Trials@uspto.gov
Tel: 571-272-7822

Paper 32
Entered July 6, 2016

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MASTERCARD INTERNATIONAL INC.,
Petitioner,

v.

LEON STAMBLER,
Patent Owner.

Case CBM2015-00044
Patent 5,793,302

Before BRYAN F. MOORE, TRENTON A. WARD, and
PETER P. CHEN, *Administrative Patent Judges.*

CHEN, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
Covered Business Method Patent Review
35 U.S.C. § 328 and 37 C.F.R. § 42.73

I. INTRODUCTION

A. Background

MasterCard International Inc. ("Petitioner") filed a corrected petition requesting a review under the transitional program for covered business method patents, of claims 51, 53, 55, and 56 (the "challenged claims") of U.S. Patent 5,793,302 (Ex. 1001, "the '302 patent") pursuant to § 18 of the Leahy-Smith America Invents Act ("AIA"). Paper 7 ("Pet."). Leon Stambler ("Patent Owner") submitted a Preliminary Response under 37 C.F.R. § 42.207. Paper 9 ("Prelim. Resp.").

Pursuant to 35 U.S.C. ¶ 324, we instituted this trial on the following grounds (Paper 10, "Dec. to Inst."):

Reference[s]	**Basis**	**Claim(s) Challenged**
Davies[1]	§ 102	51 and 53
Davies and Meyer[2]	§ 103	51, 53, 55, and 56
Davies and Nechvatal[3]	§ 103	55

[1] D. W. Davies, SECURITY FOR COMPUTER NETWORKS: AN INTRODUCTION TO DATA SECURITY IN TELEPROCESSING AND ELECTRONIC FUNDS TRANSFER (2d ed. 1989) (Ex. 1004) ("Davies").

[2] C. H. Meyer, CRYPTOGRAPHY: A NEW DIMENSION IN COMPUTER DATA SECURITY – A GUIDE FOR THE DESIGN AND IMPLEMENTATION OF SECURE SYSTEMS (1982) (Ex. 1022) ("Meyer").

[3] J. Nechvatal, PUBLIC-KEY CRYPTOGRAPHY (NIST SPECIAL PUBLICATION 800-2) (April 1991) (Ex. 1005) ("Nechvatal").

Reference[s]	Basis	Claim(s) Challenged
Davies, Fischer,[4] and Piosenka[5]	§ 103	56

Subsequently, Patent Owner filed a Patent Owner's Response. Paper 16 ("PO Resp."). Petitioner filed a Reply to Patent Owner's Response. Paper 19 ("Pet. Reply"). Petitioner filed a Motion to Exclude Evidence (Paper 22, "Mot. Excl."), Patent Owner filed an Opposition to Petitioner's Motion to Exclude Evidence (Paper 25), and Petitioner filed a Reply thereto (Paper 26). An oral hearing was held on March 18, 2016. A transcript of the hearing is included in the record. Paper 29 ("Tr."). Pursuant to our request, the parties submitted additional briefing regarding the preamble of claim 51. Papers 30 ("Pet. Suppl. Br. re Preamble") and 31 ("PO Resp. re Preamble").

We have jurisdiction under 35 U.S.C. § 6(c). This Final Written Decision is issued pursuant to 35 U.S.C. § 328(a) and 37 C.F.R. § 42.73.

B. Related Proceedings

Petitioner indicates that the '302 patent is currently the subject of a co-pending district court proceeding, styled *Stambler v. MasterCard, Inc.*, No. 0:14-cv-60830 (S.D. Fla.). Pet. 2.

Additionally, we note that the Federal Reserve Banks previously filed two petitions for *inter partes* review of the '302 patent, the first petition in *Federal Reserve Banks v. Stambler*, Case IPR2013-00341 (PTAB June 11, 2013) (Paper 3), challenging claims 7, 9, 31, 33, 34, 41–43, 45–48 and 51–56 of the '302 patent, and the second petition in *Federal Reserve Banks v. Stambler*, Case IPR2013-

[4] U.S. Patent No. 4,868,877 (Ex. 1006) ("Fischer").

[5] U.S. Patent No. 4,993,068 (Ex. 1008) ("Piosenka").

00409 (PTAB June 12, 2013) (Paper 1), challenging claims 9, 28–30, 32, 35–38, 44, 49–50, and 89–90 of the '302 patent. The Board granted joint motions to terminate each of these proceedings on December 11, 2013. *See* IPR2013-00341, Paper 12; IPR2013-00409, Paper 11. Furthermore, on December 9, 2013, Fifth Third Bank filed a petition for *inter partes* review in *Fifth Third Bank v. Stambler*, Case IPR2014-00244 (PTAB Dec. 9, 2013) (Paper 1), challenging claims 7, 8, 31, 33, 34, 41–43, 45–48, and 51–56 of the '302 patent. On March 17, 2014, the Board granted a joint motion to terminate this proceeding. *See* IPR2014-00244, Paper 9. On April 25, 2014, Visa Inc. filed a petition for *inter partes* review in *Visa Inc. v. Stambler*, Case IPR2014-00694 (PTAB Apr. 25, 2014) (Paper 1), challenging claims 51, 53, 55, and 56. The Board denied institution. *See* IPR2014-00694, Paper 10.

Finally, Petitioner herein, MasterCard International Inc., filed a petition for covered business method patent review, in *MasterCard International Inc. v Stambler*, Case CBM2015-00013 (PTAB Oct. 24, 2014) (Paper 9), challenging claims 51, 53, 55, and 56. On April 20, 2015, the Board granted a joint motion to terminate the proceeding. *See* CBM2015-00013, Paper 9.

C. The '302 Patent

The '302 patent generally relates to a transaction system for authenticating a transaction, document, or record such that the information associated with at least one of the parties involved is coded to produce a joint code. Ex. 1001, 2:7–14. Additionally, the joint code then is used to code information relevant to the transaction, document, or record, to produce a Variable Authentication Number ("VAN"). *Id.* at 2:14–17. Thus, during subsequent stages of the transaction, only parties capable of reconstructing the joint code will be able to decode the VAN properly in order to re-derive the information. *Id.* at 2:20–24.

The joint code serves to authenticate the parties, and the comparison of the re-derived information against the information recorded on the document serves to authenticate the accuracy of that information. *Id.* at 2:24–26. The '302 patent describes that at the time of enrolling as a user of the system, each user selects a Personal Identification Number ("PIN"), which is secret and cannot be recovered from other information anywhere in the system. *Id.* at 2:31–36. In some embodiments described in the '302 patent, the joint code is created by requiring one participating user to provide a PIN and using the other party's non-secret identification code. *Id.* at 2:47–51.

Figure 7 of the '302 patent is reproduced below.

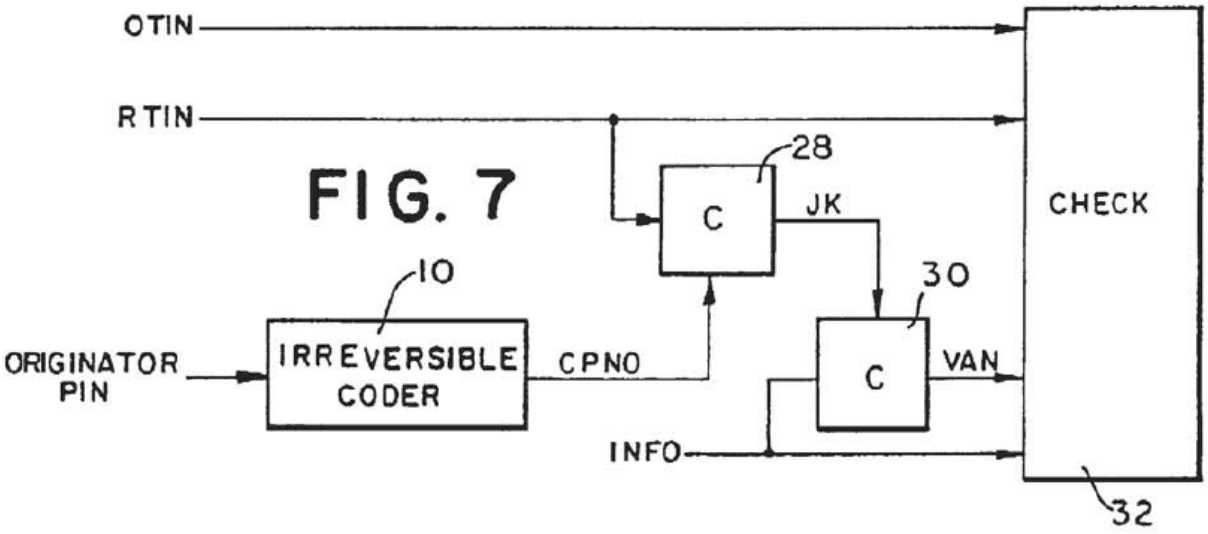


Figure 7 illustrates how an originator generates a check. *Id.* at 3:4–5. As shown in Figure 7, the originator enters a PIN at a terminal, and irreversible coder 10 converts the PIN to a Coded PIN ("CPNO"), which is applied as the key input to coder 28. *Id.* at 5:3–6. The data input to coder 28 is the Recipients Taxpayer Identification Number ("RTIN"), which has been read from the check, or accessed from computer memory, or entered by the originator. *Id.* at 5:6–9.

