

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION,
Petitioner,

v.

PROXENSE, LLC,
Patent Owner.

IPR2024-00846
Patent 8,886,954 B1

Before THU A. DANG, KEVIN F. TURNER, and DAVID C. McKONE,
Administrative Patent Judges.

McKONE, *Administrative Patent Judge.*

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. *Background and Summary*

Microsoft Corp. (“Petitioner”) filed a Petition (Paper 2, “Pet.”) requesting *inter partes* review of claims 1–29 of U.S. Patent No. 8,886,954 B1 (Ex. 1001, “the ’954 patent”). Pet. 1. Proxense, LLC (“Patent Owner”) filed a Preliminary Response (Paper 7, “Prelim. Resp.”).

We have authority to determine whether to institute an *inter partes* review. See 35 U.S.C. § 314 (2016); 37 C.F.R. § 42.4(a) (2020). The standard for instituting an *inter partes* review is set forth in 35 U.S.C. § 314(a), which provides that an *inter partes* review may not be instituted “unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” For the reasons explained below, we institute an *inter partes* review of the ’954 patent.

B. *Related Matters*

The parties advise us that the ’954 patent is involved in three district court cases, including *Proxense, LLC v Microsoft Corp.*, Case No. 6:23-cv-00319 (W.D. Tex.). Pet. 107; Paper 5, 2. Petitioner also has filed petitions for *inter partes* review of patents related to the ’954 patent, including IPR2024-00775 (challenging U.S. Patent No. 8,352,730 B2 (“the ’730 patent”)) and IPR2024-00776 and IPR2024-01335 (both challenging U.S. Patent No. 9,298,905 B1 (“the ’905 patent”)). The ’730 patent also was the subject of *Samsung Electronics America, Inc. v. Proxense LLC*, IPR2021-01444 (PTAB) (institution denied). The ’954 patent also is the subject of *Google LLC v. Proxense, LLC*, IPR2024-00233 (PTAB) (institution granted), *Microsoft Corp. v. Proxense, LLC*, IPR2024-01327 (PTAB)

(pending institution decision), and *Apple Inc. v. Proxense, LLC*, IPR2024-01334 (PTAB) (petitioner joined to IPR2024-00233). Pet. 107; Paper 5, 2.

C. The '954 Patent

The '954 patent discloses systems for “authentication responsive to biometric verification of a user being authenticated,” using “an integrated device [that] includes a persistent storage to persistently store[] a code such as a device identifier (ID) and biometric data for a user in a tamper-resistant format.” Ex. 1001, 1:60–65. The '954 patent states that “[c]onventional user authentication techniques,” such as requiring input of a password, were deficient because they “require[d] the user to memorize or otherwise keep track of the credentials” and “it can be quite difficult to keep track of them all.” *Id.* at 1:26–35. Other techniques, such as “provid[ing] the user with an access object . . . that the user can present to obtain access,” were inadequate because “authentication merely proves that the access object itself is valid; it does not verify that the legitimate user is using the access object.” *Id.* at 1:36–46. According to the '954 patent, there was a need in the art for a system for “verifying a user that is being authenticated that does not suffer from [such] limitations” and “ease[s] authentications by wirelessly providing an identification of the user.” *Id.* at 1:52–56.

Figure 2 of the '954 patent is reproduced below.

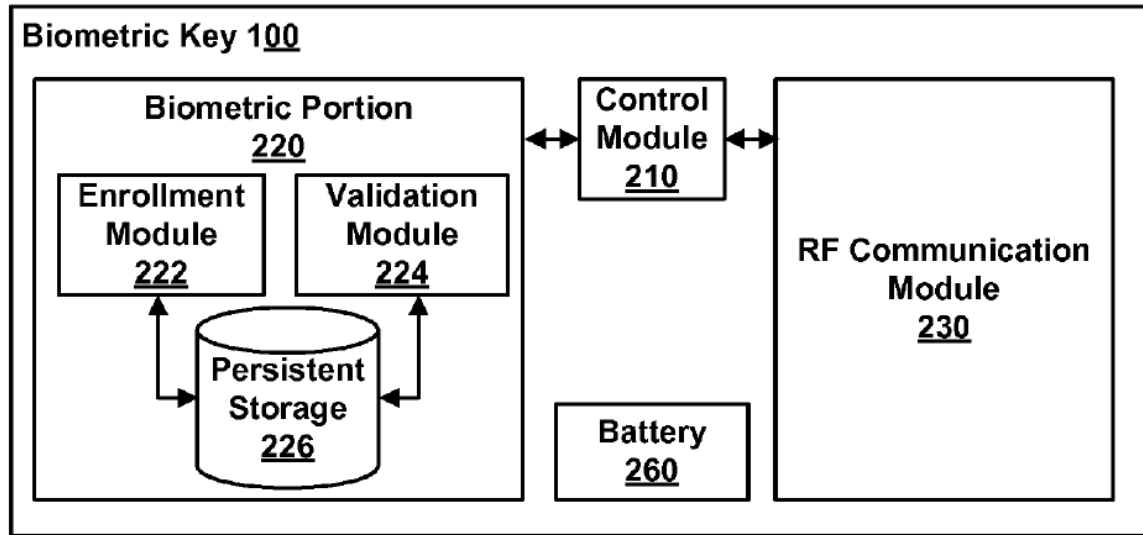


FIG. 2

Figure 2 is a block diagram of the functional modules of a biometric key.

Id. at 3:28–30. Enrollment module 222 registers a user with biometric key 100 by persistently storing biometric data associated with the user (e.g., a digital image of the retina, fingerprint, or voice sample) in persistent storage 226. *Id.* at 4:64–5:21. Enrollment module 222 registers biometric key 100 with a trusted authority by providing a code, such as a device ID, to the trusted authority or, alternatively, the trusted authority can provide a code to biometric key 100. *Id.* at 5:1–5. The code is stored in persistent storage 226. *Id.* at 5:36–38. “Persistent storage 226 is itself, and stores data in, a tamper-proof format to prevent any changes to the stored data.” *Id.* at 5:29–31. “Tamperproofing increases reliability of authentication because it does not allow any changes to biometric data (i.e., allows reads of stored data, but not writes to store new data or modify existing data).” *Id.* at 5:31–34. In a fingerprint embodiment, validation module 224 uses scan pad 120 (shown in Figure 1) to capture scan data from the user’s fingerprint

and compares the scanned data to the stored fingerprint to determine whether the scanned data matches the stored data. *Id.* at 5:6–15.

The interaction of biometric key 100 with other system components is illustrated in Figure 3, reproduced below.

