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

| | | |
|---|---|---|
| In re Patent of: | Leon Stambler | |
| U.S. Patent No.: | 5,963,541 | Attorney Docket No.: 37305-0003IP1 |
| Issue Date: | Aug. 10, 1999 | |
| Appl. Serial No.: | 08/872,116 | |
| Filing Date: | June 10, 1997 | |

Title: METHOD FOR SECURING INFORMATION RELEVANT TO A TRANSACTION

## DECLARATION OF PROFESSOR WHITFIELD DIFFIE

1. My name is Whitfield Diffie of Woodside, California. I understand that I am submitting a declaration in connection with the above-referenced *Inter Partes* review proceeding pending in the United States Patent and Trademark Office for U.S. Patent No. 5,963,541 ("the '541 Patent").

2. I have been retained on behalf of the Banks of the United States Federal Reserve System.[1] My compensation is not based on the outcome of my opinions.

3. I am not a lawyer. However, counsel has advised me that, during *inter partes* 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.

4. I have reviewed the '541 patent, including the claims of the patent in view of the specification. In addition, I have reviewed the following documents: U.S. Patent No. 4,200,770 to Hellman, Diffie, and Merkle ("Hellman"), of which I am co-inventor, as well as the X.509 standard ("X.509"), the NIST Special Publication 800-2, entitled Public-Key Cryptography and authored by James Nechvatal ("Nechvatal"), and relevant portions of the textbook Security for Computer Networks: An Introduction to

[1] Federal Reserve Bank of Atlanta, Federal Reserve Bank of Boston, Federal Reserve Bank of Chicago, Federal Reserve Bank of Cleveland, Federal Reserve Bank of Dallas, Federal Reserve Bank of Kansas City, Federal Reserve Bank of Minneapolis, Federal Reserve Bank of New York, Federal Reserve Bank of Philadelphia, Federal Reserve Bank of Richmond, Federal Reserve Bank of San Francisco, and Federal Reserve Bank of St. Louis.

Data Security in Teleprocessing and Electronic Funds Transfer, authored by D.W. Davies and W.L. Price ("Davies").

5. 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.

6. In 1965, I joined 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.

7. 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.

8. 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.

9. In 1991, I joined Sun Microsystems 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.

10. 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.

11. 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.

12. 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.

13. I am one of the founders of the International Association for Cryptologic Research.

14. 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.

15. 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.

16. 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.

17. This declaration is organized as follows:

    A. Brief tutorial on cryptographic concepts discussed in this declaration (page 4)
    B. Discussion of the Hellman reference (page 8)
    C. Discussion of the X.509 reference (page 9)
    D. Discussion of the Nechvatal reference (page 11)
    E. Discussion of the Davies reference (page 12)

**A. Brief tutorial on cryptographic concepts discussed in this declaration**

18. As shown by the following sections, the references discussed in this declaration, and the '541 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 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.

19. The resultant coded message created by the sender using its private key is an example of a digital signature on a message, also known as 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 it the signature was created by the sender.

20. In general, a signature is a coding of some input information through a cryptographic transformation, such as an encryption or decryption operation, using a private key. The output value of the transformation is different from the input, but shares a one-to-one relationship with the input information. Any change in the input information will result in a different output value of the transformation, i.e., the signature will be different.

21. In some cases, the signature may not be generated directly on the input information. Instead, the sender transforms the input information into a fixed-size value using a hash function. The resulting hash value, which is an intermediate step in the signature generation process, may be referred to as a presignature hash. The sender codes the presignature hash using its private key to generate the signature.

22. 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 non-transformed version of the input information that is received. If the two are identical, then the authenticity of the input information is successfully verified.

23. 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 a received copy of the message, and comparing the two to reveal correspondence (and hence, message authentication) or differences, as described above.

24. 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 an 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 are referred to interchangeably as such.

25. Other terms that are alike include a certifying authority, a certificate authority and a key registry, which are interchangeably used; a secret key, secret encryption key and private key are interchangeably used; and a non-secret key, public decryption key and public key are interchangeably used. A digital certificate is sometimes referred to as a credential or as simply certificate, while a digital signature is sometimes referred to simply as a signature.

