

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Leon Stambler

U.S. Patent No.: 5,936,541

Attorney Docket No.: 37305-0003IP1

Issue Date: August 10, 1999

Appl. Serial No.: 08/872,116

Filing Date: June 10, 1997

Title: METHOD FOR SECURING INFORMATION RELEVANT TO A TRANS-
ACTION

Mail Stop Patent Board

Patent Trial and Appeal Board

U.S. Patent and Trademark Office

P.O. Box 1450

Alexandria, VA 22313-1450

PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES PATENT NO. 5,936,541
PURSUANT TO 35 U.S.C. §§ 311-319, 37 C.F.R. § 42

TABLE OF CONTENTS

| | | |
|------|---|----|
| I. | MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1) | 4 |
| A. | Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)..... | 4 |
| B. | Related Matters Under 37 C.F.R. § 42.8(b)(2) | 5 |
| C. | Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3) | 5 |
| D. | Service Information | 5 |
| II. | PAYMENT OF FEES – 37 C.F.R. § 42.103 | 5 |
| III. | REQUIREMENTS FOR IPR UNDER 37 C.F.R. §§ 42.104 | 6 |
| A. | Grounds for Standing Under 37 C.F.R. § 42.104(a) | 6 |
| B. | Challenge Under 37 C.F.R. § 42.104(b) and Relief Requested | 6 |
| C. | Claim Construction under 37 C.F.R. §§ 42.104(b)(3) | 7 |
| IV. | SUMMARY OF THE ‘541 PATENT | 13 |
| A. | Brief Description..... | 13 |
| B. | Summary of the Prosecution History of the ‘302 Patent | 13 |
| V. | THERE IS A REASONABLE LIKELIHOOD THAT AT LEAST ONE IPR CLAIM OF THE ‘541 PATENT IS UNPATENTABLE | 14 |
| VI. | MANNER OF APPLYING CITED PRIOR ART TO EVERY CLAIM FOR WHICH <i>INTER PARTES</i> REVIEW IS REQUESTED | 17 |
| A. | [GROUND 1] – Hellman, X.509, and Nechvatal render obvious Claims 20, 24, 27, 28, 32, 35, 38, and 46..... | 17 |
| B. | [GROUND 2] – Hellman, X.509, Nechvatal, and Davies render obvious Claims 20, 24, 27, 28, 32, 35, 38, and 46..... | 40 |
| VII. | CONCLUSION | 54 |

EXHIBITS

| | |
|-------------|--|
| FEDRES-1001 | U.S. Patent No. 5,936,541 to Leon Stambler (“541 Patent”) |
| FEDRES-1002 | Prosecution History of the ‘541 Patent |
| FEDRES-1003 | Response dated July 21, 1998 in U.S. Patent Application No. 08/872,116 (“541 Application”) |
| FEDRES-1004 | Declaration of Prof. Whitfield Diffie (“Diffie Declaration”) |
| FEDRES-1005 | U.S. Patent No. 4,200,770 to Hellman et al. (“Hellman”) |
| FEDRES-1006 | CCIT Recommendation X.509: The Directory – Authentication Framework (1988) (“X.509”) |
| FEDRES-1007 | James Nechvatal, Public-key Cryptography (NIST Special Publication 800-2) (April 1991) (“Nechvatal”) |
| FEDRES-1008 | D. W. Davies et al., Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer, 254-332 (1989) (“Davies”) |
| FEDRES-1009 | Memorandum Order from <i>Leon Stambler v. RSA Security et al.</i> , Civil Action No. 01-65 SLR (D. Del.) (“RSA Order”) |
| FEDRES-1010 | Plaintiff’s Opening Brief on Issues of Claim Construction from <i>Leon Stambler v. RSA Security et al.</i> , Civil Action No. 01-65 SLR (D. Del.) (“RSA Brief”) |
| FEDRES-1011 | Memorandum Opinion and Order from <i>Leon Stambler v. JPMorgan Chase & Co., et al.</i> , Civil Action No. 2-08-cv-204-DF-CE (E.D. Tex.) (“JP Morgan Order”) |
| FEDRES-1012 | Memorandum Opinion and Order from <i>Leon Stambler v. Merrill Lynch & Co., Inc., et al.</i> , Civil Action No. 2:08-cv-462-DF-CE (E.D. Tex.) (“Merrill Order”) |
| FEDRES-1013 | Plaintiff’s Opening Claim Construction Brief from <i>Leon Stambler v. Merrill Lynch & Co., Inc., et al.</i> , Civil Action No. 2:08-cv-462 (E.D. Tex.) (“Merrill Brief”) |

| | |
|-------------|--|
| FEDRES-1014 | Claim Construction Order from <i>Leon Stambler v. Amazon.com, Inc., et al.</i> , Civil Action No. 2:09-cv-310 DF (E.D. Tex.) (“Amazon Order”) |
| FEDRES-1015 | Plaintiff’s Opening Claim Construction Brief from <i>Leon Stambler v. Amazon.com, Inc., et al.</i> , Civil Action No. 2:09-cv-310 (E.D. Tex.) (“Amazon Brief”) |
| FEDRES-1016 | Previous Constructions of Claim Terms of the ‘541 Patent |

The Federal Reserve Banks¹ (“Petitioners” or “Federal Reserve”) seek *Inter Partes* Review (“IPR”) under 35 U.S.C. §§ 311–319 and 37 C.F.R. § 42 of claims 20, 24, 27, 28, 32, 35, 38, and 46 (“the IPR Claims”) of U.S. Patent No. 5,936,541 (“’541 Patent”) of Leon Stambler (“Patentee”). As explained in this petition, there exists a reasonable likelihood that the Federal Reserve will prevail with respect to at least one claim challenged in this petition.

The ‘541 Patent claims methods for securing information relevant to a transaction — for example, to authenticate a financial transaction such as a transfer of funds — by including in a “credential” some modicum of “credential information” associated with a party, and by “coding” the credential information, thereby generating a “variable authentication number (VAN)” that is included in the credential and that is used to authenticate the party and/or the communications. The ‘541 Patent was improvidently granted without providing a reason for allowance and without full consideration to the wide body of applicable prior art.

The relevant patent claims are unpatentable based on teachings set forth in at least the four references presented in this petition. Petitioners respectfully submit that *Inter Partes* Review should be instituted, and that the challenged claims should be canceled as unpatentable.

I. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1)
A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)

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.

Petitioners, the Federal Reserve Banks, are the real parties-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

Petitioners are not aware of any disclaimers or reexamination certificates for the '541 Patent. Petitioners have been named as defendants in a recently-filed litigation concerning the '541 patent, Leon Stambler v. Federal Reserve Bank of Atlanta et al., Civil Action No. 2:12-cv-611-JRG (E.D. Tex.). The Petitioners have also petitioned—on this same day—for *Inter Partes* Review of the other patent at issue in that litigation, U.S. Patent No. 5,793,302 (“302 Patent”), which is a continuation of the same parent application as the '541 Patent and thus includes similar subject matter and shares a common specification.

C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Petitioners provide the following designation of counsel:

| LEAD COUNSEL | BACKUP COUNSEL |
|---|---|
| W. Karl Renner, Reg. No. 41,265 3200 RBC Plaza 60 South Sixth Street Minneapolis, MN 55402 T: 202-783-5070 F: 202-783-2331 | Thomas A. Rozylowicz, Reg. No. 50,620 3200 RBC Plaza 60 South Sixth Street Minneapolis, MN 55402 T: 202-783-5070 F: 202-783-2331 |

D. Service Information

Please address all correspondence and service to counsel at the address provided in Section I(C), or at the telephone/facsimile numbers provided below their signatures on the final pages of this Petition. Petitioner also consents to electronic service by email at 37305-0003IP1@fr.com.

II. PAYMENT OF FEES – 37 C.F.R. § 42.103

The Petitioners authorize the Patent and Trademark Office to charge Deposit Account No. 06-1050 for the fee set in 37 C.F.R. § 42.15(a) for this Petition, and further authorize payment for any additional fees to be charged to this Deposit Account.

III. REQUIREMENTS FOR IPR UNDER 37 C.F.R. §§ 42.104

A. Grounds for Standing Under 37 C.F.R. § 42.104(a)

Petitioners certify that the '541 Patent is eligible for IPR and that Petitioners are not barred or estopped from requesting IPR. The present petition is being filed within one year of service of the original complaint against Petitioners² in the district court litigation.

B. Challenge Under 37 C.F.R. § 42.104(b) and Relief Requested

Petitioners request *Inter Partes* review of the IPR Claims of the '541 patent on the grounds set forth in the table below, and request that each of the claims be found unpatentable. An explanation of how the IPR Claims are unpatentable under the statutory grounds identified below is provided in the form of detailed description and claim charts that follow, setting forth the identification of where each element can be found in the cited prior art, and the relevance of that prior art. Additional explanation and support for each ground of rejection is set forth in FEDRES-1004, the Declaration of Prof. Whitfield Diffie ("Diffie Declaration"), referenced throughout this Petition.

| Ground | '541 Patent Claims | Basis for Rejection of the IPR Claims |
|---------------|---------------------------------|--|
| Ground 1 | 20, 24, 27, 28, 32, 35, 38, and | Obvious under § 103(a) over Hellman in view of X.509 and Nechvatal |

² Each of the Federal Reserve Banks was individually served no earlier than October 1, 2012 and no later than October 17, 2012.

| Ground | '541 Patent Claims | Basis for Rejection of the IPR Claims |
|----------|------------------------------------|---|
| | 46 | |
| Ground 2 | 20, 24, 27, 28, 32, 35, 38, and 46 | Obvious under § 103(a) over Hellman in view of X.509, Nechvatal, and Davies |

The '541 Patent issued from a string of patent applications dating back to an original application filed on November 17, 1992. Accordingly, claims 20, 24, 27, 28, 32, 35, 38, and 46 of the '541 Patent may have, at best, an effective filing date of November 17, 1992.³ Hellman qualifies as prior art under 35 U.S.C § 102(b) because it issued on April 29, 1980, and thus, was issued more than one year prior to the filing date of the '541 patent. X.509, Nechvatal, and Davies qualify as prior art under 35 U.S.C § 102(b) because they were published in 1988, 1989 and April 1991, respectively, and thus, each was published more than one year prior to the effective filing date of the '541 Patent.