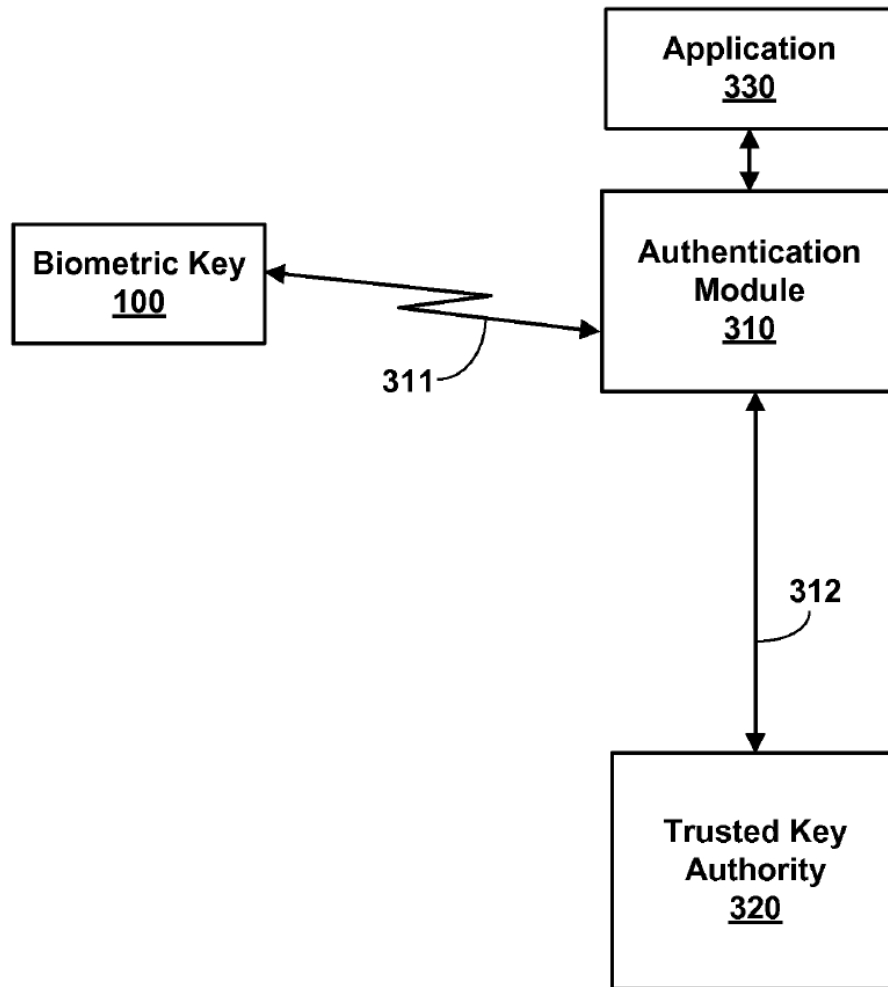


FIG. 3

Figure 3 is “a block diagram illustrating a system for providing authentication information for a biometrically verified user.” *Id.* at 3:31–33. Authentication module 310 is coupled to biometric key 100 via line 311 (a wireless medium) and with trusted key authority 320 via line 312 (a secure

data network such as the Internet). *Id.* at 6:1–5. Authentication module 310 requires the device ID code (indicating successful biometric verification) from biometric key 100 before allowing the user to access application 330. *Id.* at 6:5–11. Authentication module 310 provides the device ID code from biometric key 100 to trusted key authority 320 to verify that it belongs to a legitimate key. *Id.* at 6:11–14; *see also id.* at 6:37–43 (“In one embodiment, trusted key authority 320 verifies that a code from a biometric key is legitimate. To do so, the trusted key authority 320 stores a list of codes for legitimate biometric keys. . . . In one embodiment, trusted key authority 320 can also store a profile associated with a biometric key.”). Authentication module 310 then sends a message to application 330 to allow the user access to the application responsive to a successful authentication by trusted key authority 320. *Id.* at 6:15–17.

“Application 330 can be, for example, a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file, . . . and the like.” *Id.* at 6:19–24. Trusted key authority 320 can be operated by an agent, such as “a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness.” *Id.* at 7:30–33. “The agent can follow standardized procedures such as requiring identification based on a state issued driver license, or a federally issued passport in order to establish a true identity of the user.” *Id.* at 7:33–36.

Claim 1, reproduced below,¹ is illustrative of the claimed subject matter:

¹ We add bracketed alphanumeric characters corresponding to those Petitioner uses in the Petition.

1. A method comprising:
 - [1.1] persistently storing biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is not capable of being subsequently altered;
 - [1.2] responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;
 - [1.3] comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;
 - [1.4] responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other values from the plurality of codes and other data values for authentication to a third party that operates a trusted authority, wherein the one or more codes and other data values includes the device ID code; and
 - [1.5] receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to the application.

D. Evidence

Petitioner relies on the references listed below.

Name	Reference	Date	Exhibit No.
Burger	US 2005/0050367 A1	Mar. 3, 2005 (filed Sept. 30, 2004)	1005
Robinson	US 2003/0177102 A1	Sept. 18, 2003	1006

Name	Reference	Date	Exhibit No.
Orsini	US 2004/0049687 A1	Mar. 11, 2004	1021

Petitioner also relies on the Declaration of Patrick Traynor, Ph.D.
(Ex. 1003).

E. The Asserted Grounds

Petitioner asserts the following grounds of unpatentability (Pet. 1):

Reference(s)	35 U.S.C. §	Claim(s) Challenged
Burger	§ 103(a) ²	1, 2, 4, 5, 7–13, 15, 16, 18–24, 26–29
Burger, Robinson	§ 103(a)	3, 14, 17
Burger, Orsini	§ 103(a)	6, 25

II. ANALYSIS

A. Claim Construction

We construe a claim

using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.

² The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), amended 35 U.S.C. § 103. Because the ’954 patent has an effective filing date before the effective date of the relevant provision of the AIA, we cite to the pre-AIA version of § 103.

37 C.F.R. § 42.100(b) (2019); *see also Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

Petitioner observes that terms including “third-party trusted authority,” “tamper proof format,” and “access message” have been addressed previously by the Board. Pet. 3 (citing Ex. 1007 (Institution Decision in IPR2021-01444), 11–15). Nevertheless, Petitioner argues that “[n]o formal claim constructions are necessary” in this proceeding. *Id.* at 2.

Patent Owner requests that we adopt previous Board and district court constructions of “third-party trusted authority”³ and “access message.” Prelim. Resp. 2–9.

