Appeal Nos. 25-2168 (Lead) & 26-1283 (Consolidated)

In The United States Court Of Appeals For The Federal Circuit

PROXENSE, LLC,

Appellant,

v.

APPLE INC., MICROSOFT CORPORATION,

Appellees.

On Appeal from the U.S. Patent and Trademark Office,
Patent Trial and Appeal Board,
IPR2024-00233, IPR2024-01334, and IPR2024-00846

APPELLANT PROXENSE LLC'S OPENING BRIEF

David L. Hecht
Hecht Partners LLP
125 Park Avenue, 25th Floor
New York, NY 10017
Tel: (212) 851-6821
E: dhecht@hechtpartners.com

PATENT CLAIMS AT ISSUE

1. A method comprising:

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;

responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

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

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.

2. The method of claim 1, wherein the one or more codes and other data values are transmitted to the trusted authority over a network.

3. The method of claim 1, further comprising:

registering an age verification for the user in association with the device ID code.

4. The method of claim 1, wherein the one or more codes and other data values indicate that the biometric verification was successful.

5. The method of claim 1, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

6. The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

7. The method of claim 1, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

8. The method of claim 1, wherein the application includes a file including medical information.

9. The method of claim 1, wherein the application includes a financial account.

10. The method of claim 1, further comprising:

establishing a secure communication channel prior to sending the one or more codes and other data values for authentication.

11. The method of claim 1, further comprising:

receiving a request for the one or more codes and other data values without a request for biometric verification; and

responsive to receiving the request for the one or more codes and other data values without a request for biometric verification, sending the one or more codes and other data values without requesting the scan data.

12. An integrated device comprising:

a persistent storage media that stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the persistent storage media and not capable of being subsequently altered;

a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends one or more codes and other data values from the plurality of codes and other data values for authentication by a third party that operates a trusted authority, wherein the one or more codes and other data values includes the device ID code; and

a radio frequency communication module that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party and allowing the user access to an application.

13. The integrated device of claim 12, wherein the one or more codes and other data values are transmitted to the trusted authority over a network.

14. The integrated device of claim 12, wherein an age verification is registered in association with the device ID code.

15. The integrated device of claim 12 comprising:

an LED to be activated for requesting the biometric scan.

16. A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

wirelessly receiving one or more codes and other data values from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and other data values comprises the device ID code uniquely identifying an integrated device associated with a biometrically verified user, the device ID code being registered with a trusted authority for authentication, the trusted authority operated by a third party;

requesting authentication of the integrated device using the one or more codes and other data values by the trusted authority;

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 to the third party; and

in response to receiving the access message, allowing the biometrically verified user access to the application.

17. The method of claim 16, further comprising:

registering a date of birth or age with the trusted authority.

18. The method of claim 16, further comprising:

establishing a secure communications channel with the integrated device, wherein the one or more codes and other data values associated with the biometrically verified user is received from the integrated device.

19. The method of claim 16, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

20. The method of claim 16, wherein the application includes a file including medical information.

21. The method of claim 16, wherein the application includes a financial account.

22. A system, comprising:

an integrated hardware device that stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated hardware device and a secret decryption value in a tamper proof format written to a storage element in the integrated hardware device that is not capable of being subsequently altered, and that wirelessly sends one or more codes and other data values from the plurality of codes and other data values, wherein the one or more codes and other data values include the device ID code; and

an authentication circuit that receives the one or more codes and other data values and sends the one or more codes and other data values to a third

party that operates a trusted authority for authentication, and that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party and allows the user to access an application.

23. The system of claim 22, wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from the user to generate scan data.

24. The system of claim 22, wherein when the integrated hardware device cannot verify scan data as being from the user, the integrated hardware device does not send the one or more codes and other data values.

25. The system of claim 22, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

26. The system of claim 22, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

27. The system of claim 22, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

28. The system of claim 22, wherein the application includes a file including medical information.

29. The system of claim 22, wherein the application includes a financial account.

CERTIFICATE OF INTEREST

Counsel of Patent Owner/Appellant, Proxense LLC, certifies as follows:

1. The full name of the **Represented Entities** per Fed. Cir. R. 47(a)(1) is Proxense LLC.

2. Aside from the Represented Entities, there is no additional **Real Party in Interest** per Fed. Cir. R. 47.4(a)(2).

3. There are no **Parent Corporations and Stockholders** per Fed. Cir. R. 47.4(a)(3).

4. The following **Legal Representatives** have appeared for Proxense LLC in the originating IPR proceedings or are expected to appear before this Court on behalf of Proxense LLC per Fed. Cir. R. 47.4(a)(4):

Hecht Partners LLP: David L. Hecht, James A. Zak

5. Other than the originating *inter partes* reviews, the following cases are related per Fed. Cir. R. 47.4(a)(5):

Proxense v. Samsung Electronics, Co., Ltd. et al., No. 6:21-CV-00210-ADA (W.D. Tex.) – Settled;

Proxense v. Google, LLC, No. 6:23-cv-00320-ADA (W.D. Tex.) - Settled;

Proxense v. Microsoft Corporation, No. 6:23-cv-00319-ADA (W.D. Tex.) – Stayed;

Proxense v. Apple Inc., No. 6:24-cv-00143-ADA (W.D. Tex.) – Stayed;

Reexamination No. 90/015,052, reexamining U.S. Patent No. 8,352,730 - Reexamination Certificate issued Jan. 29, 2026;

Reexamination No. 90/015,053, reexamining U.S. Patent No. 9,289,905 – Reexamination Certificate issued June 17, 2025;

Reexamination No. 90/015,054, reexamining U.S. Patent No. 10,698,989 - Reexamination Certificate issued Mar. 19, 2025.

6. There are no **Organizational Victims and Bankruptcy Cases** per Fed. Cir. R. 47.4(a)(6).

Dated: April 3, 2026

Respectfully Submitted,

/s/ David L. Hecht

David L. Hecht
Hecht Partners LLP
125 Park Avenue, 25th Floor
New York, NY 10017
Tel: (212) 851-6821
E: dhecht@hechtpartners.com

TABLE OF CONTENTS

PATENT CLAIMS AT ISSUE i

CERTIFICATE OF INTEREST viii

TABLE OF CONTENTS x

TABLE OF AUTHORITIES xii

STATEMENT OF RELATED CASES 1

JURISDICTIONAL STATEMENT 3

INTRODUCTION 4

STATEMENT OF THE ISSUES 7

STATEMENT OF THE CASE 8

I. Conflicting Procedures 8

II. Explicit Claim Language at Issue 16

III. Final Determinations by the Office 19

SUMMARY OF ARGUMENTS 21

STANDARD OF REVIEW 23

I. Compliance with the Administrative Procedure Act 23

II. *De Novo* Claim Construction 25

ARGUMENT 26

I. Arbitrary and Capricious Proceedings 26

A. Abuse Of Discretion Through An Arbitrary And Capricious Stay 28

B. The First Arbitrary And Capricious Inconsistent Determination 31

C. The Second Arbitrary And Capricious Inconsistent Determination 35

II. Unconstitutional Proceedings Lacking Supervision 39

III. The PTAB Erred by Ignoring The Explicit Language of the Claims and Disclosure 42

A. The Explicit Language of the Claims Defines the Transaction and Principal Parties 43

B. The Disclosure Defines The Transaction and Principal Parties 44

IV. Remand is Unnecessary Because the Office has Already Determined the Claims are Patentable 48

CONCLUSION 49

ADDENDUM

CERTIFICATE OF COMPLIANCE

CERTIFICATE OF SERVICE

TABLE OF AUTHORITIES

Page(s)

Cases

Anacor Pharms., Inc. v. Iancu,
889 F.3d 1372 (Fed. Cir. 2018) 24

Arthrex, Inc. v. Smith & Nephew, Inc.,
35 F.4th 1328 (Fed. Cir. 2022) 40

Honeywell Int'l Inc. v. Arkema Inc.,
939 F.3d 1345 (Fed. Cir. 2019) 23

In re Magnum Oil Tools Int'l, Ltd.,
829 F.3d 1364 (Fed. Cir. 2016) 24, 27, 37

In re Power Integrations, Inc.,
884 F.3d 1370 (Fed. Cir. 2018) ..... *passim*

In re Suitco Surface, Inc.,
603 F.3d 1255 (Fed. Cir. 2010) 26, 43, 44, 48

In re Vivint,
14 F.4th 1342 (Fed. Cir. 2021) ..... *passim*

Microsoft Corp. v. Multi-Tech Systems, Inc.,
357 F.3d 1340 (Fed. Cir. 2004) 41, 42

Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.,
463 U.S. 29 (1983) 23

Teva Pharms. USA, Inc. v. Sandoz, Inc.,
574 U.S. 318 (2015) 25

United States v. Arthrex, Inc.,
141 S.Ct. 1970 (2021) 40

Vicor Corp. v. SynQor, Inc.,
869 F.3d 1309 (Fed. Cir. 2017) 4, 32

Statutes

5 U.S.C. §706 4

28 U.S.C. §1295(a)(4) 3

35 U.S.C. §102(e) 15, 36

35 U.S.C. §103 1

35 U.S.C. §103(a) 10

35 U.S.C. §141(c) 3

35 U.S.C. § 102 36

Regulations

37 C.F.R. §42.75(d) 8, 39

37 C.F.R. § 42.3(a) 12

37 C.F.R. § 42.8(b)(2) 29

37 C.F.R. § 1.116(b) 35

Other Authorities

MPEP § 706.0 34

MPEP § 2173.06(I) 38

STATEMENT OF RELATED CASES

This consolidated appeal arises from two final written decisions of the Patent Trial and Appeal Board ("PTAB") addressing the claims of U.S. Patent No. 8,886,954 (the 954 Patent):

- IPR2024-00233 (joined with IPR2024-01334): Determining claims 1,2, 4-7, 10, 12, 13, 15, 16, 18, 19, and 22–27 to be unpatentable under pre-AIA 35 U.S.C. §103 for being obvious over U.S. Patent No. 7,188,110 ("Ludtke") and dependent claims 3, 14, and 17 to be unpatentable under pre-AIA 35 U.S.C. §103 for being obvious over Ludtke in view of U.S. Publication No. 2002/0046336 ("Kon");
- IPR2024-00846: Determining claims 1, 2, 4, 5, 7–13, 15, 16, 18–24, and 26–29 to be unpatentable under pre-AIA 35 U.S.C. §103 for being obvious over U.S. Publication No. 2005/0050367 ("Burger"), dependent claims 3, 14 and 17 to be unpatentable under pre-AIA 35 U.S.C. §103 for being obvious over Burger in view of U.S. Publication No. 2003/0177102 ("Robinson"), and dependent claims 6 and 25 unpatentable under pre-AIA 35 U.S.C. §103 for being obvious over Burger in view of Robinson and U.S. Publication No. 2004/0049687 (Orsini).

Patent Owner/Appellants, Proxense LLC, appealed.

Co-pending with the IPRs was *ex parte* reexamination No. 90/015,052 (the 052 EPR) of the parent patent, U.S. Patent No. 8,352,730 (the 730 Patent), which terminated Jan 29, 2026, with the issuance of an *ex parte* reexamination certificate cancelling claims 1-17 and reissuing claims 18-34.

All district court proceedings involving the 954 Patent and/or its family members have been stayed pending the outcome of this appeal or terminated with settlement, as indicated below:

- *Proxense v. Samsung Electronics*, Co., Ltd. et al., No. 6:21-CV-00210-ADA (W.D. Tex.): Settled;
- *Proxense v. Google, LLC*, No. 6:23-cv-00320-ADA (W.D. Tex.): Settled;
- *Proxense v. Microsoft Corporation*, No. 6:23-cv-00319-ADA (W.D. Tex.): Stayed; and
- *Proxense v. Apple Inc.,* No. 6:24-cv-00143-ADA (W.D. Tex.): Stayed.

In *Proxense v. Apple Inc.*, a motion to lift the stay and dismiss the 954 Patent with prejudice filed by Patent Owner is fully briefed and currently pending determination.

JURISDICTIONAL STATEMENT

This is an appeal from final written decisions in *inter partes* reviews entered by the Patent Trial and Appeal Board (PTAB) on June 17 and October 17, 2025. (IPR2024-00233, Paper 35 (FWD)); and (IPR2024-00846, Paper 32 (FWD)). Appellant timely filed notices of appeals. (IPR2024-00233, Paper 39 (NOA)); and (IPR2024-00846, Paper 33 (NOA)). This Court has jurisdiction under 35 U.S.C. §141(c) and 28 U.S.C. §1295(a)(4).

INTRODUCTION

The PTAB wielded its control over its docket to suppress—and ultimately disregard—favorable determinations of patentability reached within the United States Patent and Trademark Office (Office) in contravention of the Administrative Procedure Act (APA), 5 U.S.C. §706, and binding precedent, including *In re Vivint,* 14 F.4th 1342 (Fed. Cir. 2021), and *Vicor Corp. v. SynQor, Inc.,* 869 F.3d 1309 (Fed. Cir. 2017).

At the time the challenged IPRs were instituted, *ex parte* reexamination No. 90/015,052 (the 052 EPR) on the parent patent, U.S. Patent No. 8,352,730 (the 730 Patent), was actively proceeding before the Central Reexamination Unit (CRU). *See* (IPR2024-00233, Ex. 2022 (Order Granting *Ex Parte* Reexam)). During the pendency of the IPRs, the 730 Patent and the related 954 Patent were patentably indistinct, containing nearly identical claims. Indeed, the PTAB itself recognized this overlap, rejecting claims in the 052 EPR on nonstatutory double patenting grounds over the 954 Patent, while simultaneously acknowledging that the claims were "not patentably distinct." (IPR2024-00846, Ex. 2017 (OA mailed July 29, 2025) at 12 ("Claims 18-34 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-29 of U.S. Patent No. 8,886,954. Although the claims at issue are not identical, they are not patentably distinct from each other.")).

Critically, the 052 EPR considered the same prior art and substantially the same grounds advanced in the IPR petitions—and rejected them. *See* (IPR2024-00233, Ex. 3003 (OA mailed May 20, 2025) at 4 ("The previous rejection under Ludtke is withdrawn.")); and (IPR2024-00846, Ex. 2017 (OA mailed July 29, 2025) at 15-30 and 57 ("[A]dopting the PTAB's rationale from IPR2024-00846 for Granting Institution of Inter Partes Review" but rejecting the claims on different statutory grounds)). The CRU withdrew prior rejections and declined to sustain the asserted grounds, even while acknowledging and expressly considering the PTAB's institution rationale. In short, the Office reached conclusions directly at odds with the positions advanced by the petitioners in the IPRs.

Faced with these unfavorable determinations, the PTAB intervened. Just as the CRU was poised to conclude the 052 EPR and issue a reexamination certificate, the PTAB *sua sponte* stayed the proceeding. (IPR2024-00233, Ex. 2037 (Stay) at 2 and 5 ("the parties notified the panel of a March 3, 2025, Office Action in the '052 reexam in which the Examiner proposed an Examiner's amendment to the claims… ORDERED that *ex parte* Reexamination No. 90/015,052 is stayed pending the termination or completion of IPR2024-00232."). Only after delaying the CRU's resolution did the PTAB proceed to a final written decision on the IPR, where it declared the claims of the 954 Patent unpatentable—while dismissing the CRU's contrary actions as irrelevant. (IPR2024-00233, Paper 35 (FWD) at 44) ("We treat

the Examiner's decision to withdraw the rejection involving Ludtke as a determination that that rejection is moot (and not an assessment of the merits), and her proposed amendment as withdrawn and, thus, of no relevance to this proceeding."). The PTAB characterized the Examiner's withdrawal of prior art rejections not as a merits determination, but as "moot," and disregarded the Examiner's proposed amendments altogether.

The pattern repeated itself in the second IPR (IPR2024-00846). Again, the CRU evaluated the same prior art and grounds asserted by the petitioner and declined to adopt them, issuing an Office Action that omitted those grounds in favor of different ones. *See* (IPR2024-00846, Ex. 2017 (OA mailed July 29, 2025) at 15-30 and 57 ("[A]dopting the PTAB's rationale from IPR2024-00846 for Granting Institution of Inter Partes Review" but rejecting on different statutory grounds)). Yet, although that Office Action was entered into evidence, the PTAB denied Patent Owner any meaningful opportunity to address it—precluding briefing and even prohibiting argument at the hearing. (IPR2024-00846, Ex. 3002 (RFAB) at 1); (IPR2024-00846, Paper 31 (Hr. Tr.) at 27:13-15 ("But as far as the reexam is concerned, if that's all you have to argue, then no we're not going to allow the argument of the reexam in this hearing.")). In doing so, the PTAB once more used its power of the docket to exclude and silence contrary agency findings.

The PTAB's actions did not stop there. It compounded this procedural imbalance by adopting a claim construction that departed from the plain language of the claims. To correct that misinterpretation, Patent Owner amended the claims of the 730 Patent during the 052 EPR. Upon doing so, the CRU confirmed what it had already indicated: the claims—properly construed—were patentable over the very prior art and grounds asserted in both IPRs. (EPR 90/015,052, NIRC at 14 ("However, neither Ludtke nor Burger discloses receiving an access message by an application from the agent allowing the user access to the application and complete a transaction of the user accessing the application, wherein the principal parties to the transaction are the user and the application.")). A reexamination certificate duly issued. (EPR Cert.).

This record presents a stark example of administrative overreach. By staying parallel proceedings, excluding material agency findings, and refusing to consider directly relevant evidence, the PTAB did not merely manage its docket—it used it as a tool to control the outcome. That conduct violates the APA and governing Federal Circuit precedent, and it cannot stand.

STATEMENT OF THE ISSUES

(1) Whether the PTAB violated the Administrative Procedure Act by using its control over its docket to stay parallel reexamination proceedings, exclude material

agency findings, and deny Patent Owner a meaningful opportunity to address contrary determinations of patentability by the Central Reexamination Unit.

(2) Whether disregarding contemporaneous findings of the Office—including CRU determinations evaluating the same prior art and grounds—and instead treating those findings as irrelevant or "moot," renders the PTAB's final written decisions arbitrary, capricious, and constitutes clear error.

(3) Whether the PTAB violated the Appointments Clause by issuing a FWD in IPR2024-00233 pursuant to 37 C.F.R. §42.75(d) without direction and supervision by a principal officer.

(4) Whether the PTAB erred in construing the claims of the 954 Patent contrary to their plain language, and in sustaining unpatentability determinations based on these erroneous constructions, where the properly construed claims were confirmed to be patentable during parallel reexamination proceedings.

