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

Paper 10
Entered: October 31, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

VISA INC.,
Petitioner,

v.

LEON STAMBLER,
Patent Owner.

Case IPR2014-00694
Patent 5,793,302

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

WARD, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
37 C.F.R. § 42.108

I. INTRODUCTION

A. Background

VISA Inc. ("Petitioner") filed a petition to institute an *inter partes* review of claims 51, 53, and 55–56 (the "challenged claims") of U.S. Patent 5,793,302 (Ex. 1001, "the '302 patent") pursuant to 35 U.S.C. §§ 311–319. Paper 4 ("Pet."). Leon Stambler ("Patent Owner") submitted a Preliminary Response under 37 C.F.R. § 42.107(b). Paper 9 ("Prelim. Resp."). We have statutory authority under 35 U.S.C. § 314.

The standard for instituting an *inter partes* review is set forth in 35 U.S.C. § 314(a), which provides as follows:

> THRESHOLD – The Director may not authorize an inter partes review to be instituted unless the Director determines that the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.

The information presented in the Petition sets forth Petitioner's contentions of unpatentability of the challenged claims under 35 U.S.C. §§ 102 and/or 103 based on the following specific grounds (Pet. 16–57):

Reference[s]	**Basis**	**Claim(s) challenged**
Davies[1]	§ 102	51, 53, and 55

[1] D. W. Davies, et al., SECURITY FOR COMPUTER NETWORKS: AN INTRODUCTION TO DATA SECURITY IN TELEPROCESSING AND ELECTRONIC FUNDS TRANSFER -2ND EDITION, JOHN WILEY & SONS, LTD. (1989) (Ex. 1005) ("Davies").

Reference[s]	Basis	Claim(s) challenged
Davies and Nechvatal[2]	§ 103	51, 53, and 55
Davies, Fischer,[3] Piosenka[4]	§ 103	56

For the reasons described below, we determine that the present record fails to show a reasonable likelihood Petitioner will prevail in showing the unpatentability of any claim. Accordingly, we deny institution as to the challenged claims of the '302 patent.

B. Related Proceedings

Petitioner indicates that the '302 patent is currently the subject of co-pending federal district court litigation, styled *Stambler v. Visa Inc.*, Civ. Action No. 0:14-cv-60490-KMM (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*, IPR2013-00341, challenging claims 7, 8, 31, 33, 34, 41–43, 45–48 and 51–56 of the '302 patent and the second petition in *Federal Reserve Banks v. Stambler*, IPR2013-00409, challenging claims 9, 28–30, 32, 35–38, 44, 49–50, and 89–90 of the '302 patent. *See* IPR2013-00341, Paper 1; IPR2013-00409, Paper 1. 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*, IPR2014-

[2] James Nechvatal, PUBLIC-KEY CRYPTOGRAPHY (NIST SPECIAL PUBLICATION 800-2) (April 1991) (Ex. 1006) ("Nechvatal").

[3] U.S. Patent No. 4,868,877 (Ex. 1007) ("Fischer").

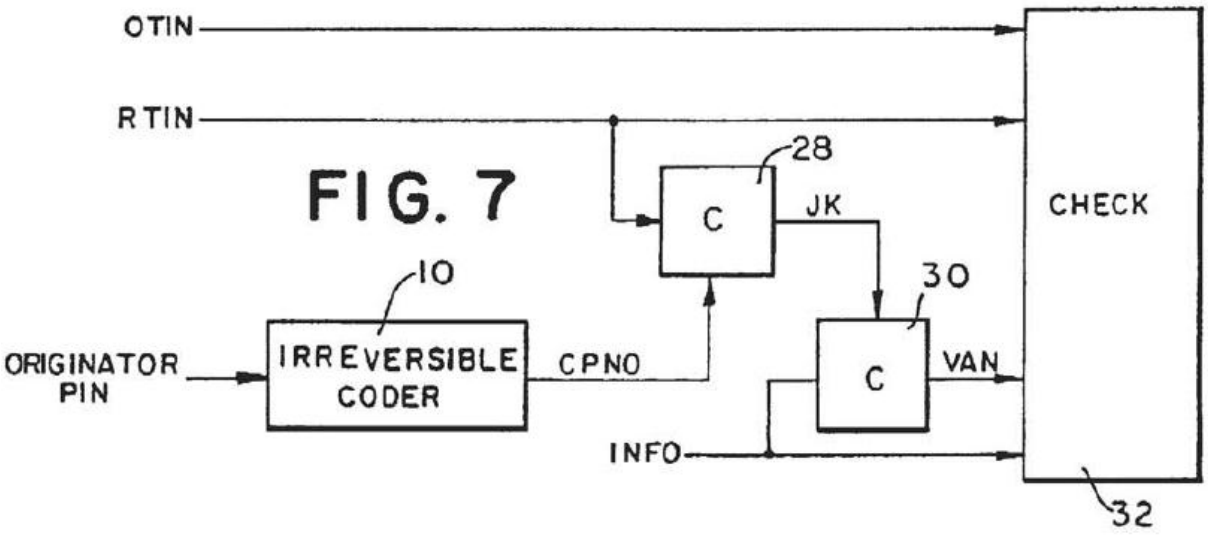
[4] U.S. Patent No. 4,993,068 (Ex. 1008) ("Piosenka").