The data output of coder 28 is a joint key ("JK"), which is applied as a key input to coder 30. *Id.* at 5:9–10. The data input to coder 30 is the information ("INFO") to be authenticated, and the data output of coder 30 is the Variable Authentication Number ("VAN"). The VAN "codes the information to be authenticated, based upon information related to the recipient and information related to the originator." *Id.* at 5:15–22. The VAN and at least a portion of the information relevant to the transaction are included with the electrical signals associated with the electronic transaction. *Id.* at 5:30–33.

Figure 8A of the '302 patent is reproduced below.

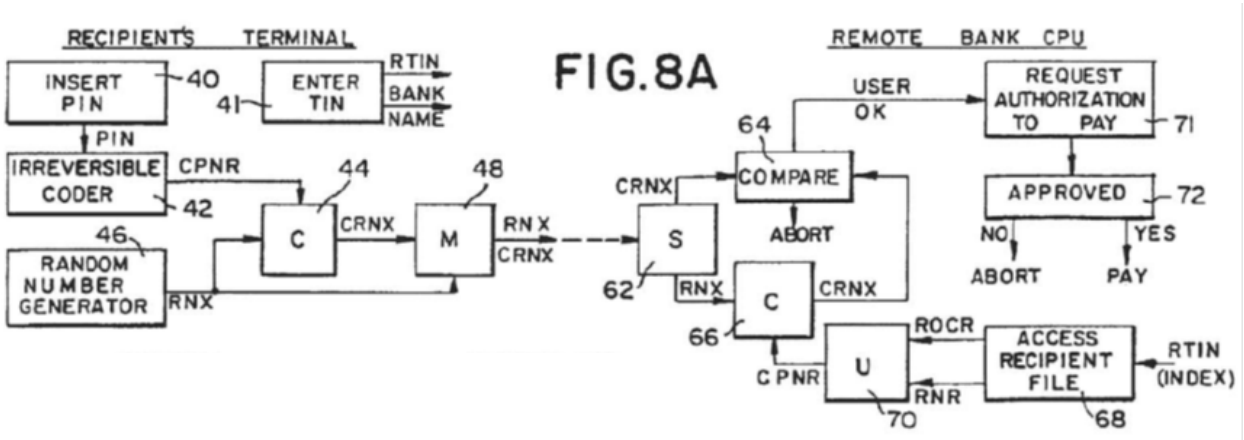


Figure 8A illustrates the authentication process at a terminal when the recipient presents the originator's check to be cashed. *Id.* at 5:55–57. As shown in Figure 8A above, at block 40 the recipient inserts a PIN, and at block 41, the recipient identifies a bank and enters a Taxpayer Identification Number ("TIN"). *Id.* at 5:55–64. Irreversible coder 42 processes the PIN to produce the Coded PIN ("CPNR"), which is applied as the key input to coder 44. *Id.* at 5:66–6:1.

A random number generator produces a random number ("RNX"), which is applied as the data input to coder 44. *Id.* at 6:1–3. Coder 44 then produces a Coded Random Number ("CRNX"), which is applied to mixer 48 along with RNX.

Id. at 6:3–5. The mixer signal along with the information read from the check is transmitted to the computer at the recipient's bank. *Id.* at 6:12–14.

At the recipient's bank, the output of mixer 48 is received at sorter 62, which separates CRNX and RNX. *Id.* at 6:22–23. Based on the RTIN, the bank's computer accesses the recipient's non-secret number and secret number, which are applied to uncoder 70 to generate the recipient's CPNR. *Id.* at 6:25–31. The CPNR is applied as the key input to coder 66, which reproduces CRNX. *Id.* at 6:31–33. If the generated CRNX matches the received CRNX in block 64, the recipient's bank communicates with originator's bank, conveying all information regarding the transaction and requesting authorization to pay in block 71. *Id.* at 6:37–45. Figure 8B of the '302 patent is reproduced below.

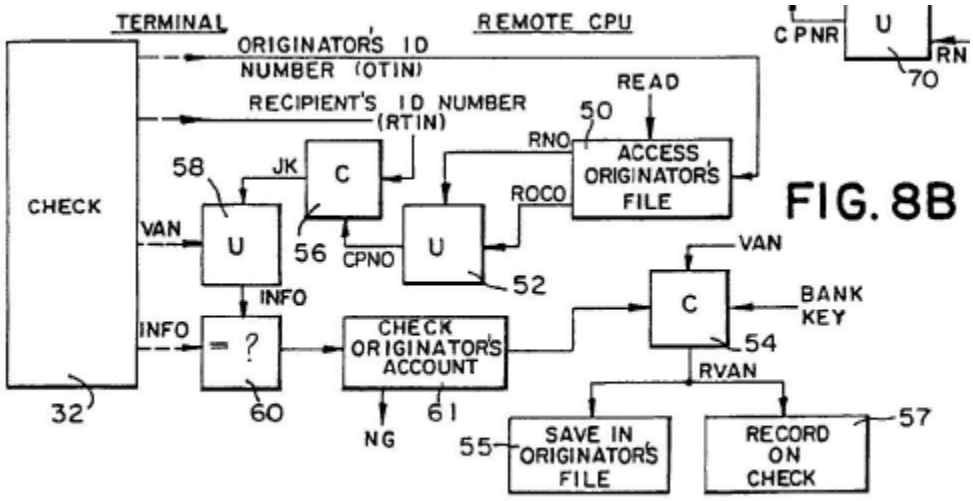


FIG. 8B

In Figure 8B, at the originator's bank, the recipient's TIN is used by coder 56 to produce joint key JK. *Id.* at 6:66–67. JK is input to uncoder 58 which receives the VAN from check 32 as its data input. *Id.* at 6:67–7:2. If the information on the check is not modified, INFO from check 32 should be reproduced by uncoder 58. *Id.* at 7:3–6. At block 60, a comparison is made

between INFO from check 32 and output of uncoder 58; alternatively, a new VAN may be generated from JK from coder 56, and compared with the VAN on the check. *Id.* at 7:12–15. In a favorable comparison, originator's bank accesses originator's account at block 61, and a redemption VAN is generated at coder 54, saved in the originator's file at block 55 and recorded on the check at block 57, and the originator's account is debited. *Id*. at 7:16–27. Figure 11 of the '302 patent is reproduced below.

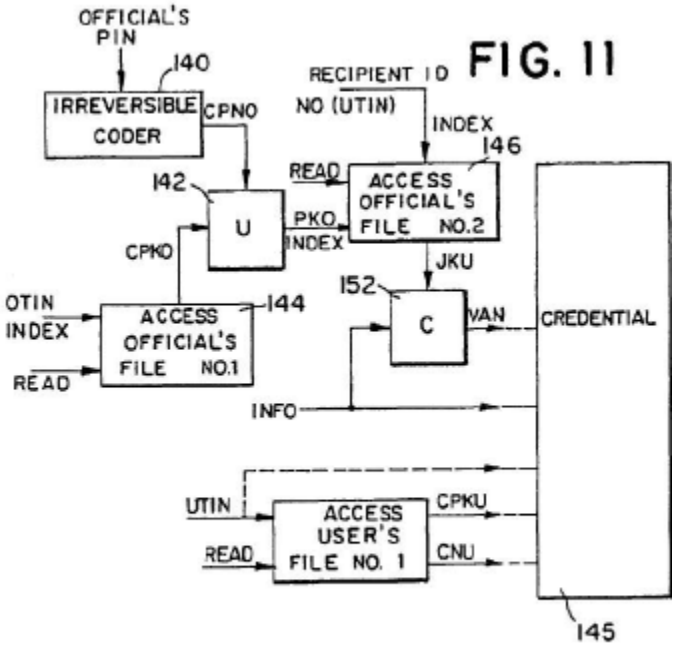


FIG. 11

Figure 11 is a block diagram illustrating the issuance of a credential after generation of a VAN. The specification states:

> The information INFO on the credential is applied as the data input to a coder 152 and [joint key] JKU is applied as the key input, whereby coder 152 codes the INFO to produce a VAN, which is recorded on the credential. After recording the VAN on the credential, the joint key, JKU, may be erased from the official's File 2, where it was stored (or held in escrow or in trust), until the credential was issued. Alternately,

> the authentic JKU may be replaced with a false or dummy JK for security purposes. This completes the issuance of the credential 145.

Id. at 11:65–12:8.

Independent claim 51, reproduced below, is illustrative of the claimed subject matter:

> 51. A method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party, a credential being previously issued to at least one of the parties by a trusted party, the information stored in the credential being non-secret, the method comprising:
>
> receiving funds transfer information, including at least information for identifying the account of the first party, and information for identifying the account of the second party, and a transfer amount;
>
> generating a variable authentication number (VAN) using at least a portion of the received funds transfer information;
>
> determining whether the at least a portion of the received funds transfer information is authentic by using the VAN and the credential information; and
>
> transferring funds from the account of the first party to the account of the second party if the at least a portion of the received funds transfer information and the VAN are determined to be authentic.