26. In a public-key cryptosystem, i.e., a system in which public-private key pairs are used, a network resource known as the certificate authority (CA) or key registry depending on the context is able to communicate with all parties and is trusted by all parties. 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.

27. 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 provided to the CA during a registration phase, at which time other information identifying the party is also provided to the CA.

28. 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 public key of party A and the information identifying party A.

29. The signature in a 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 may include the non-encoded version of A's public key and the information identifying A.

30. The certificate provided 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.

31. 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 CA's public key to verify the certificate signature as a signature by the CA on A's public key.

32. 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. If the signature is a primitive signature, 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.

33. 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, then a field of digits revealed from the signature should be same as the known field of digits, thereby verifying the signature. On the other hand, if the signature is fraudulent, or if 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.

34. In the case of a 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.

35. 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.

**B. Discussion of the Hellman reference**

36. I am co-inventor of the Hellman reference, U.S. Patent No. 4,200,770, which is entitled "Cryptographic Apparatus and Method," and which issued April 29, 1980.

37. Hellman teaches a method for securing information that is involved in a transaction between at least two parties by using information associated with the parties. *See* Hellman at Abstract. Specifically, Hellman describes a cryptographic system and method that can be used to secure a plaintext message P, which is to be communicated in a transaction between a first party and a second party, through coding of P using a cipher key K, where the cipher key K is generated based on information associated with the two parties. *Id.* at 3:47-64; 4:1-5:3.

38. In more detail, private components $X_1$ and $X_2$ are associated, respectively, with the first party and with the second party. The first party generates a public component $Y_1$ through a transformation of $X_1$, and the second party generates a public component $Y_2$ through a transformation of $X_2$. *Id.* at 4:13-17. The public components $Y_1$ and $Y_2$ are exchanged between the parties, and each of the first and second parties independently generate an identical cipher key K. *Id.* at 4:44-51. The first party generates K by transforming $Y_2$ using $X_1$, and the second party generates K by transforming $Y_1$ using $X_2$. The first party may encode plaintext P using K in order to generate encoded ciphertext C, which may be transmitted through an insecure channel to the second party. *Id.* at 3:41-64. The second party may decode ciphertext C using K in order to retrieve decoded plaintext P. *Id.* One of ordinary skill in the art, at the effective filing date of the '541 patent, would have understood that the transformation of plaintext P using cipher key K results in coded information, ciphertext C, and that the transformation of ciphertext C using cipher key K results in coded information, plaintext P.

39. In further detail, Hellman discloses that the first party accesses private component $X_1$ and signals q and a from a key source and generates, using a secure key generator and through a coding of private component $X_1$ with the signals q and a, a public component $Y_1$. *Id.* at 4:23-27, 4:44-51. The public component $Y_1$, in addition to the signals q and a, is communicated by the first party to the second party, and the second party generates, using a secure key generator and through coding of a private component $X_2$ with the signals q and a, a public component $Y_2$. *Id*. The second party communicates the public component $Y_2$ to the first party. *Id.* at 4:44-51. As described above, both parties independently generate, using their respective secure key generators, the cipher key K. *Id.* at 4:52-5:3.

**C. Discussion of the X.509 reference**

40. The X.509 standard describes an authentication framework that enables a first party to a transaction to authenticate a second party to the transaction through use of a digital certificate containing a collection of information that has been signed by a certification authority (CA) using the CA's secret key, the digital certificate having been furnished to at least one of the parties prior to the transaction. *See* X.509 at § 6; *see also* Nechvatal at § 5.3.

41. At § 3.3, X.509 defines "certificate" as "the public keys of a user, together with some other information, rendered unforgeable by encipherment with the secret key of the certification authority which issued it," and defines "certification authority" as "an authority trusted by one or more users to create and assign certificates." In more detail, a digital certificate enables a first party to a transaction to confirm, based on verification of a CA's digital signature that is included within the digital certificate, that a public key contained in the digital certificate is valid and is associated with a party named in the digital certificate. *See* X.509 at §§ 6.5-7.2. Having confirmed the validity of the public key contained in the digital certificate, the first party to the transaction can then authenticate that a second party to the transaction is the party named in the digital certificate by determining that the second party to the transaction is in possession of the secret key corresponding to the public key that is included in the digital certificate. *See id.* at §§ 6.4, 6.5, 7.1, 7.2. In addition, upon confirming the validity of the public key contained in the digital certificate, the first party to the transaction can then verify that the signatures on messages received from the second party using the public key. Accordingly, the first party can verify that the

signatures are generated by the second party, which is in possession of the secret key corresponding to the public key with which the signatures are verified. *See id.* at §§ 9.1, 9.2, 9.3.