00244, challenging claims 7, 8, 31, 33, 34, 41–43, 45–48, and 51–56 of the ’302 patent. *See* IPR2014-00244, Paper 1. On March 17, 2014, the Board granted a joint motion to terminate this proceeding. *See* IPR2014-00244, Paper 9.

C. The ’302 Patent

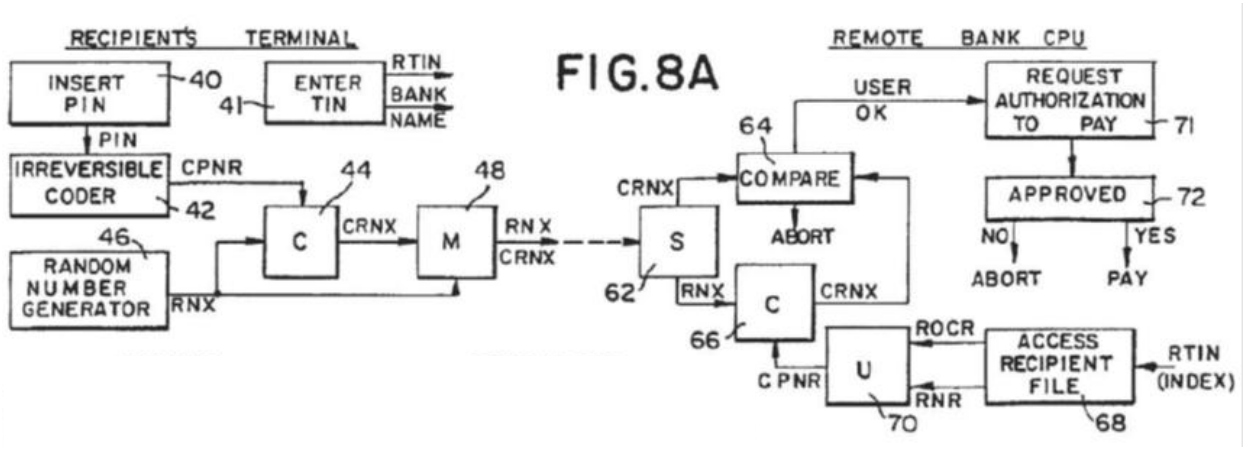
The ’302 patent generally relates to a transaction system for authenticating a transaction, document, or thing such that the information associated with at least one of the parties involved is coded to produce a joint code. Ex. 1001, 2:7–14. Additionally, the joint code then is used to code information relevant to the transaction, document, or record to produce a Variable Authentication Number (“VAN”). *Id.* at 2:14–16. 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 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, reproduced below, illustrates how an originator generates a check.



As shown above in Figure 7 of the ’302 patent, 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, reproduced below, illustrates the authentication process at a terminal when the recipient presents the originator’s check to be cashed.



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. An 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.

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.

D. Claim Construction

Petitioner states that the '302 patent has expired. Pet. 6. 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 provides an exhibit (Ex. 1016) reciting proposed claim constructions of certain terms in the '302 patent advanced by parties during various District Court proceedings involving the '302 patent and the claim constructions adopted by the District Courts in those matters. *See* Pet. 7.