Ex. 1001, 33:15–36.

D. Claim Construction

Petitioner states that the ’302 patent has expired. Pet. 15. The Board’s review of the claims of an expired patent is similar to that of a district court’s review. *In re Rambus, Inc.*, 694 F.3d 42, 46 (Fed. Cir. 2012). The principle set forth by the court in *Phillips v. AWH Corp.*, 415 F.3d 1303, 1327 (Fed. Cir. 2005) (words of a claim “are generally given their ordinary and customary meaning” as understood by a person of ordinary skill in the art in question at the time of the

invention, construing to preserve validity in case of ambiguity) should be applied because the expired claims are not subject to amendment.

Petitioner cites to an exhibit (Ex. 1018) reciting proposed claim constructions of certain terms in the '302 patent advanced by parties during various litigation matters involving the '302 patent, and the claim constructions adopted by the Courts in those matters. *See* Pet. 16.

1. "variable authentication number (VAN)"

In the Decision to Institute, we construed the term "variable authentication number" or "VAN" 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." Dec. to Inst. 8. *See also* Case IPR2014-00694, slip op. at 8–9 (PTAB Oct. 31, 2014) (Paper 10). Patent Owner "does not challenge this construction." PO Resp. 16–17. Patent Owner asserts additional construction of the term is necessary for CBM standing issues, but does not elaborate further. PO Resp. 1.

Patent Owner also argues we incorrectly applied the broadest reasonable interpretation to the term in the Decision to Institute. PO Resp. 9. The Decision to Institute noted that our review of the claims of the expired '302 patent is similar to that of a district court's review, *In re Rambus, Inc*., 694 F.3d 42, 46 (Fed. Cir. 2012); *Phillips v. AWH Corp*., 415 F.3d 1303, 1327 (Fed. Cir. 2005), but inadvertently mentioned the broadest reasonable interpretation standard in construing this term. Dec. to Inst. 7–8. We reaffirm our agreement with Patent Owner that the Phillips framework is applied to the expired '302 patent. Our construction of "VAN" is the same under either claim construction standard. We reject Patent Owner's undeveloped argument regarding standing, and maintain the construction of VAN from the Decision to Institute, as the ordinary and customary meaning of the term: "a variable number resulting from a coding operation that can

be used in verifying the identity of a party or the integrity of information or both."

2. Sequence of method steps: receiving, generating

In the Decision to Institute, we agreed with Patent Owner and construed the sequence of method steps in independent claim 51 to mean that at least a portion of the receiving step must precede the generating step. Dec. to Inst. 8. *See also* Case IPR2014-00694, slip op. at 11–14 (PTAB Oct. 31, 2014) (Paper 10). We maintain that construction as the ordinary and customary meaning of the sequence of the receiving and generating method steps.

3. Sequence of method steps: issuance of credential

The preamble of claim 51 recites, "[a] method for authenticating the transfer of funds . . . a credential being previously issued to at least one of the parties by a trusted party . . . the method comprising . . ." Patent Owner contends that the preamble is a claim limitation, asserting that claim 51 requires issuance of a credential prior to the receiving step of the method for authenticating funds transfer. PO Resp. re Preamble, 3. Petitioner disputes Patent Owner's substantive arguments, and contends the preamble is not limiting. Pet. Reply 14–16; Pet. Suppl. Br. Re Preamble 1–3.

We recognize that preamble language that merely states the purpose or intended use of an invention is generally not treated as limiting the scope of the claim. *Boehringer Ingelheim Vetmedica, Inc. v. Schering-Plough Corp*., 320 F.3d 1339, 1345 (Fed. Cir. 2003). However, "a preamble limits the invention if it recites essential structure or steps, or if it is 'necessary to give life, meaning, and vitality' to the claim." *Catalina Mktg. Int'l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002) (citing *Pitney Bowes Inc. v. Hewlett-Packard Co.*, 182 F.3d 1298, 1305 (Fed. Cir. 1999). "The effect preamble language should be given can be resolved only on review of the entirety of the patent to gain an understanding of

what the inventors actually invented and intended to encompass by the claim." *Corning Glass Works v. Sumitomo Elec. U.S.A., Inc.*, 868 F.2d 1251, 1257 (Fed. Cir. 1989). When the limitations in the body of the claim rely upon or derive essential structure from the preamble elements, e.g., the preamble serves as an antecedent basis for limitations in the claim, then the preamble acts as a necessary component of the claimed invention and is limiting. *See Eaton Corp. v. Rockwell Int'l Corp.*, 323 F.3d 1332, 1339 (Fed. Cir. 2003).

In this case, the preamble of independent claim 51 recites "a credential being previously issued," and the limitations of the claim include "determining whether the at least a portion of the received funds transfer information is authentic by using the VAN and the credential information." Ex. 1001, 33:18–19, 33:29–31. Thus, the preamble's recitation of "a credential" is an antecedent basis for the recited "the credential information" in the "determining" step, and we determine that the preamble limits the scope of the challenged independent claim 51 and dependent claims 53, 55, and 56.

The specification further describes the credential being issued after the generation of the VAN. In particular, in describing Figure 11, which is a block diagram illustrating the issuance of a credential, the specification states:

> The information INFO on the credential is applied as the data input to a coder 152 and [joint key] JKU is applied as the key input, whereby coder 152 codes the INFO to produce a VAN, which is recorded on the credential. After recording the VAN on the credential, the joint key, JKU, may be erased from the official's File 2, where it was stored (or held in escrow or in trust), until the credential was issued. Alternately, the authentic JKU may be replaced with a false or dummy JK for security purposes. This completes the issuance of the credential 145.

Id. at 11:65–12:8. In light of this description in the specification of the VAN being produced before the issuance of the credential, we construe the

ordinary and customary meaning of the preamble's term, "credential being previously issued," to mean that the credential is issued after the step of generating a VAN and before the "determining" step of determining whether at least a portion of the funds transfer information is authentic.

4. Single entity performing all method steps

Patent Owner contends that we must construe the method steps of claim 51 to be performed by a single entity. PO Resp. 2, 7, 9–14, 31–33. Petitioner asserts otherwise. Pet. Reply 2–9. We agree with Petitioner and decline to construe claim 51 to require its method steps to be performed by a single entity. First, nothing in the express claim language so requires. Ex. 1001, 33:15–36. In addition, the Patent Owner relies on just a single sentence in the specification for its contention that the entirety of the method is performed at the originator's bank, namely, in describing Figure 8B, "[a]lternatively, the joint key JK from the coder 56 can be used to code the information (INFO) from the check to generate a new VAN." *Id*. at 7:12–14. This quoted sentence, however, does not state that it describes the preferred embodiment, to the contrary, the sentence expressly describes merely an "alternative" embodiment. We agree with Petitioner that claim interpretation should not elevate an alternative embodiment over a preferred embodiment illustrated in the figures and described in the specification. *See* Pet. Reply 3–6. Moreover, "a particular embodiment appearing in the written description may not be read into a claim when the claim language is broader than the embodiment." *Superguide Corp. v. DirecTV Enterprises, Inc*., 358 F.3d 870, 875 (Fed. Cir. 2004).

Patent Owner also cites the deposition testimony of Petitioner's declarant, Mr. Whitfield Diffie, asserting he "conceded that the preferred embodiment's instance of claim 51 (Figure 8B, where a new VAN is generated) shows only one entity performing all of the steps." PO Resp. 31, 2 (citing Ex. 2005, at 18:20–22),

7 (citing Ex. 2005, at 19:7–20:15). This is incorrect for at least two reasons.

First, contrary to Patent Owner's assertion, the '302 patent does not describe Figure 8B as depicting "the preferred embodiment." Rather, the '302 patent states that "FIGS. 6-8 are functional block diagrams illustrating a check transaction in accordance with a first embodiment of the present invention." Ex. 1001, 3:1–3. The '302 patent also refers to "preferred embodiments" in the plural form (Ex. 1001, 2:58–62, 3:27–31, 24:30–35), and describes other figures as illustrating a second embodiment, and other "alternate" embodiments. *Id.* at 3:7–26. *See also* PO Resp. 2 (describing "the embodiments of FIGS. 6-8").

Second, the snippets of Mr. Diffie's testimony cited by Patent Owner are incomplete. For fuller context, Mr. Diffie testified as follows:

> Q. Okay. So in what we've just seen at figure 8B, would you agree that the originator bank in the described embodiment performed all four of those steps?
> MR. WILLIAMS: Objection to form.
> THE WITNESS: I need a moment.
> MR. WILLIAMS: I'll also object as outside the scope, but I'll permit the witness to answer.
> THE WITNESS: It appears to me that all four of those steps are performed in figure 8B that we've just been looking at in Stambler's embodiment.
> BY MR. GREENSPOON:
> Q. So in the '302 patent, in the embodiment we just walked through, all steps of the authentication activity are performed by the originator bank, one entity?
> MR. WILLIAMS: Objection to form.
> THE WITNESS: If that's his only embodiment, it appears to me that in his embodiment, that is true.
> BY MR. GREENSPOON: Q. In your understanding and review of the '302 patent, did you identify any disclosure of any way that the '302 patent describes dividing up those steps so that different actors play that role or that different actors perform the respective acts?
> MR. WILLIAMS: Objection to form. Hang on a second. Objection to form and outside the scope.