1. Third party that operates a trusted authority

Patent Owner contends that the Board has construed “third-party trusted authority” previously in several IPRs in accordance with its plain and ordinary meaning to mean “a trusted authority that is an entity separate from the parties to a transaction.” Prelim. Resp. 7–8 (citing, *inter alia*, IPR2021-01444, Paper 11 at 11–15; IPR2024-00233, Paper 10). Patent Owner does not appear to challenge this previous construction. *Id.*

However, Patent Owner contends that in three of six previous IPRs, the Board determined that the third-party trusted authority is not the application being accessed, but in three others, the Board determined that the third-party trusted authority is an active participant in facilitating a

³ The claims of the ’954 patent recite “a third party that operates a trusted authority.” Claims of related patents, such as the ’730 patent, recite “a third-party trusted authority.” The parties appear to treat these two similar terms as having the same meaning. We treated these terms as equivalent in IPR2024-00233, Paper 10 at 9, and do so in this proceeding as well.

transaction because it authenticates devices. *Id.* at 8. Patent Owner disagrees that such an authentication role renders a third-party trusted authority an active participant. *Id.* It is unclear whether Patent Owner is taking issue with our application of “third-party trusted authority”/“third party that operates a trusted authority” in previous cases or is arguing for a modified construction here (or both). In any case, we noted in IPR2024-00233, for example, that “active participation in a transaction, by itself, does not make an entity a party to that transaction.” IPR2024-00233, Paper 10 at 21. There, we determined preliminarily that the entity the petitioner had identified as a third party that operates a trusted authority, regardless of whether it was an active participant in some way in the transaction, was not the user or the vendor/retailer, which was the second party associated with the application being accessed in the petitioner’s theory. *Id.* at 20–24.

In attempting to distinguish Burger from the challenged claims, Patent Owner argues that “[t]he ‘third-party trusted authority’ is . . . a distinct entity whose role is to authenticate and provide an ‘access message’ allowing the user to enter, communicate with, or make use of an application.” Prelim. Resp. 10 (citing IPR2024-00234, Paper 10 at 10 (discussing the ’905 patent)). According to Patent Owner, “when correctly construed, . . . the third party trusted authority is not the application being accessed.” *Id.* at 9. Rather, Patent Owner argues, “[a]n important aspect of the PTAB’s construction, as shown by the application of its construction to the asserted art, is that the ‘third-party trusted authority’ is **separate from the system being accessed.**” *Id.* (citing IPR2021-01444, Paper 11 at 25–26).

In IPR2024-00233, we made clear that “exclud[ing] any active participant in a transaction” from the construction of third party that operates a trusted authority would exclude preferred embodiments of the ’954 patent

and, therefore, is presumptively incorrect. IPR2024-00233, Paper 10 at 10–12 (citing Ex. 1001, 6:37–51, 7:27–59, 8:5–17, Figs. 3–5, 7; *Sequoia Tech., LLC v. Dell, Inc.*, 66 F.4th 1317, 1327 (Fed. Cir. 2023)). We also explained that “active participation alone does not make an entity a party to the transaction.” *Id.* at 23. Instead, we evaluate a party’s relationship to the transaction to determine whether it is a principal party to the transaction or a third-party. *Id.* at 11 (“The ‘witness’ role mentioned in the Specification (Ex. 1001, 7:30–33) refers to an agent’s relationship to the principal parties to the transaction, not to the level of activity the agent engages in.”), 22 (“We agree with Petitioner that, in this example, the TPOCH is separate from, and thus a third party to, the principal parties to the transaction (the user and the vendor/retailer/service provider) and also a third party to the financial institution that pays the vendor.”).

To be clear, below, we evaluate Petitioner’s showing as to obviousness over Burger based on the ordinary meaning of third party that operates a trusted authority, namely, “a trusted authority that is an entity separate from the parties to a transaction.”

2. *Remaining claim terms (including “access message”)*

Patent Owner acknowledges that “the plain and ordinary meaning of ‘access message’ is a message enabling entry to, communication with, or use of an object,” but argues that, “to capture all the disclosed embodiments,” we should construe “access message” to mean “a signal or notification enabling or announcing access,” allegedly consistent with a district court construction. Prelim. Resp. 2–7. As Petitioner has shown a reasonable likelihood of success under the arguably narrower ordinary meaning of

“access message,” it is not necessary, at this stage of the proceeding, to further construe this term.

Based on the preliminary record, we do not find it necessary to provide express claim constructions for any other terms. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (noting that “we need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy’”) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

B. Obviousness of Claims 1, 2, 4, 5, 7–13, 15, 16, 18–24, and 26–29 over Burger

Petitioner contends that claims 1, 2, 4, 5, 7–13, 15, 16, 18–24, and 26–29 would have been obvious over Burger. Pet. 22–89. For the reasons given below, Petitioner has made a sufficient showing.

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 the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” We resolve the question of obviousness 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 skill in the art; and (4) if in evidence, objective evidence of nonobviousness, i.e., secondary considerations.⁴ *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

⁴ The record does not include allegations or evidence of objective indicia of nonobviousness.

1. Level of skill in the art

Neither party takes a position on the level of ordinary skill in the art. The description of the technology in the Specification, as well as the cited prior art, suggests that a skilled artisan would have been an experienced electrical or computer engineer.

2. Scope and content of the prior art – overview of Burger

Burger describes a method and system “for producing, distributing, storing, and using the typical contents of a person’s wallet, as well as the multiple, separate transaction authorization devices, e.g., RFID tags, owned by the person.” Ex. 1005 ¶ 93. “[T]he device may be more appropriately referred to as a multi-purpose, ‘point-of-transaction’ device.” *Id.* ¶ 94.

Figure 1, reproduced below, illustrates an example:

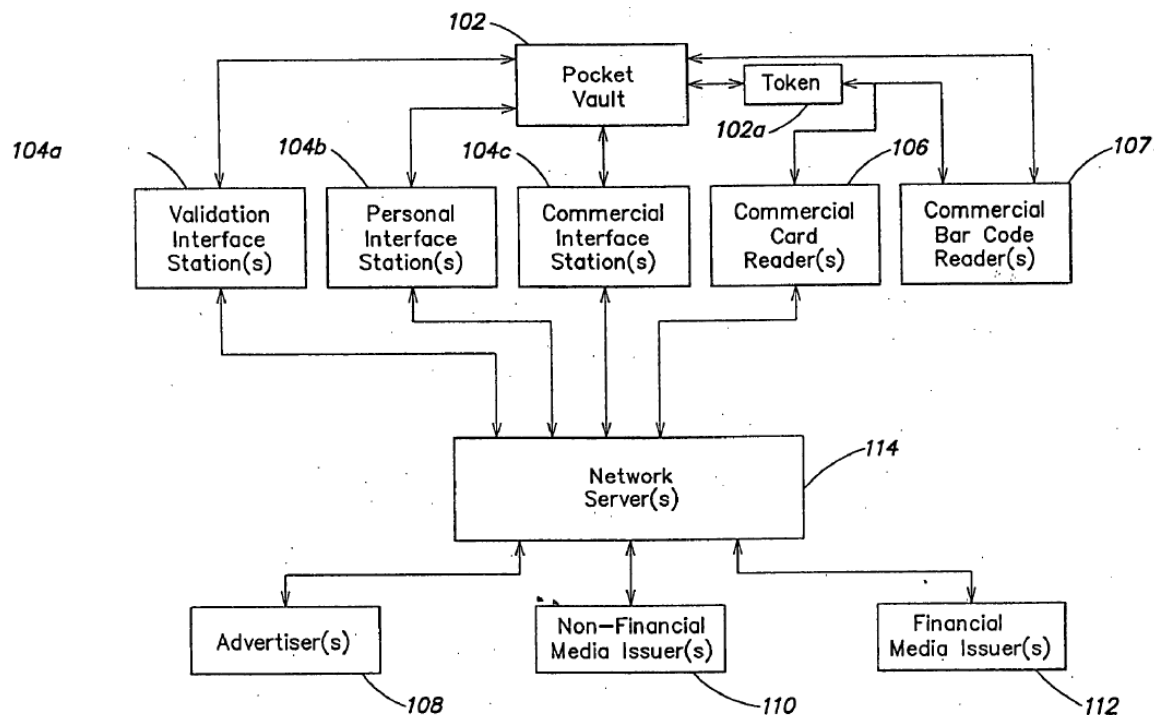


FIG. 1

Figure 1 is a block diagram of a network system in which a portable electronic authorization device (a “pocket vault”) is used. *Id.* ¶ 51.