C. Claim Construction under 37 C.F.R. §§ 42.104(b)(3)

The subject patent is expired, such that its claims and claim terms are properly given their “ordinary and custom meaning.” Phillips v. AWH Corp., 415 F.3d 1303, 1316, 75 USPQ2d 1321, 1329 (Fed. Cir. 2005) (words of a claim in 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). In determining the ordinary and

³ The Petitioners are not expressing any opinion at this point as to whether the claims of the '541 Patent are supported by the parent application. In view of the relevant dates of the currently cited references, the prior art status of the references do not change if claims 20, 24, 27, 28, 32, 25, 38, and 46 are not accorded the filing date of the parent application.

custom meaning, the words of a claim are first given their plain meaning. Id. According to Phillips, the structure of the claims may breathe additional meaning into the claims, and the specification and file wrapper also may be used to lesser extent to better construe a claim insofar as the plain meaning of the claims cannot be understood. Moreover, Phillips offers that even treatises and dictionaries may be used, albeit under limited circumstances, to determine the meaning attributed by a person of ordinary skill in the art to a claim term at the time of filing.

Other than claim terms addressed immediately below, for which information concerning constructions appropriate for this Petition is set forth, the remaining terms in the claims are not believed to require additional clarification for purposes of the present IPR.⁴ For the sake of convenience, a chart of Previous Constructions of Claim Terms of the '541 Patent has been submitted with this petition as FEDERES-1016. In more detail, the chart includes constructions that have, during litigations involving the '541 patent, been advanced by Patentee and/or resolved through Markman proceedings. Except where otherwise noted, the constructions set forth below are consistent with the narrowest of the constructions included in the chart.

i. Coding

⁴ In as much as 37 C.F.R. § 42.104(b)(2) defines a narrow scope of inquiry in this proceeding, Petitioners do not acknowledge claim compliance with 35 U.S.C. § 112, through its assessment of a broadest reasonable interpretation for terms that follow, or otherwise.

For purposes of this Petition, the term “coding” is construed as “transforming information by applying a known algorithm.” Although this construction is not the narrowest of the constructions of “coding” included in FEDRES-1016, it mimics the majority of the constructions resolved through Markman proceedings conducted in co-pending litigation involving the ‘541 patent, and it is harmonious with constructions offered by Patentee during those proceedings. See, e.g., RSA Brief (FEDRES-1010) at 15-18 (“[i]n the field of computer security, the term “coding” is commonly understood to refer to transforming information by cryptographic processes”).

In more detail, in Stambler v. Amazon.com, Inc., Amazon argued for a narrow construction of “coding” that included “transforming original information into coded information by applying a known algorithm,” but that excluded “transforming coded information back into its original state.” In advocating against Amazon’s narrow construction of “coding,” which impliedly included transformation of information by encoding algorithms but not transformation of information by decoding algorithms, Patentee stated that the broader construction identified above is “rooted in the express disclosure of coding found in the Stambler patents, which describes coding information using a ‘coder’ that ‘may be *any form of such device utilizing a known algorithm.*’” Amazon Brief (FEDRES-1015) at 6-7 (emphasis in original) (citing ‘541 at 3:37-39). Patentee further stated that, “in express terms, the [Stambler] patents describe the function of a “coder” as expansively as possible,” and denigrated Amazon’s construction as “a transparent attempt to tack on an ‘exclusion’ for non-infringement.” Id.

Petitioner takes no position as to whether “coding” should be construed broadly, to encompass transformation of information by both encoding and decoding algorithms, or should instead be construed narrowly, to exclude transformation of information by decoding algorithms. Petitioner submits that, regardless of which of these constructions of “coding” is adopted, the IPR claims are obvious, and therefore unpatentable.

ii. Credential

For purposes of this Petition, the term “credential” is construed as “a document or information obtained from a trusted source that is transferred or presented to establish the identity of a party.” This construction mimics constructions resolved through Markman proceedings conducted in co-pending litigation, and is harmonious with constructions offered by Patentee during those proceedings. See, e.g., Merrill Brief (FEDRES-1013) at pp. 13-14 (“credentials are presented as evidence or proof of identity, and the receiving party or system uses the credential for that purpose”).

iii. Credential information

For purposes of this Petition, the term “credential information” is construed as “information stored or contained in a credential.” This construction mimics the only construction of “credential information” that has been resolved through Markman proceedings conducted in co-pending litigation involving the ‘541 patent. See JP Morgan Order (FEDRES-1011) at 6.

iv. Variable Authentication Number (VAN)

For purposes of this Petition, the term “variable authentication number,” or “VAN,” is construed as “a variable number resulting from a coding operation that can be used in verifying the identity of a party or the integrity of information or both.” Although this construction is not the narrowest of the constructions of “VAN” included in FEDRES-1016, it mimics the constructions resolved through Markman proceedings conducted in co-pending litigation involving the ‘541 patent, and is harmonious with several of the constructions offered by Patentee during those proceedings. See, e.g., Merrill Brief (FEDRES-1013) at 8 (“[i]n the credential issuing and authentication context, a VAN is an encoded variable number used in authenticating a credential, which is presented for purposes of determining identity”).

v. Previously issued

For purposes of this Petition, the term “previously issued” is construed as “existing or occurring prior to something else in time or order.” This construction mimics constructions resolved through Markman proceedings conducted in co-pending litigation. See, e.g., RSA Order (FEDRES-1009) at 5.

Each of the independent claims 20, 24, 27, 28, 32, 25, 38, and 46 of the ‘541 patent include a preamble reciting that “a credential is previously issued . . . the credential including a variable authentication number (VAN),” but also include a claim step reciting “creating the VAN by coding credential information” (emphasis added). In other words, each of the independent claims 20, 24, 27, 28, 32, 35, 38, and 46 require (1) that a credential exists prior to something else in time or order; (2) that the credential includes a VAN; and (3) that

“the” VAN is created by coding credential information. The claims fail to specify, however, what, exactly, the credential is issued previous to. As a result, confusion exists as to whether the VAN that is created in the creating step is the VAN that is included in the previously issued credential recited in the preamble, or is instead a recreation of the VAN that is included in the previously issued credential.

In Stambler v. RSA Security, Inc., for example, representatives of Mr. Stambler took the position that “the credential cannot be issued before step one of claim 20 because step one creates the VAN which is included on the credential,” but the District Court ultimately construed “wherein a credential is previously issued” to mean that “the credential referenced in the claim must already be issued before the execution of the steps recited in the claim.” RSA Order (FEDRES-1009) at 5.

Petitioner takes no position as to whether “previously issued,” as recited in the preambles of claims 20, 24, 27, 28, 32, 25, 38, and 46, should be construed broadly, such that the previously issued credential may be issued after the “creating the VAN” step and previous to something else in time or order, or narrowly, such that the previously issued credential must be issued prior to the “creating the VAN step,” in which case the VAN that is created must be a recreation of the VAN included in the previously issued credential. Charted below, however, are two separate combinations of references: (1) Hellman-X.509-Nechvatal, and (2) Hellman-X.509-Nechvatal-Davies. Petitioner submits that, regardless of which of the constructions of “previously issued” is adopted, the IPR claims are obvious,

and therefore unpatentable. If “previously issued” is construed broadly, the first combination of references renders the IPR claims obvious, and the second combination of references renders the IPR claims obvious if “previously issued” is instead construed narrowly.

IV. SUMMARY OF THE ‘541 PATENT

A. Brief Description

The ‘541 Patent describes a method for securing transaction-related information and for authenticating parties to the transaction. See ‘541 at 1:1-23. In the method, at least one of the parties receives a credential. See id. at 11:65-12:2. Included within the credential is a variable authentication number (VAN) that is created by coding credential information with a secret key of the credential issuing entity. Id. The VAN is used to authenticate at least one of the parties. See id. at 5:19-25. Information associated with the two parties is coded to generate a joint code, which is used to code transaction-related information, resulting in coded information relevant to the transaction. Id. at 2:12-18.

B. Summary of the Prosecution History of the ‘541 Patent

Prosecution resulted in an improvident grant of the ‘541 patent. Specifically, in an Office Action dated March 22, 1998, the Examiner rejected the claims of the ‘541 Patent under 35 U.S.C. § 103(a) as obvious over Hellman in view of admitted prior art. FEDRES-1002. At page 20 of his July 21, 1998 response, Mr. Stambler acknowledged that “in Hellman, the common key is derived from information associated with two parties.” Id. In more detail, Stambler explained that:

Hellman discloses a method of deriving a 'common' key which is used by two parties (A and B) to encrypt and decrypt information exchanged between the parties. The common key is derived from information associated with both parties. Party A derives the common key from party A's secret key and party B's public key. Party B derives the common key from party B's secret key and party A's public key. Thus, in Hellman, the common key is derived from information associated with two parties.

Id. As recognized by Stambler, Hellman discloses coding information associated with at least two parties to a transaction to generate a joint code. Id. However, Stambler distinguished Hellman by arguing that Hellman failed to disclose (1) a credential or entity authorized to issue a credential, (2) a secret key associated with a credential issuing entity, and (3) a variable authentication number (VAN), and argued that "it would [not] have been obvious to use a credential with Hellman, since there is no suggestion to modify Hellman to incorporate a credential in its scheme." Id.

Indeed, the Examiner found the prior art to lack description of at least one of a credential, a credential issuing entity, or a VAN, and, on February 26, 1999, the Examiner therefore issued a notice of allowance. Id. No reasons for allowance were given, making it difficult to know which of these features was believed by the Examiner to have been missing from the prior art of record. Regardless, the references included in this Petition address each of these features, undermining the allowability of the claims.

V. THERE IS A REASONABLE LIKELIHOOD THAT AT LEAST ONE IPR CLAIM OF THE '541 PATENT IS UNPATENTABLE

Substantial prior art that was not of record during prosecution warrants a finding of unpatentability for the IPR claims of the '541 Patent, particularly in light of the prosecution history summarized above.

X.509, a standard issued in 1988, describes precisely those elements that were said by Stambler to have been missing from the prior art of record during the original prosecution: (1) a credential and an entity authorized to issue the credential, (2) a secret key associated with a credential issuing entity, and (3) a variable authentication number (VAN). See Diffie Declaration at ¶ 40. In more detail, X.509 describes an authentication framework that enables a first party to a transaction to authenticate a second party to the transaction through use of a certificate (credential) that is issued prior to the transaction to at least one of the parties by a certification authority (credential issuing entity), the certificate including a digital signature (VAN) created by the certification authority by signing a collection of information using the certification authority's secret key (secret key associated with a credential issuing entity). Id.

Moreover, and contrary to Mr. Stambler's assertion during the original prosecution, a person of ordinary skill in the art at the time that Mr. Stambler filed the application to which '541 claims priority would be motivated to modify Hellman to incorporate a credential in its scheme. Nechvatal, a National Institute of Standards and Technology (NIST) paper published in 1991, specifically suggests the combination of the algorithm disclosed in Hellman with the authentication framework provided by X.509. See Nechvatal at §§ 2.2, 5.3. As

Prof. Whitfield Diffie, pioneer of public-key cryptography and co-inventor of the Hellman patent, explains:

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.