> THE WITNESS: It appears to me that claim 51 could be satisfied that way, but that there is no requirement in claim 51 that the steps all be performed by the same entity.

Ex. 2005 at 18:12–19:17. Accordingly, Mr. Diffie qualified his response by saying, "[i]f that's [the] only embodiment," and then stated that claim 51 could indeed be performed by more than one entity, and that the claim did not require one entity to perform all the recited steps. *See also* Tr. 91:16–23. We are not persuaded by any of the other arguments made by Patent Owner for its proposed single-entity construction, and decline to construe the steps of claim 51 as being performed only by a single entity.

5. Credential

Patent Owner proposes that "credential" means, "a document or information obtained from a trusted source that is transferred or presented for purposes of determining the identity of a party." PO Resp. 14–16. According to Patent Owner, it is "willing to move forward under" a similar construction proposed by Petitioner in CBM2013-00013, namely, "a document or information obtained from a trusted source that is transferred or presented to establish the identity of a party." *Id*. at 16. We therefore construe the ordinary and customary meaning of "credential" to be, "a document or information obtained from a trusted source that is transferred or presented to establish the identity of a party."

We determine that no explicit construction is necessary for the other terms proposed by Patent Owner, or for any other terms in the challenged claims.

E. Principles of Law

To prevail in challenging Patent Owner's claims, Petitioner must demonstrate by a preponderance of the evidence that the claims are unpatentable. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d). A claim is unpatentable under 35 U.S.C.

§ 102 if a single prior art reference either expressly or inherently discloses every limitation of the claim. *Orion IP, LLC v. Hyundai Motor Am.*, 605 F.3d 967, 975 (Fed. Cir. 2010).

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time of the invention to a person having ordinary skill in the art. *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

F. Level of Ordinary Skill in the Art

Petitioner's proposal for the level of ordinary skill in the art is "at least a bachelors degree in computer programming and two years' experience as a programmer or developer in the field of computer science, with a working understanding of cryptographic operations for transforming original input into a coded output using a known algorithm." Pet. 14–15. Patent Owner has proposed similarly, that one of ordinary skill in the art would possess "(1) undergraduate education in mathematics, physics, computer science, electrical engineering or similar technical subject; and (2) either postgraduate education in networking, cryptography, or other discipline encompassing information theory, or equivalent experience with applications involving communication of financial, military, medical or similarly sensitive data over secure and non-secure networks." Prelim. Resp. 30–31.

We determine that an express definition of the level of ordinary skill is not required. The level of ordinary skill in the art can be reflected in the cited prior art references. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) ("[T]he absence of specific findings on the level of skill in the art does not give rise to reversible error 'where the prior art itself reflects an appropriate level and a need for testimony is not shown.'") (internal quotations omitted); *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995). Therefore, we find the level of ordinary skill in the art to be reflected in the cited references.

II. ANALYSIS

A. Covered Business Method Patent

Section 18 of the AIA provides for the creation of a transitional program for reviewing covered business method patents. A "covered business method patent" is a patent that "claims a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service, except that the term does not include patents for technological inventions." AIA § 18(d)(1); *see* 37 C.F.R. § 42.301(a). A patent need have only one claim directed to a covered business method to be eligible for review. *See* Transitional Program for Covered Business Method Patents—Definitions of Covered Business Method Patent and Technological Invention; Final Rule, 77 Fed. Reg. 48,734, 48,736 (Aug. 14, 2012) ("CBM Rules") (Comment 8).

1. Financial Product or Service

Petitioner asserts that:

> In general, the Challenged Claims recite methods of facilitating the exchange of money from one financial account to another. Patent Owner has sued a number of financial institutions. By way of example,

> Challenged Claims 51, 53, 55 and 56 each recite "a method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party." There can be no question that the process of transferring funds between accounts is "financial in nature," and that authentication of such a transfer is at least "incidental to a financial activity."

Pet. 5. Patent Owner argues that the challenged "claims are directed to authenticating the parties and the instrument of the transaction." Prelim. Resp. 18. Patent Owner's argument ignores the plain language of the claims, including, among other limitations, the recitations of "a method for authenticating the *transfer of funds*." Ex. 1001, claim 51 (emphasis added). We are persuaded that a preponderance of the evidence shows that at least claim 51 of the '302 Patent encompasses a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service. We determine that the '302 patent includes at least one claim that meets the financial in nature requirement of § 18(d)(1) of the AIA.

2. Exclusion for Technological Inventions

Petitioner asserts that the challenged claims do not fall within § 18(d)(1)'s exclusion for "technological inventions." Pet. 6–10. In particular, Petitioner argues that the '302 claims do not recite a technological feature that is novel and unobvious, and do not solve a technical problem using a technical solution. *Id*. Petitioner asserts that the '302 patent recites methods of facilitating and authenticating the exchange of money from one financial account to another. Pet. 5. Petitioner states, "the '302 patent makes clear that it utilizes nothing more than conventional elements to perform its authentication task." Pet. 7. In addition, the '302 patent specifies that the asserted novelty of the invention is not in any specific improvement of software or hardware, but in the method of authenticating

documents and "the individuals who are involved with them or responsible for them." Ex. 1001, 1:17–20. For example, the '302 patent states that "[t]here are many times in our daily lives when the need arises for highly secure transactions" and "[a] pressing need still exists for business transaction, document processing and record access systems which can assure the identity of the parties and the accuracy of the information involved in the transaction" (*id.* at 1:24–25, 1:50–54).

The '302 patent further states that the "functional building blocks utilized in the preferred embodiments . . . are conventional building blocks," while acknowledging that the "[a]lthough preferred embodiments of the invention have been disclosed for illustrative purposes, those skilled in the art will appreciate that many additions, modifications, and substitutions are possible without departing from the scope or spirit of the invention" (*id.* at 3:29–32, 24:31–34). Thus, we determine that the claims are merely the recitation of a combination of known technologies, which indicates that it is not a patent for a technological invention. *See* Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,764 (Aug. 14, 2012).

Patent Owner argues that the claims are directed toward solving the technological problem of verifying the identity and securing the interests of parties to multi-party transactions, and in particular, absent parties to a transaction. Prelim. Resp. 26–27. We are not persuaded by this argument because, as Petitioner argues, the problem being solved by the claims is a business problem—authentication of individuals and information in financial transactions. Pet. 5–10. Indeed, Patent Owner elsewhere concedes that the challenged "claims are directed to authenticating the parties and the instrument of the transaction." Prelim. Resp. 18. Thus, we are persuaded by Petitioner that a preponderance of the

evidence shows that the challenged claims do not recite a technological invention and are eligible for a covered business method patent review.

3. Conclusion

In view of the foregoing, we are persuaded by a preponderance of the evidence that the '302 patent is a covered business method patent under AIA § 18(d)(1), and is eligible for review using the transitional covered business method patent program.

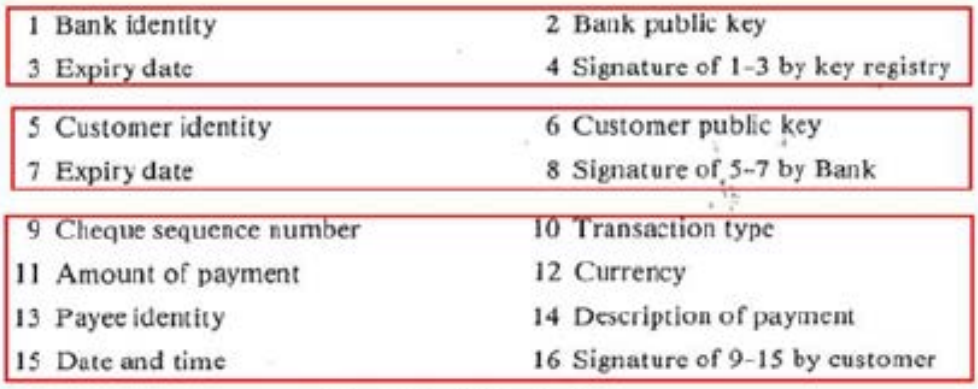
B. Proposed Anticipation by Davies

Petitioner argues that claims 51 and 53 are anticipated by Davies. Pet. 24–35; Pet. Reply 11–20. Patent Owner disputes Petitioner's position, arguing that Davies fails to anticipate all the elements required by the challenged claims. PO Resp. 28–47. We have reviewed the Petition, the Patent Owner's Response, and Petitioner's Reply, as well as the relevant evidence discussed in those papers and other record papers. As described in further detail below, we determine the record supports Petitioner's contentions and adopt Petitioner's contentions discussed below as our own. For reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that that claims 51 and 53 are unpatentable as anticipated by Davies.