In network system 100, pocket vault 102, associated token 102*a*, and network server 114 communicate with interface stations 104*a*–104*c*, commercial card readers 106, and commercial bar code readers 107. *Id.* ¶¶ 96–98, 100. Network server 114 also is coupled to advertiser computers 108, non-financial media issuers 110, and financial issuers 112. *Id.* ¶ 98. Pocket vault 102 can be equipped to generate token 102*a* such that the token has transactional information such as an actual or simulated magnetic stripe or bar code so that the token can be used by the user to engage in a transaction through card reader 106 or bar code reader 107. *Id.* ¶ 103. A trust relationship may be established between pocket vault 102 and network server 114; for example, a unique encrypted chip ID of pocket vault 102 may be registered with network server 114. *Id.* ¶ 114.

Figure 2 is reproduced below:

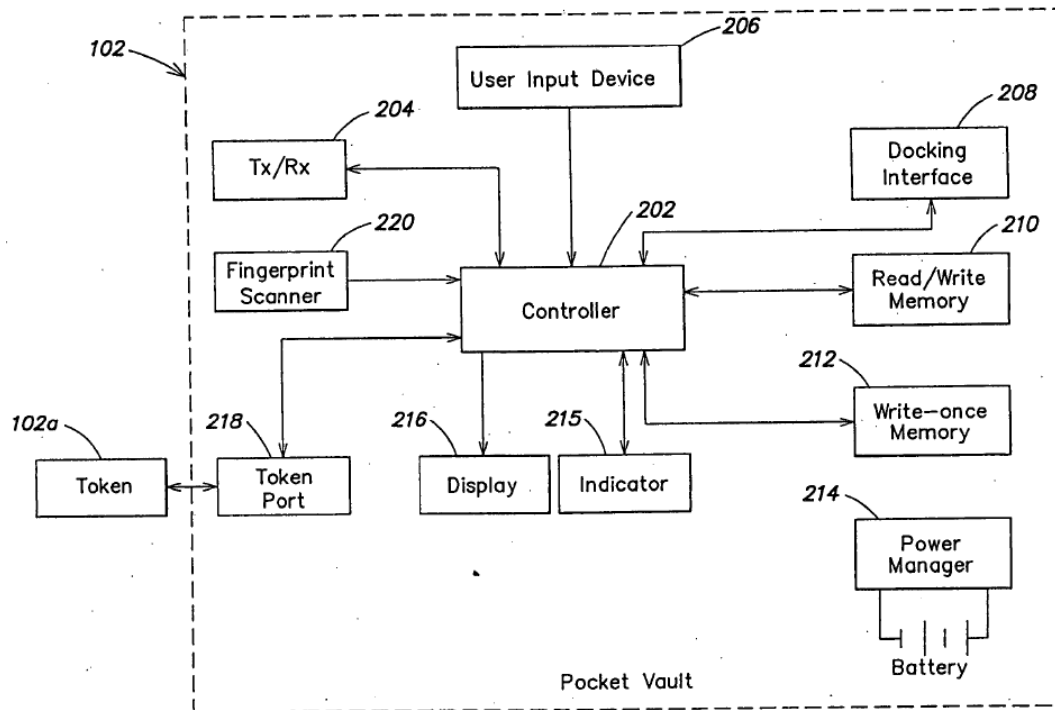


FIG. 2

Figure 2 is a block diagram of pocket vault 102. *Id.* ¶ 52. Pocket vault 102 includes controller 202, memory 210, write-once memory 212, and fingerprint scanner 220.⁵ *Id.* ¶ 118. Controller 202 includes a software-programmable and encryption protected or hard-wired unique chip ID that is released from pocket vault 102 only after fingerprint scanner 220 successfully authenticates the identity of the pocket vault's holder. *Id.* ¶ 122. Memory 210 can store various media and personal information (debit/credit cards, drivers licenses, passports, building security, etc.). *Id.* ¶¶ 127–129. Write-once memory 212 stores the user's fingerprints (or other biometric data). *Id.* ¶ 182. When the user applies a finger to fingerprint scanner 220, pocket vault 102 is authenticated by comparing the fingerprint from scanner 220 to the fingerprint stored in fingerprint memory

⁵ Burger contemplates other forms of biometric data, such as “retina scan, a speech pattern analysis, keystroke rhythm, etc.” *Id.* ¶ 112.

212. *Id.* ¶¶ 178–184, 209–210, Figs. 7A, 8A. When it is determined that pocket vault 102 has been properly authenticated, pocket vault 102 transmits an encrypted message with the unique pocket vault chip ID to an interface unit such as interface stations 104a–104c. *Id.* ¶¶ 186, 474, Figs. 7A, 8A, 19.

Figures 24 and 25 are reproduced below:

