudulent, or the public key applied to the signature does not match A's corresponding private key, or both, then the transformation of the signature using the public key yields a message digest that does not match the computed digest of the message.
36. Once B has verified A's public key as described above, B may cache a copy of the key locally or it may cache a copy of A's certificate, from which it can recover A's public key when needed using its knowledge of the CA's public key. In this way, public keys of parties, and signed messages from them, may be verified without the need to consult public directories.

C. DISCUSSION OF THE DAVIES REFERENCE

37. The Davies reference provides a discussion of digital signatures and electronic funds transfer. With respect to digital signatures, Davies describes the application of digital signatures for authenticating messages in transactions between a sender and a receiver, and the use of public-key cryptosystems, for the creation of digital signatures. (Davies at 9.2, 9.3.) As discussed in greater detail below, Davies describes that a sender may generate a digital signature using a private (i.e., secret) key, while a receiver verifies the digital signature using a public (i.e., non-secret) key. (*Id.* at 9.2, pp. 253-254; 9.3, pp. 260-262.)
38. Davies describes how public keys may be distributed using certificates. Certificates are created by entities (i.e., certificate authorities) that are trusted by senders and receivers. A sender's certificate includes the sender's public key that is used in authenticating digital signatures created using the sender's corresponding private key, along with a signature by the certifying entity that binds the certificate to the sender using the certifying entity's private key. (*Id.* at 9.6, pp. 276-277.)
39. Davies describes furnishing this sender certificate to recipients of messages from the sender, either with or separate from such messages, to allow such recipients to possess a verifiable instance of the sender's public key, and thus be able to verify messages as originating from the sender. (*Id.* at 9.6, pp. 276-277; 10.5, p. 322.)

a. Electronic Funds Transfer

40. With respect to electronic funds transfer, Davies explains payment mechanisms, including debit and credit transfers, which result in the transfer of funds from a first account associated with a first entity to a second account associated with a second entity. (*Id.* at 10.2.) Davies describes how the legitimacy of the transaction messages involved in funds transfer may be verified using digital signatures. (*Id.* at 10.5, pp. 321- 324; 10.6, pp. 328-331.) As described in greater detail below, Davies describes how the funds transfer from a first account to a second account may result in a debit to the first account and a credit to the second account. The information associated with the first and second

accounts may be stored at their respective banks (e.g., in bank computers). (*Id.* at 10.2, pp. 285-286.) In some instances, the same entity may be associated with the first and second accounts. (*Id.* at 10.4, p. 297.) Davies describes that a funds transfer may be performed by a customer at an automatic teller machine (ATM) using a personal identification number (PIN) and a card that stores the account information associated with the entity. One or more banks may be involved in the funds transfer at an ATM. (*Id.* at 10.4, pp. 297-311.) Davies also describes electronic funds transfer using point-of-sale payments where a transaction is performed between a customer and a merchant at a point-of-sale terminal associated with the merchant. The transaction is verified by a bank associated with the customer, or a bank associated with the merchant, or both, before a funds transfer payment is made from the customer's account to the merchant's account. The funds transfer transaction may be verified using digital signatures based on public key cryptography. (*Id.* at 10.5, pp. 311-327.) In Davies, a point-of-sale payment also may make use of a digitally signed message, such as an electronic check. The electronic check serves as a certificate verifying the public key of the customer. The electronic check also serves as an authenticated payment message due to the inclusion of the funds transfer information that is signed by the private key of the customer. The signatures on the electronic check are verified by the bank associated with the customer, or the bank associated with the merchant, or both, before a point-of-sale payment is made from the customer's account to the merchant's account. (*Id.* at 10.6, pp. 328-331.) Davies also describes that a customer may make a payment from his own bank account to himself (i.e., a withdrawal) using an electronic check. (*Id.* at 10.6, p. 330.)

41. In more detail, Davies describes sender generation of a digital signature of a message x by coding x using a private key associated with the sender. The coding transforms the message x to a form s , which serves as the signature for the message. A receiver can perform a coding on the signature s using a public key associated with the sender to transform it back into the form x . (*Id.* at 9.2, p. 253.)
42. The private key and the public key that are used for the coding operations maintain an inverse relationship to each other. The private key is kept secret by the sender, whereas the public key is made publicly available. The ownership of the public key is made

known through a key registry and both its value and its association with the sender can be verified using the registry's public key. (*Id.* at 9.2, p. 254.)

43. According to Davies, if the application of the sender's public key to a message signature results in a plaintext message, the signature process is successfully completed and the signature is assumed to be valid. Signatures that are verifiable using a public key allow the transmission of authenticated messages. A receiver can check the authenticity of a message by obtaining the public key of the sender and applying it to the signature associated with the message. (*Id.* at 9.2, pp. 253-254.)

b. Authentication and Encryption using Public Key Cryptography

44. Davies provides examples by which a message may be both authenticated and encrypted using public key cryptography. In one example, Davies describes a process involving two transformations – first, a “signature transformation” in which a sender A “uses his secret key k_{da} ” to sign a message, and second, an encryption transformation in which sender A “enciphers the signed message by a transformation with the public key of the receiver.” (*Id.* at 9.2, p. 256.) Therefore, the initial coding operates on a message, which is the first information, using the sender's secret key, which is the second information, to generate a signature as a result. The second coding transforms the resulting signature using the receiver's public key, which is the third information. The second coding may be reversed, i.e., decrypted, using the receiver's private key that is complementary to the receiver's public key used for the second coding.
45. Similar to the concepts outlined in ¶¶ 22-23, Davies describes how the signature of a message may be computed using a one-way function, where the signature is separate from the message itself. Per Davies, a signature of message M may be constructed by applying a “one-way function $H(M)$ ” on the message and then signing $H(M)$ using the private key of the sender. The signed $H(M)$ is sent to the receiver along with the message M . To verify that the signed $H(M)$ is a signature of the message M , the receiver encrypts the signature with the sender's public key to obtain a first $H(M)$. The receiver then applies the one-way function to the message M that it received from the sender to

produce a second $H(M)$. Then the receiver compares the first $H(M)$ to the second $H(M)$ - if the two values are equal, then the signature is valid and the message is verified. (*Id.* at 9.3, p. 260.)

46. Davies describes how “[the] function $H(M)$ reduces a message of arbitrary length to a number of a convenient and standard length for the purpose of signature” and that “[t]he essential quality of $H(M)$ is that it is a one-way function of M .” (*Id.* at 9.3, p. 264.) It would have been understood by one of ordinary skill in the art, at the effective filing date of the ‘302 patent, that the one-way function H described in Davies is an example of a hash function, and therefore Davies describes how a signature of a message M may be generated first by hashing the message to obtain the hash transformation $H(M)$, and then performing a cryptographic transformation on $H(M)$ using the sender’s private key, resulting in the signature.
47. Based on the above teaching of Davies and in view of my education and experience, it is my understanding that a person of ordinary skill in the art, at the effective filing date of the ‘302 patent, would have understood that the decipherment, encipherment and one-way function described in Davies are examples of cryptographic operations that transform original input information (which can be a message, or signature, or some other suitable input), by applying a known algorithm, into an output form that is coded and different from the form of the input. The output may be an encrypted value (which may be referred to as a ciphertext) or a decrypted value (which may be referred to as a plaintext).
48. In some cases, the transformation into the coded output information may be performed such that the coded information may not be transformed back into the original input information. For example, the result $H(M)$ of Davies’ one-way function cannot be converted back into the message M . However, in some cases, Davies’ transformation into the coded output information may be performed such that the original input information may be recovered by performing a further transformation on the coded information. For example, per Davies, a message that is encrypted by the sender using the receiver’s

public key may be decrypted by the receiver using its complementary private key to recover the message in plaintext form.

49. Encryption and decryption are complementary operations. A ciphertext, i.e., coded information, which is the result of an encryption operation can be transformed into the corresponding plaintext by a decryption operation, and vice versa, provided the same algorithm is used for the encryption and the decryption operations. The algorithm used in complementary encryption and decryption operations is known to the parties performing the encryption and decryption. In some cases, Davies' encryption or decryption by applying a suitable algorithm to transform the input information into a coded form may be performed such that the coded output information is not transformed back into the original state, i.e., the input information. For example, this may be the case when the key used for the complementary operation is not available.
50. Furthermore, the result of the one-way function $H(M)$, as described in Davies, is an example of a coding operation in which a coding algorithm is applied to original information M to create coded information $H(M)$, such that changes to the $H(M)$ can be detected without complete recovery of the original information M .
51. It is also my understanding that the digital signature or signature described in Davies is a number that results from a transformation of an input value by a cryptographic operation. In Davies, since the signature is a function of the input value and the signing key, it will be a variable number if either of these varies. The signature may be used to provide user authentication, i.e., identify the identity of a user, or may be used to provide integrity of messages, or both. (*Id.* at 9.2, pp. 253-255.) That is, according to Davies, a recipient of a signed transaction may use the transaction signature to verify the integrity of information included in the transaction. The Davies recipient also may use the signature to verify that a party to the transaction originated the transaction information. As described in Davies, the signature is a value generated by coding the transaction information with information associated with at least one party associated with the transaction (e.g., the private key of the sender). (*Id.*)

c. Verifying Public Keys using Certificates

52. Davies describes how public keys used for verifying signatures are verified by a key registry (“a key registry is the source of authentic public keys.” (*Id.* at 9.3, p. 276)). The owner of a public key obtains a certificate from the key registry that is signed by the key registry and that reveals the owner’s public key to those who possess the public key of the key registry. The certificate will be accepted by other participants in a transaction with the owner as “guaranteeing the genuineness of the public key” that is used by the owner in signing messages. (*Id.*)
53. In Davies, a new public key is registered with the key registry, with the registration process yielding a certificate that contains the identity of the owner of the public key, and an instance of the public key value that is signed by the key registry. The certificate may be used as “evidence of the public key.” (*Id.* at 9.6, p. 277.)
54. One of ordinary skill in the art, at the effective filing date of the ‘302 patent, would have understood that a certificate, as described in Davies, is a document or information obtained from a trusted source that is transferred or presented to establish the identity of a party. One of ordinary skill in the art would also recognize that the key registry described by Davies is an instance of a certificate authority, which is a universally trusted entity. The certificate includes the public key of the user to whom the certificate is assigned. A signature of the certificate that includes the public key, which is signed by a certificate authority such as the key registry, is also included in the certificate. In addition, the certificate may include other information, such as the identity of the user.
55. Davies further describes a receiver obtaining a copy of the sender’s certificate from the key registry and thus, obtaining a verified copy of the sender’s public key: “apply to the registry for a copy of the signer’s public key which is, according to custom, identified and signed by the registry.” (*Id.*)
56. Based on the above understanding of the description in Davies, one of ordinary skill in the art, at the effective filing date of the ‘302 patent, would appreciate that Davies teaches verifying a message from a sender using a digital signature. The sender computes the

digital signature of the message by coding the message using its private key. As part of computing the digital signature, the sender may apply a hash function on the message and transform the output of the hash function using its private key. The digital signature is sent along with the message.

57. Furthermore, a recipient verifies the message by performing a reverse transformation on the digital signature using the public key of the sender. (*Id.* at 9.2, p.p. 253-255; at 9.3, pp. 260-261.) The recipient may obtain the public key of the sender from a certificate associated with the sender. Since the public key obtained from the certificate is used in the verification described in Davies, one of ordinary skill in the art would appreciate that the certificate including the public key is generated in Davies prior to the verification operation. (*Id.* at 9.6, pp. 276-277.)

d. Examples of Public Key Cryptography in Electronic Funds Transfers

58. With respect to the discussion of electronic funds transfer, Davies provides examples of funds transfers that involve a payer Ann making a payment to a payee Bill. (*Id.* at 10.2, pp. 285-287.) Davies explains that money is debited from Ann's account, which is held at Ann's bank, and credited to Bill's account, which is held at Bill's bank. (*Id.*) From the description in Davies, one of ordinary skill in the art, at the effective filing date of the '302 patent, would readily appreciate that Ann's account information is stored at Ann's bank (e.g., in one or more computers at Ann's bank) and Bill's account information is stored at Bill's bank (e.g., in one or more computers at Bill's bank). Davies also describes a credit transfer mechanism where the payment information is carried in a magnetic tape. (*Id.* at 10.2, p. 286.) One of ordinary skill in the art would readily appreciate that the magnetic tape would contain information on the accounts of the payer (Ann) and the payee (Bill). Furthermore, one of ordinary skill in the art, at the effective filing date of the '302 patent, would appreciate that the debit or credit transactions described in Davies cause funds to pass from the first account of the first party (i.e., Ann) to the second account of the second party (i.e., Bill).

59. Continuing with the description of electronic funds transfer mechanisms, Davies discusses automatic teller machines (ATMs) as one mode of performing funds transfer. (*Id.* at 10.4, p. 297.) In this context, Davies describes that ATMs may be used for “transfers between the customer’s own accounts (such as deposit and checking accounts).” (*Id.*)
60. As another mode of electronic funds transfer, Davies describes point-of-sale payments, in which the customer is issued a card by a card issuer bank. A transaction request is made by the customer at the merchant’s terminal by using his card and entering his personal identification number (PIN) at the merchant’s terminal. The request “must go to the card issuer who will verify that the card is valid, the PIN correct and the account in good order.” (*Id.* at 10.5, p. 312.) It would have been understood by one of ordinary skill in the art, at the effective filing date of the ‘302 patent, that in the context described in Davies, the customer and the merchant may be the first and second parties involved in the point-of-sale payment transaction, while the card issuer is a third party that may verify the transaction between the customer and the merchant before the transaction is completed, i.e., a payment is made.
61. Tying public key cryptography to electronic funds transfer, Davies describes a system in which each of the terminal, an acquirer bank associated with the terminal, and the card issuer bank holds a private and public key pair. The key pair of each entity is registered with the key registry, which has its own private and public key pair, with the public key of the key registry known to all the entities. (*Id.* at 10.5, pp. 321-322.) Davies describes that “[w]hen 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.*) It would have been understood by one of ordinary skill in the art, at the effective filing date of the ‘302 patent, that the key registry described in this example is an example of a certificate authority.