STATEMENT OF THE CASE

I. CONFLICTING PROCEDURES

The PTAB used its power to control dockets to silence favorable determinations of patentability within the Office. Over a year prior to the filing of the Petitions, an *ex parte* reexamination was requested on the parent 730 Patent. (IPR2024-00233, Ex. 2023 (Reexam Request)). The IPRs presently at issue are three of several sequentially filed IPRs against different members of the same patent

family (i.e., IPR2024-00232, IPR2024-00233, IPR2024-00234, IPR2024-00775, IPR2024-00776, IPR2024-00846, IPR2024-01326, IPR2024-01327, IPR2024-01328, IPR2024-01333, IPR2024-01334, IPR2024-01335, IPR2024-01846, and IPR2024-01485). After institution, IPR Nos. 2024-00232, 2024-00233, and 2024-00234 were administratively joined, receiving a joint scheduling order and a joint oral argument. *See* (IPR2024-00233, Paper 11 (JSO)). Likewise, IPR Nos. 2024-00775 and 2024-00846 were administratively joined, receiving a joint scheduling order and a joint oral argument. *See* (IPR2024-00846, Paper 9 (JSO)).

In its preliminary briefing for IPR2024-00233, Patent Owner raised concerns regarding inconsistent results between the IPRs and the 052 Reexam. Specifically, Patent Owner noted that "the Petition relies on the same primary reference (Ludtke) and raises the same arguments already being considered by the Office in three pending EPRs (Applications Nos. 90/015,052, 90/015,053, and 90/015,054)." (IPR2024-00233, Paper 6 (POPR) at 20-21). In its subsequent preliminary sur-reply, Patent Owner repeated its concerns that "the risk of an inconsistent outcome is real – especially given that it appears a desire to avoid inconsistent actions has prevented the 052 and 054 Reexams from receiving their statutory mandated 'special dispatch.'". (IPR2024-00233, Paper 9 (Pre-Ins. Sur-Reply) at 5). The PTAB acknowledged that "Patent Owner state[d] that patents related to the '954 patent are

the subject of *ex parte* reexaminations in Application No. 90/015,052, reexamining the '730 patent." (IPR2024-00233, Paper 10 (DI) at 2-3).

Despite acknowledging that the 052 EPR was a related matter, the Board declined to stay the 052 EPR after institution. By permitting the 052 EPR to continue, the PTAB ceded jurisdiction to the CRU, which was allowed to decide (and did decide) the applicability of Ludtke to the question of patentability.

During the process of reaching a favorable determination of patentability, the CRU rejected the claims of the 730 Patent under pre-AIA 35 U.S.C. §103(a) over Ludtke alone. (IPR2024-00233, Ex. 2025 (OA mailed Sep. 12, 2024) at 15 ("Ludtke further discloses sending the device ID to the TPCH as part of the transaction as discussed above; however, if Ludtke is seen as not describing the specific 'transaction device information' that is provided to the TPCH or storing the secret decryption value, Okereke discloses this.")); *accord* (IPR2024-00233, Ex. 2021 (OA mailed Nov. 25, 2024) at 12); *accord* (IPR2024-00233, Ex. 2025 (FOA mailed Mar. 3, 2025) at 11). Eventually, an interview between the CRU and Patent Owner led to a determination that "[w]ere the claims to recite the ***access message being sent to/received by the application***, which is supported by the 730 Patent at col. 5, lines 23-26, the ***claims would be allowable over Ludtke***." (IPR2024-00233, Ex. 2027 (Exam. Interview Summary) at 5) (emphasis added). The Office reiterated this key determination in its subsequent Final Office Action.

> "Lastly, as presented by the Examiner in the Interview Summary mailed December 17, 2024, the claims would be allowed if amended to recite: receiving an access message by an application from the agent allowing the user to access the application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file."

(IPR2024-00233, Ex. 2035 (FOA) at 32) (emphasis in original)).

In response, Patent Owner submitted an after final amendment amending the claims as requested by the CRU. Notably, the amended limitation supporting the patentability of the 730 claims, "receiving an access message ***by an application,***" was identical to language already present in the independent claims of the 954 Patent ("receiving, ***at an application***, an access message").

On March 25, 2025, Apple and Patent Owner jointly submitted the CRU's Final Office Action and the proposed Examiner's Amendment to the PTAB. *See* (IPR2024-00233, Ex. 2036 (Joint Email)). In response, the PTAB acknowledged that "[i]n the Petition, Petitioner stated that the '730 patent is the subject of *ex parte* reexamination in *In re Proxense, LLC*, Application No. 90/015,052 (filed June 8, 2022) ('the '052 reexam')." (IPR2024-00233, Ex. 2037 (Stay) at 2). Nevertheless, the PTAB concluded that "[c]ontinuing to conduct the '052 reexam concurrently with the instant proceeding could potentially result in inconsistencies between the proceedings" and stayed the 052 EPR. (IPR2024-00233, Ex. 2037 (Stay) at 4).

Consequently, when the 052 EPR was all but concluded, the PTAB stayed the EPR thereby preventing entry of the Examiner's proposed amendment and issuance of a re-examination certificate.

The stay was subsequently lifted after Patent Owner requested Adverse Judgment in IPR2024-00232 to allow entry of the CRU's amendment. *See* (IPR2024-00233, Ex. 2038 (Judgment)). At that point, the Board no longer had jurisdiction over the 730 Patent, as the patent was no longer **involved in** an IPR proceeding before the Board. *See* 37 C.F.R. § 42.3(a) ("The Board may exercise exclusive jurisdiction within the Office over every ***involved application and patent*** during the proceeding, as the Board may order." (emphasis added)); and § 42.122(a) ("Where another matter ***involving the patent*** is before the Office, the Board may ***during the pendency of the inter partes review*** enter any appropriate order regarding the additional matter including providing for the stay, transfer, consolidation, or termination of any such matter." (emphasis added)). The amendment proposed by the Examiner was then entered and the rejection over Ludtke withdrawn. (IPR2024-00233, Ex. 3003 (OA mailed May 20, 2025) at 2-3 ("PO submitted after final amendments on March 8, 2025 ('March 2025 After Final Amendment'). These amendments are entered… The previous rejection under Ludtke is withdrawn.")). Yet, despite the amendment being entered and the rejection withdrawn, the PTAB decided to "treat the Examiner's decision to withdraw the rejection involving Ludtke

as a determination that that rejection is moot (and not an assessment of the merits), and her proposed amendment as withdrawn and, thus, of no relevance to this proceeding." (IPR2024-00233, Paper 35 (FWD) at 44). The PTAB thus failed to consider the 052 EPR and stated, "if we consider the '052 reexam, we see little relevance of its record to this proceeding." (IPR2024-00233, Paper 35 (FWD) at 44). The PTAB then proceeded to find the claims of the 954 Patent unpatentable over Ludtke.

Patent Owner requested director review of the PTAB's decision, asserting that allowing the "decision to stand would result in two inconsistent results on substantially similar issues and the same underlying facts." (IPR2024-00233, Paper 36 (Req. Dir. Review) at 1). At the time, Coke Morgan Stewart was the Acting Director of the Office. (IPR2024-00233, Paper 38 (Order) at FN. 2). Unfortunately, the Acting Director was recused and took no part in this decision and delegated her authority to Senior Lead APJ Michelle Ankenbrand. (IPR2024-00233, Paper 38 (Order) at FN. 2). Being recused, the Acting Director lacked the discretion to review the decision rendered by the Senior Lead APJ. Thus, the PTAB conducted director review of IPR2024-00233 without being directed and supervised at some level by a principal officer. Without offering a rationale to explain the inconsistent decisions, the Senior Lead APJ "ORDERED that the request for Director Review is denied." (IPR2024-00233, Paper 38 (Order) at 2).

Unlike the PTAB, Microsoft believes the 052 EPR is of significant relevance because the "'954 patent is a continuation of the '730 patent, and the claims are almost identical." (IPR2024-00846, Paper 16 (Mot. Stay) at 7). More importantly, Microsoft acknowledged "the Board found Ludtke-based prior art grounds rendered the challenged '954 patent claims invalid, whereas the [052 EPR] Examiner previously indicated allowability over Ludtke of similar claims." (IPR2024-00846, Paper 16 (Mot. Stay) at 1-2). Thus, when the "Examiner for the [052 EPR] issued a non-office action advancing new art rejections almost identical to the invalidity grounds," Microsoft immediately filed a motion to stay the EPR to "reduce the risk of inconsistent outcomes in the [052 EPR] and 954 IPR." (IPR2024-00846, Paper 16 (Mot. Stay) at 1-2). In support of its motion to stay, Microsoft further acknowledged that any inconsistencies "will likely raise (here or on appeal) APA violation concerns," which is the reason for the present appeal. (IPR2024-00846, Paper 16 (Mot. Stay) at 3).

Of course, Microsoft's motion was filed before the July 29th Office Action ((IPR2024-00846, Ex. 2017)) had issued. At that time, there was just overlapping prior art but no indication the CRU had considered the rationale underlying the institution of these proceedings. That, however, changed when the Examiner stated she "hereby adopts the PTAB's rationale from IPR2024-00846 for Granting Institution of *Inter Partes* Review ('IPR-2024-00846 GIIPR') of related U.S. Pat.

No. 8,886,954 (‘the '954 Patent’) dated November 18, 2024.” (IPR2024-00846, Ex. 2017 (OA mailed July 29, 2025) at 57). Despite considering and adopting the PTAB’s rationale, the Examiner rejected the claims “under pre-AIA 35 U.S.C. [§]102(e) as being anticipated by U.S. Pub. No. 2005/0050367 to Burger et al. (‘Burger’)” and not for being obvious over Burger as asserted in Microsoft’s Petition. ((IPR2024-00846, Ex. 2017 (OA mailed July 29, 2025) at 15)). The CRU thus considered the PTAB’s institution rationale **and rejected it** for failing to establish unpatentability by a preponderance of the evidence. Despite accurately predicting the APA violations at issue in this Appeal, the PTAB was unable to take the action Microsoft requested because Microsoft “offered no authority for [the PTAB] to stay the reexamination of a patent not at issue in this proceeding.” (IPR2024-00846, Paper 23 (Order Denying Stay) at 4).

While the PTAB may have lacked the power to stay the 052 EPR, the July 29th Office Action ((IPR2024-00846, Ex. 2017)) considered and rejected the grounds of unpatentability at issue in IPR2024-00846. Accordingly, Patent Owner requested additional briefing to address the developments in the 052 EPR. (IPR2024-00846, Ex. 3002 (RFAB) at 1). While the PTAB authorized submission of the July 29th Office Action, it did not authorize any additional briefing. (IPR2024-00846, Ex. 3002 (RFAB) at 1). The PTAB further denied Patent Owner an opportunity to address the admitted evidence during trial. When Patent Owner attempted to discuss

the July 29th Office Action, the PTAB firmly rebuked any efforts to do so, stating "as far as the reexam is concerned, if that's all you have to argue, then no we're not going to allow the argument of the reexam in this hearing." (IPR2024-00846, Paper 31 (Hr. Tr.) at 27:10-15). After denying the Patent Owner opportunity to address the EPR proceedings, the PTAB presented rationale on first instance regarding the July 29th Office Action. (IPR2024-00846, Paper 32 (FWD) at 38-41). As neither Microsoft nor Patent Owner were given the opportunity to brief or argue the July 29th Office Action, the PTAB's decision was necessarily not based on arguments that either party advanced, nor to which a party was given a chance to respond. Rather, the PTAB adopted arguments on behalf of Microsoft.

II. EXPLICIT CLAIM LANGUAGE AT ISSUE

The PTAB ignored express language of the claims that gave meaning to the construction of "a third party that operates a trusted authority". The PTAB construed the term as "a trusted authority that is an entity separate from the parties to a **transaction**." (IPR2024-00233, Paper 10 (DI) at 12); (IPR2024-00233, Paper 35 (FWD) at 9, 11); and (IPR2024-00846, Paper 32 (FWD) at 11). Petitioner had "agree[d] with the Board's construction." (IPR2024-00233, Paper 16 (Pet. Reply) at

5)[1]. Microsoft similarly failed to propose a different construction. *See* (IPR2024-00846, Paper 14 (Pet. Reply) at 3-9).

The PTAB's construction defines the third party with respect to the ***transaction*** and ***parties***. Neither term appears in the claim nor specification. Furthermore, the PTAB never defined the transaction, holding instead that "[t]he language of claim 1 does not expressly identify the parties to a transaction," (IPR2024-00233, Paper 35 (FWD) at 11). This is problematic because "we evaluate a party's ***relationship to the transaction*** to determine whether it is a principal party to the transaction or a third-party." (IPR2024-00846, Paper 8 (DI) at 11) (emphasis added). Without defining the transaction and the principal parties, the PTAB failed to construe the claims.

However, the claims do define the transaction. For instance, claim 1 includes a series of steps that ends with "allowing the user access to the application." Claim 1 defines the transaction as the user accessing the application. Furthermore, this explicit language clearly identifies the user and the application as the transaction's principal parties. The PTAB, however, held that "[t]his language does not specify, one way or the other, whether 'an application' is the second party to a transaction." (IPR2024-00233, Paper 35 (FWD) at 11). Yet, the PTAB noted with reference to Fig.

[1] After Google withdrew from the IPR, Apple—having filed a parallel petition that was joined to Google's—continued the proceeding and adopted Google's arguments.

7 (reproduced below) that "receiving a request for authentication with a code, determining whether the code is valid, authenticating the code, and transmitting an access code to the requester, which ***allows a user access to an application***" is an example of from the specification in which the principal "parties are the user and the application." (IPR2024-00233, Paper 10 (DI) at 11).

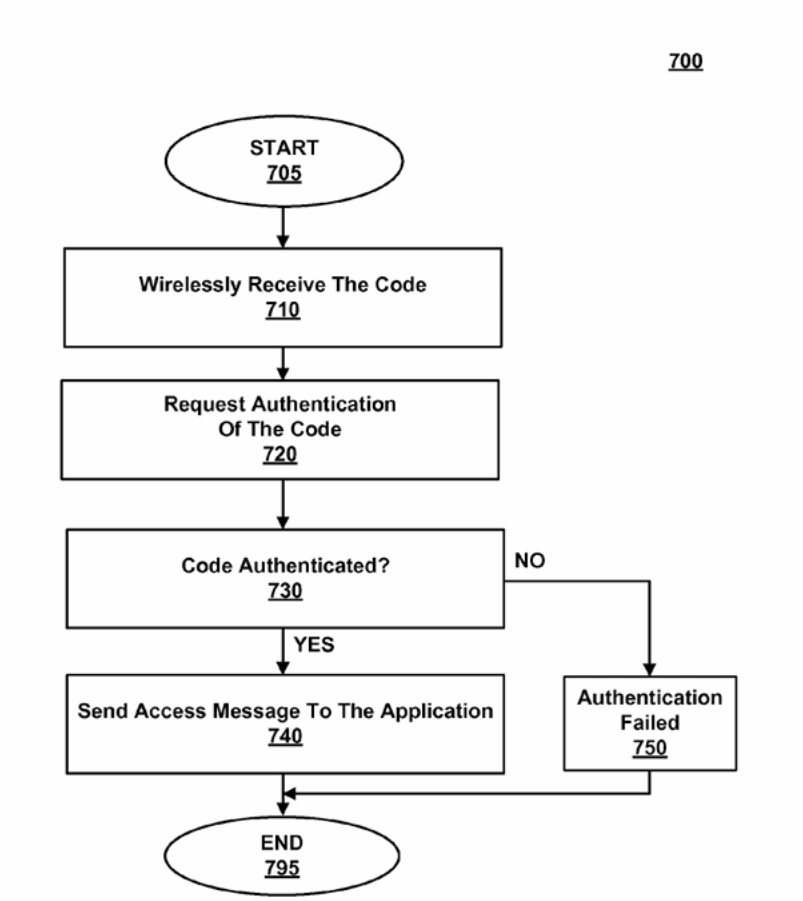


FIG. 7

The series of actions the PTAB identified as constituting a transaction in which the user and the application are the principal parties is repeated explicitly

within claim 1. For instance, claim 1 explicitly recites "***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," identical to "receiving a request for authentication with a code." Claim 1 continues by explicitly reciting "that the trusted authority successfully ***authenticated the one or more codes*** and other data values sent," i.e. the action of "authenticating the code." Finally, claim 1 concludes with "receiving, at an application, ***an access message*** from the trusted authority … ***allowing the user access to the application***" as to explicitly recite "transmitting an access code…, which allows a user access to an application."

Despite the identical transaction being recited in the claims, the PTAB failed to construe the transaction and identify the principal parties thereto. Instead, the PTAB held that "[t]he language of claim 1 does not expressly identify the parties to a transaction," (IPR2024-00233, Paper 35 (FWD) at 11). Accordingly, the PTAB ignored language of the claims reciting a transaction in which the principal parties are the user and the application. In so doing, the PTAB silenced the claims.

III. FINAL DETERMINATIONS BY THE OFFICE

After the FWDs in IPR No. 2024-00233 and IPR2024-00846, the Patent Owner amended the claims to clarify they were restricted to the transaction depicted in Fig 7 in which "1) the user to complete a transaction of the user accessing the application and 2) principal parties to the transaction be the user and the application."

(EPR 90/015,052, NIRC at 13). Citing IPR2024-00846 Final Written Decision, Oct 17, 2025, p. 10, the Examiner noted that "nowhere in the record of the related proceedings have the newly added limitations been addressed" because "the claim construction had supported a broadest reasonable interpretation that encompassed several possibilities for the parties." (EPR 90/015,052, NIRC at 13). The Examiner then noted that with respect to Ludtke, the "TPCH acts as a third-party between a vendor and user for purchases of electronic content such as software and digital files." (EPR 90/015,052, NIRC at 14). With respect to Burger, the Examiner concluded a "network server acts as a third-party and facilitates transactions between the user of the Pocket Vault and advertisers, non-financial media issuers, and financial media issuers." (EPR 90/015,052, NIRC at 14). The Examiner made the determination that "neither Ludtke nor Burger discloses receiving an access message by an application from the agent allowing the user access to the application and complete a transaction of the user accessing the application, wherein the principal parties to the transaction are the user and the application." (EPR 90/015,052, NIRC at 14). Accordingly, the Examiner found the construction that the Patent Owner consistently advanced in the IPRs, and rejected by the PTAB, rendered the claims patentable over the grounds and prior art asserted in IPR2024-00233 and IPR2024-00846. Patent Owner continues to advance that construction in this Appeal. As this construction is based on the explicit language and is fully consistent with the

specification, the Office has already determined the claims as properly construed are patentable over the grounds and prior art asserted in each IPR.