Id. at ¶ 47.

The X.509 and Nechvatal references were not before the Examiner during prosecution. These references not only disclose the apparent basis for allowance of the claims (i.e., a lack in Hellman of (1) a credential and an entity authorized to issue the credential, (2) a secret key associated with a credential issuing entity, and (3) a variable authentication number (VAN)), they also demonstrate that a credential-based authentication framework would be naturally integrated with Hellman's system. Id.

As detailed in the following section, the present petition shows how all of these references, alone or in combinations specified, render all limitations of the IPR Claims unpatentable, thus raising a reasonable likelihood of prevailing in one or more of the numerous challenges levied against these claims. Indeed, the IPR Claims are merely a combination of

“prior art elements according to known methods to yield predictable results,” and thus are unpatentable. KSR Int’l Co. v. Teleflex, Inc., 127 S. Ct. 1727, 1740 (2007) (“if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill . . . a court must ask whether the improvement is more than the predictable use of prior art elements according to their established functions”).

VI. MANNER OF APPLYING CITED PRIOR ART TO EVERY CLAIM FOR WHICH *INTER PARTES* REVIEW IS REQUESTED

In this Section, Petitioner proposes two (2) grounds of rejection for the IPR Claims and, thus, explains the justification for *Inter Partes* Review. Petitioner presents claim charts that compare the claim language as construed under the above-ascribed claim interpretations, with the disclosure of the prior art as understood by one of ordinary skill in the art.

A. [GROUND 1] – Hellman, X.509, and Nechvatal render obvious Claims 20, 24, 27, 28, 32, 35, 38, and 46.

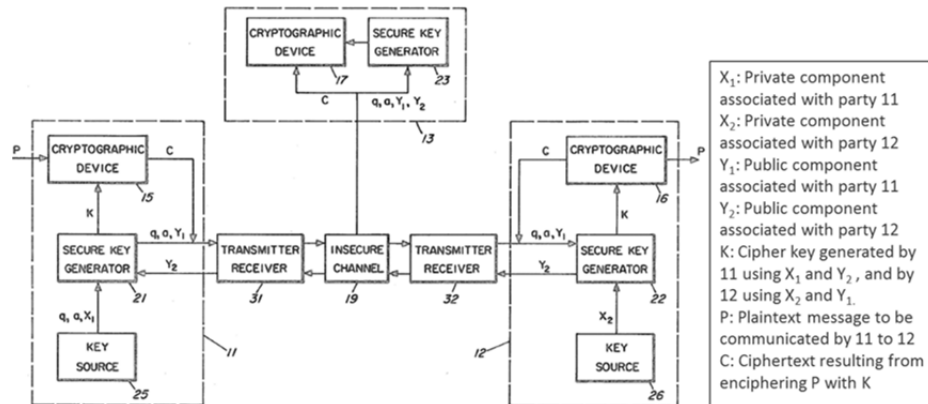
As noted above and explained in greater detail in the following Claim Chart, the features of claims 20, 24, 27, 28, 32, 35, 38, and 46 of the ‘541 patent are obvious in view of the combination of Hellman, X.509, and Nechvatal, rendering each of these claims unpatentable under 35 U.S.C. § 103(a).

A person of ordinary skill in the art at the time that Stambler filed his application would be motivated to combine Hellman with X.509, because Nechvatal describes the

Hellman algorithm and the X.509 framework in detail at sections 2.2 and 5.3, respectively, and suggests their combination. See Diffie Declaration at ¶ 47. In more detail, Nechvatal states, with reference to the algorithm described in Hellman, that “the underlying public-key cryptosystem [of Hellman] supports secrecy but not authentication . . . [and] [t]hus it may be desirable to augment a secrecy-providing system [such as Hellman] with one which provides authentication.” Nechvatal at § 2.2. Nechvatal then states that “[e]xamples of the latter will be given later,” and goes on to describe the “strong authentication” provided by the authentication framework disclosed by X.509. Id. at §§ 2.2, 5.3. Indeed, as Prof. Diffie explains, a person of ordinary skill in the art at the time that Stambler filed his application would understand that the teachings of X.509 and Nechvatal could be “naturally integrated” into Hellman’s cryptosystem, and would be motivated to make the combination. See Diffie Declaration at ¶ 47.

| Claim 20 | Hellman (U.S Patent No. 4,200,770) in view of X.509 and Nechvatal |
|--|--|
| <p>[20preA] In a multi-party transaction system, a method for securing information relevant to a transaction by using information associated with at least two parties,</p> | <p>Hellman, titled “Cryptographic Apparatus and Method,” discloses a method for securing information that is involved in a transaction (“information relevant to a transaction”) between a first party 11 and a second party 12 (“at least two parties”) by using information associated with party 11 and with party 12. <u>See</u> Hellman at Abstract (“A cryptographic system transmits a computationally secure cryptogram over an insecure communication channel without prearrangement of a cipher key. . . [a] secure cipher key is generated by the conversers from transformations of exchanged transformed signals”); <u>see also</u> Nechvatal at § 2.2 (describing the algorithm disclosed by Hellman); Diffie Declaration at ¶ 37. Specifically, and as is depicted in the annotated version of Hellman’s Fig. 1 provided below, Hellman describes a cryptographic system and method that can be used to secure a plaintext message P, which is to be communicated in an ex-</p> |

change of information (“transaction”) between a first party 11 and a second party 12, through encoding of P using a cipher key K, where the cipher key K is generated based on information associated with the two parties. See Hellman at 3:47-64; 4:1-5:3; Diffie Declaration at ¶ 37.



In more detail, private components X_1 and X_2 are associated, respectively, with party 11 and with party 12. Id. at 4:13-17; Diffie Declaration at ¶ 38. A public component Y_1 is generated by 11 through a transformation of X_1 , and a public component Y_2 is generated by 12 through a transformation of X_2 . Id. at 4:23-27; Diffie Declaration at ¶ 39. The public components Y_1 and Y_2 are exchanged between the parties, and each of the parties 11 and 12 independently generate an identical cipher key K. Id. at 4:44-51; Diffie Declaration at ¶¶ 38, 39. 11 generates K by transforming Y_2 using X_1 , and 12 generates K by transforming Y_1 using X_2 . Hellman at 4:44-51. Party 11 enciphers plaintext P using K in order to generate ciphertext C, which is transmitted to party 12. Id. at 3:41-64; Diffie Declaration at ¶ 38. Party 12 then deciphers ciphertext C using K in order to retrieve plaintext P. Hellman at 3:41-64; Diffie Declaration at ¶ 38.

Thus, Hellman discloses securing information P that is relevant to a transaction using a cipher key K that is generated using information associated with the parties 11 and 12: the private components X_1 and X_2 , and the public components Y_1 and Y_2 . Diffie Declaration at ¶¶ 37-39.

[20preB] wherein a credential is previously issued to at

X.509, an International Telecommunication Union standard titled “The Directory - Authentication Framework,” describes a digital certificate (“credential”) that is issued previous to a transaction to one or more

| | |
|--|---|
| <p>least one of the parties by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the method comprising:</p> | <p>parties to the transaction by a certification authority (“an entity authorized to issue a credential”) the certificate including a digital signature (“VAN”). <u>See</u> X.509 at §§ 6-9; <u>see also</u> Nechvatal at § 5.3 (describing the X.509 standard). Specifically, the X.509 standard describes a “strong authentication system” 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 using the certification authority’s secret key, the digital certificate having been issued by the certification authority, prior to the transaction, to at least one of the parties to the transaction. <u>See</u> X.509 at § 6; Nechvatal at § 5.3; Diffie Declaration at ¶ 40.</p> <p>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.” X.509 at § 3.3. As described by X.509, and as will be explained in greater detail below with respect to [20B], a digital certificate enables a first party to a transaction to confirm, based on verification of a certification authority’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. <u>See</u> X.509 at §§ 6.5-7.2; Diffie Declaration at ¶ 41. Having confirmed the validity of the public key contained in the digital certificate, the first party to the transaction can then corroborate 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. <u>See</u> X.509 at §§ 6.4, 6.5, 7.1, 7.2; Diffie Declaration at ¶ 41.</p> <p>Thus, like the “credential” disclosed in the ‘541 patent, the “digital certificate” described in X.509 is a collection of information obtained from a trusted source that is transferred or presented to establish the identity of a party.</p> <p>Like the “VAN” disclosed in the ‘541 patent, the “digital signature” described by X.509 is created by coding certificate information, is included within the digital certificate, and may be used to verify the</p> |
|--|---|

| | |
|---|--|
| | <p>identity of a party. See, e.g., X.509 at § 7.2 (“A certification authority produces a certificate of a user by signing . . . a collection of information, including the user’s distinguished name and public key”); § 8.1 (“Information (info) is signed by appending to it an enciphered summary of the information . . . enciphering is carried out using the secret key of the signer”); § A.3 (“The digital signature mechanism . . . proves the authenticity of the originator and the unambiguous relationship between the originator and the data that was transferred”); Diffie Decalation at ¶ 40.</p> <p>Thus, X.509 discloses a digital certificate (“credential”) that is issued previous to a transaction to one or more parties to the transaction by a certification authority (“an entity authorized to issue a credential”) the certificate including a digital signature (“VAN”).</p> |
| <p>[20A] creating the VAN by coding credential information with a secret key of the credential issuing entity;</p> | <p>X.509 discloses creating a digital signature (“VAN”) for a previously issued digital certificate (“credential”) by coding information contained in a digital certificate (“credential information”) with a secret key of a certification authority (“credential issuing entity”).</p> <p>In more detail, and as is depicted in the annotated version of X.509’s Fig. 6 provided below, the certification authority 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 certification authority, the hashed collection of information $h(\text{info})$, and (3) appending the signed hash $X_s[h(\text{info})]$ to the collection of information. X.509 at §§ 7-8; Nechvatal at § 5.3; Diffie Declaration at 42.</p> <div><p>The diagram illustrates the digital signature process in two parts: Signer (X) and Recipient. In the Signer (X) section, 'Info' is input to a hash function 'h', which outputs 'h(info)'. This is then combined with a 'Secret key (Xs)' in an encryption block 'E' to produce the signature 'Xs[h(info)]'. In the Recipient section, the received 'Info' is hashed by 'h' to produce 'h(info)'. The received signature 'Xs[h(info)]' is decrypted by block 'D' using the 'Public key (Xp)'. The outputs of 'h' and 'D' are then compared. A legend on the right defines the symbols: X: Certificate authority, Recipient: A first party to a transaction, Xs: Secret key of the certificate authority, Xp: Public key of the certificate authority, Info: Information including a name and a public key of a second party to the transaction, h: Hash function, Xs[h(info)]: Info that has been hashed using h and then enciphered using Xs.</p></div> <p>FIGURE 6/X.509</p> |