62. Davies further describes electronic funds transfer using an electronic check, which is an “electronic equivalent of a bank cheque.” (*Id.* at 10.6, p. 328.) In the implementation example provided by Davies, the electronic check has three sections. The first section, which can be referred to as the bank section, is a certificate for the bank, which includes the public key of the bank that is issuing the electronic check, along with a signature of the bank’s public key that is signed by the key registry. Anyone can verify the bank’s public key using the signature and the public key of the key registry, which is available to all parties. (*Id.*)
63. The second section of the electronic check, which can be referred to as the customer section, serves as a certificate for the customer’s public key. It includes information on the customer’s identity, the customer’s public key, and a signature of the customer’s public key that is signed by the bank using the bank’s private key. Therefore, the customer’s public key may be verified using the bank’s public key, which may be obtained from the bank section of the electronic check. (*Id.*)
64. The third section of the electronic check, which can be referred to as the transaction section, includes the identity of the payee and the payment information, such as the payment amount, transaction type, currency, check sequence number, and date and time. The transaction section also includes a signature created by the customer’s private key, which can be verified using the customer’s public key, revealed in the customer section.
65. The signature in the transaction section may be used to authenticate the information in the transaction section, including the identity of the payee and the payment information. The customer’s signature is generated using the customer’s private key, which corresponds to the customer’s public key revealed in the customer section. (*Id.* at 10.6, pp. 328-329.)
66. From Davies’s description of the electronic check, a person of ordinary skill in the art, at the effective filing date of the ‘302 patent, would readily appreciate a mechanism for using the identification information for the customer and the payee to enable provisioning the customer, or the payee, or both, with account information through an electronic check. For these reasons, the electronic check may serve to store the information

identifying the account of the payer (i.e., the customer), or the payee, or both. Furthermore, the information included in the third section of the electronic check may serve as a record of the transaction by the customer in which the customer's account is debited, or conversely, as a record of a transaction associated with the payee in which the payee's account is credited.

67. Proceeding with the discussion of electronic checks, Davies describes how the electronic check may be used for point-of-sale at a merchant's terminal. (*Id.* at 10.6, p. 330.) In more detail, Davies describes how the merchant's terminal can verify the signatures in the electronic check. The merchant's terminal transmits the electronic check to the customer's bank, where the customer's signature on the electronic check is verified and the customer's account is examined. A payment is approved by the bank only if the customer's signature is verified. (*Id.*)
68. From the above description in Davies, a person of ordinary skill in the art, at the effective filing date of the '302 patent, would have understood that the electronic check may be used for an authenticated electronic funds transfer from a customer to a merchant. The Davies merchant, or the Davies customer's bank, or both, may authenticate the payment message included in the third section of the electronic check based on the signature by the customer using its private key. In this context, the customer and the merchant may be the first and second parties involved in the point-of-sale transaction, while the Davies bank may serve as a third party in the transaction. Alternatively, or in addition to the customer's bank, the merchant's terminal (which may, for example, be a computer system) may be a third party that verifies the transaction between the customer and the merchant before the transaction is completed, i.e., a payment is made.
69. Davies's customer's signature in the third section of the electronic check may be verified using the customer's public key, which may be obtained from the second section of the electronic check that serves as the customer's certificate. The Davies bank's signature in the second section may be used to verify the customer's public key, while the key registry's signature in the first section may be used to verify the bank's public key.

70. Davies further describes that the electronic check may be stored in “an intelligent token or ‘smart card’,” which may function as an “electronic chequebook.” (*Id.* at 10.6, p. 329.) The intelligent token may be used to store Davies’s customer’s account information and the PIN which is used at a terminal for the financial transaction. (*Id.*)
71. Discussing the use of the intelligent token, Davies states that the intelligent token may be used to “‘cash a cheque’ at an ATM with on-line verification.” (*Id.* at 10.6, p. 330.) It would have been understood by a person of ordinary skill in the art, at the effective filing date of the ‘302 patent, that this is an example of a funds transfer or payment where both the source and the recipient of the transaction are associated with the same party. In this case, the source of the funds for payment is the bank account of the customer, while the recipient of the funds is the customer himself.
72. In this context, Davies provides another example of a financial transaction in which the payment request and approval messages are verified using digital signatures. The customer’s payment request message is signed by the intelligent token and sent to the ATM, which verifies the signature. The payment request is transmitted to the customer’s bank if the signature is verified as correct by the ATM. The customer’s bank also checks the signature of the payment request message and examines the customer’s account. If the signature is verified and the account is in good order, a payment approval message signed by the customer’s bank is sent back to the ATM’s bank. The latter checks the payment approval message and verifies the customer bank’s signature. If the signature verification is successful, then an authorization goes to the ATM to release the money. (*Id.* at 10.6, pp. 330-331.)
73. It would have been understood by one of ordinary skill in the art, at the effective filing date of the ‘302 patent, from the above descriptive example that the request message is signed by Davies’s customer’s private key, which may be stored in the intelligent token. Thereafter, the request message is verified by Davies’s customer’s bank using the customer’s corresponding public key, and the payment message is signed by the customer bank’s private key, and is verified by Davies’s ATM’s bank using the customer bank’s corresponding public key.

e. IPR Decision

74. I understand that the Patent Trial and Appeal Board (“Board”) in a recent decision determined that the petitioner there failed to “show a reasonable likelihood [that it] will prevail.” *See* IPR2014-00694, Paper 10 (“IPR Decision”) 3. I also understand that in the IPR Decision, the Board summarized Davies and acknowledged that Davies provides in Chapter 10 several disclosures concerning an electronic funds transfer system that uses intelligent tokens. *See* Davies at 282. I understand that 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.
75. Davies discloses at Figure 10.23, reproduced and annotated below, a shared ATM network using digital signatures.

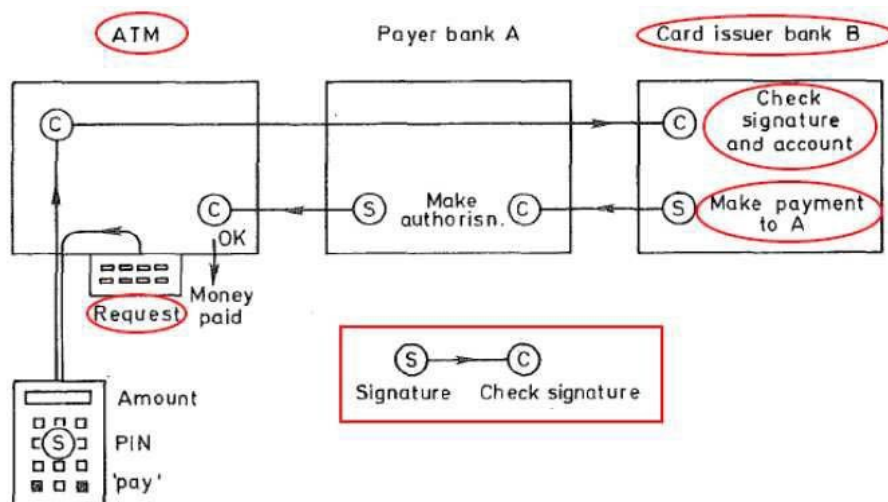


Fig. 10.23 Shared ATM network using digital signatures

76. 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.

77. 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”).
78. In my opinion, Davies discloses all of the limitations of claims 51, 53, and 55 for the reasons discussed above. A claim chart providing a limitation-by-limitation analysis for each of these claims in view of Davies is attached hereto as Exhibit A.

D. DISCUSSION OF THE MEYER REFERENCE

79. Meyer provides a discussion of public-key cryptography techniques, including applications of public-key cryptography to electronic funds transfer systems. Meyer at 386-606.
80. 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.*

81. Meyer also discloses, for purposes of authenticating a transfer of funds, the use of digital signatures 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.
82. Meyer describes these public-key cryptography techniques in the context of an electronic funds transfer transaction. Meyer discloses the transfer of funds from an account associated with a first party to an account associated with a second party. 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 *message authentication*.” *Id.*
83. According to Meyer, “[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.*

84. By way of example, Meyer illustrates an exemplary funds transfer transaction. According to Meyer “[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. It is understood, therefore, that the transfer of funds from the customer’s account to the grocer’s account is a transfer of funds from an account associated with a first party to an account associated with a second party.
85. Meyer further describes that “[t]he 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.*
86. Meyer specifies that “[u]pon 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.*
87. Additionally, according to Meyer “[i]f 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.*

88. Meyer discloses that a credential containing non-secret information is previously issued to at least one of the parties by a trusted party.
89. For example, 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.
90. Meyer describes “a digital signature procedure for 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.* As such, it is understood that the public key is a credential containing non-secret credential information.
91. Furthermore, according to Meyer, “[i]n 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.

92. “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). As such, it is understood that the KDC is considered to be a trusted party.
93. It is understood from the disclosure of Meyer that 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, the customer public key would qualify as credential information.
94. Meyer discloses 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. As shown for example in Fig. 11-44 of Meyer, reproduced below (emphasis added), a transaction request message (Mreq) (i.e., the

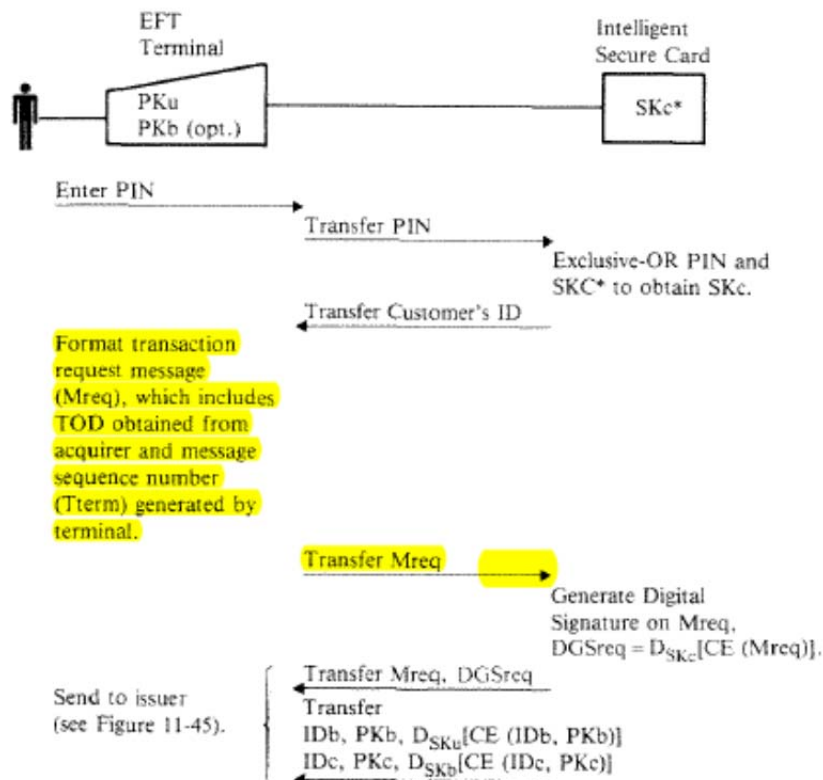


Figure 11-44. On-Line Use—EFT Terminal

“funds transfer information”) from the customer is received by Intelligent Secure Card, via EFT Terminal.

95. Meyer specifies that “the grocer enters a transfer request for \$85.00 [i.e., “a transfer amount”] 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.
96. Additionally, according to Meyer, “the information entered at the EFT terminal is assembled into a debit request message. This message or transaction request [=Mreq], 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.* As such, it is understood that the transaction request message would be considered to be funds transfer information. As specified by Meyer, the transaction request message includes at least information identifying the account of the customer, i.e., the customer's account number or “PAN”, the transfer amount entered by the grocer, and suitable routing information to route the funds transfer to the grocer's account. Thus, it is understood that the suitable routing information would necessarily include information for identifying the account of the grocer.
97. Meyer discloses generating a variable authentication number (VAN) using at least a portion of the received funds transfer information. As shown for example in Fig. 11-44, reproduced below (emphasis added), 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”).