SUMMARY OF ARGUMENTS

The PTAB repeatedly used its control over its docket to suppress contrary findings of patentability reached within the Office, in violation of the APA. First, the PTAB stayed the 052 EPR only after the Examiner in the CRU had evaluated the primary reference in IPR2024-00233 (Ludtke) and proposed an amendment that would render the claims patentable. The timing was no coincidence: the stay halted a proceeding that was poised to confirm patentability over the very grounds asserted in the IPR.

The PTAB then compounded that interference by attempting to erase the CRU's analysis from the record. It dismissed the Examiner's withdrawal of the Ludtke-based rejection as "not a determination on the merits" and incorrectly characterized the proposed Amendment as withdrawn—thereby stripping the CRU's conclusions of any legal significance. Additionally, the PTAB employed the same tactic again in IPR2024-00846, disregarding the CRU's evaluation of the primary reference (Burger) after the Office had declined to adopt the asserted grounds. This pattern is not case management—it is outcome control. By staying proceedings, excluding relevant agency findings, and denying Patent Owner the opportunity to

address them, the PTAB violated the APA's core requirement of reasoned decision-making. Its decisions therefore cannot stand and must be vacated.

The constitutional defect is equally fatal. IPR2024-00233 proceeded without direction and supervision by a principal officer, rendering the proceeding unconstitutional. Because the PTAB expressly relied on that decision in reaching its final written decision in IPR2024-00846, the latter is irreparably tainted—the paradigmatic fruit of the poisonous tree. As such, both final written decisions must be vacated on that independent ground.

The PTAB's errors extend to the merits. The Board adopted a claim construction that ignored the explicit language of the claims and the specification of the 954 Patent. The claims recite a transaction of "allowing the user access to the application," in which the principal parties are the user and the application. Rather than apply that language, the PTAB effectively rewrote the claims and specification to reach a different result. That legally erroneous construction redefines the transaction, is unreasonably broad, and cannot support a finding of unpatentability.

Finally, remand would serve no purpose. The Office has already determined—through the CRU—that the claims, when properly construed, are patentable over the same prior art and grounds asserted in both petitions. There is nothing left for the agency to decide. The Court should reverse the unpatentability determinations and bring this matter to a close.

STANDARD OF REVIEW

I. COMPLIANCE WITH THE ADMINISTRATIVE PROCEDURE ACT

Agency compliance with the APA governs every aspect of an IPR. This Court "review[s] the Board's decisions under the standards set forth in the APA." *In re Vivint,* 14 F.4th 1342, 1348 (Fed. Cir. 2021). That review "is not limited to the four corners of a final agency action" and includes "preliminary, procedural, or intermediate agency actions or rulings that are not directly reviewable before a final action." *Vivint,* 14 F.4th at 1348. Accordingly, the Court must evaluate the entirety of the proceedings under the APA and "must set aside an agency action that is either an ***abuse of discretion*** or ***arbitrary and capricious***." *Vivint,* 14 F.4th at 1351 (emphasis added).

An abuse of discretion occurs where agency action "(1) is clearly unreasonable, arbitrary, or fanciful; (2) is based on an erroneous conclusion of law; (3) rests on clearly erroneous fact findings; or (4) involves a record that contains no evidence on which the [agency] could rationally base its decision." *Vivint,* 14 F.4th at 1351; citing *Honeywell Int'l Inc. v. Arkema Inc.,* 939 F.3d 1345,1348 (Fed. Cir. 2019) "A decision is arbitrary and capricious when the agency fails to articulate a rational connection between the facts found and the choice made." *Vivint,* 14 F.4th at 1351; citing *Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.,* 463 U.S. 29, 43 (1983).

Critically, an agency also acts arbitrarily and capriciously when it "***departs from established precedent*** without a reasoned explanation." *In re Vivint,* 14 F.4th at 1351-52 (emphasis added). Such a departure arises where the agency applies the same law to the same facts yet reaches conflicting conclusions. *Vivint,* 14 F.4th at 1352-1355 (holding that the Office acted arbitrarily and capriciously when the CRU and PTAB in IPR proceedings applied the same law to the same facts and achieved inconsistent results).

Any "reasoned explanation" must itself satisfy the APA. While a reasoned explanation allows for inconsistent results, the PTAB may not supply its own theories to justify a result; rather, it must base its decision on arguments advanced by the parties and supported by evidence to which both sides had notice and an opportunity to address. The PTAB is not "***free to adopt arguments on behalf of petitioners*** that could have been, but were not, raised by the petitioner during an IPR." *In re Magnum Oil Tools Int'l, Ltd.,* 829 F.3d 1364, 1381 (Fed. Cir. 2016) (emphasis added). Nor may the Board rely on evidence without affording the parties a fair opportunity to address. *See Anacor Pharms., Inc. v. Iancu*, 889 F.3d 1372, 1380 (Fed. Cir. 2018).

Accordingly, to withstand APA review, the PTAB must ground its reasoning in the record, in arguments properly presented by the parties, and in procedures that afford notice and an opportunity to address. Where it fails to do so—particularly

where it reaches results inconsistent with parallel agency proceedings without adequate explanation—its decision cannot stand.

II. *DE NOVO* CLAIM CONSTRUCTION

This Court reviews the PTAB's claim construction *de novo* where it is based on intrinsic evidence, and reviews any subsidiary factual findings based on extrinsic evidence for clear error. *See Teva Pharms. USA, Inc. v. Sandoz, Inc.* 574 U.S. 318, 331-332 (2015). Where, as here, the intrinsic record resolves the meaning of disputed terms, review is entirely *de novo. In re Power Integrations, Inc.* 884 F.3d 1370, 1375 (Fed. Cir. 2018).

"Claim construction must begin with the words of the claims themselves". *Power Integrations,* 884 F.3d at 1376 (internal citation omitted). A construction that is overly expansive and fails to define a functional relationship is problematic. *Power Integrations,* 884 F.3d at 1376 ("Under the board's overly expansive view of the term 'coupled,' every element anywhere in the same circuit is potentially 'coupled' to every other element in that circuit, no matter how far apart they are, how many intervening components are between them, or whether they are connected in series or in parallel."); *id*. ("The problem is that the board's claim construction does not define what type of functional relationship is required."). Thus, claims cannot be construed in a manner that would render them indefinite and effectively unbounded.

Equally impermissible are constructions that render claim language meaningless. *Power Integrations,* 884 F.3d at 1376 ("Another problem with the board's claim construction is that it renders claim language meaningless."). Thus, claims must be construed in a manner that does not contradict or delete the explicit language of the claims.

Finally, "claims should always be read in light of the specification and teachings in the underlying patent." *In re Suitco Surface, Inc.,* 603 F.3d 1255, 1260 (Fed. Cir. 2010). A construction that does not "reasonably reflect the plain language and disclosure" will not pass muster. *Suitco,* 603 F.3d at 1260.

ARGUMENT

I. ARBITRARY AND CAPRICIOUS PROCEEDINGS

The PTAB repeatedly used its procedures to silence contrary findings of the CRU, in clear violation of the APA. This Court's review of PTAB's actions under the APA "is not limited to the four corners of a final agency action" but extends to "preliminary, procedural, or intermediate agency actions or rulings that are not directly reviewable before a final action." *Vivint,* 14 F.4th at 1348. The full record must therefore be considered—and that record reveals a proceeding fundamentally at odds with the APA.

The PTAB's decisions rest on clearly erroneous findings of fact that directly contradict the Office's administrative record. Such action is the definition of an

abuse of discretion. *Vivint,* 14 F.4th at 1351. At the same time, the PTAB repeatedly failed to articulate any rational connection between the facts it purported to find and the conclusions it reached—rendering its decisions arbitrary and capricious. *Vivint,* 14 F.4th at 1351.

The error is even more stark when viewed against the CRU's parallel determinations. Not once, but twice, the PTAB applied the same law to the same prior art and reached conclusions irreconcilable with those of the Office—without explanation. That is precisely the circumstance in which this Court has held agency action unlawful. *Vivint,* 14 F.4th at 1352-1355 (holding that the Office acted arbitrarily and capriciously when the CRU and PTAB in IPR proceedings applied the same law to the same facts and achieved inconsistent results). An unexplained departure from materially identical agency determinations is the hallmark of arbitrary and capricious decision-making, and the PTAB offered no reasoned basis for doing so here. *In re Vivint,* 14 F.4th at 1351-52.

Instead, the PTAB substituted its own reasoning for that of the parties, relying on arguments never advanced and never tested through the adversarial process. That, too, violates the APA. *See Magnum Oil Tools,* 829 F.3d at 1381 (holding that under the APA "the Board must base its decision ***on arguments that were advanced by a party***, and to which the opposing party was given a chance to respond." (emphasis added)).

This is not a case of ordinary error. It is a pattern: ignoring the administrative record, failing to provide reasoned explanations, and reaching inconsistent outcomes on identical facts—all while depriving the parties of a fair opportunity to respond. The APA does not permit such arbitrary and capricious decision-making. The PTAB's decisions must be vacated.

A. Abuse of Discretion through an Arbitrary and Capricious Stay

The PTAB stayed the 052 EPR only after the Examiner had evaluated the primary reference in IPR2024-00233 (Ludtke) and proposed an amendment that would render the claims patentable. That timing is dispositive. The stay rests on clearly erroneous factual findings and severs any rational connection between the facts and the PTAB's decision. The stay is thus arbitrary and capricious — an abuse of discretion that cannot stand.

As the PTAB acknowledged, the "052 reexam also consider[ed] the patentability of the claims over Ludtke, the primary reference." (IPR2024-00233, Ex. 2037 (Stay) at 4). "By email to the Board on March 25, 2025 (Ex. 3003), the parties notified the panel of a March 3, 2025, Office Action in the '052 reexam in which the Examiner proposed an Examiner's amendment to the claims." (IPR2024-00233, Ex. 2037 (Stay) at 2). Specifically, the Examiner proposed "the claims would be allowed if amended to recite: receiving an access message ***by an application*** from the agent allowing the user to access the application, wherein the application is

selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file." (IPR2024-00233, Ex. 2035 (FOA mailed Mar. 3, 2025) at 32) (emphasis in original). In other words, the Examiner had already determined that claims that were substantially identical to the ones at issue here, if those claims had been construed properly in the IPR, were patentable over the very reference (Ludtke) at issue in the IPR.

Rather than allow that determination to proceed to conclusion and be the end of IPR2024-00233, the PTAB stayed the 052 EPR. (IPR2024-00233, Ex. 2037 (Stay)).

The PTAB attempted to justify the stay by asserting that "Patent Owner's Mandatory Notices omitted the '052 reexam from the listed Related Matters pursuant to 37 C.F.R. § 42.8(b)(2)" and "did not file updated Mandatory Notices identifying such developments in the '052 reexam." (IPR2024-00233, Ex. 2037 (Stay) at 2-3). The record refutes both assertions. First, in its own Institution Decision, the PTAB acknowledged that "Patent Owner states that patents related to the '954 patent are the subject of *ex parte* reexaminations in Application No. 90/015,052, reexamining the '730 patent." (IPR2024-00233, Paper 10 (DI) at 2-3). That alone renders the PTAB's contrary finding clearly erroneous.

The PTAB's second assertion that Patent Owner failed to provide updates fares no better. By the PTAB's own account, "[b]y email to the Board on March 25, 2025 (Ex. 3003), the parties notified the panel of a March 3, 2025, Office Action in the '052 reexam in which the Examiner proposed an Examiner's amendment to the claims." (IPR2024-00233, Ex. 2037 (Stay) at 2). The PTAB simultaneously criticized Patent Owner for submitting "an unauthorized brief by email detailing communications in the '052 reexamination that occurred at least as early as December 2024"—confirming that it was, in fact, receiving notice of those developments. (IPR2024-00233, Ex. 2037 (Stay) at 2). The Board cannot both acknowledge receipt of timely updates and fault Patent Owner for failing to provide them. Its finding is internally inconsistent and unsupported by the record. And these factual errors are not incidental; they are the stated basis for the stay. Because the stay "rests on clearly erroneous fact findings," it constitutes an abuse of discretion. *Vivint*, 14 F.4th at 1351.

The PTAB's alternative justifications fare no better. The Board characterized the 052 EPR as a duplication of effort. (IPR2024-00233, Ex. 2037 (Stay) at 4). Yet, the PTAB had permitted both proceedings to run in parallel for several months, since its Institution Decision. Further, as noted above, by the time of the stay, any overlap had effectively ended: the Examiner had already evaluated Ludtke and determined that the claims—substantially identical to those at issue in the IPR—were patentable

. There was no ongoing duplication to prevent, and thus no rational connection between the facts and the decision to stay.

The PTAB also asserted that the Examiner's proposed amendment could affect the claims. (IPR2024-00233, Ex. 2037 (Stay) at 4). That is beside the point. The Examiner's proposal would have resolved the overlap between the proceedings by rendering the challenged claims allowable or moot. Far from justifying a stay, it eliminated any basis for one.

In short, the PTAB relied on factual findings contradicted by its own record and invoked justifications untethered to the actual posture of the proceedings. The only effect—and evident purpose—of the stay was to halt a proceeding that was about to confirm patentability over the very reference at issue in the IPR. The PTAB's use of its docket in this manner was not case management; it was outcome control. The stay must be set aside.

B. The First Arbitrary and Capricious Inconsistent Determination

The PTAB next attempted to silence the CRU by dismissing its determinations regarding IPR2024-00233's primary reference (Ludtke) as not a determination on the merits and by erroneously asserting that the Examiner's proposed Amendment was withdrawn. The PTAB's decision rests on clearly erroneous factual findings that sever any rational connection between the facts and the decision reached. The result is an arbitrary and capricious decision, and an abuse of discretion, that cannot stand.

Under controlling precedent, "[a]gency action that '***departs from established precedent*** without a reasoned explanation is ***arbitrary and capricious***." *In re Vivint,* 14 F.4th at 1352 (emphasis added). This Court has consistently held that concurrent parallel Office proceedings cannot produce inconsistent results without a reasoned explanation. *Id.* at 1352-1355 (holding that the Office acted arbitrarily and capriciously when the CRU and PTAB in IPR proceedings applied the same law to the same facts and achieved inconsistent results.); *Vicor Corp. v. SynQor, Inc.,* 869 F.3d 1309, 1323 (Fed. Cir. 2017) (holding that "[b]ecause the Board did not provide any reasoned explanation for the inconsistent result across the two reexaminations, we *vacate and remand* the Board's decision."). A failure to provide such an explanation violates the APA.

Here, the CRU in the 052 EPR determined that claims reciting "***receiving by an application*** an access message from the agent ***allowing the user access to the application***" were patentable over Ludtke.[2] By contrast, the PTAB held that substantively similar claims in IPR2024-00233—reciting "***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***"—were

[2] The claims of the 730 Patent define an "agent" as a "third-party trusted authority." *See* 730 Patent, claim 1 ("an agent that is a third-party trusted authority").

unpatentable over the same reference, Ludtke.[3] Despite the near identity of the claim limitations, the Board offered no reasoned explanation for its inconsistent result.

Both sets of claims recite receiving an "access message" from a "third party trusted authority" and performing the identical function of "allowing the user access to the application." The only difference is the preposition describing where the access message is received. Yet in both instances, it is the application receiving the access message. Accordingly, there is no meaningful distinction between the claims. Microsoft itself confirmed this, noting that the "'954 patent is a continuation of the '730 patent, and the claims are almost identical." (IPR2024-00846, Paper 16 (Mot. Stay) at 5). The Office corroborated this determination: the CRU determined the claims to be patentably indistinct and nearly identical, rejecting them under nonstatutory double patenting. (IPR2024-00846, Ex. 2017 (OA mailed July 29, 2025) at 12 ("Claims 18-34 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-29 of U.S. Patent No. 8,886,954. Although the claims at issue are not identical, they are not patentably distinct from each other.")).

Despite this, the PTAB concluded the claims were unpatentable over Ludtke, relying on factually erroneous statements. The Board claimed that "the Examiner's

[3] The claims of the 954 Patent define "third-party" and "trusted authority" as a "third-party trusted authority." *See* 954 Patent, claim 1 ("third party that operates a trusted authority").

decision to withdraw the rejection involving Ludtke [was] a determination that that rejection is moot (and not an assessment of the merits), and her proposed amendment as withdrawn and, thus, of no relevance to this proceeding." (IPR2024-00233, Paper 35 (FWD) at 44). Both assertions are plainly contradicted by the record.

First, the Examiner's proposed amendment was entered. The Office explicitly states: "PO submitted after final amendments on March 8, 2025... ***These amendments are entered.***" (IPR2024-00233, Ex. 3003 (OA mailed May 20, 2025) at 2) (emphasis added). Second, the Examiner had made a clear determination on the merits, proposing that "the claims ***would be allowed if amended***" in accordance with the CRU's guidance. (IPR2024-00233, Ex. 2035 (FOA mailed Mar. 3, 2025) at 32) (explaining that the amendment should "recite: receiving an access message ***by an application*** from the agent allowing the user to access the application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.") (emphasis in original). The subsequent withdrawal of the final rejection in the May 2025 Office Action confirms that the CRU concluded the amended claims were patentable over Ludtke, consistent with MPEP § 706.07(e)[4] and 37 C.F.R.

[4] "[o]nce a final rejection that is not premature has been entered in an application/reexamination proceeding, it should not be withdrawn at the applicant's or patent owner's request except on a showing under 37 C.F.R. § 1.116(b)."

§1.116(b).[5] ((IPR2024-00233, Ex. 3003)). Indeed, the May 2025 Office Action was **a non-final office action** mailed after the March 3, 2025, Final Office Action. Under Section 1.116(b), in response to the Final Office Action, Patent Owner amended the claims as directed by the CRU – *i.e.,* to recite "***receiving by an application***."

The PTAB ignored these facts, failed to engage with the CRU's reasoning, and relied on its own, unsupported factual findings. This constitutes precisely the type of arbitrary and capricious action that the APA prohibits. *In re Vivint,* 14 F.4th at 1351-52. Agency action is an abuse of discretion when it "rests on clearly erroneous fact findings." and this Court "must set aside an agency action that is either an ***abuse of discretion*** or ***arbitrary and capricious***." *Vivint,* 14 F.4th at 1351 (emphasis added).

Accordingly, the Final Written Decision in IPR2024-00233 must be vacated.

C. The Second Arbitrary and Capricious Inconsistent Determination

In addition to the stay and the final written decision in IPR2024-00233, the PTAB further attempted to silence the CRU by dismissing its determinations regarding the primary reference in IPR2024-00846 (Burger). After entering the Examiner's proposed amendment and withdrawing the rejection over Ludtke, the CRU proceeded to reject the amended claims "under pre-AIA 35 U.S.C. [§] 102(e)

[5] An amendment after a final rejection may be entered that "compl[ies] with any requirement of form expressly set forth in a previous office action."

as being anticipated by Burger." (IPR2024-00233, Ex. 3003 (OA mailed May 20, 2025) at 7). Microsoft recognized the convergence of grounds across proceedings, noting that at that time the 052 EPR and the 954 IPR involved similar claims, prior art, and construction issues, creating a "serious risk of inconsistent decisions being issued by different entities (CRU and PTAB) of the same agency (USPTO)." (IPR2024-00846, Paper 16 (Mot. Stay) at 1-2).