1. Overview of Davies (Ex. 1004)

Davies is a 1989 textbook titled, "Security for Computer Networks," and it provides an introduction to data security in teleprocessing and electronic funds transfer. Ex. 1004, 4. Chapter 10 of Davies is titled, "Electronic Funds Transfer and the Intelligent Token" and describes various electronic methods of payment. *Id*. at 282. Section 10.6 of Davies is titled, "Payments by Signed Messages" and describes the implementation of an electronic cheque by using "a digital signature facility with a key registry to authenticate public keys." *Id*. at 328. Davies

discloses that, to allow the content of the electronic cheque to be validated, it should contain the items shown in Figure 10.22 below (as annotated by Petitioner):



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

Fig. 10.22 Electronic cheque

As shown above in Figure 10.22, Davies discloses that its electronic cheque provides three sections of data. *Id*. at 328. The first is a certificate by the key registry which authenticates the bank's public key and provides an expiry date. *Id*. The second section of the electronic cheque contains the customer identity and his public key, signed by the bank and verifiable using the public key provided in the first section. *Id*. The third section provides the payment information of the cheque. *Id*. at 329. Furthermore, the "final signature by the customer, covers all the variable information in the cheque." *Id*.

Davies also discloses that private customers of the bank can carry an intelligent token or smart card to function as an electronic chequebook. *Id*. ("[f]unctioning as an electronic chequebook, the private customer's token can record the transaction[s] it makes and list them for its holders at any convenient terminal."). Furthermore, Davies discloses that a terminal can be used to generate a cheque, sign it with the aid of the token, and send it to the beneficiary. *Id*.

Davies further discloses that the "same intelligent token which provides an electronic cheque between individuals can . . . also 'cash a cheque' at an ATM

[automatic teller machine] with on-line verification." *Id.* at 330. Figure 10.23 of Davies is reproduced below.

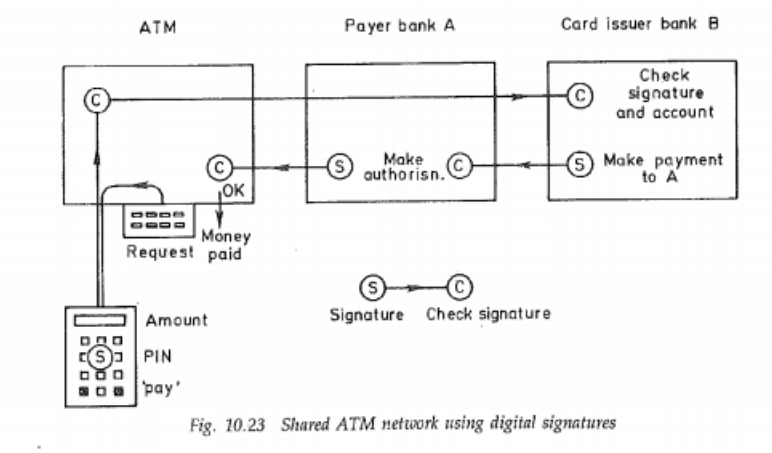


Fig. 10.23 Shared ATM network using digital signatures

Figure 10.23 illustrates a shared ATM network using digital signatures. *Id.* at 331. Petitioner quotes Davies' description of Figure 10.23:

> Figure 10.23 shows how this works in a shared ATM network. The customer's request is formed into a message and presented to the token. Here it is signed and returned to the ATM. The ATM checks the signature to avoid passing ineffective messages into the system. If it is correct, the 'cheque' passes via the payer bank, A, to the card issuer bank, B. Here the signature is checked and the customer's account examined and. if everything is in order, debited. A payment message signed by B is sent to A. The message and its signature are checked and if all is well an authorization goes to the ATM to release the money.

Pet. 18–19; *see* Pet. 28–29; Ex. 1004, 330–31.

2. Analysis of Asserted Ground of Anticipation by Davies

Petitioner argues that claims 51 and 53 are anticipated by Davies. Pet. 24–35. With respect to claim 51, Petitioner contends that Davies discloses the transfer of funds from an account associated with a first party, to an account associated with a second party. Pet. 24–25. Furthermore, Petitioner contends that Davies discloses a credential containing non-secret information by disclosing a "bank's public key" and "a certificate by the key registry which authenticates the bank's

public key." Pet. 26 (citing Ex. 1004, 328). Additionally, Petitioner contends that Davies discloses the claimed "receiving funds transfer information" by disclosing that an electronic check provides the identity of the customer, the payee and the payment amount ('transfer amount')," and that at the ATM, the customer's request is "formed into a message and presented to the token." Pet. 28–29 (citing Ex. 1004, 328–29, Figs. 10.22, 10.23). As to the claimed step of "generating a variable authentication number (VAN) using a portion of the received funds transfer information," Petitioner cites to Davies' disclosures that the "payment information . . . forms the third section of the cheque data" and the "final signature by the customer, covers all the variable information in the cheque," and that at the ATM, the message is "signed and returned to the ATM." Pet. 29–31 (citing Ex. 1004, 329).

Petitioner further contends that Davies discloses that at least a portion of the receiving step precedes the generating step, citing Figure 10.23 and Davies' disclosure that "the token both receives the funds transfer information ('the customer's request is formed into a message and presented to the token') and then, after receipt of that information, the token generates a VAN using at least a portion of that received funds transfer information ('[h]ere it is signed and returned to the ATM')." Pet. 18–19, 27–29. Pursuant to our construction of VAN, a digital signature can constitute 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." *See* Section I.D.1 above.

Finally, as to the claimed step of "transferring funds . . . if the at least a portion of the received funds transfer information and the VAN are determined to be authentic," Petitioner cites to Davies' disclosure that "the electronic cheque is transmitted . . . to the card issuer bank where the signature is checked" and the

accounts of customer and merchant can be updated if the signature is verified. Pet. 33–34 (citing Ex. 1004, 330).

Patent Owner raises several arguments why Davies does not anticipate claim 51. First, Patent Owner argues Davies does not disclose a single entity performing all four method steps. PO Resp. 31–33. We have, however, rejected Patent Owner's proposed construction requiring a single entity to perform all the method steps, *see* Section I.D.4 above.

Patent Owner also argues that Petitioner's use of Davies "conflate[s] different unrelated disclosures." PO Resp. 28, 31–32. Davies describes a "cheque" embodiment and an "ATM" embodiment, one or both of which are cited by Petitioner as disclosing all of claim 51's elements. Pet. 24–33; Ex. 1004, 325–31. In the Decision to Institute, we determined that the two embodiments were expressly and directly related, because Davies states, "[t]he same intelligent token which provides an electronic cheque . . . can also 'cash a cheque' at an ATM." Ex. 1004, 330. Davies further relates the two embodiments, stating that "for even wider use, the format of Figure 10.22 [titled, "Electronic cheque"] includes the transaction type which denotes a customer cheque, ATM request . . . and so forth." *Id*. at 331. We also agree with the additional contentions by Petitioner, *see* Pet. Reply 11–12, and find that Davies does not mix unrelated disclosures.

Patent Owner also argues Davies does not disclose the "receiving" step because it discloses a party, i.e., a bank customer, receiving information from itself. PO Resp. 34–36. Contrary to Patent Owner's argument, Petitioner asserts Davies' token, and not a customer, receives funds transfer information from a terminal, citing to Davies (e.g., "the customer's request is formed into a message and presented to the token," Ex. 1004, 330), and to the deposition testimony of Mr. Diffie ("the token receives the information wherever it gets it from . . . The

receiving and generating steps take place in the token"). Pet. Reply 14, citing Ex. 1004, 324–25, 327, 329, 330–31; Ex. 2005, 80:4–14, 82:3–25. We credit Mr. Diffie's testimony corroborating the disclosure of Davies and are persuaded by Petitioner's arguments on this issue.

Patent Owner further argues Davies fails to disclose the recited credential, or the credential being "previously issued" as recited in the preamble. PO Resp. 38–44. As construed herein, a credential is "a document or information obtained from a trusted source that is transferred or presented to establish the identity of a party." *See* section I.D.5 above. Petitioner contends Davies' credential is the blank, unpopulated check in Figure 10.22, in particular the customer "certificate" comprised of items 5, 6 (customer public key), 7, and 8. Pet. Reply 17; *see* Ex. 2005 (Diffie depo.) at 59:8–10, 78:15–20, 84:19–85:20. The information for the certificate, stored on Davies' token by the issuing bank (a "trusted party" as recited in claim 51) can be used to identify the signor of an electronic check. Pet. Reply 17–18; Tr. 85:15–86:10. We agree with Petitioner's contention that Davies discloses a credential.

Patent Owner's related assertion is Davies does not disclose its customer certificate being issued prior to the first, "receiving" step of the claimed method in which the preamble recites the "credential being previously issued." PO Resp. 36–38. We disagree, for two reasons. First, as we have construed, and as supported by the '302 patent's specification, the credential is not issued until after generation of the VAN. Ex. 1001, Fig. 11, 11:65–12:8. *See also* Pet. Reply 14–15. Accordingly, Davies need only disclose its customer certificate being issued prior to the "determining" step, where the credential is used with the VAN to determine authenticity of the funds transfer information. Second, the Petition describes that in Davies, the credential is issued when a public key (item 6 in Figure 10.22) is

issued in a certificate before the key is used. Pet. 25–27; Pet. Reply 15–16. Petitioner contends, "Davies teaches that the certificate containing the customer's identity and customer's public key are read by the terminal to form an electronic check message, which is then presented back to the token (including that customer's identity) to be signed." Pet. Reply 16. The ATM then determines the authenticity of the funds transfer information. Ex. 1004, 331. We agree that Davies' credential is "previously issued," prior to the determining step performed by the ATM.