1. "variable authentication number"

Petitioner proposes that the term "variable authentication number" or "VAN" be 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." Pet. 9 (Ex. 1004 ¶ 18). Patent Owner proposes "VAN" be construed as:

> an encoded variable number that can be used in verifying the identity of a party or the integrity of information or both, the value generated by coding information relevant to a transaction, document, or thing with either a joint key or information associated with or assigned or related to at least one party to the transaction or issuance of the document or thing

Prelim. Resp. 9.

The Specification states that the VAN "codes the information to be authenticated, based upon information related to the recipient and information related to the originator." Ex. 1001, 5:20–22. Furthermore, the Specification states that "the VAN is alternatively generated directly from INFO and information associated with at least one of the parties, without the intermediate step of generating the [joint key] JK." *Id*. at 5:23–25.

The District Court for the Eastern District of Texas adopted the construction proposed by Petitioner. Ex. 1014, 25. Furthermore, all of the District Court Claim Construction Orders cited by Petitioner adopt the definition of "VAN" proposed by Petitioner or a slight variant of that definition. *See* Ex. 1016, 2, 4. For purposes of

the decision, we construe 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."

II. ANALYSIS

A. Proposed Anticipation by Davies

1. Overview of Davies

Davies is a textbook titled "Security for Computer Networks," and it provides an introduction to data security in teleprocessing and electronic funds transfer. Ex. 1005, 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*. at 329.

Davies also discloses that private customers of the bank can carry an intelligent token or smart card to function as an electronic chequebook. *Id*. at 329 ("[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*.

2. Analysis of Asserted Ground of Anticipation by Davies

Petitioner argues that claims 51, 53, and 55 are anticipated by Davies. Pet. 16–37. 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 associate with a second party. Pet. 30. 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. 32 (Ex. 1005, 328). Additionally, Petitioner contends that Davies discloses the claimed "receiving funds transfer information" by disclosing that a "bank receives information identifying the payer, the payee and the payment amount ('transfer amount')." Pet. 22 (citing Ex. 1005, 328–330, Fig. 10.22). 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's disclosure 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." Pet. 33 (citing Ex. 1005, 329). 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's 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. 35 (citing Ex. 1005, 330).

Patent Owner disagrees with Petitioner's proposed challenge and argues that Davies does not anticipate claims 51, 53, and 55. Patent Owner argues that the embodiment relied upon in Davies does not perform the steps of "receiving" and "generating," recited in claim 51, in what Patent Owner argues is the required respective order. Prelim. Resp. 29. Specifically, Patent Owner argues that the step of "generating a variable authentication number (VAN) using at least a portion of the *received funds transfer information*" must be performed after the step of step of "receiving funds transfer information" because of the antecedent basis of the term "*received funds transfer information*." Prelim. Resp. 30.

The Federal Circuit has generally held that "[u]nless the steps of a method actually recite an order, the steps are not ordinarily construed to require one." *Interactive Gift Exp., Inc. v. Compuserve Inc.*, 256 F.3d 1323, 1342 (Fed. Cir. 2001). To determine whether a particular order is required in a method claim, the Federal Circuit has provided a two-prong approach. *Altiris, Inc. v. Symantec Corp.*, 318 F.3d 1363, 1369–70, (Fed. Cir. 2003). In the first prong, the Court "look[s] to the claim language to determine if, as a matter of logic or grammar, [the steps] must be performed in the order written." *Id*. If not, then in the second prong, the Court "look[s] to the rest of the specification to determine whether it 'directly or implicitly requires such a narrow construction.'" *Id.*

Here, at least a portion of the receiving step must precede the generating step, because the VAN is generated using a portion of the received funds transfer information, and it logically follows that the generating must occur after receipt of at least a portion of the funds transfer information in the receiving step. *See, e.g.*, *Mantech Envtl. Corp. v. Hudson Envtl. Servs., Inc.*, 152 F.3d 1368, 1375–76 (Fed. Cir. 1998) (requiring steps to be performed in order when a subsequent step requires the prior step to have been performed). Using similar reasoning to *Mantech*, we determine that claim 51 requires that at least some portion of the received funds transfer information be utilized in generating the VAN.