Microsoft acknowledged that the "'954 patent is a continuation of the '730 patent, and the claims are almost identical." (IPR2024-00846, Paper 16 (Mot. Stay) at 5). The CRU had already determined that, during the pendency of the IPR, these claims were "not patentably distinct from each other," rejecting them "on the ground of nonstatutory double patenting." (IPR2024-00846, Ex. 2017 (OA mailed July 29, 2025) at 12). To ensure consistency, the CRU expressly "adopt[ed] the PTAB's rationale from IPR2024-00846 for Granting Institution of *Inter Partes* Review … of related U.S. Patent No. 8,886,954." (IPR2024-00846, Ex. 2017 (OA mailed July 29, 2025) at 57). Notably, the CRU's analysis explicitly considered the Petition, the Institution Decision, and Dr. Traynor's testimony regarding obviousness, yet rejected the claims solely for being anticipated by Burger under 35 U.S.C. § 102, not § 103.

Despite these findings, the PTAB precluded Patent Owner from presenting arguments or addressing evidence during trial. (IPR2024-00846, Paper 31 (Hr. Tr.)

at 27:13-15) (the PTAB stating at trial that "as far as the reexam is concerned, if that's all you have to argue, then no we're not going to allow the argument of the reexam in this hearing."). And while the PTAB authorized submission of the July 29th Office Action, no additional briefing was permitted. (IPR2024-00846, Ex. 3002 (RFAB) at 1). The PTAB then presented a rationale on first instance regarding the July 29th Office Action. (IPR2024-00846, Paper 32 (FWD) at 38-41).

Under the APA, the PTAB's approach is impermissible. "[T]he Board must base its decision ***on arguments that were advanced by a party***, and to which the opposing party was given a chance to respond." *Magnum Oil Tools,* 829 F.3d at 1381 (emphasis added). Here, no such arguments were permitted. The PTAB's rationale is thus a decision of its own making——a direct violation of the APA.

The PTAB further attempted to characterize its rationale as responsive to arguments presented "for the first time at the oral argument" by Patent Owner. (IPR2024-00846, Paper 32 (FWD) at 40). This characterization is contradicted by the record: the Board explicitly told Patent Owner that "we're not going to allow the argument of the reexam in this hearing." (IPR2024-00846, Paper 31 (Hr. Tr.) at 27:13-15). It is impossible for a party to present arguments they were not allowed to argue.

The PTAB's manufactured rationale also contradicts the Office's own records. The PTAB acknowledged that the "Examiner 'adopts the PTAB's rationale from

IPR2024-00846 for Granting Institution of Inter Partes Review Paper 8 of related '954 patent." (IPR2024-00846, Paper 32 (FWD) at 40). Yet, the PTAB simultaneously described the §103 obviousness grounds as "back-up obviousness rejections based on what Patent Owner might argue in the future." (IPR2024-00846, Paper 32 (FWD) at 41). This is logically impossible: Grounds already considered and adopted by the Examiner cannot simultaneously depend on hypothetical future arguments. Furthermore, §103 rejections are based on prior art, not on arguments made by the Patent Owner. The record confirms that the Examiner had the relevant prior art, evidence, and grounds before her and chose not to assert them—yet somehow the PTAB faulted her rationale.

This reasoning is self-contradictory and violates established USPTO procedure. Under MPEP § 2173.06(I), "the examiner should ***review each claim for compliance with every statutory requirement*** for patentability in the initial review of the application and ***identify all of the applicable grounds of rejection*** in the first Office action to avoid unnecessary delays in the prosecution of the application." (Emphasis added.) (IPR2024-00846, Paper 32 (FWD) at 41). Section 103 is a statutory requirement. The PTAB acknowledges the rationale was adopted from IPR2024-00846's Institution Decision, which identified §103 as an applicable ground. Yet, the PTAB contends the Examiner chose not to assert it even if meritorious—an untenable position.

Accordingly, the PTAB's decision is grounded in clearly erroneous factual findings, contradicts the Office's own records and policies, and relies on arguments of its own making rather than those advanced by the parties. Such action is precisely what the APA forbids. The Final Written Decision in IPR2024-00846 must be vacated for violating the APA.

II. UNCONSTITUTIONAL PROCEEDINGS LACKING SUPERVISION

Between the issuance of the decisions in IPR2024-00233 and IPR2024-00846, Patent Owner requested director review pursuant to 37 C.F.R. § 42.75(d), noting that the PTAB's decision in IPR2024-00233 "violates the Administrative Procedure Act ('APA') by failing to provide a reasoned explanation for reaching an inconsistent result with a prior determination by the Office." (IPR2024-00233, Paper 36 (Req. Dir. Review) at 1). The resulting Order denying review was issued by the PTAB itself because the Acting Director was recused. (IPR2024-00233, Paper 38 (Order)).

The recusal of the Acting Director exposes the constitutional infirmity here: IPR2024-00233 was conducted without supervision or direction by a principal officer. Administrative patent judges (APJs) are inferior officers, and "unreviewable authority wielded by APJs during *inter partes* review is incompatible with their appointment by the Secretary to an inferior office." *United States v. Arthrex, Inc.,* 141 S.Ct. 1970, 1985 (2021). Accordingly, APJs "must be 'directed and supervised at some level by others who were appointed by Presidential nomination with the

advice and consent of the Senate." *Arthrex,* 141 S.Ct. at 1980. In the USPTO, that supervisory authority resides with the Director. While the Constitution does not require "the Director [to] review every decision of the PTAB. What matters is that the Director have the discretion to review decisions rendered by APJs." *Arthrex,* 141 S.Ct. at 1988.

When Patent Owner requested director review, the Director was absent, and Deputy Director Coke Morgan Stewart was serving as Acting Director of the Office. (IPR2024-00233, Paper 38 (Order) at FN. 2). Critically, the Acting Director was "recused and took no part in [the] decision" (IPR2024-00233, Paper 38 (Order) at FN. 2). Rather than delegating her authority to the Commissioner for Patent as contemplated by this Court in *Arthrex, Inc. v. Smith & Nephew, Inc.,* 35 F.4th 1328 (Fed. Cir. 2022), the Acting Director delegated authority to Senior Lead APJ Michelle Ankenbrand. (IPR2024-00233, Paper 38 (Order) at FN. 2). As a result, no principal officer had the discretion to supervise or direct the PTAB during this period. The Senior Lead APJ denied the request for Director Review without explanation. (IPR2024-00233, Paper 38 (Order) at 2). This unsupervised exercise of authority renders IPR2024-00233 unconstitutional.

The constitutional defect taints IPR2024-00846. The PTAB explicitly relied on the final written decision in IPR2024-00233 to support its determinations in IPR2024-00846, including claim construction. (IPR2024-00846, Paper 32 (FWD) at

11) ("For the same reasons, and based on the same evidence, given in the '233 FWD, we maintain our construction of 'a third party that operates a trusted authority,' namely, 'a trusted authority that is an entity separate from the parties to a transaction,' and make clear that such a transaction is not limited to those in which the principal parties are the user being allowed access and the application being accessed."). Consequently, because IPR2024-00233 was unconstitutional, the final written decision in IPR2024-00846 is tainted by the same defect and must be vacated.

Even if one assumes IPR2024-00846 were somehow cleansed of this contamination, its claim construction independently fails. The PTAB "maintain[ed its] construction of 'a third party that operates a trusted authority'" without considering the 052 EPR, which is prosecution history of the parent 730 Patent. (IPR2024-00846, Paper 32 (FWD) at 11). "Claim interpretation begins with the claims themselves, the written description, and, if in evidence, ***the prosecution history***." *Microsoft Corp. v. Multi-Tech Systems, Inc.,* 357 F.3d 1340, 1346 (Fed. Cir. 2004) (emphasis added). Furthermore, "the prosecution history of one patent is relevant to an understanding of the scope of a common term in a second patent ***stemming from the same parent application***." *Microsoft,* 357 F.3d at 1349. The PTAB, however, explicitly dismissed the 052 EPR as having "little relevance" to IPR2024-00233. (IPR2024-00233, Paper 35 (FWD) at 44).

Had the Director—or a delegated principal officer—exercised the constitutionally required supervision, the PTAB would have been directed to consider the 052 EPR in construing the claims of the 954 Patent. Doing so would have confirmed that the transaction in question necessarily involves the principal parties: the user and the application. Instead, unsupervised, the PTAB adopted a tainted construction that ignored critical prosecution history.

Accordingly, both IPR2024-00233 and IPR2024-00846 were conducted without constitutionally required supervision and direction, and the PTAB's decision in IPR2024-00846 is based on tainted claim construction. The final written decisions in both proceedings are therefore unconstitutional and must be vacated.

III. THE PTAB ERRED BY IGNORING THE EXPLICIT LANGUAGE OF THE CLAIMS AND DISCLOSURE

The PTAB silenced the claims by providing a construction that disregards the claims' explicit language. "Claim construction must begin with the words of the claims themselves." *Power Integrations,* 884 F.3d at 1376 (internal citation omitted). A construction that renders claim language meaningless is inherently flawed. *Power Integrations,* 884 F.3d at 1376 ("Another problem with the board's claim construction is that it renders claim language meaningless."). A construction that ignores functional relationships recited in the claims is likewise problematic. *Power Integrations,* 884 F.3d at 1376 ("Under the board's overly expansive view of the term 'coupled,' every element anywhere in the same circuit is potentially 'coupled' to

every other element in that circuit, no matter how far apart they are, how many intervening components are between them, or whether they are connected in series or in parallel… The problem is that the board's claim construction does not define what type of functional relationship is required."). Claims cannot be construed in a manner that reads out express limitations, leaving them indefinite and unbounded.

The proper approach is to adhere to the intrinsic record. "[C]laims should always be read in light of the specification and teachings in the underlying patent" and constructions must "reasonably reflect the plain language and disclosure." *Suitco,* 603 F.3d at 1260. The PTAB, however, disregarded explicit claim limitations and the specification, adopting an overly expansive construction that cannot stand.

A. The Explicit Language of the Claims Defines the Transaction and Principal Parties

The PTAB recognized that construing "a third party that operates a trusted authority" requires evaluating a party's relationship to a transaction. (IPR2024-00846, Paper 8 (DI) at 11). The claims of the 954 Patent explicitly recite a series of steps culminating in the ultimate action of "receiving, at an application, an access message … allowing the user access to the application." As the final step in the claims, this step defines the transaction itself. Yet the PTAB dismissed it, stating that the claim "does not specify, one way or the other, whether 'an application' is the second party to a transaction." (IPR2024-00233, Paper 35 (FWD) at 11). In doing

so, the PTAB effectively rendered the final step of the claim—its very purpose—meaningless.

The claims clearly describe the "trusted authority" as an intermediary that enables the application to receive an access message, ultimately "allowing the user access to the application." (954 Patent, claim 1). The sequence begins with the user performing biometric verification, sending a code to the trusted authority, which then authenticates the code and transmits an access message to the application. *Id.* The principal parties to this transaction are the user and the application, and the trusted authority functions as a third-party intermediary.

By ignoring this explicit sequence, the PTAB's construction divorces the term "transaction" from the claims' own language, rendering the principal parties and the role of the trusted authority opaque and nonsensical. A claim construction that renders claim language meaningless is problematic. *Power Integrations,* 884 F.3d at 1376 ("Another problem with the board's claim construction is that it renders claim language meaningless."). The PTAB's construction fails to "reasonably reflect the plain language and disclosure" and therefore cannot stand. *Suitco,* 603 F.3d at 1260.

B. The Disclosure Defines the Transaction and Principal Parties

The PTAB compounded its error by rewriting the specification to fit its construction. While it initially acknowledged that Fig. 7 (reproduced below) illustrates a transaction where the principal parties are the user and the application,

it later recast the examples to suggest the application is merely a resource of the owner, or that a casino or grocery store is the principal party. (IPR2024-00233, Paper 35 (FWD) at 13-14).

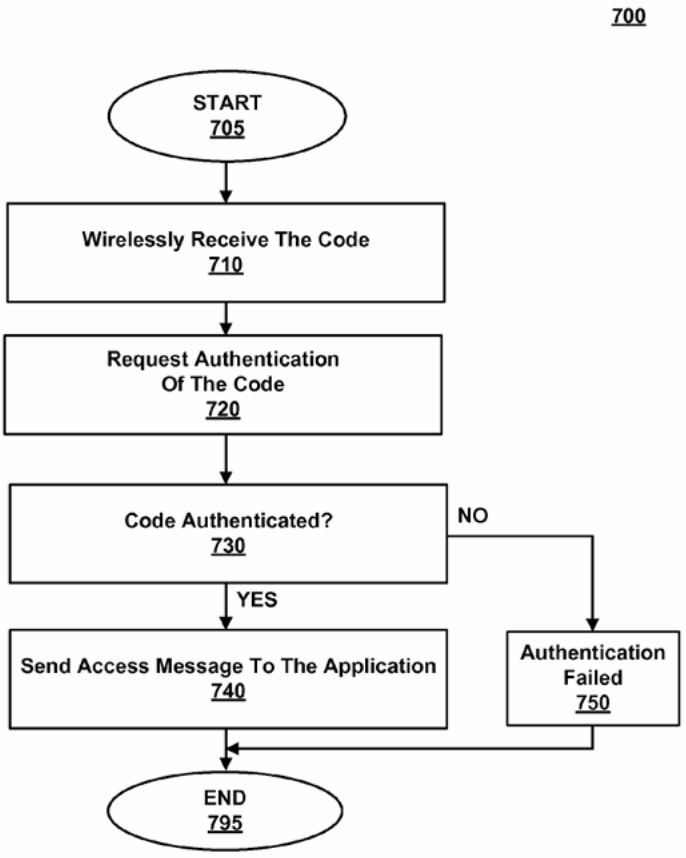


FIG. 7

The action that the PTAB identified as constituting a transaction in which the user and the application are the principal parties are repeated explicitly within claim 1. For instance, claim 1 explicitly recites "***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," identical to "receiving a request for authentication with a code." Furthermore, claim 1 continues by explicitly reciting "that the trusted authority successfully ***authenticated the one or more codes*** and other data values sent," i.e. the action of "authenticating the code." Finally, claim 1 concludes with "receiving, at an application, ***an access message*** from the trusted authority … ***allowing the user access to the application***" as to explicitly recite "transmitting an access code…, which allows a user access to an application." Accordingly, the construction consistently advanced by Patent Owner accurately reflects the disclosure.

When confronted with this undeniable truth, the PTAB began rewriting the specification. The specification explicitly states that the application is "a resource that can be accessed by a verified and authenticated user," indicating the application itself is being accessed. (954 Patent, 6:18-26). No actions after accessing the application are mentioned. Furthermore, there is no mention of any other party. Absent writing in parties and transactions, the specification does not "give[] several examples where the application being accessed is not, itself, a party to the transaction, but rather an asset of one of the parties or the mechanism by which the parties transact." (IPR2024-00233, Paper 35 (FWD) at 13).

Similarly, references to a casino or grocery store merely identify the location of the application—they do not introduce new parties or rewrite the transaction. (954

Patent, 6:67-7:6; 6:48-55). The specification only describes authentication followed by age verification to complete the transaction of accessing the application (i.e., slot machine). At most, the "casino" is only the location of the application. Likewise, the grocery store is merely a location of the application, e.g., an ATM located in the grocery store. The specification is silent regarding any transaction involving a casino, such as placing a bet. It is silent with respect to any transaction with the grocery store, such as making a purchase. Accordingly, absent writing in transactions, the specification does not disclose "the parties are the user and a casino, and the slot machine is the mechanism for the transaction, not itself a party" ((IPR2024-00233, Paper 35 (FWD) at 14)) nor "authentication of a transaction between a customer and a grocery store." (IPR2024-00233, Paper 35 (FWD) at 14).

The PTAB's creative reading would recast the specification and claims to replace "application" with "owner of the application," effectively changing the transaction to be between the user and the owner. This reinterpretation produces absurd results: in a home or garage scenario, the homeowner would be in a single-party transaction, transacting with themselves and eliminating the very possibility of a "third party that operates a trusted authority." The disclosure clearly states that "in a closed system, only known users are legitimate (e.g., owners of a home)." (954 Patent, 6:51-52). Such would be expected when the application is a keyless lock or garage door. However, extending the transaction to the owner of the application

would have the homeowner transacting with themselves to gain access to their own home or garage. This would be a one-party transaction. But it would be nonsensical for a one-party transaction to include "a third party operating as trusted authority," as the claims recite.

What the PTAB is attempting is to rewrite the disclosure, and the corresponding claims, to replace "application" with "owner of the application." This would change the end of claim 1 to recite "allowing the user access to the owner of the application." The transaction would then be between the user and the owner of the application. But this would render the claims' recitation of "a third party that operates a trusted authority" nonsensical.

By ignoring both the claims and the specification, the PTAB rewrote the disclosure and rendered critical claim limitations nonsensical. As the Federal Circuit has emphasized, constructions must "reasonably reflect the plain language and disclosure." *Suitco,* 603 F.3d at 1260. The PTAB's construction, which both rewrites the specification and ignores explicit claim language, is therefore unreasonably broad and cannot stand.

IV. REMAND IS UNNECESSARY BECAUSE THE OFFICE HAS ALREADY DETERMINED THE CLAIMS ARE PATENTABLE

The plain language of the claims, consistent with the specification and teachings of the 954 Patent, unambiguously recites a transaction of "allowing the user access to the application," in which the principal parties are the user and the

application. The Office has already determined that neither Ludtke nor Burger discloses this claimed transaction.

At the close of the 052 EPR, the Examiner expressly found that:

> "neither Ludtke nor Burger discloses receiving an access message by an application from the agent allowing the user access to the application and complete a transaction of the user accessing the application, wherein the principal parties to the transaction are the user and the application."

(EPR 90/015,052, NIRC at 14). Accordingly, the Examiner concluded that the claims, as properly construed, are patentable over the prior art grounds asserted in IPR2024-00233 and IPR2024-00846.

Given this prior determination, any remand would be unnecessary and would risk arbitrary or duplicative action by the Office. The proper course is to vacate the PTAB's determinations in their entirety. A remand would serve no purpose other than to expend resources and delay resolution. The clear and decisive record demonstrates that the claims are patentable, leaving no basis to alter that determination.