Lastly, Patent Owner asserts Davies fails to disclose the recited "information for identifying the account of the second party." PO Resp. 44–47. Petitioner refutes this contention, arguing that Davies' electronic cheque embodiment discloses such second party information (concerning the party being paid), and that Davies' ATM embodiment does so as well, citing to the depositions of Petitioner's declarant, Mr. Diffie, and Patent Owner's declarant, Dr. Nielson. Pet. Reply 18–20, citing Ex. 2005, 71:16–72:13, Ex. 1023, 100:7–102:23. We agree with and are persuaded by Petitioner's arguments and evidence that Davies discloses this limitation, and as set forth above, the other limitations of claim 51. Petitioner has demonstrated by a preponderance of the evidence that claim 51 is unpatentable as anticipated by Davies.

For dependent claim 53, which recites that the funds transfer comprises a payment made by the first party to the second party (Ex. 1001, 33:49–51), Petitioner describes Davies' disclosures of funds transfer from a customer to a payee using an electronic check, and also a transfer of funds from "Ann" to "Bill." Pet. 24–35; Pet. Reply 22. Patent Owner makes no separate arguments as to claim 53. We are persuaded by Petitioner's arguments and evidence that Davies discloses the limitations of claim 53. Petitioner has demonstrated by a

preponderance of the evidence that claim 53 is unpatentable as anticipated by Davies.

C. Proposed Obviousness Over Davies and Meyer

Petitioner argues that claims 51, 53, 55, and 56 would have been obvious in view of Davies and Meyer. Pet. 50–61; Reply 20–25. Patent Owner disputes Petitioner's position, arguing that the cited references fail to teach or suggest all the elements required by the challenged claims. PO Resp. 47–53. We have reviewed the Petition, the Patent Owner's Response, and Petitioner's Reply, as well as the relevant evidence discussed in those papers and other record papers. As described in further detail below, we determine the record supports Petitioner's contentions and adopt Petitioner's contentions discussed below as our own. For reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 51, 53, 55, and 56 would have been obvious in view of Davies and Meyer.

1. Overview of Meyer (Ex. 1022)

Meyer is a textbook titled, "Cryptography: A New Dimension in Computer Data Security–A Guide for the Design and Implementation of Secure Systems," and describes encryption and authentication methods. For background, Meyer describes "a simple transaction in which cryptography is not employed," in which a customer with a personal account number with a banking institution uses a bank card and a PIN to pay a $35 grocery bill and receive $50 in cash. Ex. 1022, 477. Meyer generally describes techniques for applying cryptography to pin-based electronic funds transfer systems. *Id.* at 429–73. For example, Meyer describes using a "message authentication code" or "MAC" that is generated by using a technique "which produces cryptographic check digits which are appended to the message. . . . These digits . . . are generated by the originator, appended to the

transmitted message, and then checked by the recipient, who also holds the same secret key used in the generation process." *Id*. at 457; *see also id*. at 469. If the same MAC can be generated by the recipient, then the message was not modified and the request can be approved ("[s]hould anyone attempt to modify the message between the time the MAC is generated and the time it is checked, he would be detected."). *Id.*

Meyer also discloses, for purposes of authenticating a transfer of funds, the use of digital signatures ("DGS") based on public-key algorithms, and specifically, for example, the use of private and public key pairs, the latter of which is shared and used to authenticate transaction request messages signed by a sender with the associated private key. *Id*. at 569–76. Figure 11-44 of Meyer is reproduced below.

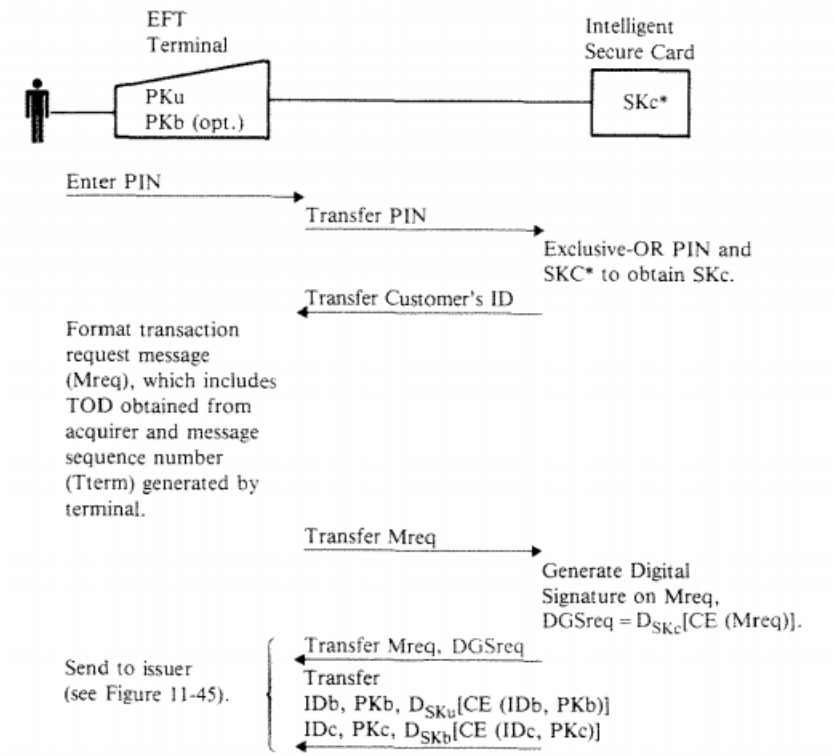


Figure 11-44. On-Line Use—EFT Terminal

Figure 11-44 depicts the use of a customer's secret card parameter SKc* to create the customer's private key, SKc, stored on an Intelligent Secure Card. Ex. 1022,

594, 596. The Intelligent Secure Card receives a transaction request message ("Mreq"), which includes transaction information, after which the Intelligent Secure Card generates digital signature DGS using the user's private key SKc. Ex. 1022, 597.

2. Analysis of Proposed Ground of Obviousness Over Davies and Meyer

Petitioner explains how Davies and Meyer teach or suggest the limitations of the four challenged claims. Pet. 50–66. For claims 51 and 53, Petitioner cites to Davies as in its arguments for proposed anticipation by Davies, and adds citations to Meyer for the generating step of the recited method, along with the sequence of the method whereby at least a portion of the receiving step occurs before the generating step. Pet. 50–63.

Patent Owner argues that "citations to Meyer do not overcome the gaps in Davies" and makes no other substantive arguments as to the teachings of Davies or Meyer as to claims 51 and 53. PO Resp. 48–49. We have determined there is a preponderance of evidence showing that Davies anticipates claims 51 and 53. *See* section II.B. In reviewing Petitioner's analysis and supporting evidence regarding the proposed ground of obviousness of claims 51 and 53, based on Davies in combination with the disclosure of Meyer, and Patent Owner's arguments and evidence in opposition, we also determine that Davies and Meyer teach or suggest the limitations of claims 51 and 53.

Claim 55 depends from claim 51, and recites the generation of the VAN "by using an error detection code derived by using at least a portion of the funds transfer information" (Ex. 1001, 33:55–57). Petitioner makes the same assertions for obviousness as in its argument for proposed anticipation by Davies, namely, that Davies teaches or suggests that the VAN is generated by an error detection

code ("Davies describes that the signature ("VAN") on a message M is generated by signing H(M) using the sender's secret key, where H(M) is obtained by applying a one-way function H to the message"). Pet. 63–64; *see also* Pet. 69 ("Davies . . . suggest[s] that the signature, i.e., VAN, is based on a one-way function").

Patent Owner makes no separate substantive arguments as to claim 55. As stated in the Decision to Institute, Petitioner's contentions were insufficient to show express disclosure by Davies of the "error detection code" required by claim 55. Petitioner argues for its proposed obviousness challenge, however, that Davies' disclosure that the signature ("VAN") on a message M is generated by signing "H(M)" using the sender's secret key, where H(M) is obtained by applying a one-way function H to the message M, thereby teaches or suggests the claimed "error detection code." Mr. Diffie's declaration states, "[i]t would have been understood by one of ordinary skill in the art, at the effective filing date of the '302 patent, that the one-way function H described in Davies is an example of a hash function." We are persuaded that Davies in combination with Meyer teaches or suggests claim 55's limitations, with Davies teaching or suggesting the error detection code in its disclosure of a one-way, or hash, function, and Davies and Meyer teaching or suggesting the elements of claim 51 from which claim 55 depends. *See* Pet. 63–64; Pet. Reply 20–23.