Contrary to Petitioner's assertions, the portions of the disclosure in Davies cited by Petitioner fail to disclose the required "receiving" and "generating" steps in the required sequence. First, Petitioner states that the "receiving" step is anticipated by Davies's disclosure that "a *bank* receives information identifying the payer, the payee, and the payment amount ("transfer amount")." Pet. 22 (citing Ex. 1005, 328–329) (emphasis added). Therefore, Petitioner relies upon the *bank* as performing the "receiving" step and receiving the funds transfer information. *See id.*[5] Second, as to the generating step, Petitioner cites to Davies's disclosure that "'the payment information . . . forms the third section of the cheque data . . . *final signature, by the customer*, covers all the variable information in the cheque . . . to form this signature the customer needs a secret key.'" Pet. 23 (quoting Ex. 1005, 329) (emphasis added). Therefore, Petitioner relies upon the *customer*, or the customer aided by a terminal, as performing the "generating" step and generating the VAN. *See id*.

[5] We note that for purposes of this decision we analyze the anticipation challenge as argued by Petitioner, not by what is recited in the claim.

Patent Owner argues that Petitioner's stated challenge is insufficient because Petitioner identifies the *bank* as receiving the funds transfer information in the form of an electronic cheque, but the *bank* does not then perform the generating a VAN step required by claim 51. Prelim. Resp. 30. The bank does not then perform the generating step because the cited Davies disclosure provides that the final signature (VAN) is already contained in the electronic cheque. Prelim. Resp. 30; Ex. 1005, 329–330. Additionally, Patent Owner argues that the bank could not generate the final signature (VAN) because such generation requires the customer's secret key, which the bank does not possess. Prelim. Resp. 31; *see also* Ex. 1005 ("In order to form this signature, the customer needs a secret key which he must protect against disclosure."). Based on the record before us, we agree with Patent Owner and determine that the anticipation challenge set forth by Petitioner in its Petition is deficient for failing to cite to sufficient anticipating disclosure in Davies for the "receiving" and "generating" steps of claim 51.

In addition to the discussion in the Petition of the bank carrying out the "receiving" step, Petitioner cites to following disclosure from Davies in its claim chart as anticipating the "receiving step" of claim 51:

> The terminal collects the cheques . . . the electronic cheque is transmitted . . . to the *card issuer bank* where the . . . drawer's account examined . . . the accounts of the customer and merchant can be updated.

Pet. 33 (citing Ex. 1005, 330) (emphasis added). As with the example cited above, Petitioner identifies the "card issuer bank" as the entity "receiving the funds transfer information," in accordance with claim 51. *See id*. With respect to this cited Davies disclosure, similar to our analysis above, we determine that Davies does not disclose that the "card issuer bank" also generates the VAN based on at least a portion of the received funds transfer information, because Davies discloses that the VAN already is included in the "electronic cheque [] transmitted . . . to the

card issuer bank." Ex. 1005, 330. Accordingly, the disclosure from Davies cited in Petitioner's claim chart is also deficient with respect to the "receiving" and "generating" steps in claim 51.

Based on the record before us, and in view of these deficiencies in the application of Davies to independent claim 51 in Petitioner's challenge, we determine that Petitioner fails to demonstrate a reasonable likelihood of prevailing in its challenge to claim 51, and claims 53, and 55 dependent therefrom, as anticipated by Davies.

B. Proposed Obviousness Over Davies and Nechvatal

1. Overview of Nechvatal

Nechvatal is titled "Public-key Cryptography," and describes, among other things, the use of digital signatures and hash functions in public key cryptography. Ex. 1006, 1–3. According to Nechvatal, usually it is not desirable to apply a signature directly to a long message. *Id.* at § 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*. (emphasis added).

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

Petitioner argues that claims 51, 53, and 55 would have been obvious over Davies and Nechvatal. Pet. 37–49. Specifically, Petitioner argues that Davies's signatures may be generated by computing hash values on the transaction

information as an intermediate step. Pet. 37. 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 of smaller size than *M*, and sign *H(M)* in a relatively quick fashion, which would improve signing efficiency, as taught by Nechvatal. *Id*.

Petitioner does not rely upon Nechvatal with respect to the "receiving" or "generating" steps recited in claim 51. *See* Pet. 37–49. Accordingly, Patent Owner argues that the Board should decline to institute review on obviousness grounds when the cited additional reference does not make up for the deficiency in the first reference. Prelim. Resp. 34. We agree with Patent Owner. Petitioner's citations to Nechvatal do not cure the deficiencies noted above in Petitioner's reliance upon Davies for the "requesting" and "generating" steps of claim 51, and the Petitioner's challenge based on Davies and Nechvatal relies upon the same cites to Davies for the "receiving" and "generating" steps of claim 51 as the anticipation challenge based on Davies alone. Accordingly, based on the record before us, we determine that Petitioner fails to demonstrate a reasonable likelihood of prevailing in its challenge that claim 51, and claims 53 and 55 dependent therefrom, would have been obvious in view of Davies and Nechvatal.