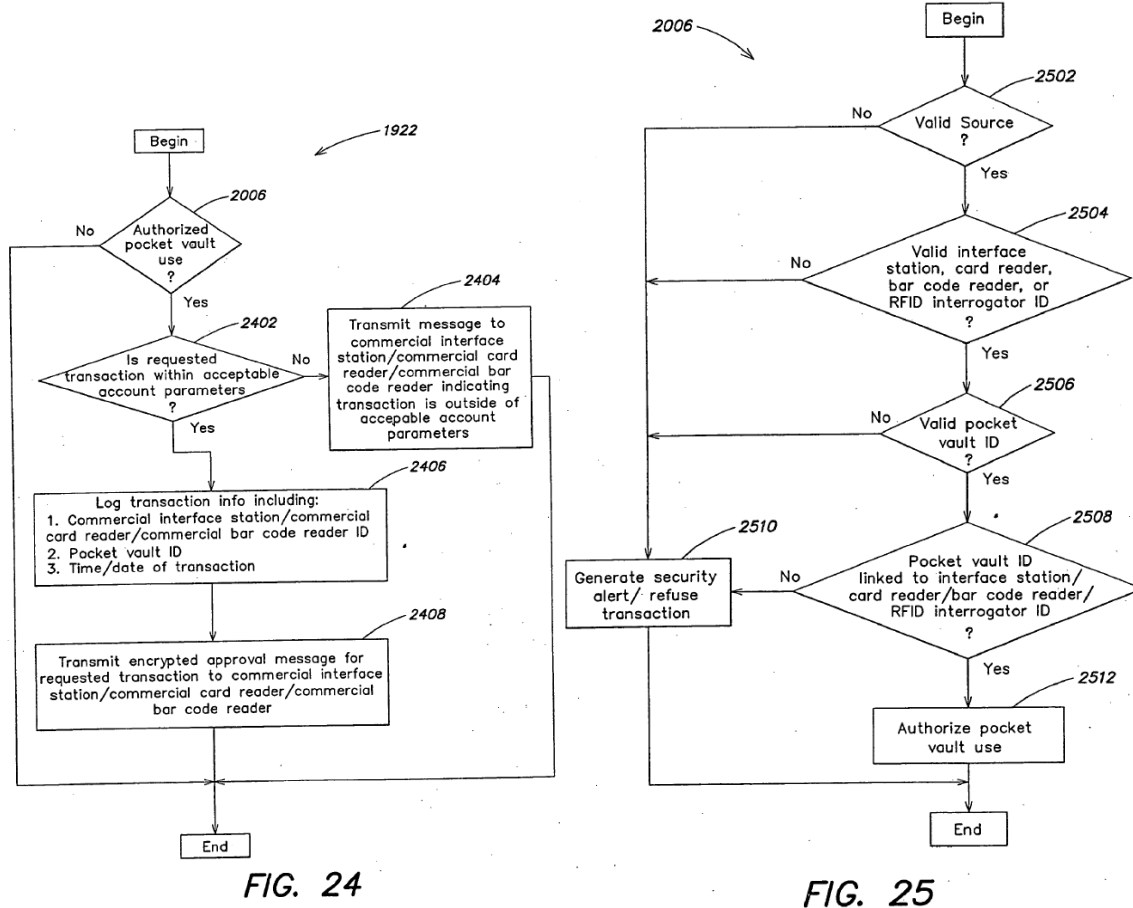


Figure 24 is a flow diagram of a process to request authorization of a transaction. *Id.* ¶ 74. Figure 25 is a flow diagram of the “authorized pocket vault use?” step 2006 of Figure 24. *Id.* ¶ 75. After network server 114 receives a request to authorize a transaction from an interface unit, the network server determines that the entity with which the user is attempting to transact (e.g., a point-of-sale terminal) is valid and properly linked (steps 2502–2504) and determines that the pocket vault ID is valid (step 2506).

Id. ¶¶ 473–474, 511–512, 520–525, Figs. 19, 24, 25. Network server 114 then determines that the pocket vault ID is linked to the ID of the commercial interface station 104, card reader 106, or barcode reader 107 and, if so, determines that the pocket vault use is authorized (steps 2508, 2512). *Id.* ¶¶ 527, 529. The network server then determines “whether the requested transaction is within acceptable account parameters (e.g., as set by the media issuer)” and, if so, logs the transaction and transmits an encrypted approval message to the entity with which the transaction is being attempted (e.g., interface station 104, card reader 106, barcode reader 107).

Id. ¶¶ 514–518.

In one example, the user uses pocket vault 102 to access a hotel room. *Id.* ¶ 679. In this example, the user secures a room using a credit card, and the prospective hotel guest may link to the network server 114 (while staying within the hotel’s website), and follow onscreen instructions for downloading the key card for his/her room onto the Pocket Vault 102 (e.g., to ensure that the Pocket Vault 102 is interfaced with the pocket vault interface unit 302, and to ensure that the Pocket Vault holder has activated the Pocket Vault 102 by the appropriate security mechanism such as a thumbprint for bio-metric ID verification).

Id. Pocket vault 102 can then encode token 102a with magnetic stripe coding to unlock the hotel room. *Id.*

3. *Differences, if any, between claims 1, 2, 4, 5, 7–13, 15, 16, 18–24, and 26–29 and Burger; reasons to modify*

Petitioner contends that Burger teaches a method for verifying a pocket vault holder during authentication of the pocket vault used in transactions involving financial and non-financial media. Pet. 22–23 (citing Ex. 1005 ¶¶ 2, 10, 127–128; Ex. 2003 ¶ 89).

As to claim limitation 1.1,

persistently storing biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is not capable of being subsequently altered,

Petitioner contends that Burger's pocket vault 102 is "an integrated device."

Id. at 23 (citing Ex. 1005 ¶¶ 94–95, 118, 134, Fig. 2; Ex. 1003 ¶ 90).

Petitioner argues that write-once memory 212, a storage element that is not capable of being subsequently altered, persistently stores biometric data of the user, and that other hard-wired memory stores a pocket vault ID and encryption/decryption information. *Id.* at 24–27 (citing Ex. 1005 ¶¶ 112, 114, 118, 127, 129, 154, 182, 551–552, Fig. 2; Ex. 1003 ¶¶ 22–23, 91–96).

Dr. Traynor testifies that it would have been obvious to implement the hard-wired memory as protected, write-once memory so that sensitive information that is not subject to change (e.g., device ID, encryption information) is kept secure and not tampered with. Ex. 1003 ¶ 98. We credit this testimony at this stage of the proceeding.

As to claim limitation 1.2, "responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan," Petitioner contends that the user applying a finger to Burger's fingerprint scanner 220 (or other physical action pursuant to a different type of biometric data) is a request for a biometric verification of the user and that responsive to this request, fingerprint scanner 220 scans the applied fingerprint and controller 202 receives the scan data. *Id.* at 28–30 (citing Ex. 1005 ¶¶ 112, 135, 178–182, Figs. 2, 7A; Ex. 1003 ¶¶ 99–100).

As to claim limitation 1.3, “comparing the scan data to the biometric data to determine whether the scan data matches the biometric data,” Petitioner points to Burger’s description of pocket vault 102 comparing the biometric data stored in write-once memory 212 to the scan data from fingerprint scanner 220. *Id.* at 30–31 (citing Ex. 1005 ¶¶ 182–184, Figs. 2, 7A; Ex. 1003 ¶ 101).

Petitioner’s evidence is sufficient, at this stage of the proceeding, to show that Burger teaches claim limitations 1.1–1.3. Patent Owner does not yet contest that Burger teaches limitations 1.1–1.3 of claim 1.

The parties dispute whether Burger teaches a “third party that operates a trusted authority,” as recited in claim limitation 1.4 (emphasis added),

responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other values from the plurality of codes and other data values for authentication *to a third party that operates a trusted authority*, wherein the one or more codes and other data values includes the device ID code.

Petitioner argues that, after pocket vault 102 authenticates the user’s biometric data, pocket vault 102 wirelessly sends an encrypted message including the pocket vault chip ID, ultimately to network server 114, which acts as a third-party trusted authority. Pet. 32–34 (citing Ex. 1005 ¶¶ 97, 99–101, 113–114, 122–123, 146, 183–184, 186, 209–210, Figs. 1, 7A; Ex. 1003 ¶¶ 96–99). Petitioner argues that network server 114 maintains a list of current pocket vault holders, identified by chip ID and linked to the list of holders and, thus, establishes a trust relationship between it and pocket vault 102. *Id.* at 44–45 (citing Ex. 1005 ¶¶ 114, 116, 146, Fig. 4; Ex. 1003 ¶ 109).