42. The "digital signature" described by X.509 is created by a CA by coding certificate information. *See*, *e.g.*, *id.* at §§ 7.2; A.3. This digital signature is included within the digital certificate issued by the CA and may be used to verify the identity of a party. Specifically, similar to the process of creating a signature described above at ¶ 21, and adopting the abbreviations for terms provided by X.509, the CA X produces a digital certificate for a party by (1) hashing, using a secure hash function h, a collection of information (info) that includes a distinguished name of the party and a public key of the party, (2) signing, using a secret key $X_s$ of the CA, the hashed collection of information h(info), and (3) appending the signed hash $X_s[h(info)]$ to the collection of information. *See id*. at §§ 7-8; *see also* Nechvatal at § 5.3.

43. According to X.509, a first party to a transaction obtains a digital certificate that has been issued by a CA X, the digital certificate including a digital signature of the CA ($X_s[h(info)]$), and a collection of information (info) that includes a public key of a second party to the transaction. *See id.* at §§ 7.2, 8.2. The first party to the transaction may verify X's digital signature by applying a hash function h to info and then comparing the hashed collection of information h(info) with a hash obtained by decoding the digital signature using X's public key, Xp. *Id.* at § 8.2.

44. Because the CA is a trusted authority, verification of the CA's digital signature confirms to the first party that the public key included in the digital certificate is valid and is associated with the party named in the digital certificate. *See id.* at §§ 6.5-7.2. Having confirmed, based on the CA's digital signature, the validity of the public key contained in the digital certificate, the first party to the transaction can authenticate that the second party to the transaction is the party named in the digital certificate by determining that the second party to the transaction is in possession of the secret key corresponding to the public key that is included in the digital certificate. *See id.* at §§ 6.4, 6.5, 7.1, 7.2. The first party to the transaction may, for example, verify the identity of the second party to the transaction by decoding, using the public key included in the digital certificate, information that has been encoded by the second party to the transaction with the second party's private key. *See id.* at § 6.4; *see also* Nechvatal at §5.3.4.

45. In addition to providing a basis for verifying the identity of a party to a transaction, digital signatures, as described by X.509, may be used to verify the integrity of information associated with the transaction. X.509 indicates at § A.3, for example, that a message may be sent by a first party to a transaction to a second party to the transaction, the message including both plaintext information, and a hash of the information that has been signed (encoded) using a secret key of the first party. Similar to the process of verifying a signature described above at ¶ 23, the second party may then (1) decode the hashed information using the public key of the first party, (2) hash the plaintext information using the same hash function employed by the first party, and (3) compare the decoded hash with the hashed information. If the decoded hash and the hashed information match, the second party will have verified that the content or structure of the information included in the message has not changed since the first party sent the message.

**D. Discussion of the Nechvatal reference**

46. Nechvatal provides a survey of the state of the art of public-key cryptography circa 1988-1990. The topics covered in Nechvatal include the theory of public key cryptography, a survey of then existing public-key systems, including systems implementing the Diffie/Hellman algorithm, and an exploration of digital signatures and hash functions.

47. I believe that one of ordinary skill in the art, at the effective filing date of the '541 patent, would have understood that the teachings of Hellman, X.509, and Nechvatal could be naturally integrated, and would have been motivated to combine Hellman with each of X.509 and Nechvatal, at least because Nechvatal describes in detail both the authentication framework disclosed by X.509 and the Diffie/Hellman algorithm, the algorithm disclosed by the Hellman patent, and suggests their combination. Specifically, Nechvatal notes, with reference to the algorithm disclosed in Hellman, that the public-key cryptosystem of Hellman protects the secrecy of information involved in transactions, but does not authenticate parties to transactions, and that it would therefore be desirable to augment a system implementing the Diffie/Hellman algorithm with one which provides authentication. Nechvatal describes X.509 as one such "strong authentication" framework.