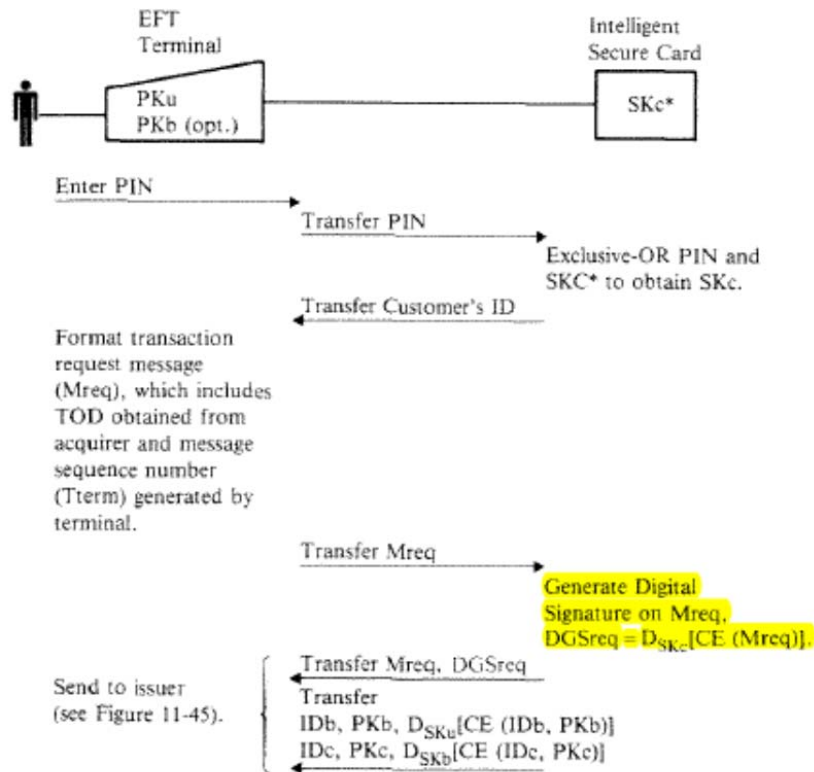


Figure 11-44. On-Line Use—EFT Terminal

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

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

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.” Meyer at 590.

99. Meyer further describes 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 ... is included in the message to ensure that it is time-variant.” *Id.* at 591-92 (emphasis added).

100. Additionally, Meyer discloses that “[t]o allow the issuer to validate the transaction request message, a DGS is generated using SKc (i.e., $D_{SKc}[CE(Mreq)]$). This is accomplished by transferring the assembled message to the card where the compressed encoding of Mreq is generated and in turn deciphered¹ 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.
101. Meyer discloses determining whether at least a portion of the received funds transfer information is authentic by using the VAN and the credential information. As shown for example in Fig. 11-45, reproduced below (emphasis added), 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”).

¹ In public-key cryptography, it is conventional to refer to transformation with the public key as encryption and transformation with the private key as decryption. In signing, the order of operations is reverse: a message is signed by transformation with the private key and verified by transformation with the public key. Nonetheless, it is common to maintain the convention of calling public-key operations encryptions and private-key operations decryptions; a signature is thus often shown as a decryption.

102. Meyer specifies that “[a]t the issuer (Figure 11-45), the corresponding PKc [= the customer’s public key] of reference is stored in the EDP system's data base, for example, in the form IDc, PKc, D_{SKb} [CE(IDc, PKc)]. Prior to its use, PKc of reference is

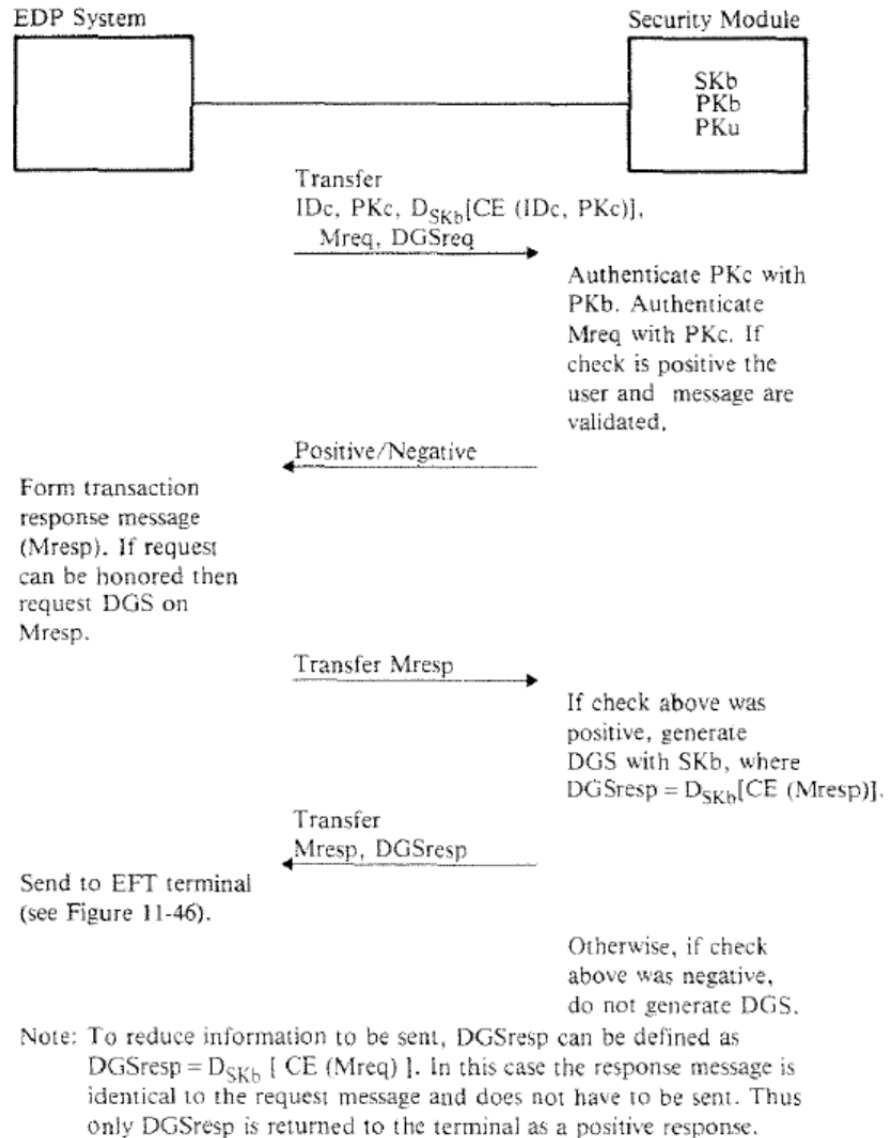


Figure 11-45. On-Line Use—Issuer's EDP System

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 $E_{PKb}(DGSreq) = E_{PKb} [D_{SKb}(CE(Mreq))]$). If they are identical, and if the TOD checks, then the issuer concludes that the 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. As such, it is

understood that the issuer determines that the transaction request message, i.e., including the at least a portion of the received funds transfer information, is authentic.

103. Meyer discloses 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.
104. For example, 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.*
105. Additionally, Meyer describes that “[i]f 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.
106. With respect to the additional limitations of claim 53, as described above, 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. As such, it is understood that the transaction described by Meyer involves a payment made by a first party, i.e., the customer, to a second party, i.e., the grocer.
107. With respect to the additional limitations of claim 55, Meyer further describes that “[a] secret user key (SK_c, 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

$$\text{DGSreq} = \text{DsKc} [\text{CE}(\text{Mreq})]$$

where $\text{CE}(\text{Mreq})$ represents the compressed encoding of Mreq . As discussed in Chapter 9, $\text{CE}(\text{M})$ 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 $\text{CE}(\text{M})$ without, at the same time, specifying the corresponding secret key. This is so because the sender and receiver use the same procedure for generating $\text{CE}(\text{M})$. To check the signature, the issuer generates the compressed encoding of the received message and compares it with $E_{\text{PKc}}(\text{DGSreq})$ (i.e., the received DGSreq encrypted under PKc). If both quantities agree Mreq is accepted; otherwise, not.” Meyer at 590. As such, it is understood that the one-way function described by Meyer constitutes an error detection code derived using the transaction request message.

108. With respect to the additional limitations of claim 56, 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., $\text{SKc}^* = \text{SKc} \text{ XOR } \text{PIN}$), which is then written on the user's intelligent secure card.” Meyer at 591. As such, it is understood that the secret card parameter would be considered a second variable authentication number or “VAN1” used to authenticate the credential, i.e., the public key.
109. 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.

110. Furthermore, Meyer describes that “[a]t 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. As such, it is understood that the issuer checks the secret card parameter SKc* is properly related to the information of the party, e.g., the claimed ID. “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.* It is understood that the negative response would be a denial of the transfer of funds.
111. In my opinion, Meyer discloses all of the limitations of claims 51, 53, 55 and 56 for the reasons discussed above. A claim chart providing a limitation-by-limitation analysis for each of these claims in view of Meyer is attached hereto as Exhibit B.

E. DISCUSSION OF DAVIES COMBINED WITH MEYER

112. Davies and Meyer each 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 328-31. Meyer similarly discloses using a message authentication code to approve or disapprove transaction requests. Meyer at 457-58 and 469. 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. 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.

113. 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.
114. The Meyer reference in combination with Davies, would render the Challenged Claims obvious to one of ordinary skill in the art.
115. 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.*
116. Meyer also discloses, for purposes of authenticating a transfer of funds, the use of digital signatures 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 above, 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.
117. 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.”

118. In my opinion, at least claims 51, 53, 55 and 56 would also have been obvious to one of ordinary skill in the art as of the effective date over the combination of Davies or Meyer with Nechvatal for the reasons discussed above. A claim chart providing a limitation-by-limitation analysis for each of these claims in view of the combination of Davies or Meyer with Nechvatal is attached hereto as Exhibit C.

F. DISCUSSION OF NECHVATAL, AND COMBINATION WITH DAVIES

119. Nechvatal provides a survey of public-key cryptography, and various public-key based cryptographic systems that existed on or before April 1991, when Nechvatal was published by the National Institute of Standards and Technology. Nechvatal discusses security requirements that may be satisfied through the application of public-key cryptosystems, and public-key cryptographic tools that achieve the security requirements. As discussed in greater detail below, Nechvatal describes how secrecy and authenticity requirements of a communication between two parties may be satisfied by public-key cryptography. (Nechvatal at §1.6.1.)
120. Nechvatal explains that one of the “major application areas for public-key cryptosystems” is digital signatures, which “provide authentication, nonrepudiation and integrity checks.” (*Id.* at §1.6.2.) Nechvatal also mentions that users in a public key cryptosystem have to possess each other’s public keys before the public-key cryptosystem may be used for signing messages: “[p]rior to using a public-key cryptosystem for establishing secret keys, signing messages etc., users A and B must exchange their public transformations (EA and EB in sec. 1.6), or equivalently their public components.” (*Id.* at §2.3.)

121. Elaborating on the management of keys in a public-key cryptosystem, Nechvatal discusses the concept of a “central issuing authority CA” and the use of certificates for the distribution of public keys. In this context, Nechvatal describes that each user in a public-key cryptosystem is in possession of the public key of the CA. In addition, each user registers its respective public key with the CA. (*Id.* at §2.3.1 and §2.4.)
122. Continuing with the discussion of certificates, Nechvatal teaches that the CA issues a certificate for each user that contains the user’s public key (“EA”); the certificate is signed by the CA using the CA’s private key (“DCA”): “A receives a certificate signed by the CA...and containing EA. That is, the CA constructs a message M containing EA, identification information for A, a validity period, etc. Then the CA computes $CERTA = DCA(M)$ which becomes A’s certificate.” (*Id.*; see also *Id.* at §1.) Nechvatal goes on to describe that the certificate is “a public document which both contains EA and authenticates it, since the certificate is signed by the CA.” (*Id.* at §2.3.1.)
123. In the context of discussing the use of certificates, Nechvatal further describes that a certificate that is issued to a user by a CA binds the user’s public key to the user’s name (i.e., the user’s identity), with the CA’s signature in the certificate authenticating the binding. (*Id.* at §5.3.1.)
124. As one application of a public-key cryptosystem, Nechvatal describes how public keys may be used for distributing a shared secret key between two users. The sender may sign the shared secret key using its private key, and then encrypt the signed shared secret key using the public key of the receiver; the encrypted and signed shared secret key is sent to the receiver. (*Id.* at §2.4.1.) In this manner, the two parties may exchange a session key, which can be considered a joint code, that may be used for securing further communications between the two parties based on symmetric key cryptography.
125. Providing a discussion of certificate management by the “central issuing authority” CA, Nechvatal describes a first party obtaining a second party’s certificate from the CA, and retrieving a copy of the second party’s public key from the obtained certificate. The first

party may cache the certificates that are obtained from the CA for future use. (*Id.* at §2.5.1.)

126. Nechvatal describes how digital signatures may be used for signing arbitrary messages in communications between users, apart from being used by the CA to sign public keys in certificates. (*Id.* at §3.) In this context, Nechvatal teaches that the digital signature is a variable value: “a digital signature cannot be a constant; it must be a function of the document that it signs.” (*Id.*)
127. While suggesting that digital signatures may be used for authenticating messages, Nechvatal mentions that hash functions may be “useful auxiliaries” “in validating the identity of a sender.” (*Id.*) Nechvatal also describes the use of hash functions as “cryptographic checksums (i.e., error-detecting codes), thereby validating the contents of a message.” (*Id.*)
128. In providing an example for using a public-key cryptosystem in authenticating arbitrary messages using digital signatures, Nechvatal describes an alternative to signing an entire message. Specifically, Nechvatal describes signing a hash transformation of the message, which provides authentication properties for the message due to the error detection code feature of hash functions. For example, Nechvatal describes a protocol in which a sender initially transforms a message by using a hash function, and then signs the hash value. The signature, which is the signed hash of the message, is sent to the receiver along with the message. The receiver may verify the digital signature by transforming the signed hash with the sender’s public key to retrieve the original hash value. This is compared with a second hash value that the receiver generates by transforming the received message by using the same hash function. (*Id.* at §3.1.1 and §3.2.)
129. Based on the teachings of Nechvatal discussed above, and in view of my education and experience, it is my understanding that the encryption and decryption transformations and the hash function described in Nechvatal are examples of cryptographic operations that transform input information (which can be a message, or signature, or some other suitable

input) into an output form that is different from the form of the input by applying a suitable algorithm.