| | |
|--|--|
| | <p>Thus, X.509 discloses creating a digital signature (“VAN”) for a previously issued digital certificate by coding, with a secret key of the certification authority (“credential issuing entity”), a collection of information that is included in a digital certificate (“credential information”).</p> |
| <p>[20B] authenticating at least one of the parties by using the VAN;</p> | <p>X.509 discloses authenticating at least one of the parties to a transaction by using a digital signature (“VAN”). <u>See</u> X.509 at §§ 6.5-7.2 (“For a user to determine that a communication partner is in possession of another user’s secret key, it must itself be in possession of that user’s public key . . . it must obtain the other user’s public key from a source that it trusts . . . [such as a] certification authority [that] produces [a] certificate of [the other] user by <u>signing</u> . . . a collection of information, including the [other] user’s distinguished name and public key”) (emphasis added).</p> <p>In more detail, and as is depicted in the annotated version of X.509’s Fig. 6 provided above, a first party to a transaction may obtain a digital certificate that has been issued by a certification authority X, the digital certificate including a <u>digital signature</u> of the certification authority ($Xs[h(\text{info})]$), and a collection of information (info) that includes a public key of a second party to the transaction. X.509 at §§ 7.2, 8.2; Diffie Declaration at ¶ 43. 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 $h(\text{info})$ with a hash obtained by deciphering the digital signature using X’s public key, Xp. <u>See</u> X.509 at § 8.2 (“The recipient of signed information verifies the signature by: . . . applying the one way hash function to the information . . . [and] comparing the result with that obtained by deciphering the signature using the public key of the signer”); Diffie Declaration at ¶ 43.</p> <p>Because the certification authority is a trusted authority, verification of the certification authority’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. <u>See</u> X.509 at §§ 6.5-7.2; Diffie Declaration at ¶ 44. Having confirmed, based on the certification authority’s digital signature, the validity of the public key contained in the digital certificate, the first party to the transaction can corroborate 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</p> |

| | |
|---|---|
| | <p>the public key included in the digital certificate. <u>See</u> X.509 at §§ 6.4, 6.5, 7.1, 7.2; Diffie Declaration at ¶ 44. The first party to the transaction may, for example, verify the identity of the second party to the transaction by deciphering, using the public key included in the digital certificate, information that has been enciphered by the second party to the transaction. <u>See</u> X.509 at § 6.4; <u>see also</u> Nechvatal at §5.3.4; Diffie Declaration at 44.</p> <p>Thus, X.509 discloses authenticating at least one of the parties to a transaction by using the certification authority's ("credential issuing entity") digital signature ("VAN"). <u>See</u> Diffie Declaration at 40.</p> |
| <p>[20C] coding information associated with the at least two parties to generate a joint code; and</p> | <p>Hellman discloses coding information associated with the at least two parties to a transaction to generate a cipher key, K ("joint code"). <u>See</u> Diffie Declaration at 38. Specifically, and as explained above with reference to Hellman's Fig. 1, Hellman discloses generating a cipher key K using information associated with the two parties to the transaction: the public components X_1 and X_2, and the private components Y_1 and Y_2. <u>See</u> [20pre]; <u>see also</u> Hellman at 3:47-64; 4:1-5:3; Diffie Declaration at 38. In more detail, private components X_1 and X_2 are associated, respectively, with party 11 and with party 12. Hellman at 4:13-17; Diffie Declaration at 38. A public component Y_1 is generated by 11 through a transformation of X_1, and a public component Y_2 is generated by 12 through a transformation of X_2. Hellman at 4:23-27; Diffie Declaration at 39. The public components Y_1 and Y_2 are exchanged between the parties, and each of the parties 11 and 12 independently generate an identical cipher key K. Hellman at 4:44-51; Diffie Declaration at 39. 11 generates K by transforming Y_2 using X_1, and 12 generates K by transforming Y_1 using X_2. Hellman at 4:52-5:3; Diffie Declaration at 38. In other words, Hellman discloses that each party to the transaction codes information that is associated with itself and with the other party to the transaction in order to generate a joint code.</p> <p>Indeed, as Stambler noted in his July 21, 1998 response to a rejection of claims 110-150 under 35 U.S.C. § 103 over Hellman in view of admitted prior art, "in Hellman, the common key is derived from information associated with two parties." In more detail, Stambler explained that:</p> <p style="text-align: center;">Hellman discloses a method of deriving a 'common'</p> |

| | |
|---|--|
| | <p>key which is used by two parties (A and B) to encrypt and decrypt information exchanged between the parties. The common key is derived from information associated with both parties. Party A derives the common key from party A's secret key and party B's public key. Party B derives the common key from party B's secret key and party A's public key. Thus, in Hellman, the common key is derived from information associated with two parties.</p> <p><u>Id.</u> In other words, and as recognized by Stambler, Hellman discloses coding information (“X_1, X_2, Y_1, and Y_2”) associated with at least the two parties to the transaction (“party 11 and party 12”) to generate a joint code (“cipher key K”). <u>See also</u> Diffie Declaration at 37.</p> |
| [20D] coding the information relevant to the transaction with the joint code to generate coded information relevant to the transaction. | <p>Hellman discloses coding plaintext P (“information relevant to the transaction”) with a cipher key K (“joint code”) to generate ciphertext C (“coded information relevant to the transaction”). <u>See</u> Diffie Declaration at 37. Specifically, and as explained above with reference to Hellman’s Fig. 1, Hellman discloses that a first party to the transaction enciphers plaintext P using the cipher key K in order to generate ciphertext C, which is transmitted to the second party to the transaction. <u>See [20pre]</u>; Hellman at 3:41-64; Diffie Declaration at ¶ 38.</p> |
| [24] The method of claim 20 wherein the information associated with the at least two parties used to generate the joint code comprises information associated with at least one present party and information associated with at least one absent party. | <p>Hellman discloses that private components X_1 and X_2 and public components Y_1, and Y_2 (“information”) that are associated with party 11 and party 12 (“at least two parties to the transaction”) are used to generate a cipher key K (“joint code”), and that the private and public components are associated with party 11 (“at least one present party”) and with party 12 (“at least one absent party”). <u>see</u> Hellman at 3:47-64; 4:1-5:3; <u>see also [20C]</u> (explaining Hellman’s disclosure of coding information (X_1, X_2, Y_1, and Y_2) associated with at least the two parties to the transaction (party 11 and party 12) to generate a joint code (cipher key K)); Diffie Declaration at ¶¶ 38, 39.</p> <p>In more detail, the cipher key K described by Hellman is used by party 11 to encipher plaintext P, producing ciphertext C, which may then be transmitted by party 11 to party 12. Hellman at 3:41-68; Diffie Declaration at ¶ 38. In other words, Hellman discloses that the information used to generate the cipher key K is associated with a present party 11, the party that initiates the transaction by transmitting the ciphertext C, and an absent party 12, the party that receives the trans-</p> |

| | |
|---|--|
| | <p>mitted ciphertext C. <u>See</u> Diffie Declaration at ¶¶ 38, 39. Thus, Hellman, X.509, and Nechvatal render obvious that the information associated with the at least two parties used to generate the joint code comprises information associated with at least one present party and information associated with at least one absent party.</p> |
| <p>[27] The method of claim 20 wherein the information relevant to the transaction comprises at least one information group which was previously coded to enable detection of a change in the content or structure of the information group.</p> | <p>X.509 discloses that information that is involved in a transaction (“information relevant to the transaction”) includes a digital signature (“at least one information group which was previously coded to enable detection of a change in the content or structure of the information group”).</p> <p>As explained previously with respect to claim 20, X.509 describes producing a digital signature by hashing, using a secure hash function h, a collection of information, enciphering the hash, and appending the enciphered hash to the collection of information, thereby enabling a recipient of the information to detect a change in the content or structure of the information. <u>See</u> [20A], [20B]; <u>see also</u> X.509 at §§ 7-8; Nechvatal at § 5.3; Diffie Declaration at ¶ 42. In more detail, X.509 discloses that a recipient of the information may verify it by (1) deciphering the hash that was appended to the information, (2) applying a hash function to the information, and then (3) comparing the hashed information to the deciphered hash. <u>See</u> X.509 at § 8; Diffie Declaration at ¶ 43. A match of the hashed information to the deciphered hash verifies that the content or structure of the information has not changed since it was sent. X.509 at § A.3 (“<i>data integrity</i>: this mechanism involves the encipherment of a compressed string of the relevant data to be transferred. Together with the plain data, this message is sent to the recipient. The recipient repeats the compressing and subsequent encipherment of the plain data and compares the results with that created by the originator to prove integrity”) (emphasis in original); Diffie Declaration at ¶ 45.</p> <p>Thus, Hellman, X.509, and Nechvatal render obvious that the information relevant to the transaction comprises at least one information group which was previously coded to enable detection of a change in the content or structure of the information group. <u>See</u> Diffie Declaration at ¶ 45.</p> |

| | |
|---|---|
| <p>[28preA] In a transaction system, a method for securing information relevant to a transaction, the transaction including at least one party,</p> | <p>As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious, in a transaction system, a method for securing information relevant to a transaction, the transaction including at least one party. <u>See</u> [20preA].</p> |
| <p>[28preB] wherein a credential is previously issued to the at least one party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the method comprising:</p> | <p>As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious a credential that is previously issued to the at least one party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN). <u>See</u> [20preB].</p> |
| <p>[28A] creating the VAN by coding credential information with a secret key of the credential issuing entity;</p> | <p>As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious creating the VAN by coding credential information with a secret key of the credential issuing entity. <u>See</u> [20A].</p> |
| <p>[28B] authenticating the at least one of the party by using the VAN;</p> | <p>As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious authenticating at least one of the parties by using the VAN. <u>See</u> [20B].</p> |
| <p>[28C] generating a joint code by coding first information accessed from a first one or more data storage means with second information associated with the at least one party to the transaction; and</p> | <p>Hellman discloses generating a cipher key K (“joint code”) by coding X₁ (“first information accessed from”) accessed from key source 25 (“a first one or more data storage means”) with Y₂ (“second information”) associated with party 12 (“the at least one party to the transaction”). <u>See</u> [20C] (explaining Hellman’s disclosure of coding information (X₁, X₂, Y₁, and Y₂) associated with at least the two parties to the transaction (party 11 and party 12) to generate a joint code (cipher key K)); Diffie Declaration at ¶¶ 37-39.</p> <p>In more detail, Hellman describes generating a joint code K by coding first information X₁ that is accessed by party 11 from key source 25</p> |