CONCLUSION

The PTAB's decisions in IPR2024-00233 and IPR2024-00846 are arbitrary, capricious, and in clear violation of the Administrative Procedure Act. The Board disregarded established procedural safeguards, failed to consider critical evidence, and relied on reasoning of its own making rather than arguments advanced by the

parties. Moreover, the PTAB adopted a claim construction that ignores the explicit language of the claims and the disclosure of the 954 Patent, rendering key limitations meaningless.

Proxense respectfully submits that these errors require reversal of the PTAB's determinations that claims 1-29 of the 954 Patent are unpatentable. Because the Office, through the 052 EPR, has already determined that the claims—when properly construed—are patentable over the primary references and grounds asserted in the IPRs, there is no need for remand. The record demonstrates that vacatur of the PTAB's decision is the only appropriate remedy.

Dated: April 3, 2026

Respectfully Submitted,

/s/ David L. Hecht

David L. Hecht
Hecht Partners LLP
125 Park Avenue, 25th Floor
New York, NY 10017
Tel: (212) 851-6821
E: dhecht@hechtpartners.com

ADDENDUM

ADDENDUM TABLE OF CONTENTS

Dkt.	Date	Document	Origin	Beg. No.
35	06/17/25	Final Written Decision: original	IPR2024-00233	Appx1
138	08/13/25	Order Denying Director Review of Final Written Decision	IPR2024-00233	Appx48
10	06/17/25	Final Written Decision: original	IPR2024-01334	Appx51
32	10/17/25	Final Written Decision: original	IPR2024-00846	Appx98
1001	N/A	U.S. Patent No. 8,886,954	ALL	Appx141

Trials@uspto.gov
571-272-7822

Paper 35
Entered: June 17, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

PROXENSE, LLC,
Patent Owner.

IPR2024-00233[1]
Patent 8,886,954 B1

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

MCKONE, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

[1] IPR2024-01334 has been joined with this proceeding.

I. INTRODUCTION

A. Background and Summary

Google LLC filed a Petition (Paper 1, "Pet.") requesting *inter partes* review of claims 1–7, 10, 12–19, and 22–27 of U.S. Patent No. 8,886,954 B1 (Ex. 1001, "the '954 patent"). The Board instituted an *inter partes* review of the challenged claims pursuant to 35 U.S.C. § 314. Paper 10 ("Inst. Dec."). Apple, Inc. ("Petitioner") joined the proceeding as a party on October 8, 2024, filing a duplicate petition. Paper 13. We terminated the proceeding as to Google, leaving Apple as the sole Petitioner. Paper 21.

After institution, Patent Owner filed a Patent Owner Response (Paper 14, "PO Resp."), Petitioner filed a Reply (Paper 16, "Reply"), and Patent Owner filed a Sur-reply (Paper 22, "Sur-reply"). The parties then presented oral arguments via a (video) Hearing (April 22, 2025), and the Board entered a Hearing transcript into the record (Paper 31, "Tr."). After the oral arguments, and pursuant to our authorization, Petitioner and Patent Owner submitted briefs addressing the preclusive effect, if any, of Patent Owner's Request for Adverse Judgement in IPR2024-00232. Paper 32 ("Pet. Estoppel Br."); Paper 33 ("PO Estoppel Br.").

For the reasons set forth in this Final Written Decision pursuant to 35 U.S.C. § 318(a), we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 1–7, 10, 12–19, and 22–27 are unpatentable.

B. Related Matters

The parties advise us that the '954 patent is involved in two district court cases, including *Proxense, LLC v. Google LLC*, No. 6.23-CV-00320 (W.D. Tex.). Pet. 70; Paper 4, 2. Petitioner also has filed petitions for *inter*

partes review of patents related to the '954 patent, including IPR2024-00232 (challenging U.S. Patent No. 8,352,730 B2 ("the '730 patent"); terminated after Patent Owner request for adverse judgment) and IPR2024-00234 (challenging U.S. Patent No. 9,298,905 B1 ("the '905 patent"); terminated after Patent Owner request for adverse judgment). Patent Owner states that patents related to the '954 patent are the subject of *ex parte* reexaminations in Application No. 90/015,052 ("the '052 reexam"), reexamining the '730 patent, Application No. 90/015,053, reexamining the '905 patent, and Application No. 90/015,054, reexamining U.S. Patent No. 10,698,989. Paper 6, 14. The '730 patent also was the subject of *Microsoft Corp. v. Proxense, LLC*, IPR2024-00775 (PTAB) (terminated after Patent Owner request for adverse judgment). The '954 patent also is the subject of *Microsoft Corp. v. Proxense, LLC*, IPR2024-00846 (PTAB) (currently pending).

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.

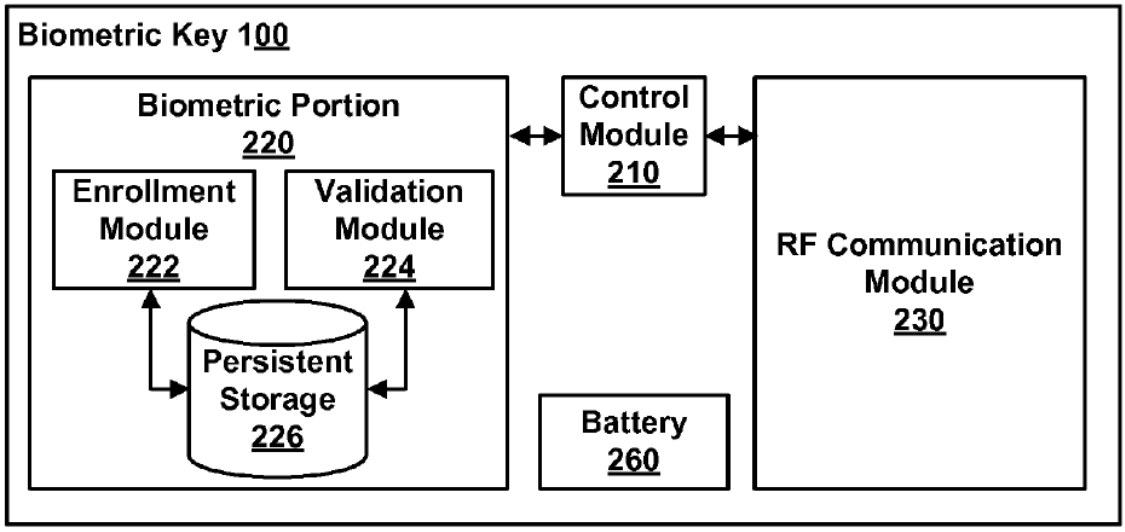


FIG. 2

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.

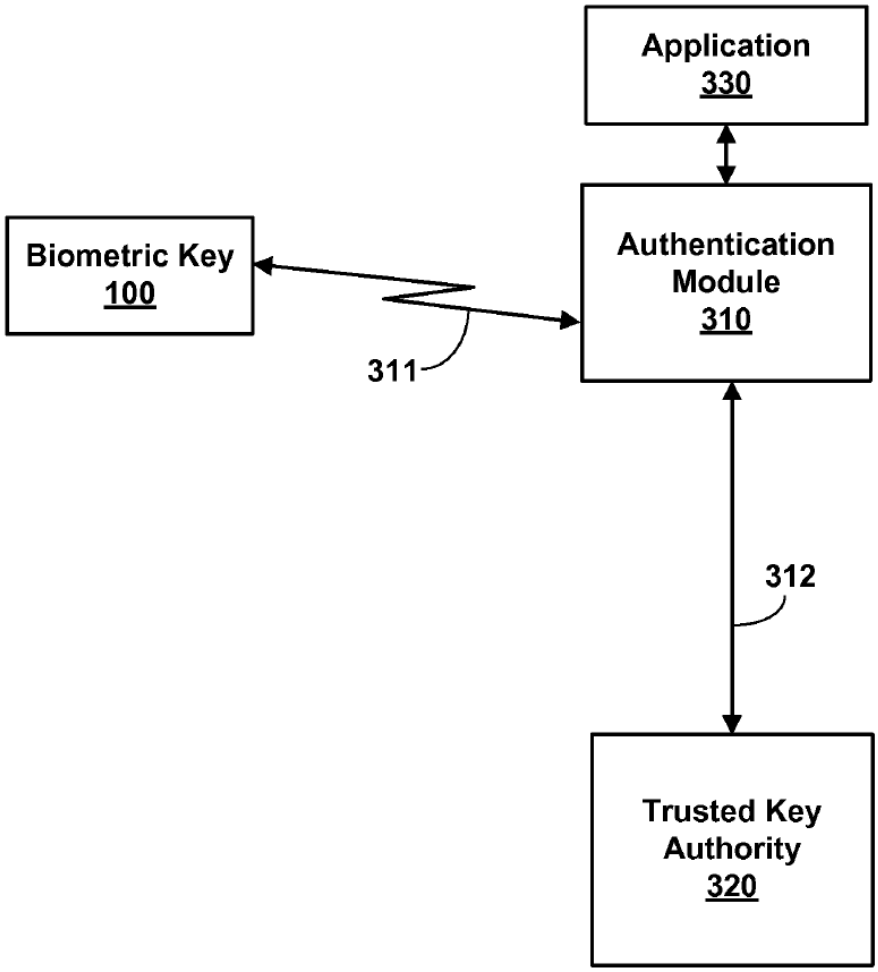


FIG. 3

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,[2] is illustrative of the claimed subject matter:

> 1. A method comprising:
>
> [1ai] persistently storing biometric data of a user and [1aii] a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and [1aiii] a secret decryption value in a tamper proof format written to a storage

[2] We add bracketed alphanumeric characters corresponding to those Petitioner uses in the Petition.

element on the integrated device that is not capable of being subsequently altered;

[1b] responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;

[1c] comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

[1d] 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

[1e] 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.
Ludtke	US 7,188,110 B1	Mar. 6, 2007 (filed Dec. 11, 2000)	1005
Kon	US 2002/0046336 A1	Apr. 18, 2002	1006

Petitioner also relies on the Declaration of Stephen Gray (Ex. 1003) and the Reply Declaration of Stephen Gray (Ex. 1026).

Patent Owner relies on the Declaration of Troy Carrothers (Ex. 2018).

E. The Asserted Grounds of Unpatentability

We instituted a trial under the following grounds:

Reference(s)	35 U.S.C. §	Claim(s) Challenged
Ludtke	103(a)[3]	1, 2, 4–7, 10, 12, 13, 15, 16, 18, 19, 22–27
Ludtke, Kon	103(a)	3, 14, 17

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.

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

[3] 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.

1. Third party that operates a trusted authority

Independent claims 1, 12, 16, and 22 each recite "a third party that operates a trusted authority."[4] In the Institution Decision, we preliminarily construed this term to mean "a trusted authority that is an entity separate from the parties to a transaction." Inst. Dec. 9–12.

Petitioner "agrees with the Board's construction, and submits that no further interpretation of third party trusted authority is warranted." Reply 5.

"Patent Owner agrees with this construction but challenges its application in the Petition, in particular the finding that the 'parties to a transaction' of the Patent (relative to the claimed third party trusted authority) can be a user and a vendor or merchant." PO Resp. 6. Instead, Patent Owner argues, "the parties could be either a user and an application (where a user is utilizing the claimed device or method) or, in another embodiment, a vendor and an application (where a vendor is utilizing the claimed device or method as a type of user)." *Id.* at 6–7. According to Patent Owner, "the specification and claim language at issue requires that at least one of the parties to the claimed transaction must be the application being accessed." *Id.* at 7.

[4] The parties also refer to this term as "third party trusted authority." The '730 patent, a parent of the '954 patent, was the subject of *Samsung Electronics America, Inc. v. Proxense LLC*, IPR2021-01444 (PTAB) (institution denied). *See* Ex. 1007 (IPR2021-01444, Paper 11 (PTAB Feb. 28, 2022) ("Samsung DDI")). In the Samsung DDI, the Board construed "third-party trusted authority" to mean "a trusted authority that is an entity separate from the parties to a transaction." Ex. 1007, 15. Patent Owner appears to contend that "third party that operates a trusted authority," recited in the '954 patent claims, has the same meaning as "third-party trusted authority," recited in the '730 patent claims. Petitioner does not appear to dispute this. We treat these terms as equivalent.

The language of claim 1 does not expressly identify the parties to a transaction. Claim 1 recites storing and processing biometric data of "a user." This suggests that a user could be a party to a transaction within the scope of claim 1. Claim limitation 1e recites "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." Independent claims 12, 16, and 22 have similar language. Patent Owner argues that "for all independent claims, the access message must be *received* from the 'trusted authority' and thus that 'trusted authority' **cannot be the same entity as the application under these claims**." PO Resp. 12–13. This language does not specify, one way or the other, whether "an application" is the second party to a transaction and Patent Owner cites no evidence to suggest that it does. Patent Owner cites *SIMO Holdings* for the proposition that an embodiment in the specification might not be included in a claim where there is probative evidence to the contrary. *Id.* (citing *SIMO Holdings Inc. v. Hong Kong uCloudlink Network Tech. Ltd.*, 983 F.3d 1367, 1378 (Fed. Cir. 2021)). However, that case does not support Patent Owner's overly narrow reading of the plain language of the claims.[5] Thus, the plain language of claim 1 does not limit the parties to a transaction between the user and an application, or require that one of the parties to a transaction be the application ultimately accessed.

[5] Patent Owner introduces and discusses new Exhibit 2034 in the Sur-reply, at 6–7. This exhibit violates Rule 42.23(b), which provides "[a] sur-reply may only respond to arguments raised in the corresponding reply and may not be accompanied by new evidence other than deposition transcripts of the cross-examination of any reply witness." We do not consider this new exhibit.

"We depart from the plain and ordinary meaning in only two instances," namely, "when a patentee acts as his own lexicographer," and "when the patentee disavows the full scope of the claim term in the specification or during prosecution." *Poly-Am., L.P. v. API Indus., Inc.*, 839 F.3d 1131, 1136 (Fed. Cir. 2016) (citing *Hill–Rom Servs., Inc. v. Stryker* Corp., 755 F.3d 1367, 1371 (Fed. Cir. 2014)). "Disavowal can be effectuated by language in the specification or the prosecution history. In either case, the standard for disavowal is exacting, requiring clear and unequivocal evidence that the claimed invention includes or does not include a particular feature." *Id.* (citing *Phillips*, 415 F.3d at 1316–17). According to the Federal Circuit, "disavowal requires that 'the specification [or prosecution history] make[ ] clear that the invention does not include a particular feature.'" *GE Lighting Sols., LLC v. AgiLight, Inc.*, 750 F.3d 1304, 1309 (Fed. Cir. 2014) (quoting *SciMed Life Sys. Inc. v. Advanced Cardiovascular Sys., Inc.*, 242 F.3d 1337, 1341 (Fed. Cir. 2001) (alterations in *GE Lighting*)).

As to the specification, Patent Owner argues that the '954 patent "only discloses embodiments where the parties to the transaction are a user and an application being accessed by that user." PO Resp. 10. In particular, Patent Owner cites to the examples of '954 patent Figures 3, 4, and 7. *Id.* at 10–12 (citing Ex. 1001, 2:35–48, 5:65–67, 6:8–34, 6:45–55, 6:64–66, 8:12–16, Figs. 3, 4, 7).

In one example cited by Patent Owner, describing Figure 3, the '954 patent states that "[s]ystem 300 comprises an authentication module 310 in communication with biometric key 100, a trusted key authority 320, and an application 330." Ex. 1001, 5:65–67. This passage does not state

that application 330 is a party to the transaction. The specification continues:

> Application 330 is a resource that can be accessed by a verified and authenticated user. 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, a financial account (e.g. a savings account, checking account, brokerage account, credit card account, credit line, etc.) and the like. In one embodiment, a file includes medical information such as a medical record, insurance information or other healthcare information.

Id. at 6:18–26. Petitioner argues that "an ATM is not a party to a transaction—the parties are the user and the bank, and the ATM is the mechanism through which the bank's accounts are accessed." Reply 5–6 (citing Ex. 1026 ¶ 13). Similarly, Petitioner argues, a file "is not a principal party to a transaction—rather the user and the provider of the file (e.g., a vendor) are the parties." *Id.* at 6 (citing Ex. 1026 ¶ 13). Petitioner makes similar arguments for financial accounts, savings accounts, medical records, and insurance information. *Id.* (citing Ex. 1001, 6:18–26; Ex. 1026 ¶ 14). We agree with Petitioner. The specification, here, gives several examples where the application being accessed is not, itself, a party to the transaction, but rather an asset of one of the parties or the mechanism by which the parties transact.

Patent Owner (PO Resp. 10) cites another example in which the '954 patent states "[i]n one embodiment, authentication can be required prior to allowing access to an application (e.g., application 330)." Ex. 1001, 6:64–66. However, the specification continues: "For example, a user can be standing proximate to a slot machine in a casino which requires that a user be over the age of 21. The slot machine can detect the biometric key in the

user's pocket, and, in response, spawn a conspicuous pop-up window on the slot machine requesting age verification." *Id.* at 6:66–7:4. Here, the parties are the user and a casino, and the slot machine is the mechanism for the transaction, not itself a party.

In another example, the '954 patent describes an "open system" in which "users can attempt authentication (e.g., in a public grocery store)." Ex. 1001, 6:48–51. The specification contrasts this with "a closed system," where "only known users are legitimate (e.g., owners of a home)." *Id.* at 6:51–55. Patent Owner argues that the grocery store example is only referring to the location of the application being accessed, and is not a transaction between a merchant and a user. PO Resp. 11–12. We disagree, and find that the '954 patent describes authentication of a transaction between a customer and a grocery store. Ex. 1001, 6:48–51. But even if Patent Owner's reading is correct, this example does not support limiting the claims to transactions in which one of the parties to the transaction is the application being accessed.

In short, Patent Owner points to no language in the specification limiting the claims to transactions in which the application being accessed is, itself, a party to the transaction and Petitioner points to several examples in which the application being accessed is not a party to the transaction. Thus, Patent Owner has provided no persuasive basis to depart from the plain and ordinary meaning of the claims.

In the Sur-reply, Patent Owner argues that, even if the specification supports a transaction having principal parties other than a user and the application being accessed, the language of the claims is limited to the parties being the user and the application being accessed; thus, the language of the claims controls and the unclaimed subject matter in the specification

should be disregarded. Sur-reply 7–8 (citing *Rolls-Royce, PLC v. United Technologies Corp.*, 603 F. 3d 1325, 1334 (Fed. Cir. 2010); *TIP SYSTEMS, LLC v. Phillips & Brooks/Gladwin*, 529 F. 3d 1364, 1373 (Fed. Cir. 2008)). However, as explained above, the plain language of the claims does not limit the parties to a transaction to the user and an application. Thus, Patent Owner's argument is unpersuasive.