130. I also understand that the hash function described in Nechvatal is an example of a coding operation in which a coding algorithm is applied to original information (for example, a message) to create coded information (i.e., the hash value) such that changes to the coded information can be detected without recovery of the original information.
131. It is also my understanding that the digital signature described in Nechvatal is an example of a transformation of an input value using a cryptographic operation and a signing key, and as such the signature is a variable number that will vary if either the input value or the signing key varies. Per Nechvatal, the signature may be used to provide user authentication, or message integrity, or both. That is, a recipient of signed transaction information may use the signature to verify the integrity of the signed transaction information. The recipient also may use the signature to verify that a party to the transaction originated the transaction information. As described in Nechvatal, the signature is a value generated by coding the transaction information with information associated with at least one party associated with the transaction (i.e., the private key of the sender in the transaction).
132. Furthermore, a certificate as described in Nechvatal is an example of a collection of information obtained from a trusted source that is transferred or presented to establish the identity of a party. The certificate includes the public key of the user to whom the certificate is assigned, with the certificate being signed by the certifying authority. Nechvatal teaches that a certificate containing the public key of a user is issued by a certificate authority before the public key may be used in securing communications.
133. A person of ordinary skill in the art at the effective filing date of the '302 patent would have combined Davies or Meyer with Nechvatal for at least the reasons discussed below.
134. Davies, Meyer and Nechvatal each provide examples in similar fields of endeavor. Each reference describes cryptographic systems and security for communications, including public-key cryptosystems, and the applications of digital signatures and certificates.

Davies and Meyer each describes how private and public keys may be used for generating and verifying digital signatures for authentication of electronic funds transfers. Nechvatal describes the management of keys in a public-key cryptosystem using a certificate authority, which distributes public keys using certificates. Nechvatal further describes how hash functions may be used for transforming a message as an intermediate step in generating a digital signature for the message.

135. A person of ordinary skill in the art, at the effective filing date of the '302 patent, would have combined the teachings of Davies or Meyer with Nechvatal to implement an electronic funds transfer system in which the transactions are verified by digital signatures, as taught by Davies and Meyer, alone or in combination. Davies and Meyer each discloses that hash values or one-way functions on the transaction information may be used as an intermediate step in generating signatures on messages. Nechvatal teaches that a hash function or one-way function may be used for verification of message integrity. According to Nechvatal, the result of a hash of a message serves as a cryptographic checksum (i.e., error detecting code) for the message, which Nechvatal refers to as a message authentication code. (Nechvatal, §3.2.) Any change to the input message would result in a change in the output of the hash function or one-way function. Consequently, a change in the input would be detected by detecting the change in the output value. Indeed, according to Nechvatal, a hash function or one-way function may be used for verifying message integrity, in addition to, or independent of, authenticating the message sender based on the sender signing the hash value of the message. Accordingly, Nechvatal teaches that using a hash function without a signature "may be useful in a case where secrecy and authenticity are unimportant but accuracy is paramount. For example, if a key is sent in unencrypted form, even if the key is only a few hundred bits it might be useful to transmit a checksum along with it." (*Id.*)
136. Even in the context of signatures, Nechvatal teaches that using hash functions in computing signatures may be desirable because hash functions improve the performance of cryptographic operations. Nechvatal discloses that generation of digital signatures by applying private keys to the entire message may result in effectively lower transmission bandwidth, i.e., reduced processing speed. As described in ¶¶ 22-23, hash functions allow

the sender to condense a variable-sized message M into a fixed-size representation $H(M)$ that is generally of smaller size than M , and sign $H(M)$ with a single private key operation, which would improve signing efficiency, as taught by Nechvatal. (*Id.*)

137. In my opinion, at least claim 55 would also have been obvious to one of ordinary skill in the art as of the effective date over the combination of Davies or Meyer with Nechvatal for the reasons discussed above. A claim chart providing a limitation-by-limitation analysis for each of these claims in view of the combination of Davies or Meyer with Nechvatal is attached hereto as Exhibit D.

G. DISCUSSION OF FISCHER, AND COMBINATION WITH DAVIES

138. Fischer describes a public-key cryptographic system “with enhanced digital signature certification” that “authenticates the identity of the public key holder.” (Fischer, abstract.) As described in greater detail below, the certifying entity in Fischer may generate certificates that include information on counter-signature and joint-signature requirements, apart from identifying the public key that is being certified, and the name of the corresponding user.
139. Fischer describes a procedure for creating digital signatures on objects. In this context, Fischer specifies that an object may be a “primary” object such as a purchase order or check, or money transfer; or a “secondary” object such as a certificate, or another signature. (*Id.* at 10:4-6.) The digital signature creation procedure in Fischer may be applied “not only to general objects such as arbitrary computer files, letters, electronic purchase orders, etc., but also to specialized objects such as signatures and certificates.” (*Id.* at 10:37-40.)
140. In creating the digital signature of the object, Fischer’s sender is said to apply a “hashing algorithm” to the object and other information such as the type of the object, the signing date and a comment, along with the sender’s certificate that includes the sender’s public key. The result of applying the hashing algorithm is a first “presignature hash” value, which is transformed with the sender’s private key to generate a signature. The signature,

along with the objects that are signed, is included in a “signature packet” that is transmitted with the object to the recipient. (*Id.* at 10:20-41 and Fig. 2.)

141. Fischer describes a complementary procedure for verifying a digital signature of an object. In more detail, Fischer describes the recipient of the object applying the same hashing algorithm as used by the sender to the object and other items as indicated above. The result of applying the hashing algorithm is a second “presignature hash” value. (*Id.* at 11:45-53 and Fig. 3.)
142. The recipient transforms the received signature with the sender’s public key, which may be obtained from the sender’s certificate that is sent as part of the signature packet. In doing this, the recipient reveals the contents of the sender’s signature, which is the first presignature hash value generated by the sender. The recipient compares the first and second “presignature hash” values, and accepts the received signature as valid if the two values match. (*Id.* at 11:54-65 and Fig. 3.)
143. Fischer describes how, as part of verifying the signature, the recipient ensures that the “public key belongs to the person named in the associated certificate and that the person has the authority stipulated in the certificate.” (*Id.* at 12:8-12.) “To complete the validation process, the recipient analyzes the certificates associated with the signature to determine that the proper authority has been conveyed to each certificate through its signatures and the antecedent certificate(s) of these authorizing signatures.” (*Id.* at 12:13-18.)
144. Fischer also discusses the concept of “cosignatures,” in which “[an] object may be accompanied by more than one signature,” which may be “either a joint signature or a counter signature.” (*Id.* at 12:19-21.) Distinguishing the variations of “cosignatures,” Fischer describes that “[a] joint signature is simply another signature of an object by a different party,” while “[a] counter signature is a signature of a signature.” (*Id.* at 12:21-26.)
145. Elaborating on the concept of counter signatures, Fischer provides an example of a user A signing an object, in which the “signature may itself be thought of as an object.”

Another user C may then countersign A's signature by signing A's signature, instead of the original object. (*Id.* at 12:41-13:14 and Fig. 4.)

146. In view of the above teachings in Fischer, a person of ordinary skill in the art, at the effective filing date of the '302 patent, would have understood that the concept of a joint signature or a counter signature may be considered as generating a signature using information that is associated with two or more parties. Fischer's joint signature of an object requires that two or more parties sign the object using their respective private keys. Fischer's counter signature requires that a first party sign an object using its private key to generate a first signature of the object. Subsequently, a second party signs the first signature using the second party's private key to generate a second signature, i.e., the counter signature, of the object.
147. Fischer also provides an example of certifying party B that creates a certificate for party A. Fischer describes that party B uses its own certificate, which includes its public key, in creating the certificate for A. The created certificate includes party A's public key, along with a signature of party A's public key that is generated by B. Per Fischer, in addition to the signature of A's public key, the certificate may include one or more of "A's full name, A's title and other important attributes such as his address, and telephone number. B may also include a comment to go with the certification which will be available to any person in the future who needs to examine A's certificate. B additionally will indicate an expiration date of the certificate." (*Id.* at 14:12-18 and Fig. 4.) Indeed, the certificate also may include other fields such as "cosignature requirements" "which specify how many and what type of cosignatures are required to accompany A's signature" when A subsequently uses this certificate (*Id.* at 14:38-41 and Fig. 4.); and "the current date and time which reflects the moment of...creation of the certificate." (*Id.* at 15:12-13.) The cosignature requirements are analogous to statements on some traditional bank checks, which declare that a cosignature is required for payment amounts over a certain threshold (e.g., for payments over \$10,000).

148. Fischer mentions that sender A sends, along with a signed message, “B’s signature and the hierarchy of all certificates and signatures which validate it . . . whenever A uses his certificate.” (*Id.* at 15:18-20.)
149. In view of the above teachings in Fischer, one of ordinary skill in the art, at the effective filing date of the ‘302 patent, would have understood that Fischer teaches that the signature creation procedure described in Fischer may be used for generating a signature of a sender’s public key using the certifying authority’s certificate and the certifying authority’s private key. The certifying authority may generate a signature of a sender’s public key by signing the sender’s certificate that includes the sender’s public key. Fischer teaches that the certifying authority may generate an intermediate “presignature hash” by performing a hash computation on the sender’s public key (or the sender’s certificate) being signed, and then signing the presignature hash using the certifying authority’s private key.
150. One of ordinary skill in the art also would have understood that the signature verification procedure described in Fischer is used for verifying the signature of a sender’s certificate that is generated by the certifying authority for authenticating the sender’s public key, which is included in the sender’s certificate. The recipient verifies the sender’s certificate by generating and comparing intermediate “presignature hash” values. The signature of the sender’s certificate is verified using the public key of the certifying authority that signed the sender’s certificate. As described in greater detail in ¶ 109 below, upon verifying the signature of Fischer’s sender’s certificate, the sender’s public key is authenticated.
151. Per Fischer, the public key of the certifying authority may be obtained from the certifying authority’s certificate. Fischer’s sender’s certificate also includes the certifying authority’s certificate. Further, the sender’s certificate includes additional information that is publicly available to other users, such as a comment inserted by the certifying authority while generating the sender’s certificate. In addition, following Fischer’s description that the sender’s public key obtained from the sender’s certificate is used in verifying the message from the sender, one of ordinary skill in the art would appreciate

that the sender's certificate, which includes the sender's public key, is generated in Fischer prior to the verification operation.

152. Based on the teachings of Fischer discussed above, and in view of my education and experience, it is my understanding that Fischer's encryption, decryption and hash functions each is an example of a cryptographic operation that transforms an input object (which can include a purchase order, check or money transfer, a signature or certificate, or some other suitable input) into an output form that is different from the form of the input by applying a suitable algorithm.
153. It is also my understanding that the digital signature described in Fischer is an example of a transformation of an input value using a cryptographic operation and a signing key, and, as such, the signature is a variable number that will vary if either the input value or the signing key varies. As described in Fischer, the signature may be used to provide user authentication or message integrity or both. That is, a recipient of signed transaction information may use the signature to verify the integrity of the transaction information. The recipient also may use the signature to verify that a party to the transaction originated the transaction information. Per Fischer, the signature is a value generated by coding the transaction information with information associated with at least one party involved in the transaction (i.e., the private key of the sender in the transaction).
154. I also understand that the hash function described in Fischer is an example of a coding operation in which a coding algorithm is applied to original information (for example, Fischer's object) to create coded information (i.e., the presignature hash) such that changes to the coded information can be detected without complete recovery of the original information.
155. Furthermore, a certificate as described in Fischer is understood to be an example of a collection of information obtained from a trusted source that is transferred or presented to establish the identity of a party. The certificate stores the public key of the user to whom the certificate is assigned, along with a signature of the certificate that is signed by the certifying authority's private key.

156. A person of ordinary skill in the art at the effective filing date of the '302 patent would have combined Davies with Fischer at least for the reasons discussed below.
157. Based on the teachings of Davies and Fischer as outlined above, a person of ordinary skill in the art, at the effective filing date of the '302 patent, would readily appreciate that the two references provide teachings in similar fields of endeavor. Both describe cryptographic systems and security for transactions using public-key cryptosystems, digital signatures and certificates. The two references also describe how private and public keys are used for generating and verifying signatures for transactions, where the public keys are included in certificates generated by a trusted party.
158. A person of ordinary skill in the art at the effective date of the '302 patent would have combined the teachings of Davies with the teachings of Fischer for securing messages end-to-end. In more detail, Davies teaches generation/application of a signature of a message that is sent by a sender to a recipient. Along with the message, the Davies 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 Davies recipient is able to verify the message signature. However, Davies does not explicitly disclose that the recipient may authenticate the sender's public key itself before using it to verify the message signature. Such verification is performed using Fischer's signature verification procedure. Specifically, according to Fischer's signature verification procedure, the sender's certificate includes certificates and signatures by higher authorities that may be used to verify the sender's certificate. The receiver verifies the sender's public key by authenticating the signature of the sender's certificate (which includes the sender's public key), where the signature of the sender's certificate is generated by a higher authority using its private key. The signature on the sender's certificate is verified using the higher authority's corresponding public key, which is obtained from the higher authority's certificate that is included as part of the sender's certificate.
159. One of ordinary skill in the art also would 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 has to approve any commitment/signature made at a lower level. Davies describes electronic funds transfer payments between two parties where the transaction messages are verified using digital signatures. The payment that is made from the payer to the payee may be executed using as an intermediate step, a payment from the payee's bank to the payee's account upon receiving, and successfully verifying, a signed payment approval message from the payer's bank. The payer's bank, in turn, debits the payer's account for the payment amount. The two banks settle the transaction by an interbank payment from the payer's bank to the payee's bank during the settlement process. (*Id.* at 10.4, p. 306; 10.5, p. 312; 10.6, pp. 330-331.) The interbank payment messages between the banks are signed by the banks themselves.