The parties’ disagreement centers around an identification of the application to be accessed and the party associated therewith. We evaluate

claim limitation 1.4 in the context of claim limitation 1.5, “receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to the application.”

As to claim limitation 1.5, Petitioner argues that, after Burger’s network server 114 authenticates the user’s pocket vault ID, the user is granted access to pocket vault 102 and can select a transaction from a displayed menu. Pet. 42–44 (citing Ex. 1005 ¶¶ 95–96, 125, 155–158, 189, 236–238, 320, Figs. 7B, 10A, 19). In one example, Petitioner argues, pocket vault 102, or token 102*a* coupled to it, displays credit card information to be used by a retailer in a transaction. *Id.* Dr. Traynor testifies that it would have been obvious that pocket vault 102 would have received an access message from network server 114 in order for pocket vault 102 to grant access to the user and display credit card information. Ex. 1003 ¶ 115. In a related example, Petitioner argues that the encrypted approval message from network server 114 can be transmitted to an interface station (e.g., 104*c*, 106, 107). Pet. 45–48 (citing Ex. 1005 ¶¶ 101, 182–186, 517–527, Figs. 24, 25; Ex. 1003 ¶ 116). Dr. Traynor testifies that it would have been obvious that the encrypted approval message from network server 114 could be sent to the pocket vault 102 in addition to or instead of interface stations 104*c*, 106, 107. Ex. 1003 ¶ 116.

In Petitioner’s first example, and pursuant to claim limitation 1.5, the “application” that is accessed is “a file” or computer software that stores credit card information. Pet. 52. As to claim limitation 1.4, Petitioner argues that the first party to the transaction is the user of pocket vault 102, the second party is either the retailer or financial media issuer 112 (e.g., a

bank or credit card company), and the third party, a third party that operates a trusted authority, is network server 114 and the party that operates it. *Id.* at 34–35, 38–39 (citing Ex. 1005 ¶¶ 95, 158, 320, 511–513, Figs. 19, 24, 25, 27; Ex. 1003 ¶ 110).

As to this example, Patent Owner responds that

the user is requesting from the Pocket Vault System the issuance of credit. In essence, the user is going to Pocket Vault to get money – as if it were an ATM. Instead of cash, the user receives the equivalent of a promissory note from the Pocket Vault System to tender payment to the merchant.

Prelim. Resp. 17. According to Patent Owner, “[t]he transaction, accordingly, is between only the user and the Pocket Vault System.” *Id.* (citing Ex. 1005, Figs. 19, 24, 25).

Referring to Figures 24 and 25, Patent Owner argues that network server 114 determines that a use of pocket vault 102 is authorized (step 2006 of Fig. 24; step 2506 of Fig. 25). *Id.* at 18–19 (citing Ex. 1005 ¶¶ 511, 519, Figs. 24, 25). Patent Owner argues that after network server 114 authenticates pocket vault 102, it determines whether the requested transaction is within acceptable account parameters and, if so, logs the transaction and transmits an encrypted approval message to the entity with which the user seeks to transact (commercial interface station 104c, card reader 106, barcode reader 107). *Id.* at 20 (citing Ex. 1005 ¶ 513, Fig. 24, steps 2402, 2406, 2408); *see also id.* at 23 (“The acquisition of an approval message is an element of the authorization element of a credit card transaction process terminating in the issuing bank sending an authorization response to [the] merchant.” (citing Ex. 1005 ¶¶ 437, 513; Ex. 2008)). Thus, Patent Owner argues, “server 114 is making the determination to approve the request for credit.” *Id.* at 20; *see also id.* at 24 (“Per settlement, the

merchant would send the Pocket Vault transaction approval to payment processor to be presented to Pocket Vault acting as the issuing bank. Pocket Vault would then transfer the funds to the merchant account for deposit into the merchant's account.”). From this, Patent Owner concludes that “server 114 is the system being accessed to authorize the transaction by issuing credit to the Pocket Vault user, making it a party to the transaction.” *Id.* at 20; *see also id.* at 21–23 (similar arguments for the example of Exhibit 1005 ¶¶ 436–437, Figs. 17A–17B).

We disagree with Patent Owner's understanding of Burger. First, it does not account for Petitioner's characterization of Burger, supported by Dr. Traynor's testimony, in which an access message is sent from network server 114 to pocket vault 102 allowing access to credit card information that can be provided, via token 102a, to commercial card reader 106 or commercial bar code reader 107. Pet. 42–48 (citing Ex. 1005 ¶¶ 95–96, 101, 155–158, 182–186, 189, 236–238, 320, 517–527, Figs. 7B, 10A, 19, 24, 25; Ex. 1003 ¶¶ 114–116). In this scenario, the user of pocket vault 102 and token 102a is the first party and either the retailer or the bank/credit card company is the second party, with the application accessed being the file or computer software that stores credit card information. *Id.* at 34–35, 52. As token 102a presents credit card information to commercial card reader 106 or commercial bar code reader 107, the preliminary record suggests that a financial media issuer (e.g., financial media issuer 112), and not network server 114, is acting as the bank, or approver of the credit card information. Ex. 1005 ¶¶ 95, 97, 103, 158, 242. In this case, network server 114 determines that pocket vault 102 is authorized to be used and sends a message to pocket vault 102 allowing the user to access credit card

information. Ex. 1003 ¶¶ 115–116. Thus, on the current record, network server 114 acts as a third-party that operates a trusted authority.

Moreover, even in the scenario where network server 114 transmits an approval message directly to commercial card reader 106 or commercial bar code reader 107 (Ex. 1005 ¶ 518), the current record does not suggest that network server 114 is acting as an issuing bank or ATM machine, authorizing credit, or issuing a promissory note. Rather, Burger explains that network server 114 can “serve as . . . a service provider for financial and non-financial media issuers, [and] advertisers,” such as computers 108, 110, and 112. *Id.* ¶ 98. “[N]etwork server 114 may facilitate transactions involving media issued by media issuers.” *Id.* ¶ 117. Thus, on the current record, it appears that network server 114, at most, acts as an intermediary between a user of pocket vault 102 and financial media issuer 112.