Claim 56 also is dependent from claim 51, and recites the use of a second VAN to secure credential information and denial of funds transfer if the credential information in the second VAN is not validated, in particular, "the credential information including information associated with the at least one party, and a second variable authentication number (VAN1), the VAN1 being used to secure at least a portion of the credential information to the at least one party, authentication

and the transfer of funds being denied to the at least one party if the at least a portion of the credential information cannot be secured to the at least one party by using the VAN1." Ex. 1001, 33:60–67. For dependent claim 56's limitations, Petitioner cites to Meyer's disclosure of a second VAN (the secret card parameter SKc*) and of sending a "negative response" to the terminal if the requested transaction cannot be honored. Pet. 64–66; Ex. 1022, 597.

Patent Owner asserts Meyer's secret SKc* cannot teach or suggest the recited VAN1 "since it cannot be used to verify or determine the association of some different nonsecret information with a particular party." PO Resp. 49–51. Petitioner contends Meyer teaches SKc* generates the customer's secret key SKc and also secures the non-secret public key credential PKc to the customer, citing to the testimony of Patent Owner's declarant. Pet. Reply 25, citing Ex. 1022, 596; Ex. 1023 at 119:12–120:6. We determine there exists sufficient evidence that Meyer teaches or suggests securing non-secret credential information.

Patent Owner also argues Petitioner has not provided sufficient analysis of a reason to combine Davies with Meyer. PO Resp. 51–53. Petitioner states that both references address similar issues and that combining Meyer with Davies would facilitate the predictable result of Davies token's generation of the VAN after receiving funds transfer information:

> [C]ombining Davies with Meyer demonstrates that all the elements at issue were known in the prior art, and their combination yielded nothing but predictable results. Both references address methods for facilitating financial transactions and for providing data security for electronic funds transfer. Davies' method uses "a digital signature facility with a key registry to authenticate public keys," and to approve transactions. Davies at 328-331. Meyer similarly discloses using a message authentication code, or equivalently a digital signature in the context of public-key algorithms, to approve or disapprove transaction requests. Meyer at 457-58, 469 and 590. Applying the Meyer process of having

> an originator generate MACs after receiving transaction information to Davies would have yielded predict[t]able results: using the Davies token to first receive the funds transfer information to then generate the VAN. *See KSR Int'l Co. v. Teleflex Inc*., 550 U.S. 398, 416 (2007) ("The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results."). Thus, these references in their similar purpose of dealing with financial transactions and services, and overlapping teachings, confirm a motivation to combine Davies and Meyer.

Pet. 22–23 (citing to Ex. 1020 ¶¶ 112–18); *see* Pet. 51; Pet. Reply 21–22. As Mr. Diffie testified at his deposition:

> Q. So you've made the point that in each case you have a reference that accomplishes similar functions and, therefore, that gives some weight to a reason for a person of skill in the art to combine them?
> A. No, they are in similar subject areas. I might even have said in conversation the same subject area, which is the use of cryptographic techniques to secure various kinds of communication and transactions on networks. The two books [Davies and Meyer] are similar in that respect.

Ex. 2005, 101:7–17. In addition, the relevant chapter of the Davies reference expressly cites to the Meyer reference, and to another article authored by Mr. Meyer and others. Ex. 1004, 301, 323, 339. We find that the citation by Davies to Meyer further supports Petitioner's contention that one of ordinary skill in the art would have been motivated to combine Meyer with Davies because of their similar subject areas, overlapping teachings, cross-referencing, and the predictable results yielded by their being combined. Petitioner has shown sufficiently a reason to combine Davies and Meyer, providing articulated reasoning supported by rational underpinnings for combining the references, and we adopt Petitioner's contentions as our own. *KSR*, 550 U.S. at 418 (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)) (internal quotation marks omitted). We conclude that Petitioner has

proved by a preponderance of the evidence that claims 51, 53, 55, and 56 are obvious over Davies and Meyer.

D. Claim 55: Proposed Obviousness Over Davies and Nechvatal

Petitioner argues that claim 55 would have been obvious in view of Davies and Nechvatal. Pet. 66–69; Pet. Reply 22–24. Patent Owner disputes Petitioner's position, arguing that the cited references fail to teach or suggest all the elements required by the challenged claims. PO Resp. 53–58. We have reviewed the Petition, the Patent Owner's Response, and Petitioner's Reply, as well as the relevant evidence discussed in those papers and other record papers. As described in further detail below, we determine the record supports Petitioner's contentions and adopt Petitioner's contentions discussed below as our own. For reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claim 55 would have been obvious in view of Davies and Nechvatal.

1. Overview of Nechvatal (Ex. 1005)

Nechvatal is a 1991 National Institute of Standards and Technology ("NIST") Special Publication titled, "Public-key Cryptography," and describes, among other things, the use of digital signatures and hash functions in public key cryptography. Ex. 1005, §§ 1–3. According to Nechvatal, usually it is not desirable to apply a signature directly to a long message. *Id.* § 3.2. Accordingly, Nechvatal discloses the use of hash function, *H,* to accept a variable size message, *M,* as input, to produce a fixed-size representation, *H(M),* as output. *Id*. Nechvatal discloses that, in general, *H(M)* will be much smaller than *M,* and, thus, a digital signature can be applied to *H(M)* in a relatively quick fashion. *Id*.

Nechvatal further discloses that the "hash function can also serve to detect modification of a message, independent of any connection with signatures," and, thereby, the hash function "can serve as a cryptographic checksum." *Id*.

Nechvatal expressly describes hash functions as error detection codes, stating, "hash functions are useful auxiliaries in this context, i.e., in validating the identity of a sender. They can also serve as cryptographic checksums (i.e., error-detecting codes), thereby validating the contents of a message." *Id*. at § 3.

2. Analysis of Proposed Ground of Obviousness Over Davies and Nechvatal

Petitioner argues that claim 55 would have been obvious over Davies and Nechvatal. Pet. 66–69. Specifically, Petitioner argues that Davies signatures may be generated by computing hash values on the transaction information as an intermediate step. *Id.* at 66. Furthermore, Petitioner relies upon Nechvatal for its disclosures regarding the use of hash functions to mitigate the effects of data expansion and lower bandwidth transmission that result from generating digital signatures. *Id*. Additionally, Petitioner proposes that Davies be combined with Nechvatal to allow the signing entity in Davies to condense the information *M* included in a certificate into a fixed size representation *H(M)* that is smaller than *M*, and sign *H(M)* in a relatively quick fashion, which would improve signing efficiency, as taught by Nechvatal. *Id*. at 66–67. Finally, Petitioner states that while Davies "suggests that the signature, i.e., VAN, is based on a one-way function, Nechvatal explicitly mentions that the one-way function is an error detection code . . . Nechvatal discloses that a signature ('VAN') is generated using a hash function, which is an error detection code." *Id.* at 69; Pet. Reply 23. *See* Ex. 1005 § 3.

Patent Owner argues Petitioner "does not assert a proper 'reason to combine.'" PO Resp. 53–58. Petitioner, however, explains that Nechvatal's hash functions improve signing efficiency and that it would be obvious for a person of ordinary skill in the art to combine the teachings of Davies "with Nechvatal to

implement an electronic funds transfer system in which the transactions are authenticated by digital signatures, as taught by Davies." Pet. 67, Pet. Reply 23; Ex. 1020 ¶¶ 135–36. As Mr. Diffie testified at his deposition:

> My notion has always been that one would, of course, look at Nechvatal because it's national standards guidance and, therefore, anybody working on the subject would look at Nechvatal. The -- the concept that these things were error detection was well known at the time and it is, I thought, jointly expressed by these two documents [Davies and Nechvatal] very nicely.

Ex. 2005, 29:23–30:5. We agree with and adopt Petitioner's arguments and evidence. In addition, while not argued by Petitioner, we note that Nechvatal cites to an article by Davies and Price, the authors of the Davies reference (Ex. 1005 § 4.3.2), and to another article by Davies (*id*. at References). The citation by Nechvatal to these articles further supports Petitioner's contention that one of ordinary skill in the art would have been motivated to combine Nechvatal with Davies. Lastly, we further agree with Petitioner that Davies does not teach away from the use of hash functions; to the contrary, Davies describes using a hash function to generate a signature. Ex. 1004, 260–61; *cf.* Pet. Reply 23, PO Resp. 54–58.

We are persuaded that Davies and Nechvatal teach or suggest the recited error detection code and related elements of dependent claim 55, and are satisfied that Petitioner's articulated reasoning to combining the references is supported by sufficient rational underpinnings. *See KSR*, 550 U.S. at 418. Based on the foregoing, Petitioner has demonstrated by a preponderance of the evidence that claim 55 is unpatentable as obvious over Davies and Nechvatal.

E. Claim 56: Asserted Obviousness Over Davies, Fischer, and Piosenka

Petitioner argues that claim 56 would have been obvious in view of Davies, Fischer, and Piosenka. Pet. 69–76; Reply 24–25. Patent Owner disputes Petitioner's position, arguing that the cited references fail to teach or suggest all the elements required by the challenged claims. PO Resp. 58–62. We have reviewed the Petition, the Patent Owner's Response, and Petitioner's Reply, as well as the relevant evidence discussed in those papers and other record papers. As described in further detail below, we determine the record supports Petitioner's contentions and adopt Petitioner's contentions discussed below as our own. For reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claim 56 would have been obvious in view of Davies, Fischer, and Piosenka.