160. Although Davies does indicate the importance of verifying signatures by, for example, checking with the key registry particularly when the signed message is of great significance (*Id.* at 9.6, p. 278), Davies does not otherwise explicitly teach that different levels of security may be associated with transactions that involve varying levels of payment amounts. Whether the payment amounts are large or small, they are all verified using the payer's signature of the payment information. In case of a fraudulent transaction, for example due to a compromised payer's private key, the consequences of a financial loss may be greater if the transaction amount is large, compared to the case where the transaction amount is small. The certificate and cosignature taught by Fischer may be useful in limiting the consequences of fraudulent transactions. For example, the payer's certificate in Davies may specify the maximum payment amount that would be allowed based only on the payer's signature, as taught by Fischer. Furthermore, for transactions in Davies that involve amounts beyond certain thresholds, the payment messages may require authentication using cosignatures by more than one party, as taught by Fischer. For example, interbank payment messages in Davies may be verified using joint signatures or counter signatures, as taught by Fischer.

H. DISCUSSION OF PIOSENKA, AND COMBINATION WITH DAVIES AND FISCHER

161. Piosenka describes a personal identification system that generates credentials for a user. (Piosenka, abstract.) As described in greater detail below, an identification system in Piosenka receives identifying information from a user, verifies the information and, upon verification, generates a credential for the user.
162. Piosenka describes several sections in its identification system. One of these is an authorization site that receives requests for generating credentials and collects appropriate data to form credentials. Before generating a credential for a user, the authorization site obtains background information on the user, which may include public information, such as public records and references, among others. (*Id.* at 4:430-41.) The authorization site verifies the collected information and makes a decision on whether to provide credentials or reject the request from the user. (*Id.* at 4:37-45.) As described in Piosenka, the authorization site may reject the request if the user's information cannot be verified.
163. If the authorization site approves the request, Piosenka describes collecting the user's identification information, which is used in generating the credential, by a trusted computer system that forms the core of the identification system. (*Id.* at 4:45-63.) The trusted computer system formats the collected identification information into a form that is ready for encryption, which is called the composite data set (CDS). (*Id.* at 5:28-51.) The authorization site generates an encrypted version of the CDS by performing an encryption operation on the CDS using a secret encryption key and a prescribed mathematical algorithm based on public-key cryptography. (*Id.* at 5:52-68.)
164. Piosenka describes that the encrypted CDS "represents the unforgeable credentials for a particular user." (*Id.* at 6:32-33.) The encrypted CDS, along with additional plaintext, are written to a digital storage medium and given to the user as its credential.
165. The user's credential is used to verify the identity of the user at a validation site, which decrypts the credential presented by the user using a decrypt key corresponding to the secret encryption key used by the authorization site. Piosenka discloses that the

authorization site publishes the public decryption key corresponding to the secret encryption key that is used in generating the credential. (*Id.* at 6:55-68.) In some cases, the authorization site may encrypt different subsets of the CDS using different secret encryption keys, and provides the decrypt portions of different key pairs to different validation sites as needed. (*Id.* at 6:1-31.)

166. Continuing with the discussion of the validation site, Piosenka describes that the validation site “determines whether the cryptographic signature it calculates matches the cryptographic signature recorded on the memory medium.” (*Id.* at 11:17-20.) The validation site rejects the user’s request if the cryptographic signatures do not match.
167. The validation site, upon decrypting the credential by performing a decryption function using the decrypt public key known to it, recovers the original unencrypted CDS. If the cryptographic signatures match, the validation site collects relevant information from the user and compares the collected information to the information included in the unencrypted CDS. If the comparison yields a match, the user’s request is granted. Otherwise, the user’s request is denied. (*Id.* at 11:25-41.)
168. Based on the teachings of Piosenka discussed above, and in view of my education and experience, it is my understanding that the encryption and decryption functions described in Piosenka are examples of cryptographic operations that transform the input information into an output form that is different from the form of the input by applying a prescribed algorithm.
169. It is also my understanding that the encrypted CDS described in Piosenka, which is a transformation of an input value by a cryptographic encryption operation, may be used to provide user authentication, or integrity of information, or both.
170. Furthermore, the credential with the encrypted CDS and additional plaintext, as described in Piosenka, would be an example of a certificate since it is a collection of information obtained from a trusted source that is transferred or presented to establish the identity of a party. The trusted source in Piosenka is the authorization site along with the trusted computer system.

171. Based on the teachings of Davies, Fischer and Piosenka as outlined above, a person of ordinary skill in the art at the effective filing date of the '302 patent would have combined Davies and Fischer with Piosenka at least for the reasons discussed below.
172. The three references provide examples in similar fields of endeavor. All three references describe security systems, and in particular, they disclose using certificates/credentials for authenticating users.
173. 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. It was well-known to one of ordinary skill in the art, as of the effective filing date of the '302 patent, to deny the user's request if verification of the signed messages, as taught by the combination of Davies and Fischer, is unsuccessful. This is explicitly disclosed, for example, by Piosenka, who describes that a user's request for access is denied if the signature of the user's credential cannot be verified. (Piosenka at 6:41-42; 11:15-23; Fig. 3B).
174. One of ordinary skill in the art, at the effective filing date of the '302 patent, would be motivated 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. 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.
175. Furthermore, a person of ordinary skill in the art at the effective filing date of the '302 patent would combine Fischer with Piosenka for at least the reasons discussed below.
176. Piosenka describes issuance by a personal identification system of a credential to a user that is signed by a secret key owned by the personal identification system. However, Piosenka does not teach including information identifying the personal identification system within the issued credential, or providing its corresponding public key, and thus,

Piosenka limits the use of the credential only to validation systems that are apriori aware of the personal identification system's public key. Fischer, on the other hand, describes issuing certificates to the users that include information on the certifying authority, for example, the user certificate being sent along with the certificates and signatures of higher authorities that signed the user certificate. Therefore, combining Fischer with Piosenka would allow different identification systems in Piosenka to issue user credentials that include information on the respective identification systems, which are therefore readily identifiable based on the credentials themselves. Consequently, many more validation systems would be able to use the credentials. A validation system that receives a credential may ascertain the personal identification system that issued the credential from the credential information and therefore ascertain the right personal identification system public key to use for the validation.

177. In my opinion, claim 56 would have been obvious to one of ordinary skill in the art as of effective date over the combination of Davies, Fischer and Piosenka for the reasons discussed above. A claim chart providing a limitation-by-limitation analysis for each of these claims in view of the combination of Davies, Fischer and Piosenka is attached hereto as Exhibit E.
178. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Respectfully submitted,


Whitfield Diffie

Date: December 11, 2014

EXHIBIT A

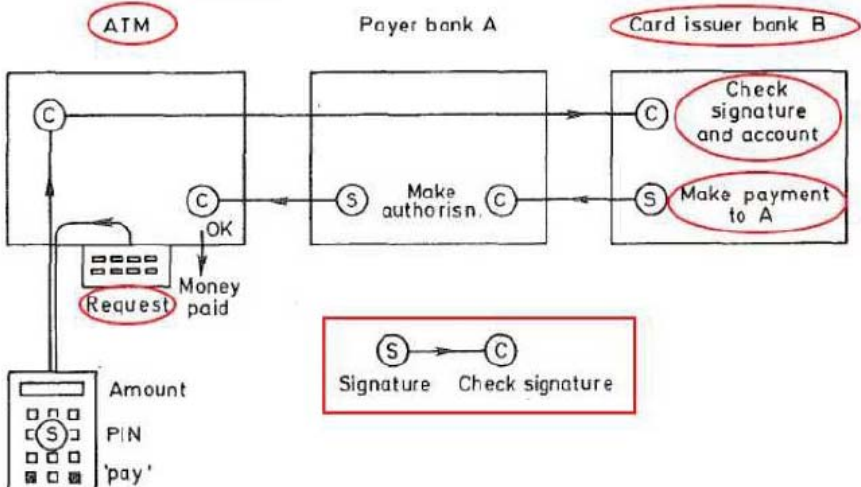
Invalidity Chart for Claims 51, 53 and 55 of U.S. Patent No. 5,793,302 Based on Davies

Claims	Davies
<p><u>Claim 51</u> [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,</p>	<p>Davies discloses the transfer of funds from an account associated with a first party to an account associated with a second party.</p> <p><u>Example I</u></p> <p>Davies describes funds transfer from Ann's ("first party") bank account to Bill's ("second party") bank account. MasterCard Exh. 1020 (Diffie Declaration) at ¶40 and ¶58). "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." MasterCard Exh. 1004 (Davies) at 10.2, p. 285; Fig. 10.1 (reproduced and annotated below). <i>See also id.</i> at 10.2, pp. 286-287 and Fig. 10.2; <i>see also</i> MasterCard Exh. 1020 (Diffie Declaration) at ¶58.</p> <div data-bbox="625 989 1369 1396" data-label="Diagram"> <p>The diagram illustrates the cheque payment mechanism between Ann's Bank and Bill's Bank. Ann's Bank is on the left, and Bill's Bank is on the right. A Clearing house is in the center. Ann is at the bottom left, and Bill is at the bottom right. The process is as follows: 1. Ann presents a cheque to her bank (Ann's A/C). 2. Ann's Bank debits Ann's account (labeled 'debit' with a minus sign). 3. Ann's Bank sends a 'Statement' to Ann. 4. Ann's Bank sends a 'debit transfer' to the Clearing house. 5. The Clearing house sends a 'debit transfer' to Bill's Bank. 6. Bill's Bank credits Bill's account (labeled 'credit' with a plus sign). 7. Bill's Bank sends a 'Cheque presented' to Bill. 8. Bill's Bank sends a 'Settlement' to Ann's Bank. 9. A note on the right says 'Use of credit delayed'.</p> </div> <p><i>Fig. 10.1 Cheque payment mechanism</i></p> <p><u>Example II</u></p> <p>Davies describes funds transfer from a customer ("first party") to a payee ("second party") using an electronic check "[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</p>

Claims	Davies																
	<p>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.” MasterCard Exh. 1004 (Davies) at 10.6, pp. 328-329; see also Fig. 10.22 (reproduced and annotated below).</p> <table border="1" data-bbox="586 457 1377 768"> <tr> <td>1 Bank identity</td><td>2 Bank public key</td></tr> <tr> <td>3 Expiry date</td><td>4 Signature of 1-3 by key registry</td></tr> <tr> <td>5 Customer identity</td><td>6 Customer public key</td></tr> <tr> <td>7 Expiry date</td><td>8 Signature of 5-7 by Bank</td></tr> <tr> <td>9 Cheque sequence number</td><td>10 Transaction type</td></tr> <tr> <td>11 Amount of payment</td><td>12 Currency</td></tr> <tr> <td>13 Payee identity</td><td>14 Description of payment</td></tr> <tr> <td>15 Date and time</td><td>16 Signature of 9-15 by customer</td></tr> </table> <p style="text-align: center;"><i>Fig. 10.22 Electronic cheque</i></p> <p>“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 MasterCard Exh. 1020 (Diffie Declaration) at ¶70 and ¶73. 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.”)</p>	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
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																
<p>[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:</p>	<p>Davies discloses that a credential containing non-secret information is previously issued to at least one of the parties by a trusted party, as shown by the following examples.</p> <p><u>Example I</u></p> <p>Davies 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”).</p> <p>Davies discloses that a credential having non-secret information stored therein is issued to at least one</p>																

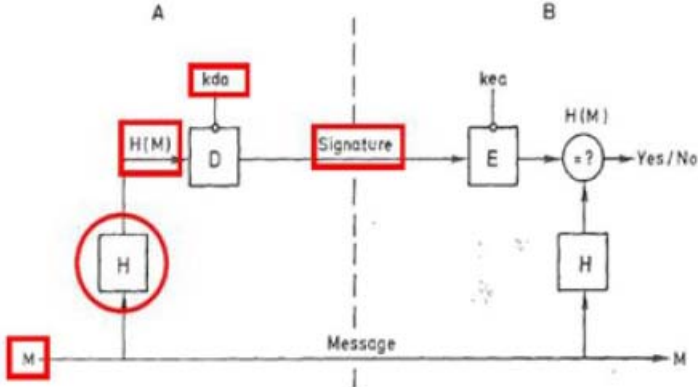
Claims	Davies
	<p>entity by a trusted entity in the context of describing that the public key of a sender (“entity”) is contained in a certificate that is issued by a key registry: “[s]ignatures can use the same public keys... A key registry is the source of authentic public keys.” MasterCard Exh. 1004 (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.” <i>Id.</i> at 9.6, pp. 276-277.</p> <p>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. Since the public keys are used in the transaction, the public keys are provided prior to the execution of the transaction: “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.” MasterCard Exh. 1004 (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.” <i>Id.</i> at 10.5, p. 322; <i>see also</i> MasterCard Exh. 1020 (Diffie Declaration) at ¶57.</p> <p><u>Example II</u></p> <p>Davies describes an electronic check used for funds transfer from a customer (“first party”) to a payee (“second party”). Davies teaches that the electronic check serves as a certificate (“credential”) for the customer that includes the customer public key signed by the bank. The check also serves as a certificate for the bank: “[the] registry authenticates the bank’s public key and the bank authenticates the customer’s public key...the cheque...</p>