Patent Owner also argues that Petitioner improperly applies "third-party trusted authority" in IPR2024-00232 (challenging the '730 patent). Sur-reply 8–9. In this proceeding, we evaluate whether Petitioner has shown that the challenged claims of the '954 patent are unpatentable, using the language of the claims of the '954 patent. Thus, Patent Owner's argument is inapposite and unpersuasive. Moreover, Patent Owner has admitted that the claims of the '730 patent, at issue in IPR2024-00232, are unpatentable and requested (and received) adverse judgment against itself. IPR2024-00232, Papers 29, 33; *see also* IPR2024-00775, Papers 14 (requesting adverse judgment as to claims 1–17 of the '730 patent), 15 (granting adverse judgment).

We maintain our construction of "a third party that operates a trusted authority," namely, "a trusted authority that is an entity separate from the parties to a transaction." Such a transaction is not limited to those in which the application being accessed is a party.

2. "access message"

Claim limitation 1e recites "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*." Independent claims 12, 16, and 22 recite similar language.

Petitioner notes that a District Court has construed "access message" to mean "[a] signal or notification enabling or announcing access." Pet. 4 (citing Ex. 1009, 3; Ex. 1010, 15, 20). However, Petitioner "maintains that the Board need not construe the term 'access message.'" Reply 6.

Patent Owner states that it "agree[s] on the construction of the term 'access message' to mean 'a signal or notification enabling or announcing access.'" PO Resp. 7. However, Patent Owner argues that applying "access message" to Ludtke's transaction confirmation "fails to account for the claim term 'access to an application.'" *Id.* at 7–8. Rather, Patent Owner argues, a transaction confirmation "is a message announcing that a transaction has been completed." *Id.* at 8. Patent Owner contends that "[t]he plain and ordinary meaning of 'access message' is a message enabling entry to, communication with, or use of an object wherein the object is the claimed application." *Id.* (citing *access*, MERRIAM-WEBSTER DICTIONARY (available at https://www.merriam-webster.com/dictionary/access)). Here, Patent Owner appears to retreat on its agreement that "access message" can include a signal "announcing" access, and suggests that we limit "access message" to a signal "enabling" access. However, Patent Owner then returns to its agreement, stating that "[i]t would be improper to construe 'access message' as something other than a signal or notification enabling or announcing a user's access to (ability to enter, communicate with, or make use of) an application." *Id.*

What Patent Owner appears to be arguing is that "access message" should be construed to mean "a signal or notification enabling or announcing

access," but that we should be further cognizant of the additional language in claim limitation 1e, "allowing the user access to the application."

We see no basis to depart from the District Court's construction of "access message," on which the parties appear to agree. However, we evaluate below Ludtke's applicability to the full scope of claim limitation 1e, including the language "allowing the user access to the application."

3. Remaining claim terms

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, 4–7, 10, 12, 13, 15, 16, 18, 19, and 22–27 over Ludtke

Petitioner contends that claims 1, 2, 4–7, 10, 12, 13, 15, 16, 18, 19, and 22–27 would have been obvious over Ludtke. Pet. 8–58. For the reasons given below, Petitioner has made a sufficient showing.

A claim is unpatentable under 35 U.S.C. § 103 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.[6] *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

1. Level of skill in the art

Petitioner contends that a person of ordinary skill in the art "would have had at least a bachelor's degree in Computer or Electrical Engineering or an equivalent engineering discipline, and at least three years of experience in the field of encryption and security, or the equivalent," and that "[a]dditional education could substitute for professional experience, and significant work experience could substitute for formal education." Pet. 4 (citing Ex. 1003 ¶¶ 31–32, 53–55). Patent Owner does not challenge Petitioner's proposed level of skill or propose an alternative in its papers.

Nevertheless, at the oral argument, Patent Owner argued that the level of skill we find should depend on how we construe the claims, namely, if we construe the claims broadly enough to encompass settlement of financial transactions where funds are transferred, then the level of skill should be found to include expertise in financial transactions. Tr. 38:21–41:10. We dismiss this argument as untimely. *See Dell Inc. v. Acceleron, LLC*, 884 F.3d 1364, 1369 (Fed. Cir. 2018) (noting that the "Board was obligated to dismiss [the petitioner's] untimely argument . . . raised for the first time during oral argument"). In any case, Patent Owner has pointed to no authority, and we are aware of no authority, in support of its position that the

[6] The complete record does not include allegations or evidence of objective indicia of nonobviousness.

level of skill in the art for a patent can change based on how the claims of the patent are construed.

Petitioner's proposal is consistent with the technology described in the specification and the cited prior art. On the complete record, we adopt Petitioner's proposed level of skill.

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

Ludtke describes techniques for identifying an authorized user with a biometric device and enabling the authorized user to access private information over a voice network. Ex. 1005, Abstract. Figure 4 of Ludtke, reproduced below, illustrates an example:

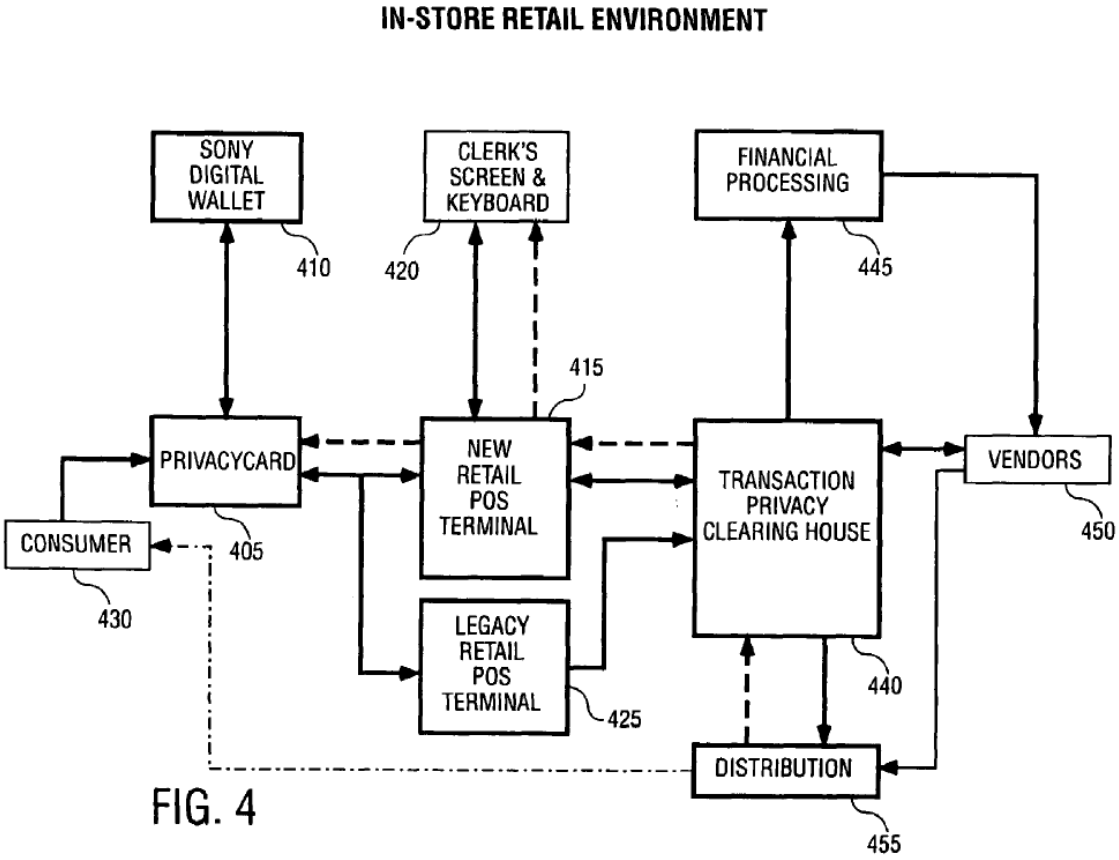


Figure 4 is a block diagram of an in-store retail system. *Id.* at 2:8–9.

In the retail environment of Figure 4, privacy card 405 interfaces with digital wallet 410 and retail point of sale (POS) terminal 415. *Id.* at 8:53–56. User 430 provides privacy card 405 and digital wallet 410 to POS terminal 415 or legacy retail POS terminal 425. *Id.* at 8:59–67. Transaction privacy clearing house (TPCH) 440 receives user 430's privacy card identification and determines whether the user has sufficient funds to perform the transaction. *Id.* at 9:1–3.

> In one embodiment, the transaction device(s), POS terminals and/or TPCH may function to verify the authenticity of each other. For example, a privacy card and digital wallet may be configured to verify the legitimacy of each other. Similarly, the transaction device may be configured to verify the legitimacy of the POS terminal and/or TPCH. A variety of verification techniques may be used. For example[,] lists of devices with account and/or access issues may be maintained. For example, in one embodiment, the public key infrastructure (PKI) may be used to verify legitimacy.

Id. at 5:11–20. "One means of authentication is some kind of PIN code entry. Alternately, authentication may be achieved by using more sophisticated technologies such as a biometric solution (e.g., fingerprint recognition)." *Id.* at 4:65–5:1. TPCH 440 interfaces with financial processing system 445, vendors 450, and distribution systems 455 to complete the transaction. *Id.* at 9:4–6.

Figure 17 of Ludtke is reproduced below:

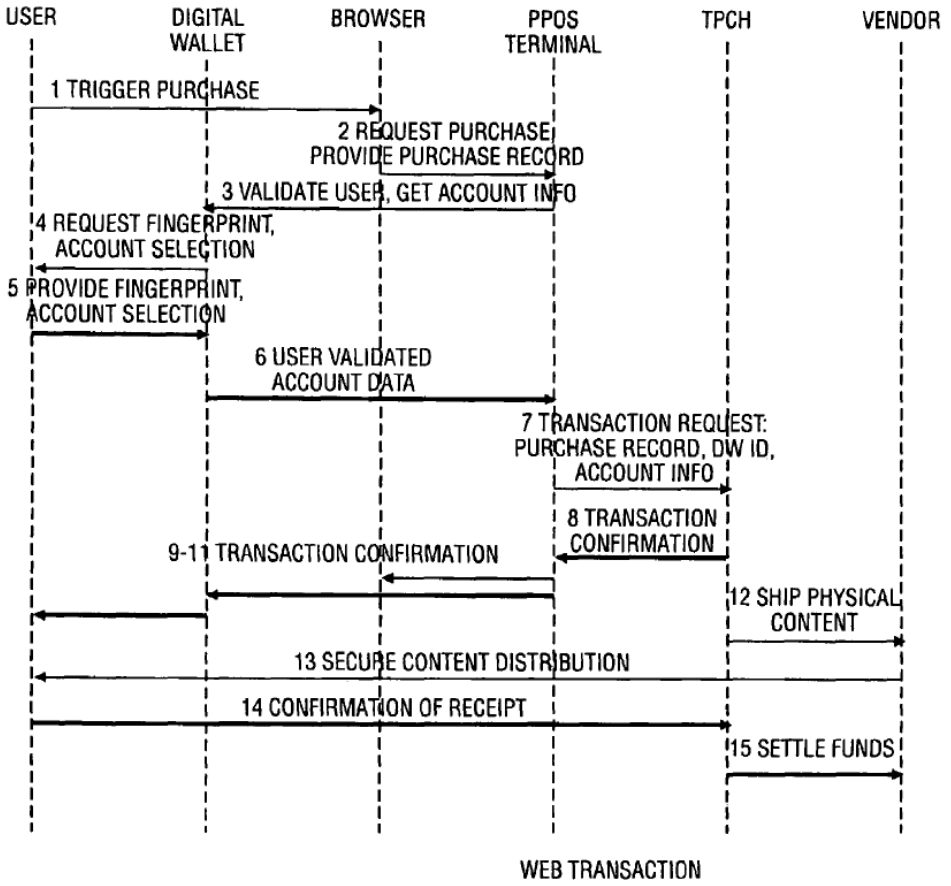


FIG. 17

Figure 17 is a flowchart of a process for performing a web-based transaction. *Id.* at 2:37–38. In this example,

> the user may be at home with a PC, cable, satellite or digital television device, a web browser, and a personal POS terminal device as described herein. The user has selected items to be purchased and is ready to trigger a purchase. The user may either navigate to a web page by using the facilities of the web browser, or by triggering a shopping activity using the transaction device.

Id. at 28:19–25.

The user triggers a purchase by clicking on a "Buy!" button in a web browser (step 1). *Id.* at 28:34–35. The browser, via a plug-in that allows it to communicate with a personal POS (PPOS) terminal integrated into the host personal computer (PC), communicates with the PPOS to initiate the

transaction and provide a record to the vendor (step 2). *Id.* at 28:35–40, 28:50–56. The PPOS terminal asks the transaction device to validate the user and get payment information from the user (step 3). *Id.* at 28:57–62. The user confirms the transaction and shows he or she is authorized by providing a fingerprint recognition sample to the transaction device (steps 4–5). *Id.* at 28:64–29:4. The transaction device validates that the user is authorized and the PPOS terminal sends to the TPCH the transaction record and the unique ID of the transaction device (steps 6–7). *Id.* at 29:5–14. The TPCH validates the transaction device, determines that the selected financial account has sufficient funds, and issues a transaction confirmation to the PPOS terminal (step 8). *Id.* at 29:15–18. The PPOS terminal sends the transaction confirmation to the web browser and transaction device (steps 9–11). *Id.* at 29:18–20. Secure distribution of physical or electronic content to the user is performed once the transaction is authorized (steps 12–13). *Id.* at 29:29–30. The TPCH then receives confirmation that content was delivered to the user and the TPCH processes settlement of funds. *Id.* at 29:31–34.

Ludtke describes various alternatives for the TPCH's involvement in funds settlement:

> The settlement of funds involves the transfer of the appropriate financial credit into the vendor's account. For the purposes of this example, it is assumed that the account is managed completely by the TPCH, and thus the funds transfer is handled completely inside of the TPCH. The vendor is not given any user identity information regarding the transaction; rather, the user is represented only by the transaction device identification information.
>
> In an alternative embodiment, the TPCH may issue a funds settlement request to a third party financial institution on behalf of the user, causing the necessary funds to be transferred to the vendor from the user's account. In yet another alternative

> embodiment, the TPCH may act as a proxy for the user, whereby the TPCH takes the funds from the user's account as managed by a third party financial institution, and then issues a funds transfer from the TPCH account to the vendor's account. This embodiment further preserves the user's identity by not linking it with the funds transfer into the vendor's account.

Id. at 29:35–53.

3. Differences, if any, between claims 1, 2, 4–7, 10, 12, 13, 15, 16, 18, 19, and 22–27 and Ludtke; reasons to modify

Regarding claim limitations 1ai, 1aii, and 1aiii, Petitioner argues that Ludtke teaches persistently storing, in a user identity/account information block of the transaction device, biometric information (e.g., fingerprint, retinal scan, voice, DNA, hand profile, face recognition), a plurality of codes and other values comprising a device ID code uniquely identifying the transaction device (e.g., globally unique silicon ID (GUID), magnetic strip, bar codes), and a secret decryption value (e.g., public key infrastructure (PKI) public keys and private keys). Pet. 9–21 (citing Ex. 1005, 5:11–20, 8:63–67, 9:18–25, 10:64–67, 11:1–5, 13:27–29, 13:39–41, 14:13–21, 19:9–14, 19:29–40, 23:11–19, 30:18–27, 37:39–45, 38:1–3, 38:9–21, 38:25–29, 38:40–61, 39:7–18, 40:5–26, Figs. 7B–7C, 27, 33; Ex. 1003 ¶¶ 73–94). Patent Owner does not contest Ludtke's applicability to these aspects of claim 1. Based on Petitioner's evidence, we find that Ludtke teaches claim limitations 1ai, 1aii, and 1aiii. More particularly, we find that Ludtke's fingerprint, retinal scan, etc., are "biometric data"; that Ludtke's GUID, magnetic strip, etc., are examples of "a device ID code uniquely identifying an integrated device"; and that PKI keys are examples of "a secret decryption value."

Regarding claim limitation 1b, Petitioner argues that Ludtke's transaction device requests and receives a fingerprint sample or other biometric data. *Id.* at 21–22 (citing Ex. 1005, 14:33–42, 14:40–46, 16:47–50; Ex. 1003 ¶¶ 95–96). As to claim limitation 1c, Petitioner argues that Ludtke's transaction device compares the fingerprint sample to stored authorized samples to determine a match. *Id.* at 22 (citing Ex. 1005, 14:40–46; Ex. 1003 ¶ 97). Patent Owner does not contest Ludtke's applicability to these aspects of claim 1. We agree with Petitioner and find that Ludtke teaches claim limitations 1b and 1c.

Claim limitation 1d recites:

> responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes from the plurality of codes and the 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 Ludtke describes the transaction device sending, over a wireless network, to the TPCH, a communication including a unique transaction device ID. Pet. 22–23 (citing Ex. 1005, 5:63–64, 7:46–48, 9:26–30, 9:35–42, 9:51–59, 28:50–29:12, 30:23–27; Ex. 1003 ¶¶ 98–106).

As to whether Ludtke teaches a determination of whether the scan data matches the biometric data, Petitioner points to Ludtke's description of the transaction device (digital wallet or privacy card) prompting the user to supply a fingerprint recognition sample, comparing the sample to stored fingerprints, and determining that the user is authorized if the supplied sample is recognized. *Id.* at 23–25 (citing Ex. 1005, 1:22–31, 1:37–38, 4:62–5:1, 14:33–46, 18:45–50, 18:52–55, 27:12–13, 28:13–18, 28:26–45, 28:50–29:12, 34:25–27; Ex. 1003 ¶¶ 99–103). As to whether Ludtke teaches wirelessly sending one or more codes for authentication, Petitioner points to

Ludtke's description of its transaction device sending the unique transaction device ID to the TPCH using wireless or cellular signals. *Id.* at 25 (citing Ex. 1005, 9:26–42; Ex. 1003 ¶ 103). Patent Owner does not contest Ludtke's applicability to these aspects of claim limitation 1d. We agree with Petitioner, and find that Petitioner's evidence shows that Ludtke teaches these aspects of claim limitation 1d.

Petitioner contends that Ludtke's TPCH is a third party that operates a trusted authority because it is an entity that is separate from the parties to the transaction. *Id.* at 25. Specifically, Petitioner contends that the parties to the transaction are the user (using the transaction device) and the external retailers and vendors that complete the transaction. *Id.* at 25–26 (citing Ex. 1005, 7:46–48 ("This allows the TPCH 110 to retain user privacy by not exposing addressing information and possibly email addresses to third parties."), 9:26–30, 9:35–39, 9:43–59, Fig. 6. As Ludtke states, "[i]n one embodiment of electric distribution, the TPCH 110 functions as the middleman of the distribution channel." Ex. 1005, 7:44–46.