| | |
|--|--|
| | <p>with second information Y_2 that is associated with party 12. Diffie Declaration at ¶ 39. In more detail, Hellman discloses that private components X_1 and X_2 are associated, respectively, with party 11 and with party 12, and are accessed, respectively, from key sources 25 and 26. Hellman at 4:13-17. A public component Y_1 is generated by 11, using secure key generator 21, through a transformation of X_1, and a public component Y_2 is generated by 12, using secure key generator 22, through a transformation of X_2. <u>Id.</u> at 4:23-27; Fig. 1. The public components Y_1 and Y_2 are exchanged between the parties, and each of the parties 11 and 12 independently generate an identical cipher key K. <u>Id.</u> at 4:44-51. 11 generates K by transforming Y_2 using X_1, and 12 generates K by transforming Y_1 using X_2. <u>Id.</u> at 4:52-5:3.</p> <p>In other words, Hellman discloses that party 11 generates a joint code K by coding its private component X_1, accessed from a key source 25, with a public component Y_2 that is associated with the other party to the transaction, party 12. <u>See Id.</u> at 3:47-64; 4:1-5:3; Diffie Declaration at ¶¶ 37-39. Thus, Hellman, X.509, and Nechvatal render obvious generating a joint code by coding first information accessed from a first one or more data storage means with second information associated with the at least one party to the transaction.</p> |
| [28D] coding the information relevant to the transaction with the joint code to generate coded information relevant to the transaction. | As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious coding the information relevant to the transaction with the joint code to generate coded information relevant to the transaction. <u>See [20D]</u> . |
| [32preA] A method for coding clear information by using information associated with at least one party, | Hellman discloses coding plaintext P (“clear information”) by using cipher key K (“information associated with at least one party”). <u>See [20preA]</u> . In more detail, and as explained above, Hellman discloses securing information P that is relevant to a transaction using a cipher key K that is generated using information associated with parties 11 and 12: public components X_1 and X_2 , and private components Y_1 and Y_2 . <u>See</u> Hellman at 3:47-64; 4:1-5:3; Diffie Declaration at ¶¶ 37-39. Hellman describes the information P as “unenciphered,” and as “plaintext,” and explains that the plaintext information P may be secured for transmission over an insecure channel by enciphering it with the cipher key K in order to produce ciphertext C . <u>Id.</u> at 3:47-49 |

| | |
|--|---|
| | <p>(“Conversor 11 possesses an unenciphered or plaintext message P to be communicated to conversor 12”); <u>Id.</u> at 3:59-64 (“The cryptographic device 15 enciphers the plaintext message P into an enciphered message or ciphertext C on line C that is transmitted by conversor 11 through the insecure channel 19; the ciphertext C is received by conversor 12 and deciphered by cryptographic device 16 to obtain the plaintext message P”); Diffie Declaration at ¶ 38.</p> <p>Thus, Hellman discloses coding clear information P by using information K that is associated with at least one party, and Hellman, X.509, and Nechvatal render obvious a method for coding clear information by using information associated with at least one party, wherein a credential is previously issued to the at least one party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN).</p> |
| [32preB] wherein a credential is previously issued to the at least one party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the method comprising: | As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious that a credential is previously issued to the at least one party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN). <u>See [20preB]</u> . |
| [32A] creating the VAN by coding credential information with a secret key of the credential issuing entity; | As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious creating the VAN by coding credential information with a secret key of the credential issuing entity. <u>See [20A]</u> . |
| [32B] authenticating the at least one of the party by using the VAN; | As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious authenticating at least one of the parties by using the VAN. <u>See [20B]</u> . |
| [32C] coding a first information group with a second information group to | Hellman discloses coding Y ₂ (“a first information group”) with X ₁ (“a second information group”) to generate a cipher key K (“third information group”), where Y ₂ is associated with party 12 and where X ₁ is associated with party 11 (“at least one of the first and second infor- |

| | |
|--|--|
| <p>generate a third information group, at least one of the first and second information groups being associated with the at least one party; and</p> | <p>mation groups being associated with the at least one party”). <u>See [20C]</u> (explaining Hellman’s disclosure of coding information associated with party 11 and party 12 (“the at least two parties to a transaction”) to generate a cipher key K (“joint code”)); Diffie Declaration at ¶¶ 37-39.</p> <p>In more detail, and with respect to the specific language of claim 32, Hellman describes coding a first information group X_1 with a second information group Y_2 to generate a third information group K, where the first and second information groups X_1 and Y_2 are associated, respectively, with parties 11 and 12. <u>See</u> Diffie Declaration at ¶¶ 37-39. Specifically, Hellman discloses that private components X_1 and X_2 are associated, respectively, with party 11 and with party 12. Hellman at 4:13-17. A public component Y_1 is generated by 11 through a transformation of X_1, and a public component Y_2 is generated by 12 through a transformation of X_2. <u>Id.</u> at 4:23-27. The public components Y_1 and Y_2 are exchanged between the parties, and each of the parties 11 and 12 independently generate an identical cipher key K. <u>Id.</u> at 4:44-51. 11 generates K by transforming Y_2 using X_1, and 12 generates K by transforming Y_1 using X_2. <u>Id.</u> at 4:52-5:3.</p> <p>In other words, Hellman discloses that party 11 generates a cipher key K by coding its private component X_1 with a public component Y_2 that is associated with the other party to the transaction, party 12. <u>See Id.</u> at 3:47-64; 4:1-5:3; Diffie Declaration at ¶¶ 37-39. Thus, Hellman, X.509, and Nechvatal render obvious coding a first information group with a second information group to generate a third information group, at least one of the first and second information groups being associated with the at least one party.</p> |
| <p>[32D] coding the clear information with the third information group to generate coded information.</p> | <p>Hellman discloses coding plaintext P (“the clear information”) with the cipher key K (“third information group”) to generate ciphertext C (“coded information”) . <u>See</u> Hellman at 3:41-64; <u>see also [20D]</u>; Diffie Declaration at ¶ 38. Thus, Hellman, X.509, and Nechvatal render obvious coding the clear information with the third information group to generate coded information.</p> |

| | |
|---|---|
| <p>[35preA] In a multi-party transaction system, a method for securing information relevant to a transaction, the transaction including a first party and a second party,</p> | <p>Hellman discloses, in a multi-party transaction system, a method for securing information involved in a transaction (“information relevant to a transaction”), the transaction including a first party 11 and a second party 12. <u>See</u> [20preA] (explaining Hellman’s disclosure of a method for securing, in a transaction system, information relevant to a transaction, the transaction including at least one party).</p> <p>In more detail, and as explained above, Hellman discloses securing information communicated in a transaction between party 11 and party 12 using a cipher key K that is generated using information that is associated with the two parties: public components X_1 and X_2, and private components Y_1 and Y_2. <u>See</u> Hellman at 3:47-64; 4:1-5:3; <u>see also id.</u> at 3:59-64 (“The cryptographic device 15 enciphers the plaintext message P into an enciphered message or ciphertext C on line C that is transmitted by converser 11 through the insecure channel 19; the ciphertext C is received by converser 12 and deciphered by cryptographic device 16 to obtain the plaintext message P”); Diffie Declaration at ¶¶ 37-39.</p> <p>Thus, Hellman, X.509, and Nechvatal render obvious, in a multi-party transaction system, a method for securing information relevant to a transaction, the transaction including a first party and a second party.</p> |
| <p>[35preB] wherein a credential is previously issued to at least one of the first party and the second party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the method comprising:</p> | <p>As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious a credential is previously issued to the at least one party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN). <u>See</u> [20preB].</p> |
| <p>[35A] creating the VAN by coding credential information with a secret key of the credential issu-</p> | <p>As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious creating the VAN by coding credential information with a secret key of the credential issuing entity. <u>See</u> [20A].</p> |

| | |
|---|---|
| ing entity; | |
| [35B] authenticating at least one of the first and second parties by using the VAN; | As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious authenticating at least one of the parties by using the VAN. <u>See</u> [20B] . As such, Hellman, X.509, and Nechvatal render obvious authenticating at least one of the first and second parties by using the VAN. |
| [35G] coding the information relevant to the transaction with first information associated with the first party to derive first coded information; and | <p>As shown by the following two examples, Hellman discloses coding information relevant to the transaction with first information associated with the first party to derive first coded information.</p> <p><u>Example I</u></p> <p>Hellman discloses coding plaintext P (“information relevant to the transaction”) with cipher key K (“first information associated with the first party”) to derive ciphertext C (“first coded information”). <u>See</u> Hellman at 3:47-64; 4:1-5:3; Diffie Declaration at ¶ 38 (“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”).</p> <p>In more detail, and as explained above with reference to Hellman’s Fig. 1, Hellman describes generating a cipher key K using information associated with the two parties to the transaction: the private components X_1 and X_2, and the public components Y_1 and Y_2. [20pre]; <u>see also</u> Hellman at 3:47-64; 4:1-5:3. Private components X_1 and X_2 are associated, respectively, with party 11 and with party 12. Hellman at 4:13-17. A public component Y_1 is generated by 11 through a transformation of X_1, and a public component Y_2 is generated by 12 through a transformation of X_2. <u>Id.</u> at 4:23-27. The public components Y_1 and Y_2 are exchanged between the parties 11 and 12, and each party independently generates an identical cipher key that is associated with the parties: cipher key K. <u>Id.</u> at 4:44-51. 11 generates K by transforming Y_2 using X_1, and 12 generates K by transforming Y_1 using X_2. <u>Id.</u> at 4:52-5:3.</p> <p>Following the generation by both parties of the cipher key K, plaintext P may be enciphered by party 11 with the cipher key K to generate ciphertext C, which may then be transmitted by party 11 to party 12. <u>See</u> Hellman at 3:41-64.</p> |

| | |
|---|--|
| | <p>In other words, Hellman discloses coding information relevant to the transaction (plaintext P) with first information associated with the first party (cipher key K), to derive first coded information (ciphertext C). <u>See</u> Hellman at 3:47-64; 4:1-5:3; Diffie Declaration at ¶ 38. Thus, for at least this reason, Hellman, X.509, and Nechvatal render obvious coding the information relevant to the transaction with first information associated with the first party to derive first coded information.</p> <p><u>Example II</u></p> <p>Hellman discloses coding private component X_1 (“information relevant to the transaction”) with signals q and a (“first information associated with the first party”) to derive public component Y_1 (“first coded information”). <u>See</u> Hellman at 4:11-27; Diffie Declaration at ¶ 39.</p> <p>Hellman describes accessing a private component X_1 and signals q and a from party 11’s key source 25, and generating, using party 11’s secure key generator 21, a public component Y_1 by coding X_1 with q and a. <u>See</u> Hellman at 3:47-64; 4:1-5:3; Fig. 1. Hellman further describes that signals q and a are communicated in a transaction between party 11 and party 12, and that private component X_1 is associated with party 11. <u>Id.</u> at 4:11-17 Therefore, private component X_1 and signals q and a are each relevant to the transaction, and are each associated with party 11.</p> <p>Thus, Hellman discloses coding private component X_1 (“information relevant to the transaction”) with signals q and a (“first information associated with the first party”) to derive public component Y_1 (“first coded information”) and, for at least this reason, Hellman, X.509, and Nechvatal render obvious coding the information relevant to the transaction with first information associated with the first party to derive first coded information.</p> |
| <p>[35H] coding the first coded information with first information associated with the second party to derive second coded information relevant to</p> | <p>As shown by the following two examples, Hellman discloses coding the first coded information with first information associated with the second party to derive second coded information relevant to the transaction.</p> <p><u>Example I</u></p> <p>Hellman discloses coding ciphertext C (“the first coded information”) with cipher key K (“first information associated with the second party”)</p> |