Claims	Davies
	<p>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.” MasterCard Exh. 1004 (Davies) at 10.6, p. 328; <i>see also</i> Figs. 10.22 (reproduced and annotated previously at [51preA]), and 10.23 (reproduced below), and accompanying text.</p> <p>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: “[a]nyone can verify the bank’s public key using the signature ... the customer identity and his public key [are] verifiable.” MasterCard Exh. 1004 (Davies) at 10.6, p. 328-331.</p> <p>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.</p>
<p>[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;</p>	<p>Davies discloses 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, at least in the following context. 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”). MasterCard Exh. 1004 (Davies) at 10.6, pp. 328-329 and Fig. 10.22 (reproduced and annotated previously at [51preA]); and Fig. 10.23 reproduced here:</p>

Claims	Davies
	 <p data-bbox="706 703 1242 730"><i>Fig. 10.23 Shared ATM network using digital signatures</i></p> <p data-bbox="532 756 1388 955">Fig. 10.23 shows how point-of-sale payments by electronic cheque are processed, including the step of receiving, by the token, information about the transaction (the “customer’s request is formed into a message and presented to the token”).</p>
<p data-bbox="180 976 456 1344">[51b] generating a variable authentication number (VAN) using at least a portion of the received funds transfer information;</p>	<p data-bbox="532 976 1372 1134">Davies discloses generating a variable authentication number (VAN) using at least a portion of the received funds transfer information, as shown by the following examples.</p> <p data-bbox="630 1144 787 1176"><u>Example I</u></p> <p data-bbox="532 1186 1372 1648">Davies describes that a customer generates a signature on transaction information included in the electronic check with its secret key: “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.” MasterCard Exh. 1004 (Davies) at 10.6, p. 329; <i>see also</i> Figs. 10.22 and 10.23 (reproduced and annotated previously) and accompanying text (e.g., “Here it is signed and returned to the ATM”).</p> <p data-bbox="532 1659 1388 1816">Based on the explanation in the Diffie Declaration (<i>see</i>, MasterCard Exh. 1020 at ¶51, ¶87 and ¶109) and upon applying the ascribed claim interpretations, a signature would qualify as a VAN as described in the</p>

Claims	Davies
	<p>'302 Patent.</p> <p><u>Example II</u></p> <p>Fig. 10.23 Shared ATM network using digital signatures</p> <p>Davies describes a point-of-sale payment using an intelligent token in which the token generates a signature (“VAN”) on a payment request: “[t]he customer’s request is formed into a message and presented to the token. Here it is signed and returned to the ATM.” MasterCard Exh. 1004 (Davies) at 10.6, pp. 330-331; <i>see also</i> Fig. 10.23 (reproduced and annotated below).</p>
<p>[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</p>	<p>Davies discloses determining whether at least a portion of the received funds transfer information is authentic by using the VAN and the credential information, as shown below.</p> <p><u>Example I</u></p> <p>Davies 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 teaches that the payment information in the check (“the funds transfer information”) is signed by the customer using his public key. A merchant terminal and an issuer bank verify the customer’s signature (“VAN” – <i>see</i> [51b]) using the customer public key obtained from the check itself: “[t]he second section of</p>

Claims	Davies
	<p>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.” MasterCard Exh. 1004 (Davies) at 10.6, 328-329; <i>see also</i> Fig. 10.22 (reproduced and annotated previously at [51preA]). “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.” <i>Id.</i> at 10.6, p. 330.</p> <p><u>Example II</u></p> <p>Davies describes a payment transaction in which the signature (“VAN”) on a payment request (“funds transfer information”) is checked by a bank: “[t]he customer’s request is...signed...the ‘cheque’ passes...to the card issuer bank, B. Here the signature is checked.” <i>Id.</i> at 10.6, p. 330-331; <i>see also</i> Fig. 10.23 (reproduced and annotated previously at [51b]).</p> <p>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”): “[s]ender A is transmitting a message <i>M</i> and signing it, using his secret key <i>kda</i>...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 <i>kea</i>.” <i>Id.</i> at 9.3, p. 260; <i>see also</i> 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.” <i>Id.</i> at 9.6, pp. 277.</p>

Claims	Davies
	 <p>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.</p>
<p>[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.</p>	<p>Davies discloses 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, as shown by the following examples.</p> <p>Example I</p> <p>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: "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." MasterCard Exh. 1004 (Davies) at 10.6, p. 330.</p> <p>Example II</p> <p>Davies describes a payment transaction ("transferring funds") where cash is provided from a customer's bank account ("account of the first party") to</p>

Claims	Davies
	<p>the customer (“account of the second party”) after the customer’s bank checks the signature (“VAN”) on the request: “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.” <i>Id.</i> at 10.6, pp. 330-331; <i>see also</i> Fig. 10.23 (reproduced and annotated previously at [51b]).</p> <p>The above example 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.</p>
<p><u>Claim 53</u> The method of claim 51 wherein the funds transfer comprises a payment made by the first party to the second party.</p>	<p>As shown below, Davies discloses funds transfer comprising a payment made by the first party to the second party.</p> <p><u>Example I</u></p> <p>Davies describes the transfer of funds where a payment is made by Ann (“first party”) to Bill (“second party”), as construed previously in [51pre]. <i>See</i> [51pre], Example I.</p> <p><u>Example II</u></p> <p>Davies describes funds transfer from a customer (“first party”) to a payee (“second party”) using an electronic check, as construed previously in [51pre]. <i>See</i> [51pre], Example II.</p>
<p><u>Claim 55</u> The method of claim 51 wherein the VAN is generated by using an error detection code derived by</p>	<p>Davies discloses that the VAN is generated by using at least a portion of the funds transfer information, as shown by the following examples.</p> <p><u>Example I</u></p> <p>Davies describes the generation of a signature (“VAN”) based on a portion of the transaction information (“funds transfer information”). <i>See</i>, for</p>

Claims	Davies
<p>using at least a portion of the funds transfer information.</p>	<p>example, [51b].</p> <p><u>Example II</u></p> <p>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.</p> <p>Davies describes generating a separate signature by applying to a message M a one-way function H to return the value $H(M)$, which is signed using the secret key kda of the sender: “[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.” MasterCard Exh. 1004 (Davies) at 9.3, p. 260; <i>also</i> Fig. 9.5 (reproduced and annotated previously at [51c]).</p> <p>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 construed above. Also, as discussed above, Davies discloses that the entity is a person or computer program.</p>

EXHIBIT B

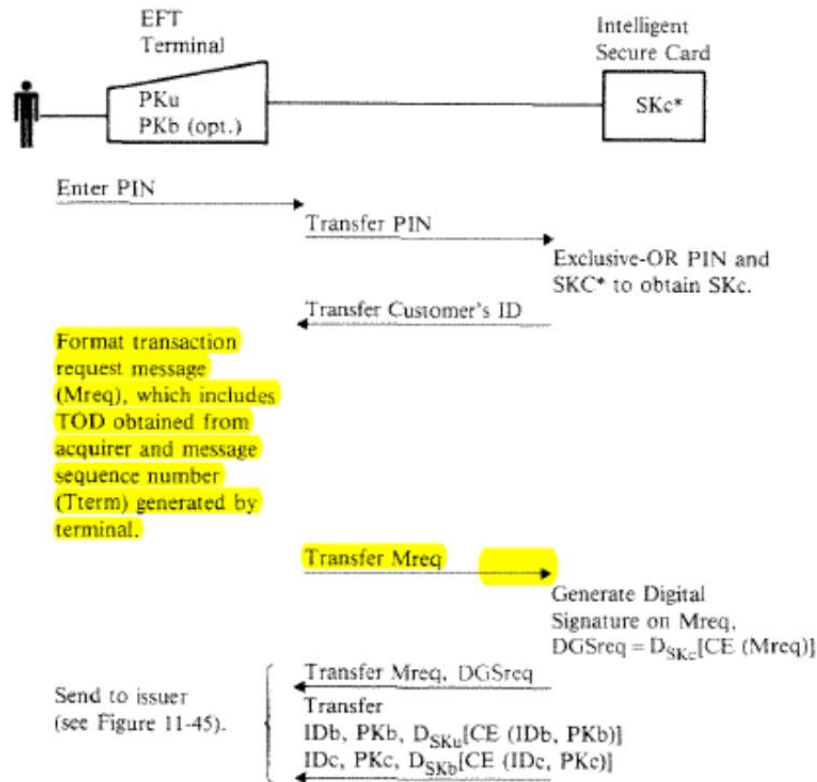
Invalidity Chart for Claims 51, 53, 55 and 56 of U.S. Patent No. 5,793,302 Based on Meyer

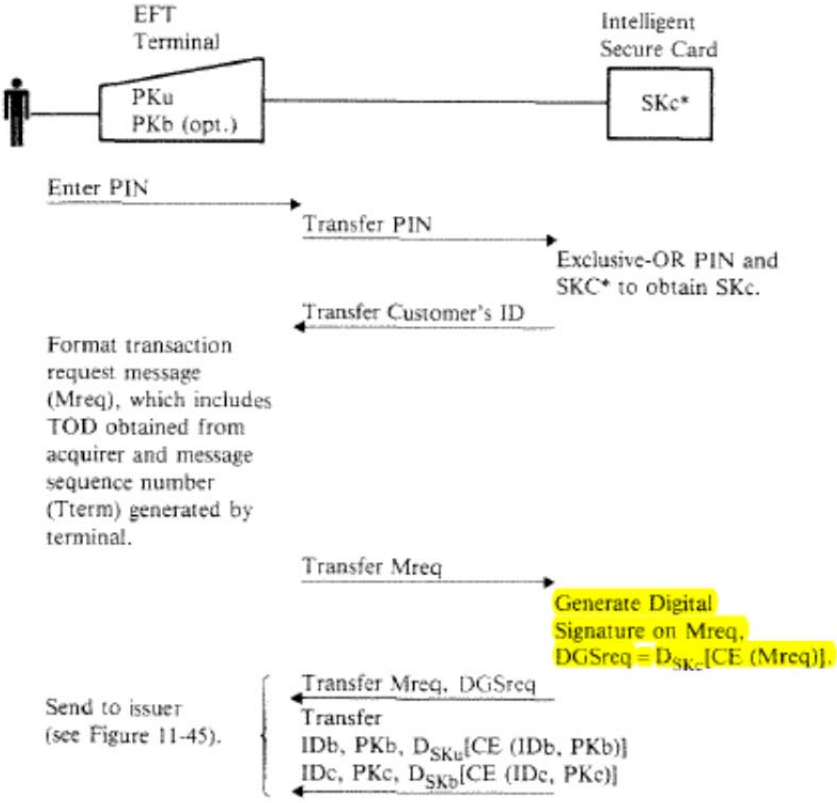
Claims	Meyer
<u>Claim 51</u> [51preA] A method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party,	<p>Meyer discloses the transfer of funds from an account associated with a first party to an account associated with a second party.</p> <p>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.</p> <p>“[T]he process of validating messages is called <i>message authentication</i>.” <i>Id.</i></p> <p>“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 <i>primary account number</i> (PAN). The institution at which the customer opens his account, and which provides the user with a bank card, is called the <i>issuer</i>. 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 <i>personal identification number</i> (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.” <i>Id.</i></p> <p>“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</p>

Claims	Meyer
	<p>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 <u>[i.e., “a first party”]</u> to the grocer's account <u>[i.e., “a second party”]</u> (\$35.00 for the groceries plus the \$50.00 to be given to the customer).” <i>Id.</i> at 477 (underlined and bolded annotation added).</p> <p>“The information entered at the EFT terminal is assembled into a <i>debit request</i> message. This message or <i>transaction request</i>, 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).” <i>Id.</i></p> <p>“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.” <i>Id.</i></p> <p>“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</p>

Claims	Meyer
	transaction. (Although other protocols are possible, the one described above will be assumed throughout the present discussion.)” <i>Id.</i>
[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:	<p>Meyer discloses that a credential containing non-secret information is previously issued to at least one of the parties by a trusted party.</p> <p>For example, 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 (<i>see</i> 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.</p> <p>“Consider a digital signature procedure for 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 <u>[i.e., “a credential”]</u> is shared with each other institution and published in a major newspaper to allow each public key to be independently validated <u>[i.e., “the credential is non-secret”]</u>.” <i>Id.</i> (underlined and bolded annotations added).</p> <p>“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 <u>[i.e., a “trusted party”]</u>. (Otherwise an opponent could masquerade as a legitimate system user.) Once this process is completed, the KDC has the added</p>

Claims	Meyer
	<p>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.” <i>Id.</i> at 578 (underlined and bolded annotation added).</p> <p>“<i>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.</i>” <i>Id.</i> at 583 (emphasis added).</p>
[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;	<p>Meyer discloses 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. As shown for example in Fig. 11-44, reproduced below (emphasis added), a transaction request message (Mreq) (i.e., the “funds transfer information”) from the customer is received by Intelligent Secure Card, via EFT Terminal.</p>