Patent Owner contests Petitioner's identification of the user and the retailer as the parties to the transaction, and contends, instead, that the TPCH is both the application being accessed and a party to the transaction and, therefore, is not a third party that operates a trusted authority, as recited in claim limitation 1d. We address those arguments below with our analysis of Patent Owner's arguments for claim limitation 1e.

As to claim limitation 1e, Petitioner argues that, after the TPCH authenticates the transaction device ID, a webpage receives from the TPCH an indication of an approval of the transaction to be performed, and that the indication allows the user to access content or a reference to content on a

webpage. Pet. 28–29 (citing Ex. 1005, 24:17–32, 28:26–40, 29:15–20, 29:29–30, 31:41–52; Ex. 1003 ¶¶ 107–114). For example, Ludtke states:

> After validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction, the TPCH issues a transaction confirmation back to the personal POS terminal. The personal POS terminal reflects the transaction confirmation back to the web browser and the transaction device. The transaction device may display a transaction confirmation to the user and may additionally record the transaction in its local storage.
>
> . . .
>
> Secure distribution of physical (or electronic) content to the user is performed once the transaction is authorized.

Ex. 1005, 29:15–30. Mr. Gray testifies that "[t]he distributed content includes the content itself or a reference to that content, such as a 'web URL.'" Ex. 1003 ¶ 110. In this example, Petitioner contends that the "transaction confirmation" is an "access message" and that the content the user is allowed to access on the webpage is an "application." Pet. 30 (citing Ex. 1005, 29:15–22, 29:29–30; Ex. 1003 ¶ 110).

Petitioner relies on specific examples from Ludtke of new functionality and software that a user can download to the transaction device. *Id.* at 30–31 (citing Ex. 1005, 31:11–16, 19:45–50, 31:11–52; Ex. 1003 ¶¶ 112–113). For example, Ludtke states:

> In one embodiment, the transaction device can adapt to new services and functionality, either automatically by the transaction device or manually by the user. For example, on a web site the user might click a button that causes new functionality to be downloaded to the transaction device for access at a future time.

Ex. 1005, 31:12–16. In a specific example, "when arriving at a new airport, the transaction device might download a new service that provides

instructions for how to buy a train ticket to certain destinations." *Id.* at 31:30–33. Or, "if the transaction device finds itself in the presence of a service that is managed by an alternate system, it can download not only the service software, but also the necessary underlying 'transaction system' software. This might include new security protocols, etc." *Id.* at 31:35–40. Mr. Gray testifies that "[t]he downloaded functionality and software/service is an 'application' within the meaning of the '954 patent, which defines 'application' as 'a resource that can be accessed by a verified and authenticated user.'" Ex. 1003 ¶ 113 (citing Ex. 1005, 18:45–50, 31:11–52; Ex. 1001, 6:18–24).

Patent Owner argues that Ludtke's TPCH is the application being accessed in Ludtke's transactions and, therefore, that the TPCH cannot be a third party that operates a trusted authority because the trusted authority must not be the same entity as the application being accessed. PO Resp. 13. Patent Owner argues that "[t]he TPCH of Ludtke authenticates the transaction device, and confirms the transaction and authorizes it, [but] it does not split these steps up like the claims of the Patent at Issue require." *Id.* Patent Owner then points to examples in Ludtke where Patent Owner contends Ludtke confirms a transaction, and concludes that "[i]n all of the foregoing embodiments, TPCH both authenticates the device and confirms the transaction and the merchant accepts the confirmation as payment." *Id.* at 13–14 (citing Ex. 1005, 27:13–16, 29:15–34; Ex. 2018 ¶¶ 20–22). Patent Owner does not offer any persuasive support for its argument that the claims require that the third party that operates a trusted authority must not split up confirming and authorizing a transaction. If Patent Owner is arguing for a claim construction here, Patent Owner has not explained why the language of the claims, the specification, or the prosecution history support

this limitation, and we see no such evidence. Thus, Patent Owner's attempt to divide up the transaction in order to assign the TPCH the role of party rather than middleman is not persuasive.

Patent Owner argues that "the TPCH is being accessed to provide a payment to the merchant via a confirmation message (i.e., authorization), which completes the transaction," and that "[t]he TPCH of Ludtke is thus the application that the user is trying to access -- the ability to pay the vendor with the user's account (the private information) is the application." *Id.* at 14 (citing Ex. 2018 ¶¶ 20, 21, 30, 31). As we explained in our Institution Decision, however, the fact that "the TPCH is capable in certain embodiments of settling funds does not make it a 'party' to the transaction because it remains independent of the user, POS, and 'external' vendors." Inst. Dec. 21 (quoting Pet. 28). Rather, as we explained when preliminarily construing "third party that operates a trusted authority," active participation in a transaction, by itself, does not make an entity a party to that transaction. *Id.* at 11. Patent Owner offers no persuasive evidence suggesting that it does. Instead, we agree with Petitioner (Pet. 25–26) and find that the parties to the transactions described in Ludtke are the user of the transaction device (who seeks to purchase a good or service) and the retailer or vendor of that good or service.

Patent Owner further argues that "[i]n an attempt to establish an 'application' that is separate from the TPCH and the user, the Petition points to the disclosures of Ludtke that deal with settlement (the actual transfer of funds at some point after the transaction has been completed) rather than either authorization or transaction confirmation." PO Resp. 15 (citing Ex. 2018 ¶¶ 20–28); *see also* Sur-reply 11 ("Petitioner's rationale for why the TPCH is a 'third-party trusted authority' is that the TPCH processes

payments for 'web transactions.'"), 12 ("Thus, the rationale asserted in the Petition and reiterated in the Reply is that the online vendor completes the transaction by distributing the purchased items to the user after the user has provided payment via the TPCH."), 13 ("However, just because the user may engage in one transaction to fulfill their obligations in a second does not mean that the parties to the first transaction also become third parties with respect to the second. Rather, the web transaction is a separate and distinct transaction between the user and the vendor that is ***completed by the vendor***."). Patent Owner then discusses four examples in Ludtke and concludes that "[a]ll four of these settlement methods taught by Ludtke occur after the merchant has accepted the transaction confirmation (transaction authorization) issued by the TPCH as payment and has tendered the goods or services." PO Resp. 15–17 (citing Ex. 1005, 6:51–55, 7:12–20, 29:35–39, 29:43–46; Ex. 2018 ¶¶ 24–30).

Petitioner responds that the TPCH is not an "application," as claimed, because "it is not accessed by a *verified and authenticated user of the transaction device*—it 'functions as the middleman of the distribution channel.'" Reply 7–8 (quoting Ex. 1005, 7:44–48). We agree. Claim limitation 1e, for example, recites "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." Thus, according to the claim language, the claimed "application" is the application that receives an access message that indicates that the information received by the trusted authority from the user is authentic. Because the TPCH does not receive such an access message (the information it receives has not yet been authenticated), it is not the claimed application.

And, contrary to Patent Owner's arguments, we do not understand Petitioner to be arguing that issuance of payment (be it by the TPCH or by some other entity, such as a bank) is the transaction for purposes of identifying the parties and the application. Rather, Petitioner identifies the delivery of electronic content, new functionality, software, and services (e.g., electronic train tickets) to Ludtke's transaction device or to the user's web browser, in response to the transaction confirmation sent by the TPCH. Pet. 30–32; Reply 10–12. According to Mr. Gray, "Ludtke discloses receiving at the downloaded software/functionality (application) a transaction confirmation (access message) that allows the user to access the services prescribed by the downloaded software/functionality (application)." Ex. 1003 ¶ 114.

As to such additional software and services, Patent Owner argues that "the Petition does not identify an access message enabling or announcing access to these additional functionalities." Sur-reply 13. However, as Petitioner observes, Ludtke describes:

> After validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction, the TPCH issues a transaction confirmation back to the personal POS terminal. The personal POS terminal reflects the transaction confirmation back to the web browser and the transaction device. The transaction device may display a transaction confirmation to the user and may additionally record the transaction in its local storage. . . .
>
> Secure distribution of physical (or electronic) content to the user is performed once the transaction is authorized.

Ex. 1005, 29:15–23, 29:29–30. Mr. Gray testifies that "Ludtke discloses receiving at a web browser webpage (application) a transaction confirmation (access message) that allows the user to access electronic content on the web

browser (application)." Ex. 1003 ¶ 110 (citing Ex. 1005, 29:15–23, 29–30). Thus, Ludtke describes a webpage receiving a message that both enables and announces access to the additional functionality, software, and services. We find that this is an example of receiving, at an application (web browser or webpage), an access message (transaction confirmation) from the trusted authority (TPCH) indicating that the trusted authority successfully authenticated the codes from the transaction device and allowing the user access to the application (new electronic content available on the webpage).

Patent Owner further argues that each challenged claim "requires that the access message allow access to or announce access to an application" and that Petitioner "fails to account for this claim term." PO Resp. 17–18. Patent Owner argues that "Ludtke only discloses confirming a transaction," and "only provides a confirmation once the transaction has been fully completed." *Id.* at 18 (citing Pet. 29–31, 41–42, 54; Ex. 1005, 29:10–23; Ex. 1003 ¶ 112). Similarly, Patent Owner argues that

> Ludtke does not disclose a signal or notification enabling or announcing access to the digital content; Ludtke only discloses the delivery of that digital content to the user following the completion of a transaction. Thus, even if a vendor could be considered the application being accessed, the only thing disclosed in Ludtke is that a vendor can determine whether to deliver physical or digital goods to a user based on whether or not the vendor gets payment or a promise to pay **not** a signal enabling or announcing access.

Id. at 21–22 (citing Ex. 1005, 28:15–18, 28:26–40; 29:15–20, 31:41–50). Patent Owner misunderstands Ludtke. In the example of Figure 17, "[s]ecure distribution of physical (or electronic) content to the user is performed once the transaction is authorized," the TPCH then receives confirmation that the content was shipped to the user, and "[o]nce the

confirmation is received, the TPCH processes the settlement of funds." Ex. 1005, 29:29–34.

Patent Owner argues that Ludtke's transaction confirmation does not allow access to various entities that Patent Owner argues Petitioner identifies as applications. PO Resp. 18–22. For example, Patent Owner argues that Ludtke's transaction confirmation does not allow access to the POS terminals discussed in the examples of Figures 12–14 and 17. *Id.* at 18–20 (citing Ex. 1005, 21:51–57, 23:50–55, 25:34–58, 28:58–62, 29:6–14). This argument is inapposite, as Petitioner does not argue that the POS in these examples is the application being accessed. Pet. 30–32.

As to the example of Figure 17, Patent Owner argues that "the transaction confirmation received from the TPCH of Ludtke does not allow access to a website; the user already has access to the website at the beginning of a transaction." PO Resp. 20 (citing Ex. 1005, 28:34–35, 28:50–52). Here, Patent Owner refers to Ludtke's user clicking a "Buy!" button on a webpage in a web browser and the web browser communicating with the PPOS terminal to request that it initiate a transaction (steps 1 and 2 of Fig. 17). *Id.*; *see* Ex. 1005, 28:34–35, 28:50–52. Petitioner, however, does not argue that a user first opening a webpage corresponds to allowing access to an application. Rather, Petitioner argues that the transaction confirmation from Ludtke's TPCH allows the user to access new functionality, software, and services corresponding to an application, either on the webpage or the transaction device (steps 8–11 and 13 of Fig. 17). Pet. 30 (citing Ex. 1005, 29:15–22, 29:29–30). Patent Owner's argument is not directed to Petitioner's allegations and, thus, is not persuasive.

Similarly, Patent Owner argues that "the transaction confirmation of Ludtke does not allow access to the functions of the transaction

device/digital wallet; the user already has access to all of those functions." PO Resp. 20. Petitioner, however, does not argue that a user first accessing the transaction device corresponds to allowing access to an application. Rather, Petitioner argues that the transaction confirmation from Ludtke's TPCH allows the user to access new functionality, software, and services corresponding to an application on the transaction device. Pet. 30 (citing Ex. 1005, 29:15–22, 29:29–30). We find that it does, as Ludtke describes electronic delivery of content to the user after the transaction is authorized. Ex. 1005, 29:29–30; *see also id.* at 31:11–16 (new functionality to be downloaded to the transaction device), 31:19–52 (examples including electronic train tickets and other digital content).

Patent Owner argues that "[a]s seen in figure 17 above, and in the teaching of Ludtke, the only reference to a 'signal' that Petitioner points to is the access message is **the signal whereby the user initially requests the content**, not the delivery of the content." PO Resp. 23. Here, Patent Owner "refers to step 1 of figure 17, wherein the signal relates only to the user **triggering the purchase**," and argues that "Figure [17] above and Ludtke's teachings make clear that the transaction confirmation to the transaction device is an independent step from the delivery of goods (whether physical or digital) to the user." *Id.* It is unclear what contention of Petitioner Patent Owner refers to here. In any case, Petitioner identifies signals 8–11 of Figure 17, not signal 1, as the access message. Pet. 30 (citing Ex. 1005, 29:12–22, 29:29–30; Ex. 1003 ¶ 110). We find that signals 8–11 correspond to an access message received by an application (e.g., a webpage with new content). Thus, Patent Owner's argument is not persuasive.

In sum, we find that the parties to the transactions described in Ludtke are the user of the transaction device and the retailer or vendor of the good

or service (e.g., web content, electronic train ticket, software) the user seeks to buy; and we further find that the TPCH, which merely acts as a middleman to facilitate the transaction, is not a party to the transactions described in Ludtke. Ex. 1005, 9:35–39, 28:34–56; Ex. 1003 ¶¶ 105–106. The web content, electronic train ticket, software, etc., is the application accessed. Ex. 1003 ¶ 113. We find that the TPCH sends (and the application receives) an access message (Ludtke's transaction confirmation) that indicates that the TPCH successfully authenticated codes from the transaction device and that allows the user access to the train ticket, software, etc. Ex. 1005, 29:15–31, 31:11–52; Ex. 1003 ¶¶ 110–114. Accordingly, Ludtke teaches claim limitations 1d and 1e.

Therefore, Ludtke teaches each limitation of claim 1.

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 to, and largely incorporate, its arguments and evidence for claim 1. Pet. 38–42, 45–54. Patent Owner presents its arguments for claims 1, 12, 16, and 22 together, and only as to the terms "third party that operates a trusted authority," "access message," and "application" appearing in each of these claims. PO Resp. 1–2. For the reasons given for claim 1, Petitioner has shown that Ludtke teaches each limitation of claims 12, 16, and 22.

Claim 2 depends from claim 1; claim 13 depends from claim 12. As to claims 2 and 13, we find that the device ID of Ludtke's transaction device is transmitted to the TPCH over a wireless or cellular network. Ex. 1005,

9:35–42, 5:63–64; Ex. 1003 ¶ 116; Pet. 32, 42. Thus, Ludtke teaches the additional limitation of claims 2 and 13.

Claim 4 depends from claim 1. We find that Ludtke teaches the transaction device sending a device ID to the TPCH when biometric scan data from the user matches stored biometric data. Ex. 1005, 14:33–46, 28:57–62, 29:5–6; Ex. 1003, 117–121; Pet. 32–34. Thus, Ludtke teaches the additional limitation of claim 4.

Claim 5 depends from claim 1; claim 26 depends from claim 22. We find that Ludtke teaches various examples of biometric data, including fingerprint and retinal scan data. Ex. 1005, 35:61–64; Ex. 1003 ¶ 122; Pet. 34, 58. Thus, Ludtke teaches the additional limitation of claims 5 and 26.

Claim 6 depends from claim 1; claim 25 depends from claim 22. We find that Ludtke teaches various examples of transaction devices, including pagers and cellular phones. Ex. 1005, 9:39–41, 11:66–12:7, 15:65–16:8, 17:65–18:4, 26:56–57, 33:49–54, Figs. 7A, 9A; Ex. 1003 ¶¶ 124–125; Pet. 35–36, 58. Thus, Ludtke teaches the additional limitation of claims 6 and 25.

Claim 7 depends from claim 1; claim 19 depends from claim 16; claim 27 depends from claim 22. We find that one example of an application accessed in Ludtke's transactions is a website. Ex. 1005, 29:15–20, 29:29–30, 31:41–52; Ex. 1003 ¶ 129; Pet. 37, 50, 58. Thus, Ludtke teaches the additional limitation of claims 7, 19, and 27.

Claim 10 depends from claim 1; claim 18 depends from claim 16. We find that Ludtke's description of establishing a secure connection to a back-end system teaches the additional limitation of claims 10 and 16. Ex. 1005,

37:39–45; Ex. 1003 ¶ 130; Pet. 37, 50. Thus, Ludtke teaches the additional limitation of claims 10 and 18.

Claim 15 depends from claim 12. We find that Ludtke's verification unit includes a liquid crystal display (LCD) screen that, conventionally, would have been back-lit using LEDs, and that the LCD screen requests a biometric scan. Ex. 1005, 11:37–41, 14:54–63, 16:53–56, 28:63–9:4; Ex. 1017 ¶ 41; Ex. 1018 ¶¶ 24, 108, 110, 135, 141, 154, 187; Ex. 1003 ¶¶ 142–145; Pet. 42–44. Thus, Ludtke teaches the additional limitation of claim 15.

Claim 23 depends from claim 22. We find that Ludtke teaches that its transaction device (an integrated hardware device) receives a validation request from a POS terminal and, upon receiving the request, prompts the user to scan their fingerprint. Ex. 1005, 14:33–46, 16:47–49, 28:57–62, 29:5–6; Ex. 1003 ¶¶ 171–173; Pet. 55–56. Thus, Ludtke teaches the additional limitation of claim 23.

Claim 24 depends from claim 23. We find that when Ludtke's integrated device cannot verify a fingerprint scan from the user, it does not send a device ID or other information to the TPCH. Ex. 1005, 4:62–5:1, 12:23–25, 14:40–46, 18:23–31, 29:5–6, 39:50–56 ("If a match does not occur, then at 3110 an error message is output and the DW [digital wallet] returns to checking to see if a fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes."); Ex. 1003 ¶¶ 174–177. Thus, Ludtke teaches the additional limitation of claim 24.

Patent Owner does not present separate arguments for the dependent claims.

In sum, Ludtke teaches each limitation of claims 1, 2, 4–7, 10, 12, 13, 15, 16, 18, 19, and 22–27.

4. Conclusion of obviousness

As detailed above, we find that Ludtke teaches each limitation of claims 1, 2, 4–7, 10, 12, 13, 15, 16, 18, 19, and 22–27. The record does not contain evidence of objective indicia of nonobviousness. Upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claims 1, 2, 4–7, 10, 12, 13, 15, 16, 18, 19, and 22–27 would have been obvious over Ludtke.