In another example, Petitioner argues, Burger describes that pocket vault 102 receives and displays, on its screen, an advertising message from advertiser 108 via network server 114. Pet. 39–41 (citing Ex. 1005 ¶¶ 117, 146, 189–195, 236–238, 541, Figs. 1, 10, 11; Ex. 1003 ¶¶ 111–112), 48–51 (citing Ex. 1005 ¶¶ 110, 194, 236–237, 242, Figs. 7B, 10A, 14, 26H–26K). Dr. Traynor testifies that it would have been obvious that, for pocket vault 102 to display an advertisement, it would have received an access message from network server 114 conditioned on network server 114 authenticating the pocket vault ID. Ex. 1003 ¶ 117. In this example, and pursuant to claim limitation 1.5, the “application” that is accessed is a file, computer software, or a website containing advertising data that are displayed. Pet. 52. As to claim limitation 1.4, Petitioner argues that the first party to the transaction is the user of pocket vault 102, the second party is advertiser 108, and the third

party, a third party that operates a trusted authority, is network server 114 and the party that operates it. *Id.* at 36, 41–42 (citing Ex. 1003 ¶ 113).

As to this example, Patent Owner responds that “server 114 forms the hub of the system and serves as the entity storing information, acting as a service provider, and controlling access.” Prelim. Resp. 11–14 (citing Ex. 1005 ¶¶ 51, 98, 144–146, Figs. 1, 4). Patent Owner argues that network server 114 includes memory 404 and database 406 that act as websites and execute software accessed by the user. *Id.* at 14–16 (citing Ex. 1005 ¶¶ 145, 539⁶). Patent Owner further argues that database 406 also maintains a listing of registered and authorized pocket vaults, making network server 114 the key authority. *Id.* at 15 (citing Ex. 1005 ¶¶ 146, 530, Fig. 27). According to Patent Owner, network server 114 has a “dual nature” in that it “is the application to be accessed” and also “the key authority performing authentication.” *Id.* at 15–16 (citing Ex. 1005 ¶¶ 539, 541, 558, Fig. 27); *see also id.* at 25 (“the network server 114 may therefore serve as: (1) a repository of information for the network, (2) the entity that controls access to the Stored information by the other network devices, and (3) a service provider for financial and non-financial media issuers, advertisers, as well as Pocket Vault holders.” (quoting Ex. 1005 ¶¶ 98, 145, 538)).

We agree with Petitioner as to this example. In this example, as Petitioner argues, the first party is the user of pocket vault 102, which displays a file including an advertisement, and the second party is the advertiser (e.g., advertiser 108 in Figure 1). Network server 114 can act as an intermediary between advertiser 108 and pocket vault 102, but the

⁶ Patent Owner cites Exhibit 1005 ¶ 538. Prelim. Resp. 15–16. This appears to be a typographical error, as the material quoted appears at paragraph 539.

transaction is between the advertiser and the pocket vault user. As explained in Burger, “network server 114 may serve as a conduit for advertisers to target particular classes of Pocket Vault holders, and channel information to them.” Ex. 1005 ¶ 117. “The advertiser 108 (FIG. 1) may, for example, have made arrangements with the company operating the network server 114 to have certain advertising information uploaded to Pocket Vaults 102 when particular Pocket Vault holders interface their Pocket Vaults 102 with their personal interface stations 104b.” *Id.* ¶ 237. Network server 114 may send to pocket vault 102 an advertisement received from advertiser 108. *Id.* ¶¶ 237–238. However, the transaction is between the user and the advertiser. Dr. Traynor testifies that it would have been obvious that network server 114 would send to pocket vault 102 a message allowing it to access the advertisement upon authenticating the pocket vault ID. Ex. 1003 ¶ 117. We credit this uncontroverted testimony at this stage of the proceeding. Thus, on the current record, network server 114 acts as a third party that operates a trusted authority in this example as well.

In a third example, Petitioner argues that Burger describes a user downloading a hotel room key to pocket vault 102, and using pocket vault 102 to unlock a guest room. Pet. 52–53 (citing Ex. 1005 ¶¶ 94, 102, 128–129, 679–680). In this example, and pursuant to claim limitation 1.5, the “application” that is accessed is a keyless lock. *Id.* at 52. As to claim limitation 1.4, Petitioner argues that the first party to the transaction is the user of pocket vault 102, the second party is non-financial media issuer 110 (e.g., hotel card key issuer), and the third party, a third party that operates a trusted authority, is network server 114 and the party that operates it. *Id.* at 35–36.

As to this example, Patent Owner argues that “Burger clearly details that the key is **downloaded from the Pocket Vault network server 114**, making the network server 114 the application being accessed.” Prelim.

Resp. 25 (citing Ex. 1005 ¶ 676). According to Burger,

the prospective hotel guest may link to the network server 114 (while staying within the hotel’s website), and follow on-screen instructions for downloading the key card for his/her room onto the Pocket Vault 102 (e.g., to ensure that the Pocket Vault 102 is interfaced with the pocket vault interface unit 302, and to ensure that the Pocket Vault holder has activated the Pocket Vault 102 by the appropriate security mechanism such as a thumbprint for bio-metric ID verification).

Ex. 1005 ¶ 679. This is consistent with the user downloading the key card onto pocket vault 102 from the hotel’s website, which the user stays within, rather than via network server 114 as an intermediary. However, even if the user downloads the key card from network server 114, we agree with Petitioner that the transaction is between the user (first party) and the hotel (second party), with network server 114 acting as a third party that operates a trusted authority and that activates the key card on pocket vault 102.

Pet. 35–36, 52–53.

Thus, in each of the three examples in Burger that Petitioner relies on, Petitioner has shown sufficiently that Burger teaches claim limitations 1.4–1.5.

In sum, on the current record, Petitioner has shown a reasonable likelihood that claim 1 would have been obvious over Burger.

Independent claim 12 is directed to an integrated device with modules that perform functions similar to the steps of claim 1. Independent claim 16 is a method with steps substantially similar to those of claim 1. Independent claim 22 is a system with components that perform functions similar to the

steps of claim 1. Petitioner's arguments and evidence for claims 12, 16, and 22 are similar, and largely incorporate, its arguments for claim 1. Pet. 62–65, 67–78, 79–83. Patent Owner presents its arguments for claims 12, 16, and 22 together, and only as to the term “third party that operates a trusted authority” appearing in each of these claims. Prelim. Resp. 9–26. For the reasons given for claim 1, Petitioner has shown a reasonable likelihood that it would prevail with respect to claims 12, 16, and 22 as obvious over Burger.

Claims 2, 4, 5, and 7–11 depend from claim 1. Claims 13 and 15 depend from claim 12. Claims 18–21 depends from claim 16. Claims 23, 24, and 26–29 depend from claim 22. We have evaluated Petitioner's evidence as to these dependent claims (Pet. 53–62, 65–67, 78–79, 83–89) and are persuaded, on the current record, that Petitioner has shown a reasonable likelihood that it would prevail with respect to claims 2, 4, 5, 7–11, 13, 15, 18–21, 23, 24, and 26–29 as obvious over Burger. Patent Owner does not yet present separate arguments for the dependent claims. Prelim. Resp. 26.

C. Obviousness of Claims 3, 14, and 17 over Burger and Robinson

Petitioner contends that claims 3, 14, and 17 would have been obvious over Burger and Robinson. Pet. 89–97. Claim 3 depends from claim 1 and adds “registering an age verification for the user in association with the device ID code.” Claim 14 depends from claim 12 and claim 17 depends from claim 16. Claims 14 and 17 add limitations similar to that of claim 3.