| | |
|-------------------------|---|
| <p>the transaction.</p> | <p>to derive plaintext P (“second coded information relevant to the transaction”). <u>See</u> Hellman at 3:47-64; 4:1-5:3; Diffie Declaration at ¶ 38 (“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”).</p> <p>In more detail, and as explained above with reference to Hellman’s Fig. 1, Hellman discloses that, following the generation by both parties, based on information associated with both parties, of the cipher key K, plaintext P may be encoded by party 11 with the cipher key K to generate ciphertext C, which may then be transmitted by party 11 to party 12. <u>See</u> Hellman at 3:41-64; <u>see also</u> [20A]. Party 12 may then decode ciphertext C using cipher key K in order to derive plaintext P. <u>Id.</u></p> <p>Thus, Hellman discloses coding first coded information (ciphertext C) with first information associated with the second party (cipher key K) to derive second coded information relevant to the transaction (plaintext P, having been encoded and then decoded) and, for at least this reason, Hellman, X.509, and Nechvatal render obvious coding the first coded information with first information associated with the second party to derive second coded information relevant to the transaction.</p> <p><u>Example II</u></p> <p>Hellman discloses coding public component Y_1 (“the first coded information”) with private component X_2 (“first information associated with the second party”) to derive cipher key K (“second coded information relevant to the transaction”). <u>See</u> Hellman at 3:47-64; 4:1-5:3; Diffie Declaration at ¶ 38.</p> <p>Hellman describes that party 12 codes, using secure key generator 22, public component Y_1 received from party 11 with private component X_2 retrieved from key source 26 to derive cipher key K. <u>See</u> Hellman at 4:60-65; Fig. 1.</p> <p>Thus, Hellman discloses coding public component Y_1 (“the first coded information”) with private component X_2 (“first information associ-</p> |
|-------------------------|---|

| | |
|--|---|
| | ated with the second party”) to derive cipher key K (“second coded information relevant to the transaction”) and, for at least this reason, Hellman, X.509, and Nechvatal render obvious coding the first coded information with first information associated with the second party to derive second coded information relevant to the transaction. |
| [38preA] In a transaction system, a method for securing information relevant to a transaction, the transaction including at least one party, | As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious, in a transaction system, a method for securing information relevant to a transaction, the transaction including at least one party. <u>See [20preA]</u> . |
| [38preB] wherein a credential is previously issued to the at least one party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the method comprising: | As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious a credential that is previously issued to at least one party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN). <u>See [20preB]</u> . |
| [38A] creating the VAN by coding credential information with a secret key of the credential issuing entity; | As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious creating the VAN by coding credential information with a secret key of the credential issuing entity. <u>See [20A]</u> . |
| [38B] authenticating the at least one of the party by using the VAN; | As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious authenticating at least one of the parties by using the VAN. <u>See [20B]</u> . |
| [38G] coding information relevant to the transaction using information accessed from one or more data storage | As shown by the following two examples, Hellman discloses coding information relevant to the transaction using information accessed from one or more data storage means to derive first coded information. In a first context, Hellman discloses coding information relevant to a |

| | |
|---|--|
| <p>means to derive first coded information; and</p> | <p>transaction (plaintext P) using information accessed from one or more data storage means (cipher key K) to derive first coded information (ciphertext C), that can later be decoded with cipher key K to derive decoded plaintext P. <u>See</u> Hellman at 3:47-64; 4:1-5:3; Diffie Declaration at ¶¶ 37. 38.</p> <p>In a second context, Hellman discloses coding information relevant to a transaction (signals q and a) using information accessed from one or more data storage means (private component X_1) to derive first coded information (public component Y_1) that can later be coded with private key X_2 to derive cipher key K. <u>Id.</u>; Diffie Declaration at ¶¶ 38, 39.</p> <p><u>Example I</u></p> <p>Hellman discloses coding plaintext P (“information relevant to the transaction”) using cipher key K (“information accessed from one or more data storage means”) to derive ciphertext C (“first coded information”). <u>See</u> Hellman at 3:47-64; 4:1-5:3. In more detail, Hellman discloses that, following the generation by parties 11 and 12 of the cipher key K, a cryptographic device 15 belonging to party 11 may access cipher key K from secure key generator 12, and may encipher plaintext P using cipher key K to generate ciphertext C, which may then be transmitted by party 11 to party 12. <u>See</u> Hellman at 3:41-5:3; see also Hellman Fig. 1.</p> <p>In other words Hellman discloses coding information relevant to the transaction (plaintext P) using information accessed from one or more data storage means (cipher key K) to derive first coded information (ciphertext C). <u>See</u> Hellman at 3:47-64; 4:1-5:3; Diffie Declaration at ¶ 38. Thus, Hellman, X.509, and Nechvatal render obvious, for at least this reason, coding information relevant to the transaction using information accessed from one or more data storage means to derive first coded information.</p> <p><u>Example II</u></p> <p>Hellman discloses coding signals q and a (“information relevant to the transaction”) using private component X_1 (“information accessed from one or more data storage means”) to derive public component Y_1 (“first coded information”). <u>See</u> Hellman at 4:11-27.</p> |
|---|--|

| | |
|--|---|
| | <p>Hellman describes accessing a private component X_1 and signals q and a from key source 25, and generating, by secure key generator 21, a public component Y_1 by coding q and a using X_1. <u>See</u> Hellman at 3:47-64; 4:1-5:3; Fig. 1. Hellman further describes that signals q and a are generated by party 11 and are communicated in a transaction between party 11 and party 12, and that private component X_1 is associated with party 11. <u>Id.</u> at 4:11-17. Therefore, private component X_1 and signals q and a are each relevant to the transaction, and are each associated with party 11.</p> <p>Thus, Hellman discloses coding signals q and a (“information relevant to the transaction”) using private component X_1 (“first information associated with the first party”) to derive public component Y_1 (“first coded information”) and, for at least this reason, Hellman, X.509, and Nechvatal render obvious coding information relevant to the transaction using information accessed from one or more data storage means to derive first coded information.</p> |
| <p>[38H] coding the first coded information using information associated with the at least one party to the transaction to derive second coded information relevant to the transaction.</p> | <p>As shown by the following two examples, Hellman discloses coding the first coded information with first information associated with the second party to derive second coded information relevant to the transaction.</p> <p><u>Example I</u></p> <p>Hellman discloses coding ciphertext C (“the first coded information”) using cipher key K (“information associated with the at least one party to the transaction”) to derive plaintext P (“second coded information relevant to the transaction”). <u>See</u> Hellman at 3:47-64; 4:1-5:3; Diffie Declaration at ¶ 38.</p> <p>In more detail, and as explained above with reference to Hellman’s Fig. 1, Hellman discloses that, following the generation by both parties, based on information associated with both parties, of the cipher key K, plaintext P may be enciphered by party 11 with the cipher key K to generate ciphertext C, which may then be transmitted by party 11 to party 12. <u>See</u> Hellman at 3:41-64; <u>see also</u> [20A]. Party 12 may then decipher ciphertext C using K in order to derive plaintext P. <u>Id.</u></p> <p>In other words, Hellman describes coding the first coded information (ciphertext C) using information (cipher key K) associated with the at</p> |

| | |
|--|---|
| | <p>least one party to the transaction to derive second coded information relevant to the transaction (plaintext P, having been encoded and then decoded). <u>See</u> Hellman at 3:47-64; 4:1-5:3; Diffie Declaration at ¶ 38. Thus, for at least this reason, Hellman, X.509, and Nechvatal render obvious coding the first coded information using information associated with the at least one party to the transaction to derive second coded information relevant to the transaction.</p> <p><u>Example II</u></p> <p>Hellman discloses coding public component Y_1 (“the first coded information”) using private component X_2 (“information associated with the at least one party to the transaction”) to derive cipher key K (“second coded information relevant to the transaction”). <u>See</u> Hellman at 3:47-64; 4:1-5:3; Diffie Declaration at ¶ 39.</p> <p>Hellman describes that party 12 codes, using secure key generator 22, public component Y_1 received from party 11 with private component X_2 retrieved from key source 26 to derive cipher key K. <u>See</u> Hellman at 4:60-65; Fig. 1.</p> <p>Thus, Hellman discloses coding public component Y_1 (“the first coded information”) using private component X_2 (“information associated with the at least one party to the transaction”) to derive cipher key K (“second coded information relevant to the transaction”) and, for at least this reason, Hellman, X.509, and Nechvatal render obvious coding the first coded information using information associated with the at least one party to the transaction to derive second coded information relevant to the transaction. <u>See</u> Diffie Declaration at ¶ 39.</p> |
| <p>[46preA] In a multi-party transaction system, a method for securing information relevant to a transaction, the transaction including a first party and a second party,</p> | <p>As explained previously with respect to claim 35, Hellman, X.509, and Nechvatal render obvious, in a multi-party transaction system, a method for securing information relevant to a transaction, the transaction including a first party and a second party, wherein a credential is previously issued to at least one of the first party and the second party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN). <u>See</u> [35preA]; <u>see also</u> [20preA].</p> |

| | |
|---|---|
| <p>[46preB] wherein a credential is previously issued to at least one of the first party and the second party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the method comprising:</p> | <p>As explained previously with respect to claim 35, Hellman, X.509, and Nechvatal render obvious a credential that is previously issued to at least one of the first party and the second party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN). <u>See [35preA]; see also [20preB].</u></p> |
| <p>[46A] creating the VAN by coding credential information with a secret key of the credential issuing entity;</p> | <p>As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal describe creating the VAN by coding credential information with a secret key of the credential issuing entity. <u>See [20A].</u></p> |
| <p>[46B] authenticating at least one of the first and second parties by using the VAN; and</p> | <p>As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious authenticating at least one of the parties by using the VAN. <u>See [20B].</u> As such, Hellman, X.509, and Nechvatal render obvious authenticating at least one of the first and second parties by using the VAN.</p> |
| <p>[46G] coding the information relevant to the transaction with information associated with the first party to derive coded information relevant to the transaction,</p> | <p>As explained previously with respect to claim 35, Hellman, X.509, and Nechvatal render obvious coding the information relevant to the transaction with first information associated with the first party to derive first coded information. <u>See [35G].</u> As such, Hellman, X.509, and Nechvatal render obvious coding the information relevant to the transaction with information associated with the first party to derive coded information relevant to the transaction.</p> |