C. Proposed Obviousness Over Davies, Fischer, and Piosenka

1. Overview of Fischer

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, Abstr. Figure 3 of Fischer is reproduced below.

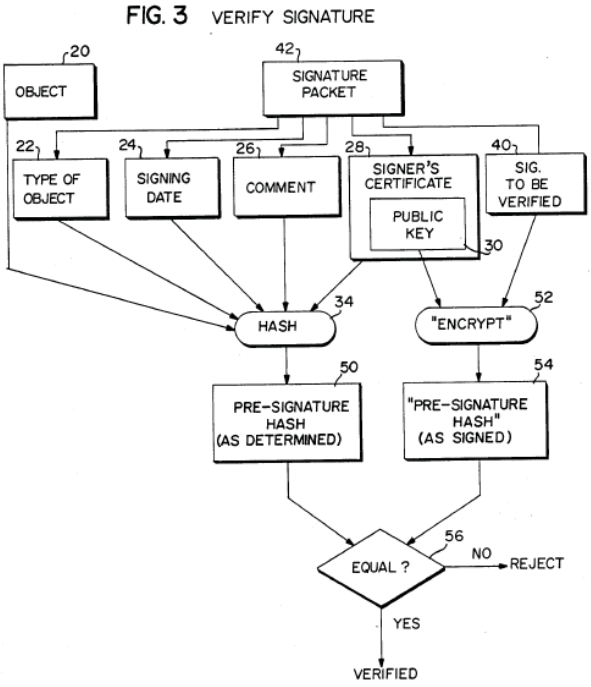


Figure 3 of Fischer above illustrates how a recipient of a transmitted message, including signature packet 42, verifies the signature. *Id.* at 11:45–48. Fischer discloses that the recipient applies hashtag algorithm 34 to the signature packet and associated fields 22, 24, 26, and 28 to result in presignature 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. *Id.* at 17:33–38. 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

Piosenka is titled "Unforgeable Personal Identification System," and discloses a system for identifying users at remote access sites. Ex. 1008, Abstr. 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.* at Abstr. 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.

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. 49–56. Claim 56 is dependent on claim 51 and includes the requirement that "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." Petitioner cites to Fischer's disclosure regarding a signature verification procedure that includes a hierarchy of certificates as teaching the claimed "second variable authentication

number (VAN1)." Pet. 50, 56 (citing Ex. 1007, 17:34–47). 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. 51, 56 (citing Ex. 1008, 6:41–42, 11:15–23).

Petitioner does not rely upon either Fischer or Piosenka with respect to the "receiving" or "generating" steps recited in claim 51. *See* Pet. 49–56. Accordingly, Patent Owner argues that the Board should decline to institute review on obviousness grounds when the cited additional references do not make up for the deficiency in the first reference. Prelim. Resp. 38. We agree with Patent Owner. Petitioner's citations to Fischer and Piosenka for dependent claim 56 do not cure the deficiencies noted above in Petitioner's reliance upon Davies for the "requesting" and "generating" steps of independent claim 51. Accordingly, based on the record before us, we determine that Petitioner fails to demonstrate a reasonable likelihood of prevailing in its challenge that dependent claim 56 would have been obvious in view of Davies, Fischer, and Piosenka.

III. CONCLUSION

For the foregoing reasons, we determine that Petitioner fails to demonstrate a reasonable likelihood of prevailing on its challenge to the patentability of claims 51, 53, and 55–56 of the '302 Patent.

IV. ORDER

For the reasons given, it is

ORDERED that the petition is *denied* as to all challenged claims of the '302 Patent.

PETITIONER:

Joseph Melnik
An P. Doan
JONES DAY
1755 Embarcadero Road
Palo Alto, CA 94303
jmelinik@jonesday.com
apdoan@jonesday.com

PATENT OWNER:

Robert P. Greenspoon
Joseph C. Drish
FLACHSBART & GREENSPOON, LLC
333 N. Michigan Ave., Suite 2700
Chicago, IL 60601
rpg@fg-law.com
jcd@fg-law.com