Robinson relates to a tokenless system and method for age verification using biometric information and a system identification number (“SID”).

Ex. 1006 ¶ 5. Figure 3 of Robinson is reproduced below:

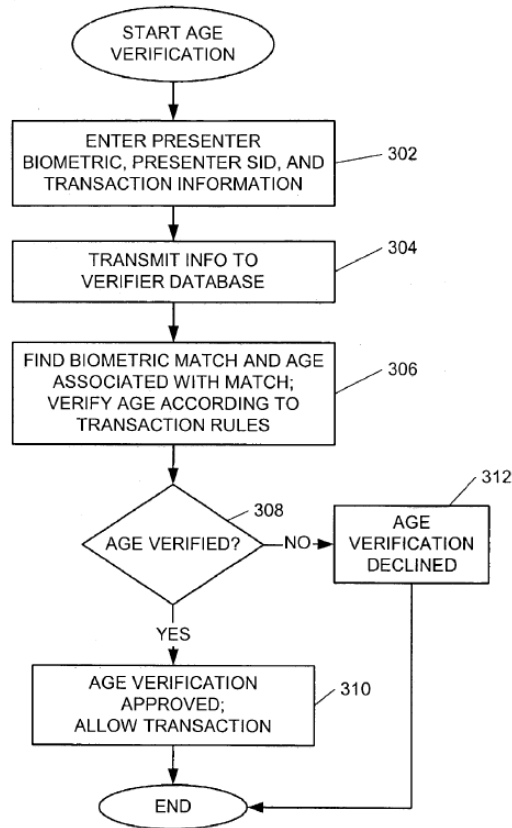


FIG. 3

Figure 3 is a flowchart of a process for age verification with remote biometric matching. *Id.* ¶ 22.

A presenter enters their SID and biometric sample (e.g., fingerprint, retinal scan, face geometric scan, voice print) at a point of verification (“POV”) device, and transaction information, such as a rule by which the presenter’s age can be evaluated, is entered (step 302). *Id.* ¶¶ 14, 30, 54. The presenter SID, biometric information, and transaction information are sent to a verifier database (step 304), which compares the biometric information to stored biometric information (step 306) and evaluates the presenter’s age. *Id.* ¶¶ 30, 55. If the presenter’s age is verified (step 308), the verifier database approves the presenter’s access to purchasing age-

restricted goods and/or services, or entry to an age-restricted area (step 310). *Id.* ¶ 57.

Petitioner contends that “it would have been obvious to a [person of ordinary skill in the art] to incorporate the age verification method of Robinson in Burger so that Burger’s system can be used by businesses interested in conducting transactions that require age-verification.” Pet. 93. Petitioner argues that it would have been predictable to include Robinson’s age-verification feature in Burger’s system in light of Robinson’s explanation that merchants and their employees face penalties if they sell age-restricted goods (e.g., alcohol or tobacco) to underage individuals. *Id.* at 94–95 (citing Ex. 1006 ¶ 5; Ex. 1003 ¶¶ 79–80). Dr. Traynor testifies that there would have been “a reasonable expectation of success because it merely involves combining known elements in a manner that would have been easily implemented and obvious to” a skilled artisan. Ex. 1003 ¶ 80. At this stage of the proceeding, we credit Dr. Traynor’s uncontroverted testimony.

As to claims 3, 14, and 17, Petitioner points to Robinson’s description of a user registering a biometric sample, identity-verifying information (SID), and age-verifying information with a database of an age-verification system. Pet. 95–96 (citing Ex. 1006 ¶¶ 14–15, 28, 43, 48; Ex. 1003 ¶¶ 175–178). Petitioner argues that, in the combination of Burger and Robinson, Robinson’s age-verifying information would be stored in the database of Burger’s network server 114. *Id.* at 95 (citing Ex. 1003 ¶ 176). Patent Owner does not yet provide separate arguments for claims 3, 14, and 17. Prelim. Resp. 26.

On the current record, Petitioner has shown sufficiently that Robinson teaches the additional limitations of claims 3, 14, and 17, and that a skilled

artisan would have had reasons, with rational underpinning, for combining Burger and Robinson.

D. Obviousness of Claims 6 and 25 over Burger and Orsini

Petitioner contends that claims 6 and 25 would have been obvious over Burger and Orsini. Pet. 97–102. Claim 6 depends from claim 1 and adds “wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.” Claim 25 depends from claim 22 and adds substantially the same limitation.

Orsini describes a cryptographic system that includes a user system in communication with a trust engine. Ex. 1021 ¶ 62. The user system includes a biometric device that captures biometric information from the user and sends it to the trust engine. *Id.* ¶¶ 63, 67. The user system can include “a computer workstation, an interactive television, an interactive kiosk, a personal mobile computing device, such as a digital assistant, mobile phone, laptop, or the like, a wireless communications device, a smartcard, an embedded computing device, or the like.” *Id.* ¶ 65.

As to claims 6 and 25, Petitioner contends that a skilled artisan “would have implemented the Pocket Vault such that it comprises a mobile phone or laptop—devices that are similar and, in some cases, the same as modern personal digital assistants and palm top computers—as disclosed by Orsini.” Pet. 99, 102 (citing Ex. 1021 ¶ 182; Ex. 1003 ¶¶ 181–182). Petitioner contends that this would have merely involved combining prior art elements according to known methods to yield predictable results. *Id.* at 99–101 (citing Ex. 1005 ¶¶ 93–95, 118; Ex. 1021 ¶¶ 63, 65, 67; Ex. 1003 ¶¶ 84–

88). Patent Owner does not yet provide separate arguments for claims 6 and 25. Prelim. Resp. 26.

On the current record, Petitioner has shown sufficiently that Orsini teaches the additional limitations of claims 6 and 25, and that a skilled artisan would have had reasons, with rational underpinning, for combining Burger and Orsini.

III. CONCLUSION

Petitioner has shown a reasonable likelihood that it would prevail with respect to at least 1 of the claims challenged in the Petition.

Our factual findings, conclusions of law, and determinations at this stage of the proceeding are preliminary, and based on the evidentiary record developed thus far. This is not a final decision as to the patentability of the claims for which *inter partes* review is instituted. Our final decision will be based on the record as fully developed during trial.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that pursuant to 35 U.S.C. § 314(a), an *inter partes* review is instituted as to claims 1–29 of the '954 patent on the grounds set forth in the Petition; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial; the trial will commence on the entry date of this decision.

IPR2024-00846
Patent 8,886,954 B1

PETITIONER:

W. Karl Renner
Roberto Devoto
Usman Khan
FISH & RICHARDSON P.C.
axf-ptab@fr.com
devoto@fr.com
khan@fr.com

PATENT OWNER:

David L Hecht
James Zak Reg
HECHT PARTNERS LLP
dhecht@hechtpartners.com
jzak@hechtpartners.com