Claims	Meyer
	 <p data-bbox="609 997 1031 1024">Figure 11-44. On-Line Use—EFT Terminal</p> <p data-bbox="544 1039 1372 1281">Meyer specifies that “the grocer enters a transfer request for \$85.00 <u>[i.e., “a transfer amount”]</u> 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).” <i>Id.</i> at 477 (underlined and bolded annotation added).</p> <p data-bbox="544 1291 1372 1795">“The information entered at the EFT terminal <u>[i.e., the “funds transfer information” including the “transfer amount” entered above]</u> is assembled into a <i>debit request</i> message. This message or <i>transaction request</i> [=Mreq], which includes the customer's PIN, his account number (PAN) <u>[i.e., “information for identifying the account of the first party”]</u>, and suitable routing information <u>[i.e., “information for identifying the account of the second party”]</u>, is then sent via the acquirer (HPC X) and switch to the issuer (HPC Y).” <i>Id.</i> (underlined and bolded annotation added).</p>
[51b] generating a	Meyer discloses generating a variable

Claims	Meyer
<p>variable authentication number (VAN) using at least a portion of the received funds transfer information;</p>	<p>authentication number (VAN) using at least a portion of the received funds transfer information. As shown for example in Fig. 11-44, reproduced below (emphasis added), a Digital Signature (DGSreq) (i.e., a “variable authentication number (VAN)”) is generated by the Intelligent Secure Card <i>after</i> receiving and using the transaction request message (Mreq) (i.e., including the “received funds transfer information”).</p>  <p>Figure 11-44. On-Line Use—EFT Terminal</p> <p>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</p>

Claims	Meyer
	<p>define DGSreq as $DGSreq = D_{SKc} [CE(Mreq)]$ 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.” Meyer at 590.</p> <p>“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 <i>SKc is then used to generate a DGS on the transaction request message via the public-key algorithm.</i> 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.” <i>Id.</i> at 591-92 (emphasis added).</p> <p>“To allow the issuer to validate the transaction request message, a DGS is generated using SKc (i.e., $D_{SKc}[CE(Mreq)]$). 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).” <i>Id.</i> at 597</p>
[51c] determining whether the at least a portion of the received funds transfer information is authentic by using the VAN and	<p>Meyer discloses determining whether at least a portion of the received funds transfer information is authentic by using the VAN and the credential information. As shown for example in Fig. 11-45, reproduced below (emphasis added), the transaction request message (Mreq) (i.e., the “received funds transfer information”) is authenticated using the digital</p>

Claims	Meyer
the credential information; and	<p>signature (DGSreq) (i.e., the “VAN”) and the customer’s public key (i.e., the “credential information”).</p> <p>“At the issuer (Figure 11-45), the corresponding PKc [= the customer’s public key] 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 $E_{PKb}(DGSreq) = E_{PKb}[D_{SKb}(CE(Mreq))]$). If they are identical, and if the TOD checks, then the issuer concludes that the content of the message is correct [<u>i.e., “the at least a portion of the received funds transfer information is authentic”</u>], the message is not stale, and the secret information supplied by the user, SKc* and PIN, is properly related to the claimed ID.” <i>Id.</i> at 597 (underlined and bolded annotation added).</p>
[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.	<p>Meyer discloses 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.</p> <p>For example, 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.” <i>Id.</i></p> <p>“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</p>

Claims	Meyer
	transaction.” <i>Id.</i> at 477.
<p><u>Claim 53</u> The method of claim 51 wherein the funds transfer comprises a payment made by the first party to the second party.</p>	<p>Meyer discloses securing the transfer of funds, as construed previously with respect to claim 51. <i>See</i> claim 51.</p> <p>Additionally, Meyer specifies that “the grocer enters a transfer request for \$85.00 to be transferred from the customer's account <u>[i.e., “a first party”]</u> to the grocer's account <u>[i.e., “a second party”]</u> (\$35.00 for the groceries plus the \$50.00 to be given to the customer).” <i>Id.</i> at 477 (underlined and bolded annotation added).</p>
<p><u>Claim 55</u> 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.</p>	<p>Meyer discloses securing the transfer of funds, as construed previously with respect to claim 51. <i>See</i> claim 51.</p> <p>Additionally, Meyer specifies that “[a] secret user key (SK_c, 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</p> $\text{DGSreq} = \text{D}_{\text{SK}_c} [\text{CE}(\text{Mreq})]$ <p>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 E_{PK_c} (DGSreq) (i.e., the received DGSreq encrypted under PK_c). If both</p>

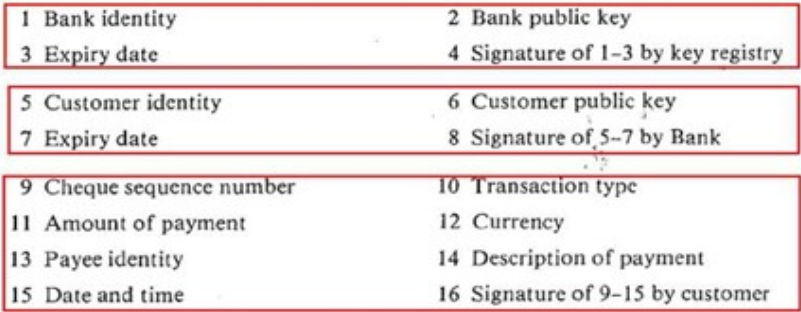
Claims	Meyer
	quantities agree Mreq is accepted; otherwise, not.” Meyer at 590.
<p><u>Claim 56</u> [56a] The method of claim 51 for further securing the transfer of funds, at least one party being previously issued a credential by a trusted party, the credential information including information associated 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,</p>	<p>Meyer discloses securing the transfer of funds, as construed previously with respect to claim 51. <i>See</i> claim 51.</p> <p>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., $SKc^* = SKc \text{ XOR } PIN$) <u>[i.e., “a second variable authentication number (VAN1)”]</u>”, which is then written on the user's intelligent secure card.” Meyer at 591 (underlined and bolded annotation added).</p>
<p>[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.</p>	<p>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</p>

Claims	Meyer
	<p>described earlier) is included in the message to ensure that it is time-variant.” <i>Id.</i> at 591-92.</p> <p>“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 <u>[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]</u>.” Meyer at 597 (underlined and bolded annotation added). “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 <u>[i.e., the transfer of funds is denied]</u>.” <i>Id.</i> (underlined and bolded annotation added).</p>

EXHIBIT C

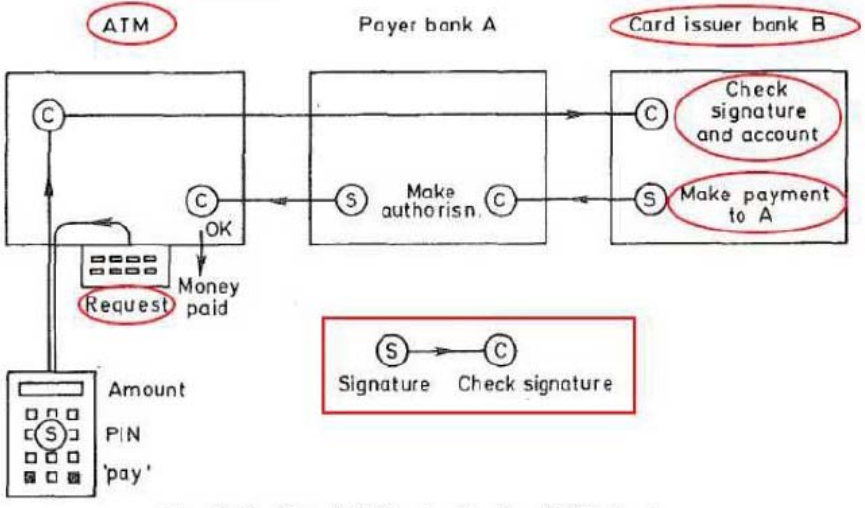
Invalidity Chart for Claims 51, 53, 55 and 56 of U.S. Patent No. 5,793,302 Based on Davies in View of Meyer

Claims	Davies in view of Meyer
<p><u>Claim 51</u> [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,</p>	<p>Davies discloses the transfer of funds from an account associated with a first party to an account associated with a second party.</p> <p><u>Example I</u></p> <p>Davies describes funds transfer from Ann's ("first party") bank account to Bill's ("second party") bank account. MasterCard Exh. 1020 (Diffie Declaration) at ¶40 and ¶58). "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." MasterCard Exh. 1004 (Davies) at 10.2, p. 285; Fig. 10.1 (reproduced and annotated below). <i>See also id.</i> at 10.2, pp. 286-287 and Fig. 10.2; <i>see also</i> MasterCard Exh. 1020 (Diffie Declaration) at ¶58.</p> <div data-bbox="581 1024 1330 1434" data-label="Diagram"> <p>The diagram illustrates the cheque payment mechanism. At the top, a curved arrow labeled 'Settlement' connects Ann's Bank and Bill's Bank. In the center is a box labeled 'Clearing house'. On the left, 'Ann's Bank' contains a box for 'Ann's A/C' with a minus sign and a 'debit' label. A 'Statement' arrow points from Ann's Bank to a circle labeled 'Ann'. On the right, 'Bill's Bank' contains a box for 'Bill's A/C' with a plus sign and a 'credit' label. A 'Cheque presented' arrow points from a circle labeled 'Bill' to Bill's Bank. A 'debit transfer' arrow points from Bill's Bank to the Clearing house, and another 'debit transfer' arrow points from the Clearing house to Ann's Bank. A 'Cheque payment' arrow points from Ann to Bill. A note on the right says 'Use of credit delayed'.</p> </div> <p style="text-align: center;"><i>Fig. 10.1 Cheque payment mechanism</i></p> <p><u>Example II</u></p> <p>Davies describes funds transfer from a customer ("first party") to a payee ("second party") using an electronic check "[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</p>

Claims	Davies in view of Meyer
	<p>the payment to be made... The final signature, by the customer, covers all the variable information in the cheque.” MasterCard Exh. 1004 (Davies) at 10.6, pp. 328-329; see also Fig. 10.22 (reproduced and annotated below).</p>  <p style="text-align: center;">Fig. 10.22 Electronic cheque</p> <p>“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 MasterCard Exh. 1020 (Diffie Declaration) at ¶70 and ¶73. 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.”)</p>
<p>[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:</p>	<p>Davies discloses that a credential containing non-secret information is previously issued to at least one of the parties by a trusted party, as shown by the following examples.</p> <p><u>Example I</u></p> <p>Davies 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”).</p> <p>Davies discloses that a credential having non-secret information stored therein is issued to at least one entity by a trusted entity in the context of describing that</p>

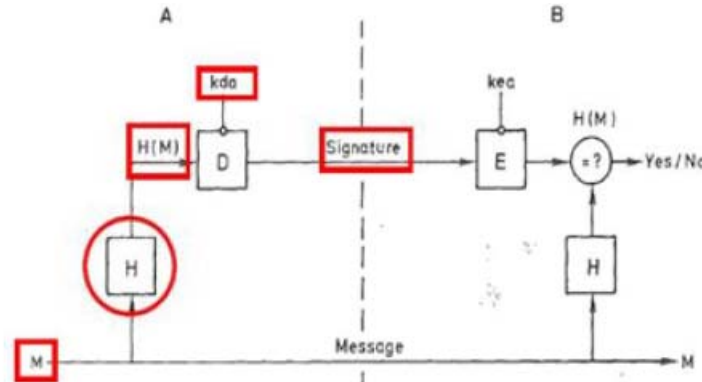
Claims	Davies in view of Meyer
	<p>the public key of a sender (“entity”) is contained in a certificate that is issued by a key registry: “[s]ignatures can use the same public keys... A key registry is the source of authentic public keys.” MasterCard Exh. 1004 (Davies) at 9.6, p. 276. “[A] person P wishes 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.” <i>Id.</i> at 9.6, pp. 276-277.</p> <p>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. Since the public keys are used in the transaction, the public keys are provided prior to the execution of the transaction: “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.” MasterCard Exh. 1004 (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.” <i>Id.</i> at 10.5, p. 322; <i>see also</i> MasterCard Exh. 1020 (Diffie Declaration) at ¶57.</p> <p><u>Example II</u></p> <p>Davies describes an electronic check used for funds transfer from a customer (“first party”) to a payee (“second party”). Davies teaches that the electronic check serves as a certificate (“credential”) for the customer that includes the customer public key signed by the bank. The check also serves as a certificate for the bank: “[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</p>

Claims	Davies in view of Meyer
	<p>registry which authenticates the bank’s public key...the cheque contains the customer identity and his public key signed by the bank.” MasterCard Exh. 1004 (Davies) at 10.6, p. 328; <i>see also</i> Figs. 10.22 (reproduced and annotated previously at [51preA]), and 10.23 (reproduced below), and accompanying text.</p> <p>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: “[a]nyone can verify the bank’s public key using the signature ... the customer identity and his public key [are] verifiable.” MasterCard Exh. 1004 (Davies) at 10.6, p. 328-331.</p> <p>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.</p>
[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;	<p>Davies discloses 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, at least in the following context. 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”). MasterCard Exh. 1004 (Davies) at 10.6, pp. 328-329 and Fig. 10.22 (reproduced and annotated previously at [51preA]); and Fig. 10.23 reproduced here:</p>