| | |
|--|---|
| <p>[461] wherein the information relevant to the transaction includes information associated with the second party.</p> | <p>As shown by the following two examples, Hellman discloses that the information relevant to the transaction includes information associated with the second party.</p> <p><u>Example I</u></p> <p>Hellman discloses that plaintext P (“the information relevant to the transaction”) includes information associated with the second party. In more detail, and as explained previously with reference to claim 20, Hellman describes a cryptographic system and method that can be used to secure information relevant to a transaction, a plaintext message P that is to be communicated in a transaction between a first party 11 and a second party 12. <u>See [20A]</u>; <u>see also</u> Hellman at 3:47-64; 4:1-5:3; Diffie Declaration at ¶¶ 37-39. At least because the plaintext message P of Hellman is to be communicated by the first party 11 to the second party 12, it includes information that is associated with the second party 12. Thus, Hellman, X.509, and Nechvatal render obvious that the information relevant to the transaction includes information associated with the second party.</p> <p><u>Example II</u></p> <p>Hellman discloses that signals q and a (“the information relevant to the transaction”) include information associated with the second party. <u>See</u> Hellman at 4:11-27. In more detail, Hellman describes accessing a private component X_1 and signals q and a from key source 25, and generating, by secure key generator 21, a public component Y_1 by coding q and a using X_1. <u>See</u> Hellman at 3:47-64; 4:1-5:3; Fig. 1; Diffie Declaration at ¶ 39. Hellman further describes that signals q and a are generated by party 11 and are communicated in a transaction between party 11 and party 12, and that private component X_1 is associated with party 11. Hellman at 4:11-17; Diffie Declaration at ¶ 39. At least because the signals q and a of Hellman are communicated by the first party 11 to the second party 12, the signals q and a include information that is associated with the second party 12. Thus, Hellman, X.509, and Nechvatal render obvious that the information relevant to the transaction includes information associated with the second party.</p> |
|--|---|

B. [GROUND 2] – Hellman, X.509, Nechvatal, and Davies render obvious Claims 20, 24, 27, 28, 32, 35, 38, and 46.

As noted above and explained in greater detail in the following Claim Chart, the features of claims 20, 24, 27, 28, 32, 35, 38, and 46 of the '541 patent are obvious in view of the combination of Hellman, X.509, Nechvatal, and Davies, rendering each of these claims unpatentable under 35 U.S.C. § 103(a).

A person of ordinary skill in the art at the time that Stambler filed his application would be motivated to combine Hellman with X.509, at least because Nechvatal describes the algorithm disclosed by Hellman and the framework disclosed by X.509 in detail at sections 2.2 and 5.3, respectively, and suggests their combination. Diffie Declaration at ¶ 47. In more detail, Nechvatal states, with reference to the algorithm described in Hellman, that “the underlying public-key cryptosystem [of Hellman] supports secrecy but not authentication . . . [and] [t]hus it may be desirable to augment a secrecy-providing system [such as Hellman] with one which provides authentication.” Nechvatal at § 2.2. Nechvatal then states that “[e]xamples of the latter will be given later,” and goes on to describe the “strong authentication” provided by the authentication framework disclosed by X.509. *Id.* at §§ 2.2, 5.3.

A person having ordinary skill in the art at the time that Stambler filed his application would be further motivated to combine Hellman, X.509, and Nechvatal with Davies, at least because Davies provides a detailed explanation of both public-key cryptography and certifi-

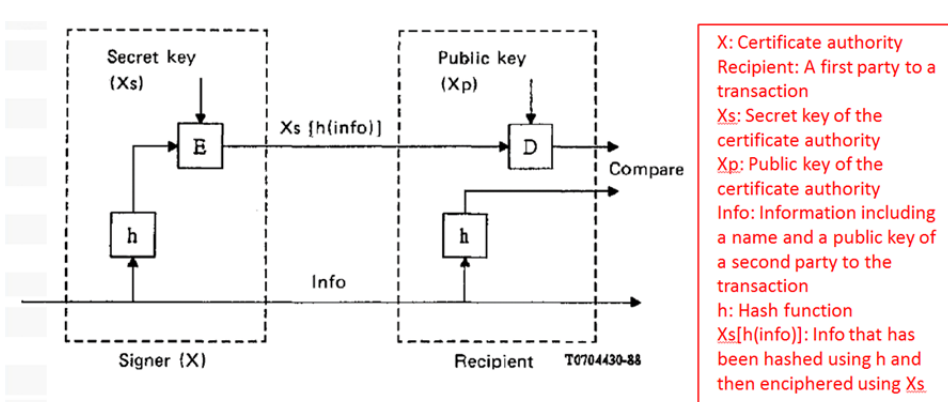
cate-based authentication systems, and for that reason usefully supplements the descriptions provided in each of Hellman, X.509, and Nechvatal. See Diffie Declaration at ¶ 48.

In more detail, as explained by Prof. Whitfield Diffie:

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 key management techniques taught by each of X.509, Nechvatal, and Davies.

Diffie Declaration at ¶ 73.

| Claim 20 | Hellman (U.S Patent No. 4,200,770) in view of X.509, Nechvatal, and Davies |
|---|---|
| [20preA] In a multi-party transaction system, a method for securing information relevant to a transaction by using information associated with at least two parties, | As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious the features of [20preA] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |
| [20preB] wherein a credential is previously issued to at least one of the parties by an entity authorized to issue a | As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious the features of [20preB] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |

| | |
|---|--|
| <p>credential, the credential including a variable authentication number (VAN), the method comprising:</p> | |
| <p>[20A] creating the VAN by coding credential information with a secret key of the credential issuing entity;</p> | <p>As shown by the following three examples, X.509 and Davies each disclose creating the VAN by coding credential information with a secret key of the credential issuing entity, and at least Davies discloses <u>re</u>creating the VAN by coding credential information with a secret key of the credential issuing entity. <u>See</u> Diffie Declaration at ¶ 71.</p> <p><u>Example I</u></p> <p>X.509 discloses creating a digital signature (“VAN”) by coding information contained in a digital certificate (“credential information”) with a secret key of a certification authority (“credential issuing entity”). In more detail, and as is depicted in the annotated version of X.509’s Fig. 6 provided below, the certification authority 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 certification authority, the hashed collection of information $h(\text{info})$, and (3) appending the signed hash $X_s[h(\text{info})]$ to the collection of information. X.509 at §§ 7-8; Nechvatal at § 5.3; Diffie Declaration at ¶ 42.</p> <div data-bbox="487 1365 1429 1764">  <p>The diagram illustrates the X.509 digital signature process. On the left, the 'Signer (X)' box contains a 'Secret key (X_s)' and a hash function 'h'. An arrow labeled 'Info' enters the 'h' box, and another arrow labeled '$X_s[h(\text{info})]$' exits the 'E' (encrypt) box. On the right, the 'Recipient' box contains a 'Public key (X_p)' and a hash function 'h'. An arrow labeled '$X_s[h(\text{info})]$' enters the 'D' (decrypt) box, and another arrow labeled 'Info' enters the 'h' box. A 'Compare' arrow points from the 'D' box to the right. A legend on the right lists: X: Certificate authority, Recipient: A first party to a transaction, X_s: Secret key of the certificate authority, X_p: Public key of the certificate authority, Info: Information including a name and a public key of a second party to the transaction, h: Hash function, $X_s[h(\text{info})]$: Info that has been hashed using h and then enciphered using X_s. The reference 'T0704430-88' is at the bottom right of the diagram.</p> </div> <p>FIGURE 6/X.509</p> <p>Thus, X.509 discloses creating a digital signature (“VAN”) by coding,</p> |

with a secret key of the certification authority (“credential issuing entity”), a collection of information that is included in a digital certificate (“credential information”). As such, for at least this reason, Hellman, X.509, Nechvatal, and Davies render obvious creating the VAN by coding credential information with a secret key of the credential issuing entity.

Example II

Davies discloses both creating and recreating a digital signature (“VAN”) included in a previously issued certificate (“credential”) by coding information contained in the certificate (“credential information”) with a secret key of a key registry (“credential issuing entity”); See Diffie Declaration at ¶¶ 49, 71.

Titled “Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer,” Davies provides a detailed explanation of public-key digital certificates that are issued by a key registry and that contain a digital signature of the key registry. See, e.g., Davies at 242, 276, 311, 322; Diffie Declaration at ¶ 48.

In more detail, Davies defines “digital signature” as “[a] number depending on all the bits of a message and also on a secret key,” and states that the “correctness [of the digital signature] can be verified by using a public key.” Davies at 363. Davies explains that “[t]he requirement of authenticity in public key distribution can be met by a public register of keys run by a trust-worthy organization” such that “when an entity generates public and private keys, it may register its public key with a key registry.” Id. at 322. The key registry issues certificates that contain the identity and public keys of registrants (“credential information”) signed using a secret key of the key registry. See, e.g., id. at 276-277 (“Suppose that a person P wishes to register a new key with the registry R... P must send to the registry the public key... receive in response the 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”); Diffie Declaration at ¶ 43.

Davies discloses that digitally signed certificates are previously issued in the context of describing that a public key is issued in a certif-

icate to the owner of the public key prior to the public key being used, the issued certificate including a digital signature of the key registry that is created using the key registry's secret key. Davies at 276-277 ("administration of the public key registry must be designed very carefully... registering new public keys... means 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"); see also id. at 363; Diffie Declaration at ¶ 49. For at least this reason, Davies teaches that a digital signature ("VAN") is created by coding information contained in a certificate ("credential information") with a secret key of the key registry ("entity authorized to issue a credential") and that the digital signature is included in the previously issued certificate.

Davies further discloses recreating the digital signatures contained in certificates as part of the process of key registry. See Id. at 276; Diffie Declaration at ¶ 71. 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. Davies at 276 ("During the temporary registration period . . . [the registrant] must send to the registry the public key, identifying data and a time variant quantity X. [The key registry] responds by returning all this information together with a digital signature, which forms a temporary certificate"); Diffie Declaration at ¶ 71. A second "effective certificate" that contains the same digital signature is issued by the key registry after the registration phase. Davies at 276-277 ("As soon as . . . registration is effective . . . [i]t is now possible to enquire for the value of the public key and receive in response the certificate containing the identity and public key value signed by R. This is the effective certificate and may be used as evidence of the value of the public key"); see also Diffie Declaration at ¶ 71.