1. Overview of Fischer (Ex. 1006)

Fischer is titled, "Public Key/Signature Cryptosystem with Enhanced Digital Signature Certification," and discloses a public key cryptographic system with a hierarchy of nested certifications and signatures. Ex. 1007, Abstract.
Figure 3 of Fischer is reproduced below.

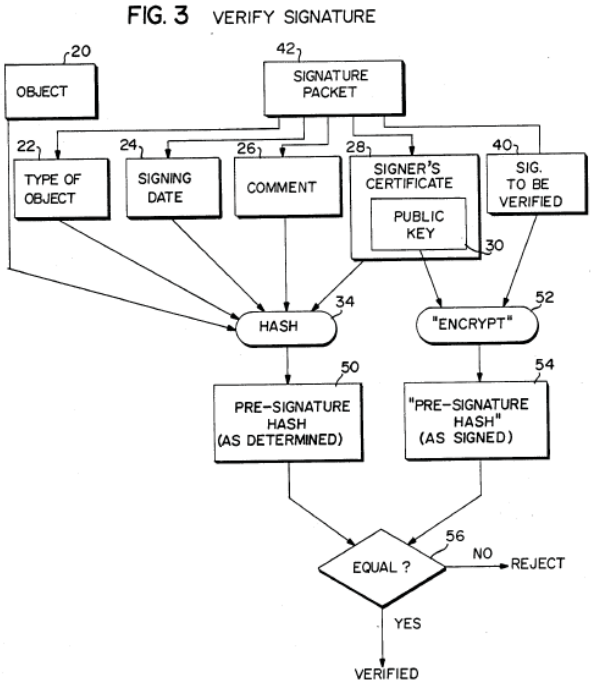


Figure 3 of Fischer illustrates how a recipient of a transmitted message, including signature packet 42, verifies the signature. *Id.* at 11:45–48. Fischer discloses that the recipient applies hashtag algorithm 34 to the signature packet and associated fields 22, 24, 26, and 28 to result in presignature hash 50. *Id.* at 11:48–53. Fischer discloses that the recipient then utilizes the public encrypting key transmitted with the signer's certificate, which certificate was transmitted with the signature packet, and performs encrypt (verification) operation 52 on the signature to be verified 40 to generate presignature hash 54. *Id.* at 11:54–58. The recipient then compares this value with the encryption (verification) of the signer's signature. *Id.* at 11:59–61.

Fischer discloses that, in accordance with the procedure detailed in Figure 3, the recipient ensures that each signature includes a corresponding validated certificate and that certificate information is verified based on the signature in the certificate. *Id.* at 17:33–47. Furthermore, if the certificate requires joint

signatures, then the recipient ensures that the necessary signatures are present. *Id.* at 17:40–41.

2. Overview of Piosenka (Ex. 1008)

Piosenka is titled "Unforgeable Personal Identification System," and discloses a system for identifying users at remote access sites. Ex. 1008, Abstract. Piosenka discloses that a user's credentials can be stored on a portable memory device from which the encrypted identification credentials can be read. *Id.* Piosenka discloses that, in its validation procedure, the memory medium is read, and the information is decrypted using the public decryption key. *Id.* at 11:14–17. Furthermore, Piosenka discloses a comparison of whether the calculated cryptographic signature matches the cryptographic signature recorded on the memory medium, and, if they do not match, the "request is denied and the process ended." *Id.* at 11:17–23, Fig. 3B.

3. Analysis of Proposed Obviousness Over Davies, Fischer, and Piosenka

Petitioner argues that claim 56 would have been obvious over Davies, Fischer, and Piosenka. Pet. 69–76.

Petitioner contends Davies teaches or suggests the recited second variable authentication number ("VAN1") that is used to secure at least a portion of the credential information to the at least one party that was previously issued a credential by a trusted party. Pet. 72, 74–75, citing Ex. 1004, 328–330, Fig. 10.22. Petitioner contends Fischer discloses a signature verification procedure that includes a hierarchy of certificates, all of which are examined for verification of certificate information based on the signature in the certificate. Pet. 70, 72, 75, citing Ex. 1006, 17:34–47; *see* Ex. 1020, ¶¶ 138–155. Furthermore, Petitioner cites to Piosenka's disclosure of denying a user's request for access if the signature

on the user's credential cannot be validated, as teaching the claimed "funds being denied to the at least one party if the at least a portion of the credential information cannot be secured to the at least one party by using the VAN1." Pet. 71–73, 75–76 (citing Ex. 1008, 6:41–42, 11:15–23).

Patent Owner does not identify any element of this dependent claim missing in the combination of Davies, Fischer, and Piosenka, and instead argues only that "the asserted 'reason to combine'" is insufficient. Pet. Reply 24; *see* PO Resp. 59–62. Petitioner, however, explains that for Davies and Fischer:

> A person of ordinary skill in the art would be motivated, at the time of the effective filing date of the '302 Patent, to combine the teachings of Davies with the teachings of Fischer for securing messages, end-to-end. . . . It would also be obvious for a person of ordinary skill in the art to augment the authenticated electronic funds transfer mechanisms using digital signatures, which is taught by Davies, with the counter signature of Fischer, as this would allow for the electronic funds transfer transaction using a chain of authority, where each higher level approves any commitment/signature made at a lower level.

Pet. 69–71 (citing Ex. 1020 ¶¶ 158–60, 171–74); Pet. Reply 24. Thus, Petitioner explains why one of ordinary skill would combine Davies and Fischer, namely, "as this would allow for electronic funds transfer transactions using a chain of authority." Pet. 70; Ex. 1020 ¶ 159. We also note, that, while not argued by Petitioner, a patent to Davies, the co-author of the Davies reference, is a cited reference in Fischer. Ex. 1006.

Petitioner explains that although Davies and Fischer do not explicitly describe what happens if an authentication is unsuccessful:

> [I]t would be common sense to one of ordinary skill in the art as of the priority date of the '302 Patent to have the system reject a transaction if the authentication was unsuccessful. Nevertheless, this rejection is explicitly disclosed by Piosenka, who describes that a user's request for access is denied if the signature on the user's credential cannot be

> validated. A person of ordinary skill in the art would be motivated, at the time of filing the application to which the '302 Patent claims priority, to augment the verification of message signatures and public keys, as taught by the combination of Davies and Fischer, with the denial of request upon failure to verify the user's credential, as taught by Piosenka.

Pet. 71 (citing Ex. 1020 ¶¶ 171–74); Pet. Reply 24. Mr. Diffie states that "combining Fischer with Piosenka would allow different identification systems in Piosenka to issue user credentials that include information on the respective identification systems, which are therefore more readily identifiable based on the credentials themselves." Ex. 1020 ¶ 176. We agree with and adopt the Petition's arguments and Mr. Diffie's testimony, in particular paragraphs 173–76 of his declaration, where he explains why one of ordinary skill would have combined the references.

We are persuaded that Davies, Fischer, and Piosenka teach or suggest the limitations of dependent claim 56, and that Petitioner has provided articulated reasoning supported by rational underpinnings for combining the references. We conclude that Petitioner has proved by a preponderance of the evidence that dependent claim 56 is obvious over Davies, Fischer, and Piosenka.

F. Petitioner's Motion to Exclude Evidence

Petitioner moves to exclude paragraphs 46, 48, 51, 55, 57, 60, 62–64, 84, 89, 90, 100, 101, 104, 108 and 113 of the Declaration of Patent Owner's declarant, Seth Nielson, Ph.D., regarding claim construction, on the ground that it was "not based on adequate 'knowledge, skill, experience, training, or education' and is not the 'product of reliable principles and methods,'" Mot. Excl. 1–7, citing Federal Rules of Evidence, Rule 702. Because we do not rely on Dr. Nielson's testimony

in arriving at our claim constructions set forth above, Petitioner's motion is dismissed as moot.

G. Patent Owner's Constitutional Challenge

Patent Owner argues this CBM trial is unconstitutional. PO Resp. 62–63. We agree with Petitioner that the constitutional challenge is without merit. Pet. Reply 2 n.5. *See MCM Portfolio LLC v. Hewlett Packard Co.*, 812 F.3d 1284 (Fed. Cir. 2015).

III. CONCLUSION

Based on the evidence and arguments, Petitioner has demonstrated by a preponderance of the evidence that claims 51 and 53 of the '302 patent are anticipated by Davies, claims 51, 53, 55, and 56 would have been obvious over Davies and Meyer, claim 55 would have been obvious over Davies and Nechvatal, and claim 56 would have been obvious over Davies, Fischer, and Piosenka.

IV. ORDER

For the reasons given, it is

ORDERED that Claims 51 and 53, 55, and 56 of U.S. Patent No. 5,793,302 have been shown to be unpatentable;

FURTHER ORDERED that Petitioner's Motion to Exclude is dismissed; and

FURTHER ORDERED that, because this is a final written decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

Robert Scheinfeld
Robert.scheinfeld@bakerbotts.com

Eliot Williams
Eliot.williams@bakerbotts.com

PATENT OWNER:

Robert Greenspoon
rpg@fg-law.com

John Fitzgerald
patents@rutan.com