Claims	Davies in view of Meyer
	 <p data-bbox="706 703 1242 730">Fig. 10.23 Shared ATM network using digital signatures</p> <p data-bbox="527 756 1356 961">Fig. 10.23 shows how point-of-sale payments by electronic cheque are processed, including the step of receiving, by the token, information about the transaction (the “customer’s request is formed into a message and presented to the token”).</p>
<p data-bbox="203 976 479 1354">[51b] generating a variable authentication number (VAN) using at least a portion of the received funds transfer information;</p>	<p data-bbox="527 976 1372 1134">Davies discloses generating a variable authentication number (VAN) using at least a portion of the received funds transfer information, as shown by the following examples.</p> <p data-bbox="625 1144 787 1186">Example I</p> <p data-bbox="527 1186 1372 1648">Davies describes that a customer generates a signature on transaction information included in the electronic check with its secret key: “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.” MasterCard Exh. 1004 (Davies) at 10.6, p. 329; <i>see also</i> Figs. 10.22 and 10.23 (reproduced and annotated previously) and accompanying text (e.g., “Here it is signed and returned to the ATM”).</p> <p data-bbox="527 1659 1372 1816">Based on the explanation in the Diffie Declaration (<i>see</i>, MasterCard Exh. 1020 at ¶51, ¶87 and ¶109) and upon applying the ascribed claim interpretations, a signature would qualify as a VAN as</p>

Claims	Davies in view of Meyer
	<p>described in the '302 Patent.</p> <p><u>Example II</u></p> <p>The diagram illustrates a transaction flow between three entities: an ATM, Payer bank A, and Card issuer bank B. The ATM initiates a 'Request' (marked with a circled 'C') to Payer bank A. Payer bank A sends a 'Make authorisn.' message (marked with a circled 'S') to Card issuer bank B. Card issuer bank B responds with a 'Check signature and account' message (marked with a circled 'C') back to Payer bank A, which then sends an 'OK' message (marked with a circled 'C') to the ATM. The ATM also displays 'Amount', 'PIN', and 'pay' on its screen. A separate box shows a 'Signature' (S) being converted to a 'Check signature' (C). The ATM also displays 'Money paid' and 'Request'.</p> <p><i>Fig. 10.23 Shared ATM network using digital signatures</i></p> <p>Davies describes a point-of-sale payment using an intelligent token in which the token generates a signature (“VAN”) on a payment request: “[t]he customer’s request is formed into a message and presented to the token. Here it is signed and returned to the ATM.” MasterCard Exh. 1004 (Davies) at 10.6, pp. 330-331; <i>see also</i> Fig. 10.23 (reproduced and annotated below).</p> <p>Although, as discussed above, Davies teaches that the “receiving” step of [51a] is performed before the “generating” step of [51b], 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.” <i>Id.</i> at 457; <i>see also id.</i> 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</p>

Claims	Davies in view of Meyer
	<p>to modify the message between the time the MAC is generated and the time it is checked, he would be detected.”). <i>Id.</i></p> <p>As such, 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).” <i>Id.</i> at 457-58; <i>see also</i> 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.”</p>
<p>[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</p>	<p>Davies discloses determining whether at least a portion of the received funds transfer information is authentic by using the VAN and the credential information, as shown below.</p> <p><u>Example I</u></p> <p>Davies 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 teaches that the payment information in the check (“the funds transfer information”) is signed by the customer using his public key. A merchant terminal and an issuer bank verify the customer’s signature (“VAN” – <i>see</i> [51b]) using the customer public key obtained from the check itself: “[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.” MasterCard Exh. 1004 (Davies) at 10.6, 328-329; <i>see also</i> Fig. 10.22</p>

Claims	Davies in view of Meyer
	<p>(reproduced and annotated previously at [51preA]). “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.” <i>Id.</i> at 10.6, p. 330.</p> <p><u>Example II</u></p> <p>Davies describes a payment transaction in which the signature (“VAN”) on a payment request (“funds transfer information”) is checked by a bank: “[t]he customer’s request is...signed...the ‘cheque’ passes...to the card issuer bank, B. Here the signature is checked.” <i>Id.</i> at 10.6, p. 330-331; <i>see also</i> Fig. 10.23 (reproduced and annotated previously at [51b]).</p> <p>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”): “[s]ender A is transmitting a message <i>M</i> and signing it, using his secret key <i>kda</i>...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 <i>kea</i>.” <i>Id.</i> at 9.3, p. 260; <i>see also</i> 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.” <i>Id.</i> at 9.6, pp. 277.</p>  <p>As shown above, Davies describes that a message is verified by verifying the signature on the message</p>

Claims	Davies in view of Meyer
	<p>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.</p>
<p>[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.</p>	<p>Davies discloses 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, as shown by the following examples.</p> <p><u>Example I</u></p> <p>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: "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." MasterCard Exh. 1004 (Davies) at 10.6, p. 330.</p> <p><u>Example II</u></p> <p>Davies 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: "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." <i>Id.</i> at 10.6, pp. 330-331; <i>see also</i> Fig. 10.23 (reproduced and annotated previously at [51b]).</p> <p>The above example is also consistent with the Patentee's own interpretation of the '302 patent: "the</p>

Claims	Davies in view of Meyer
	<p>[‘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.</p>
<p><u>Claim 53</u> The method of claim 51 wherein the funds transfer comprises a payment made by the first party to the second party.</p>	<p>As shown below, Davies discloses funds transfer comprising a payment made by the first party to the second party.</p> <p><u>Example I</u></p> <p>Davies describes the transfer of funds where a payment is made by Ann (“first party”) to Bill (“second party”), as construed previously in [51pre]. <i>See</i> [51pre], Example I.</p> <p><u>Example II</u></p> <p>Davies describes funds transfer from a customer (“first party”) to a payee (“second party”) using an electronic check, as construed previously in [51pre]. <i>See</i> [51pre], Example II.</p>
<p><u>Claim 55</u> 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.</p>	<p>Davies discloses that the VAN is generated by using at least a portion of the funds transfer information, as shown by the following examples.</p> <p><u>Example I</u></p> <p>Davies describes the generation of a signature (“VAN”) based on a portion of the transaction information (“funds transfer information”). <i>See</i>, for example, [51b].</p> <p><u>Example II</u></p> <p>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.</p> <p>Davies describes generating a separate signature by applying to a message M a one-way function H to return the value $H(M)$, which is signed using the secret key k_{da} of the sender: “[s]ender A is transmitting a message M and signing it, using his secret key k_{da}...A one-way function $H(M)$ is formed using...the message</p>

Claims	Davies in view of Meyer
	<p>and then...transformed by the public key signature method, to form the signature.” MasterCard Exh. 1004 (Davies) at 9.3, p. 260; <i>also</i> Fig. 9.5 (reproduced and annotated previously at [51c]).</p> <p>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 <i>kda</i> is associated with the sender, as construed above. Also, as discussed above, Davies discloses that the entity is a person or computer program.</p>
<p><u>Claim 56</u> [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,</p>	<p>Davies discloses that at least one party is previously issued a credential by a trusted party, wherein the credential information includes information associated with at least one party. <i>See</i> [51preB].</p> <p>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) <u>[i.e., “a second variable authentication number (VAN1)”]</u>, which is then written on the user's intelligent secure card.” Meyer at 591 (underlined and bolded annotation added).</p>
<p>[56b] authentication and the transfer of</p>	<p>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</p>

Claims	Davies in view of Meyer
<p>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.</p>	<p>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.” <i>Id.</i> at 591-92.</p> <p>“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 <u>[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]</u>.” Meyer at 597 (underlined and bolded annotation added). “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 <u>[i.e., the transfer of funds is denied]</u>.” <i>Id.</i> (underlined and bolded annotation added).</p>

EXHIBIT D

Invalidity Chart for Claim 55 of U.S. Patent No. 5,793,302 Based on Davies or Meyer in View of Nechvatal

Claims	Davies or Meyer in view of Nechvatal
<u>Claim 55</u> The method of claim 51	Davies and Meyer each discloses the method of claim 51, as discussed above. <i>See</i> Exhibits A-C, <i>supra</i>
wherein the VAN is generated by using an error detection code derived by using at least a portion of the funds transfer information.	<p>Davies and Meyer each discloses that the VAN is generated by using an error detection code derived by using at least a portion of the funds transfer information, as shown by the following examples.</p> <p style="text-align: center;"><u>Example I</u></p> <p>Davies describes the generation of a signature (“VAN”) based on a portion of the transaction information (“funds transfer information”). <i>See</i>, for example, [51b].</p> <p style="text-align: center;"><u>Example II</u></p> <p>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.</p> <p>Davies describes generating a separate signature by applying to a message M a one-way function H to return the value $H(M)$, which is signed using the secret key kda of the sender: “[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.” MasterCard Exh. 1004 (Davies) at 9.3, p. 260; <i>also</i> Fig. 9.5 (reproduced and annotated previously at [51c]).</p> <p>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 construed above. Also, as discussed above, Davies discloses that the entity is a person or computer program.</p> <p>Similarly, Meyer specifies that a digital signature [e.g., the VAN] is formed from a compressed encoding of the transaction request message [i.e., including the funds transfer information]. Meyer at 590. That is, Meyer</p>

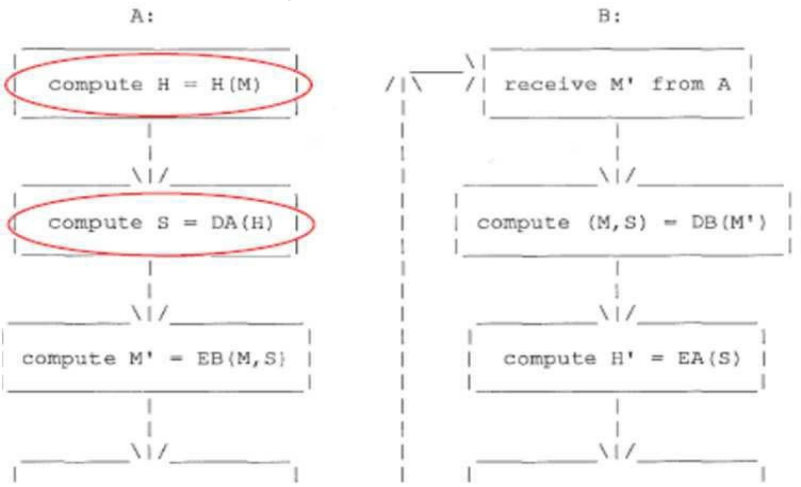
Claims	Davies or Meyer in view of Nechvatal
	<p>specifies that the digital signature is formed from a one-way function encoding of the transaction request message. <i>Id.</i></p> <p>While Davies and Meyer each suggests that the signature, i.e., VAN, is based on a one-way function, Nechvatal explicitly 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: “[i]f a hash function H is used, A computes [signature] $s = DA(H(M))$ and sends both M [message] and s to B.” MasterCard Exh. 1005 (Nechvatal), 3.1.1; <i>see also</i> Figure 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.” <i>Id.</i> at 3.</p>  <pre> sequenceDiagram participant A participant B Note over A: compute H = H(M) Note over A: compute S = DA(H) Note over A: compute M' = EB(M, S) Note over B: receive M' from A Note over B: compute (M, S) = DB(M') Note over B: compute H' = EA(S) </pre> <p style="text-align: center;">Nechvatal, Fig. 5</p>

EXHIBIT E

Invalidity Chart for Claim 56 of U.S. Patent No. 5,793,302 Based on Davies in View of Fischer and Piosenka

Claim	Davies in view of Fischer and Piosenka
Claim 56 [56pre] The method of claim 51 for further securing the transfer of funds,	Davies discloses securing the transfer of funds, as construed previously with respect to claim 51. <i>See</i> Exhibit A, <i>supra</i> .
[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,	<p>Davies discloses that at least one party is previously issued a credential by a trusted party, wherein the credential information includes information associated with at least one party. <i>See</i> [51preB].</p> <p>Davies discloses that the credential information includes a second variable authentication number (VAN1) that is used to secure at least a portion of the credential information to the at least one party, as shown by the examples below.</p> <p style="text-align: center;"><u>Example I</u></p> <p>Davies describes that an electronic check (“credential”) includes a signature (“VAN1” – <i>see</i> [51b]) by the bank that binds the customer (“one party”) identity to the customer public key (“secure...the credential information to the...one party”). The bank’s signature may be verified using the bank’s public key, which is signed by the trusted key registry (“trusted party” – <i>see</i> [51preB]) and thus the bank itself may be a trusted party. Davies, 10.6, p. 328; <i>see also</i> [51preB].</p> <p>Based on the ascribed claim interpretations and my Declaration at ¶40 and ¶62-69, an electronic check would qualify as a credential per the ‘302 Patent. <i>See</i> Declaration at ¶¶ 40, 62-69.</p> <p style="text-align: center;"><u>Example II</u></p> <p>Alternatively, Davies 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</p>

Claim	Davies in view of Fischer and Piosenka
	check (“secure at least a portion of the credential information to the at least one party”). Davies at 10.6, p. 328; <i>see also</i> [51preB].
[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.	<p>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.</p> <p>As discussed in [51preB], 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. <i>Id.</i> at 10.6, pp. 328-330 and Fig. 10.22 (reproduced and annotated previously at [51preA]); <i>also</i> [51preB].</p> <p>Since Davies states that the payment is approved if the signature is verified, as discussed above, 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.</p> <p>While Davies suggests checking the bank’s signature to verify the customer’s public key, Fischer discloses that certificate information is verified based on the signature in the certificate: “[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, 17:34-47.</p>

Claim	Davies in view of Fischer and Piosenka
	<p>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: “user’s credentials...written on to...card having memory.” Piosenka, 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.” <i>Id.</i>, 11:15-23; <i>see also</i> Fig. 3B (reproduced and annotated below).</p>