**E. Discussion of the Davies reference**

48. 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.

49. Davies describes that 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.

50. 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 confidently 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.

51. With respect to electronic funds transfer, Davies describes 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.

52. 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. *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 an 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 leverage 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.

53. 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 back into the form x. *Id.* at 9.2, p. 253.

54. 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.

55. 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.

56. 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 kda" 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 signature transformation generates a signature, and the encryption transformation codes this to generate an encrypted signed message.

57. 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. For example, 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.

58. 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 '541 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 the decryption transformation on *H(M)* using the sender's private key, resulting in the signature.

59. Based on the above teaching of Davies and in view of my education and experience, I believe that one of ordinary skill in the art, at the effective filing date of the '541 patent, would have understood that the decipherment, encipherment, and hash function described in Davies 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. The output may be an encrypted value (typically referred to as a ciphertext) or a decrypted

value (typically referred to as a plaintext). Encryption and decryption are complementary operations. A ciphertext that 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.

60. 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, and it may be used to provide user authentication, or integrity of messages, or both. *Id.* at 9.2, pp. 253-255. Since the signature is a function of the input value and the signing key, the signature will vary if either of these varies.

61. 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 private key" that is used by the owner in signing messages. *Id.*

62. 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.

63. One of ordinary skill in the art, at the effective filing date of the '541 patent, would have understood that a certificate, as described in Davies, is a collection of 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 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.

64. 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: as Davies puts it, the receiver may "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.*

65. Based on the above understanding of description in Davies, one of ordinary skill in the art, at the effective filing date of the '541 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 transforming 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 hash function using its private key. The digital signature is sent along with the message.

66. 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.

67. With respect to the discussion of electronic funds transfer, 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.*

68. 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 '541 patent, that in the context described in Davies, the PIN entered by the customer serves to verify the identity of the customer initiating the transaction. The card issuer is a third party that may verify a transaction between the customer and the merchant before the transaction is completed, i.e., a payment is made.

69. 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 '541 patent, that the key registry described in this example is an example of a certificate authority.

70. Davies further discloses that, whenever an authentic public key is required for purposes of executing a transaction, it can be provided, in a digitally signed certificate, to the party interacting with the owner of the public key. *Id.* at 322.

71. Davies further discloses a multiple-phase registration process involving the creation of a digital signature of the key registry in two different phases. *Id.* at 276. In more detail, Davies describes a "temporary certificate" that is signed by the key registry and that is issued by the key registry to the registrant during a "temporary" registration phase that is prior to any transaction taking place, in addition to a second "effective certificate" that is issued by the same key registry after the registration phase, and that bears the key registry's signature. *Id.* It would have been understood by one of ordinary skill in the art, at the effective filing date of the '541 patent, that the multiple-phase registration process described in Davies involves resigning, prior to a transaction, of a digital signature that is included in a certificate issued to a public key owner.

72. By supplementing the descriptions provided in each of Hellman, X.509, and Nechvatal, the teachings of Davies would lead a person having ordinary skill in the art at the time that Mr. Stambler filed the application to which '541 claims priority to recognize that the teachings of Hellman, X.509, Nechvatal, and Davies could be naturally integrated, and to combine Hellman, X.509, and Nechvatal with Davies.

73. In more detail, one of ordinary skill in the art, at the effective filing date of the '541 patent, would have recognized that Hellman, X.509, Nechvatal, and Davies are in similar fields of endeavor. Each reference describes cryptographic systems and security for communications, including public-key

cryptosystems, and X.509, Nechvatal, and Davies each describe applications of digital signatures and certificates. Davies, for example, describes the use of private and public keys to generate and verify digital signatures that are included in certificates, for purposes of authenticating electronic funds transfers. Similarly, Nechvatal and X.509 each describe the management of keys in a public-key cryptosystem by a certification authority, which uses certificates to distribute authenticated public keys. As such, a person having ordinary skill in the art would be motivated to augment the cryptosystem described in Hellman with the various key management techniques taught by each of X.509, Nechvatal, and Davies.

74. 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,

Date: 10 June 2013

/Whitfield Diffie/
Whitfield Diffie