Thus, for at least this reason, Davies discloses both creating a digital signature ("VAN") included in a previously issued certificate ("credential"), and recreating the digital signature by coding information contained in the certificate ("credential information") with a secret key of a key registry ("credential issuing entity").

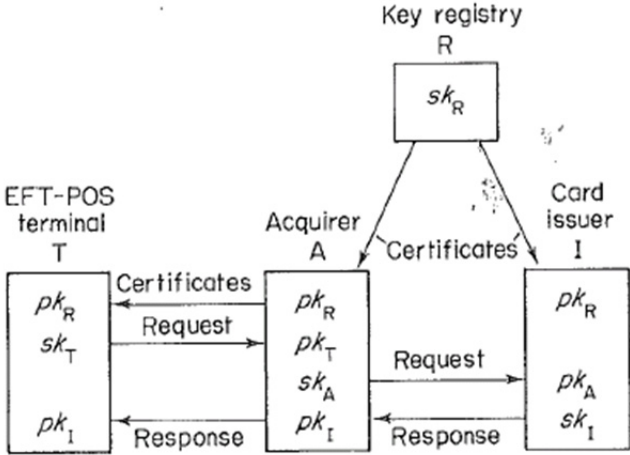
For at least this reason, Hellman, X.509, Nechvatal, and Davies ren-

der obvious creating the VAN by coding credential information with a secret key of the credential issuing entity.

Example III

Davies further discloses recreating the digital signatures in certificates in the context of electronic funds transfer at a point of sale terminal. Specifically, Davies discloses that, whenever an authentic public key is required for purposes of executing a transaction, it must be provided, in a digitally signed certificate, to the party interacting with the owner of the public key: “[w]hen . . . [a party] 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.” Davies at 322; Diffie Declaration at ¶ 70.

In more detail, and as illustrated in Figure 10.20 of Davies, which is reproduced below, Davies teaches that a key registry may issue certificates to an acquirer that are digitally signed with a secret key (sK_R) of the key registry. Davies at 322. When an authentic public key is needed at a terminal, the terminal may request the certificate containing the authentic public key from the acquirer, and the certificate containing the authentic public key may be received by the terminal from the acquirer. Id. Because received data is digitally recreated in the memory of a receiving device upon receipt, the digital signatures contained in previously issued certificates, which were initially created by coding certificate information with a secret key sK_R of the key registry, are recreated when they are received by terminals.

| | |
|---|--|
| |  <p>Fig. 10.20 Public key relationships for EFT-POS</p> <p>For at least this additional reason, Hellman, X.509, Nechvatal, and Davies render obvious creating the VAN by coding credential information with a secret key of the credential issuing entity.</p> |
| <p>[20B] authenticating at least one of the parties by using the VAN;</p> | <p>As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious the features of [20B]. For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious.</p> |
| <p>[20C] coding information associated with the at least two parties to generate a joint code; and</p> | <p>As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious the features of [20C]. For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious.</p> |
| <p>[20D] coding the information relevant to the transaction with the joint code to generate coded information relevant to the transaction.</p> | <p>As explained previously with respect to claim 20, Hellman, X.509, and Nechvatal render obvious the features of [20D]. For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious.</p> |
| <p>[24] The method of claim 20 wherein the information associated with the at least two parties used to generate</p> | <p>As explained previously with respect to claim 24, Hellman, X.509, and Nechvatal render obvious the features of [24]. For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious.</p> |

| | |
|--|---|
| the joint code comprises information associated with at least one present party and information associated with at least one absent party. | |
| [27] The method of claim 20 wherein the information relevant to the transaction comprises at least one information group which was previously coded to enable detection of a change in the content or structure of the information group. | As explained previously with respect to claim 27, Hellman, X.509, and Nechvatal render obvious the features of [27] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |
| [28preA] In a transaction system, a method for securing information relevant to a transaction, the transaction including at least one party, | As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [28preA] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |
| [28preB] wherein a credential is previously issued to the at least one party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the | As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [28preB] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |

| | |
|--|---|
| method comprising: | |
| [28A] creating the VAN by coding credential information with a secret key of the credential issuing entity; | As explained previously with respect to claim 20, Hellman, X.509, Nechvatal, and Davies render obvious creating the VAN by coding credential information with a secret key of the credential issuing entity. <u>See</u> [20A] . |
| [28B] authenticating the at least one of the party by using the VAN; | As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [28B] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |
| [28C] generating a joint code by coding first information accessed from a first one or more data storage means with second information associated with the at least one party to the transaction; and | As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [28C] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |
| [28D] coding the information relevant to the transaction with the joint code to generate coded information relevant to the transaction. | As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [28D] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |

| | |
|--|--|
| [32preA] A method for coding clear information by using information associated with at least one party, | As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [32preA] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |
| [32preB] wherein a credential is previously issued to the at least one party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the method comprising: | As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [32preB] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |
| [32A] creating the VAN by coding credential information with a secret key of the credential issuing entity; | As explained previously with respect to claim 20, Hellman, X.509, Nechvatal, and Davies render obvious creating the VAN by coding credential information with a secret key of the credential issuing entity. <u>See [20A]</u> . |
| [32B] authenticating the at least one of the party by using the VAN; | As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [32B] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |
| [32C] coding a first information group with a second information group to generate a third information group, at least one of the first and second information groups being associated with the at least one party; and | As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [32C] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |
| [32D] coding the | As explained previously, Hellman, X.509, and Nechvatal render obvi- |

| | |
|--|--|
| clear information with the third information group to generate coded information. | ous the features of [32D] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |
| [35preA] In a multi-party transaction system, a method for securing information relevant to a transaction, the transaction including a first party and a second party, | As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [35preA] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |
| [35preB] wherein a credential is previously issued to at least one of the first party and the second party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the method comprising: | As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [35preB] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |
| [35A] creating the VAN by coding credential information with a secret key of the credential issuing entity; | As explained previously with respect to claim 20, Hellman, X.509, Nechvatal, and Davies render obvious creating the VAN by coding credential information with a secret key of the credential issuing entity. <u>See</u> [20A] . |
| [35B] authenticating at least one of the first and second parties by using the VAN; | As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [35B] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |
| [35G] coding the information relevant | As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [35G] . For at least the reasons presented above, |

| | |
|--|--|
| to the transaction with first information associated with the first party to derive first coded information; and | Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |
| [35H] coding the first coded information with first information associated with the second party to derive second coded information relevant to the transaction. | As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [35H] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |
| [38preA] In a transaction system, a method for securing information relevant to a transaction, the transaction including at least one party, | As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [38preA] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |
| [38preB] wherein a credential is previously issued to the at least one party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the method comprising: | As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [38preB] . For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious. |
| [38A] creating the VAN by coding credential information with a secret key of the credential issuing entity; | As explained previously with respect to claim 20, Hellman, X.509, Nechvatal, and Davies render obvious creating the VAN by coding credential information with a secret key of the credential issuing entity. <u>See</u> [20A] . |

| | |
|--|--|
| <p>[38B] authenticating the at least one of the party by using the VAN;</p> | <p>As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [38B]. For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious.</p> |
| <p>[38G] coding information relevant to the transaction using information accessed from one or more data storage means to derive first coded information; and</p> | <p>As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [38G]. For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious.</p> |
| <p>[38H] coding the first coded information using information associated with the at least one party to the transaction to derive second coded information relevant to the transaction.</p> | <p>As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [38H]. For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious.</p> |
| <p>[46preA] In a multi-party transaction system, a method for securing information relevant to a transaction, the transaction including a first party and a second party,</p> | <p>As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [46preA]. For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious.</p> |

| | |
|---|--|
| <p>[46preB] wherein a credential is previously issued to at least one of the first party and the second party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the method comprising:</p> | <p>As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [46preB]. For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious.</p> |
| <p>[46A] creating the VAN by coding credential information with a secret key of the credential issuing entity;</p> | <p>As explained previously with respect to claim 20, Hellman, X.509, Nechvatal, and Davies describe creating the VAN by coding credential information with a secret key of the credential issuing entity. <u>See [20A]</u>.</p> |
| <p>[46B] authenticating at least one of the first and second parties by using the VAN; and</p> | <p>As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [46B]. For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious.</p> |
| <p>[46G] coding the information relevant to the transaction with information associated with the first party to derive coded information relevant to the transaction,</p> | <p>As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [46G]. For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious.</p> |
| <p>[46I] wherein the information relevant to the transaction includes information associated with the second party.</p> | <p>As explained previously, Hellman, X.509, and Nechvatal render obvious the features of [46I]. For at least the reasons presented above, Petitioner submits that Hellman, X.509, Nechvatal, and Davies render these features obvious.</p> |

VII. CONCLUSION

The cited prior art references identified in this Petition contain pertinent technological teachings (both cited and uncited), either explicitly or inherently disclosed, which were not previously considered in the manner presented herein, or relied upon on the record during original examination of the '541 patent. At least by virtue of disclosing the limitations that served as the basis for the Office's allowance of the claims at issue, the references relied upon herein should be considered important in determining patentability. In sum, these references provide new, non-cumulative technological teachings which indicate a reasonable likelihood of success as to Petitioner's claim that the IPR Claims of the '541 patent are not

patentable pursuant to the grounds presented in this Petition. Accordingly, Petitioner respectfully requests institution of *Inter Partes* Review for those claims of the '541 patent for each of the grounds presented herein.

Respectfully submitted,

/W. Karl Renner/

Dated: 6/11/2013

W. Karl Renner, Reg. No. 41,265
Fish & Richardson P.C.
P.O. Box 1022
Minneapolis, MN 55440-1022
T: 202-783-5070
F: 202-783-2331

/Thomas A. Rozylowicz/

Dated: 6/11/2013

Thomas A. Rozylowicz, Reg. No. 50,620
Fish & Richardson P.C.
P.O. Box 1022
Minneapolis, MN 55440-1022
T: 202-783-5070
F: 202-783-2331

(Trial No. IPR2013-00344)

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on June 11, 2013, a complete and entire copy of this Petition for *Inter Partes* Review, and all supporting exhibits, were provided via FedEx, costs prepaid, to the Patent Owner by serving the correspondence address of record as follows:

Lawrence R. Youst
Lawrence Youst PLLC
One Waterway Court
Suite 3B
The Woodlands, TX 77380

/Edward G. Faeth/
Edward G. Faeth
Fish & Richardson P.C.
3200 RBC Plaza
60 South Sixth Street
Minneapolis, MN 55402
(202) 626-6420