C. Obviousness of Claims 3, 14, and 17 over Ludtke and Kon

Petitioner contends that claims 3, 14, and 17 would have been obvious over Ludtke and Kon. Pet. 58–68. 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.

Kon describes examples of identifying a person using a person identification certificate (IDC) which can include information such as fingerprints, retina patterns, voice, etc. Ex. 1006 ¶¶ 173, 241. The IDC can include the age of the user. *Id.* ¶ 234, Fig. 5 (Subject Directory Attributes, including "Personal information . . . used to authenticate subject Age, sex, etc."). The user registers personal information with a person identification certificate authority (IDA), which issues the IDC to the user. *Id.* ¶ 178. Service providers verify the authenticity of the user based on the IDC. *Id.*

Petitioner contends that Kon describes registering and storing a user's age in association with a user device's device ID. Pet. 63–67 (citing

Ex. 1006 ¶¶ 194, 234, 241, 265–266, Figs. 5, 9; Ex. 1003 ¶¶ 184–185). Petitioner argues that "[t]he user's age, like the biometric information, provides another data point for identifying the user," and would have been especially useful when a transaction has an age minimum, such as purchasing alcohol or cigarettes. *Id.* at 68 (citing Ex. 1003 ¶¶ 186–187). Accordingly, Petitioner argues, a skilled artisan would have registered a user's age, as taught by Kon, with Ludtke's device ID to facilitate age-prohibitive transactions. *Id.* Petitioner makes the same arguments for claims 10 and 13. Pet. 69 (citing Ex. 1003 ¶ 188). Patent Owner does not provide separate arguments for claims 3, 14, and 17.

On the complete record, for the reasons articulated by Petitioner, we find that Kon teaches the additional limitations of claims 3, 14, and 17, and that a skilled artisan would have had reasons, with rational underpinning, for combining Ludtke and Kon. The record does not contain evidence of objective indicia of nonobviousness. Upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claims 3, 14, and 17 would have been obvious over Ludtke and Kon.

D. Patent Owner's Declaration Testimony and Sur-reply Exhibits

Patent Owner offers the declaration testimony of Troy Carrothers (Ex. 2018). Specifically, Patent Owner offers Mr. Carrothers' testimony to show that Ludtke's system, in particular the TPCH, implemented steps according to a standard credit card transaction. PO Resp. 13–17 (citing Ex. 2018 ¶¶ 20–31).

Petitioner argues that Mr. Carrothers' testimony should be given no weight because he does not have the education or experience required of a

person of ordinary skill in the art. Reply 2–4 (citing *Kyocera Senco Indus. Tools Inc. v. Int'l Trade Comm'n*, 22 F.4th 1369, 1376–77 (Fed. Cir. 2022)).

The Federal Circuit has made clear that:

> To offer expert testimony from the perspective of a skilled artisan in a patent case—like for claim construction, validity, or infringement—a witness must at least have ordinary skill in the art. Without that skill, the witness' opinions are neither relevant nor reliable. The opinions would not be based on any specialized knowledge, training, or experience that would be helpful to the factfinder. In fact, "[a]dmitting testimony from a person . . . with no skill in the pertinent art serves only to cause mischief and confuse the factfinder." That testimony would "amount[ ] to nothing more than advocacy from the witness stand."

Kyocera, 22 F.4th at 1376–77 (quoting *Sundance, Inc. v. DeMonte Fabricating Ltd.*, 550 F.3d 1356, 1362, 1364–65 (Fed. Cir. 2008) (alterations in *Kyocera*)).

As explained above, a person of ordinary skill in the art would have had at least a bachelor's degree in Computer or Electrical Engineering or an equivalent engineering discipline, and at least three years of experience in the field of encryption and security, or the equivalent, while additional education could substitute for professional experience, and significant work experience could substitute for formal education. Mr. Carrothers claims to be "a financial services and retail leader with approximately thirty years of experience working in a variety of leadership roles in retail payments." Ex. 2018 ¶ 1. He lists professional and consulting experience with retail payments, operational and risk management of a credit card portfolio, and payment insurance and acceptances in stores and online. *Id.* ¶¶ 1–5. His Curriculum Vitae (Ex. 2018, Appendix A) lists education including a Bachelor of Business Administration and a Master of Business

Administration. Mr. Carrothers does not claim to, or demonstrate that, he has either the technical education or the technical experience to be a person of ordinary skill in the art.

In response to Petitioner's challenge to Mr. Carrothers' qualifications, Patent Owner does not contend that Mr. Carrothers is at least a person of ordinary skill in the art.[7] Rather, Patent Owner argues that "[t]o put the asserted portions of Ludtke in context, Mr. Carrothers provided testimony regarding the processing of credit and debit card payments with respect to online transactions based on his expertise and experience with retail payments." Sur-reply 1.

Patent Owner uses Mr. Carrothers' testimony to support arguments regarding the timing and parties to the communications generated by Ludtke's system, and to support arguments that the TPCH is a party to Ludtke's transactions. PO Resp. 13–17 (citing Ex. 2018 ¶¶ 20–31). We find that Mr. Carrothers testifies on technical details regarding unpatentability, and that a declarant testifying as to such subject matter should have at least ordinary skill in the art. Thus, Mr. Carrothers' testimony is entitled to no weight. *See Kyocera*, 22 F.4th at 1376–77.

In the Sur-reply, Patent Owner contends that we should consider Mr. Carrothers' testimony because his testimony "can be corroborated by independent sources." Sur-reply 1. Patent Owner then introduces, and argues the contents of, several new exhibits not introduced into the record before the Sur-reply was filed. *Id.* at 1–5 (discussing Exhibits 2029–2033). Patent Owner's introduction of new exhibits violates our rules. 37 C.F.R.

[7] As noted above, we dismiss Patent Owner's belated attempt at oral hearing to challenge Petitioner's statement of the level of skill in the art (which we adopt).

§ 42.23(b) (emphasis added) provides that "[a] sur-reply may only respond to arguments raised in the corresponding reply and *may not be accompanied by new evidence* other than deposition transcripts of the cross-examination of any reply witness." According to our Trial Practice Guide, "[w]hile replies and sur-replies can help crystalize issues for decision, a reply or sur-reply that raises a new issue or belatedly presents evidence may not be considered." Consolidated Trial Practice Guide[8] at 974; *see also* 84 Fed. Reg. 64,280 (Nov. 21, 2019). Patent Owner's new evidence (Exhibits 2029–2033) and the argument that discusses the new evidence (Sur-reply 1–5) are improper and will not be considered.

E. The '052 Reexam

As noted above, the '730 patent, a patent related to the '954 patent, is the subject of the co-pending '052 reexam. Patent Owner argues that the Examiner in the '052 reexam has rejected arguments substantially the same as those presented by Petitioner in this proceeding. Setting aside whether the prosecution of a co-pending reexamination of a different patent is relevant to this proceeding, Patent Owner's characterization of the Examiner's position in the '052 reexam is incorrect and, therefore, unpersuasive.

Patent Owner argues that the Request for the '052 reexam was based on Ludtke's TPCH being a third-party trusted authority because Ludtke's TPCH processes a financial transaction.[9] Sur-reply 14–15 (citing Ex. 2023, 65, 69). Patent Owner argues that it explained to the Examiner that the

[8] Available at https://www.uspto.gov/TrialPracticeGuideConsolidated.
[9] As explained above, this is not Petitioner's allegation in this proceeding.

TPCH was the application being accessed by the user to tender payment to the vendor and reiterated (and expanded upon) that argument in response to a first office action. *Id.* at 15 (citing Ex. 2024, 5–10; Ex. 2025, 11–14; Ex. 2020,[10] 12–17). Patent Owner further argues that the '052 reexam "has addressed—and refuted—the argument that Ludtke's TPCH is a 'third-party trusted authority' due to processing a financial transaction." *Id.* (citing Ex. 2021, 27–28). However, the Examiner did not accept Patent Owner's argument; rather, the Examiner issued new grounds of rejection and determined that "[t]his argument is moot in view of the updated rejections." Ex. 2021, 27–28; *see also* moot, BLACK'S LAW DICTIONARY, 1099 (9th ed. 2009) ("Having no practical significance; hypothetical or academic <the question on appeal became moot once the parties settled their case>"). Thus, the '052 reexam record does not reflect that Patent Owner refuted an argument that Ludtke's TPCH is a third-party trusted authority because it processes a financial transaction.

Patent Owner also argues that the first Office Action in the '052 reexam "asserted that an access message received from Ludtke's TPCH enabled or announced access to additional functionalities, including access to the digital wallet itself." Sur-reply 15–16 (citing Ex. 2025, 15). Patent Owner argues that it "responded by detailing why Ludtke fails to disclose the TPCH sending an 'access message' allowing the user to access additional functionalities," and that "[t]he CRU found Patent Owner's arguments persuasive" and the '052 reexam "addressed -- and refuted -- the

[10] Patent Owner cites to Exhibit 2026, which is a December 6, 2024, Interview Summary and, therefore, not the correct exhibit. Sur-reply 15. Exhibit 2020 is an October 9, 2024, Response to Office Action, and appears to be the exhibit to which Patent Owner intended to cite.

argument that Ludtke's TPCH sends an access message allowing access to additional functionalities." *Id.* at 16 (citing Ex. 2020, 17–19; Ex. 2021, 28). However, the Examiner did not accept Patent Owner's argument; rather, the Examiner issued new grounds of rejection and determined that "[t]his argument is moot in view of the updated rejections." Ex. 2021, 28.

Finally, Patent Owner argues that it refuted, in a Response to Office Action, that Ludtke's TPCH provides an access message permitting access to a webpage and that "[t]he CRU found the Patent Owner's remarks persuasive." Sur-reply 16–17 (citing Ex. 2020, 19; Ex. 2021, 28). However, the Examiner did not accept Patent Owner's argument; rather, the Examiner issued new grounds of rejection and determined that "[t]his argument is moot in view of the updated rejections." Ex. 2021, 28.

Thus, the '052 reexam does not reflect that the Examiner was persuaded by the arguments Patent Owner presents in this proceeding.

In a December 17, 2024, Interview Summary, the "Examiner notes the claims [of the '730 patent] are silent as to where the access message is sent," and "[w]ere the claims [of the '730 patent] to recite the access message being sent to/received by the application . . ., the claims would be allowable over Ludtke," and that "[a]n Examiner's Amendment could achieve this." Ex. 2027, 4. The Examiner followed this up with a March 3, 2025, Final Rejection proposing an amendment. Ex. 2035, 31. Although Patent Owner did not address it in its briefs, at the oral argument Patent Owner attempted to belatedly argue that we should defer to the Examiner's statements as to language Patent Owner considers substantially similar in the claims of the '954 patent. Tr. 44:3–46:17. In the bulk of its Estoppel Brief, Patent Owner argued that we are bound, under the Administrative Procedures Act, to follow this "final determination" by the Examiner, that we "cannot

overrule the Examiner," and that we allegedly "ceded jurisdiction to the Examiner" and "lack[] jurisdiction" over the '052 reexamination. PO Estoppel Br. 2–6. These arguments are untimely, and we give them no weight. *See Dell*, 884 F.3d at 1369.

Moreover, the Examiner in the '052 reexam has withdrawn the Final Rejection, including the proposed amendment, on which Patent Owner's belated argument relies. Ex. 3003 (May 20, 2025, Office Action), 3 ("This is a Non-Final Office Action addressing amended claims 1–17. The previous rejection under Ludtke is withdrawn."). The Examiner gave no reason for withdrawing the rejection, and instead proceeded to reject claims 1–17 of the '730 patent over Burger[11] (US 2005/0050367 A1). We treat the Examiner's decision to withdraw the rejection involving Ludkte as a determination that that rejection is moot (and not an assessment of the merits), and her proposed amendment as withdrawn and, thus, of no relevance to this proceeding.

Even if we consider the '052 reexam, we see little relevance of its record to this proceeding.

III. ESTOPPEL

Because we conclude that Petitioner has proved on the merits that claims 1–7, 10, 12–19, and 22–27 of the '954 patent are unpatentable, we need not address Petitioner's argument (Pet. Estoppel Br.) that Patent Owner is collaterally estopped from arguing the patentability of the claims of the '954 patent.

[11] Burger is part of the challenges raised in IPR2024-00775 and IPR2024-00846.

IV. CONCLUSION[12]

Petitioner has proved by a preponderance of the evidence that claims 1–7, 10, 12–19, and 22–27 of the '954 patent are unpatentable.

The outcome for the challenged claims of this Final Written Decision follows. In summary:

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
1, 2, 4–7, 10, 12, 13, 15, 16, 18, 19, 22–27	103(a)	Ludtke	1, 2, 4–7, 10, 12, 13, 15, 16, 18, 19, 22–27	
3, 14, 17	103(a)	Ludtke, Kon	3, 14, 17	
Overall Outcome			1–7, 10, 12–19, 22–27	

[12] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

V. ORDER

It is hereby:

ORDERED that 1–7, 10, 12–19, and 22–27 of the '954 patent are unpatentable;

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:

Erika Arner
Kara Specht
Cory Bell
Safiya Aguilar
Shawn Chang
FINNEGAN, HENDERSON, FARABOW, GARRETT, & DUNNER LLP
erika.arner@finnegan.com
kara.specht@finnegan.com
cory.bell@finnegan.com
safiya.aguilar@finnegan.com
shawn.chang@finnegan.com

Philip W. Woo
D. Stuart Bartow
Monte T. Squire
Paul Belnap
DUANE MORRIS LLP
pwwoo@duanemorris.com
dsbartow@duanemorris.com
mtsquire@duanemorris.com
phbelnap@duanemorris.com

PATENT OWNER:

David L. Hecht
James Zak

HECHT PARTNERS LLP
dhecht@hechtpartners.com
jzak@hechtpartners.com

Director PTABDecision Review@uspto.gov
571.272.7822

Paper 38
Date: August 13, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE OFFICE OF THE UNDER SECRETARY OF COMMERCE FOR INTELLECTUAL PROPERTY AND DIRECTOR OF THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLE INC.,
Petitioner,

v.

PROXENSE, LLC,
Patent Owner.

IPR2024-00233[1]
Patent 8,886,954 B1

Before MICHELLE N. ANKENBRAND,[2] *Senior Lead Administrative Patent Judge*, *performing the duties of Director Review Executive*.

---

[1] Google LLC ("Google") originally filed this proceeding. *See* Paper 1. The Board subsequently joined Apple Inc., who filed a petition in IPR2024-01334, as a petitioner in this proceeding. Paper 13. The Board terminated Google as a petitioner based on settlement. Paper 21.

[2] Coke Morgan Stewart, Acting Under Secretary of Commerce for Intellectual Property and Acting Director of the United States Patent and Trademark Office, is recused and took no part in this decision. The Acting Director delegated her authority in a Notice of Delegation. *See* https://www.uspto.gov/sites/default/files/documents/delegation-of-authority-ptab.pdf.

ORDER

The Office received a request for Director Review of the Final Written Decision in the above-captioned case and an authorized response to the request. *See* Papers 36, 37.

Having reviewed the request and response, it is:

ORDERED that the request for Director Review is denied.

FOR PETITIONER:

Erika Arner
Kara Specht
Cory Bell
Safiya Aguilar
Shawn Chang
FINNEGAN, HENDERSON, FARABOW, GARRETT, & DUNNER LLP
erika.arner@finnegan.com
kara.specht@finnegan.com
cory.bell@finnegan.com
safiya.aguilar@finnegan.com
shawn.chang@finnegan.com

Philip W. Woo
D. Stuart Bartow
Monte T. Squire
Paul Belnap
DUANE MORRIS LLP
pwwoo@duanemorris.com
dsbartow@duanemorris.com
mtsquire@duanemorris.com
phbelnap@duanemorris.com

FOR PATENT OWNER:

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

Trials@uspto.gov
571-272-7822

Paper 35
Entered: June 17, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

PROXENSE, LLC,
Patent Owner.

IPR2024-00233[1]
Patent 8,886,954 B1

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

MCKONE, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

[1] IPR2024-01334 has been joined with this proceeding.

I. INTRODUCTION

A. Background and Summary

Google LLC filed a Petition (Paper 1, "Pet.") requesting *inter partes* review of claims 1–7, 10, 12–19, and 22–27 of U.S. Patent No. 8,886,954 B1 (Ex. 1001, "the '954 patent"). The Board instituted an *inter partes* review of the challenged claims pursuant to 35 U.S.C. § 314. Paper 10 ("Inst. Dec."). Apple, Inc. ("Petitioner") joined the proceeding as a party on October 8, 2024, filing a duplicate petition. Paper 13. We terminated the proceeding as to Google, leaving Apple as the sole Petitioner. Paper 21.

After institution, Patent Owner filed a Patent Owner Response (Paper 14, "PO Resp."), Petitioner filed a Reply (Paper 16, "Reply"), and Patent Owner filed a Sur-reply (Paper 22, "Sur-reply"). The parties then presented oral arguments via a (video) Hearing (April 22, 2025), and the Board entered a Hearing transcript into the record (Paper 31, "Tr."). After the oral arguments, and pursuant to our authorization, Petitioner and Patent Owner submitted briefs addressing the preclusive effect, if any, of Patent Owner's Request for Adverse Judgement in IPR2024-00232. Paper 32 ("Pet. Estoppel Br."); Paper 33 ("PO Estoppel Br.").

For the reasons set forth in this Final Written Decision pursuant to 35 U.S.C. § 318(a), we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 1–7, 10, 12–19, and 22–27 are unpatentable.

B. Related Matters

The parties advise us that the '954 patent is involved in two district court cases, including *Proxense, LLC v. Google LLC*, No. 6.23-CV-00320 (W.D. Tex.). Pet. 70; Paper 4, 2. Petitioner also has filed petitions for *inter*

partes review of patents related to the '954 patent, including IPR2024-00232 (challenging U.S. Patent No. 8,352,730 B2 ("the '730 patent"); terminated after Patent Owner request for adverse judgment) and IPR2024-00234 (challenging U.S. Patent No. 9,298,905 B1 ("the '905 patent"); terminated after Patent Owner request for adverse judgment). Patent Owner states that patents related to the '954 patent are the subject of *ex parte* reexaminations in Application No. 90/015,052 ("the '052 reexam"), reexamining the '730 patent, Application No. 90/015,053, reexamining the '905 patent, and Application No. 90/015,054, reexamining U.S. Patent No. 10,698,989. Paper 6, 14. The '730 patent also was the subject of *Microsoft Corp. v. Proxense, LLC*, IPR2024-00775 (PTAB) (terminated after Patent Owner request for adverse judgment). The '954 patent also is the subject of *Microsoft Corp. v. Proxense, LLC*, IPR2024-00846 (PTAB) (currently pending).

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.

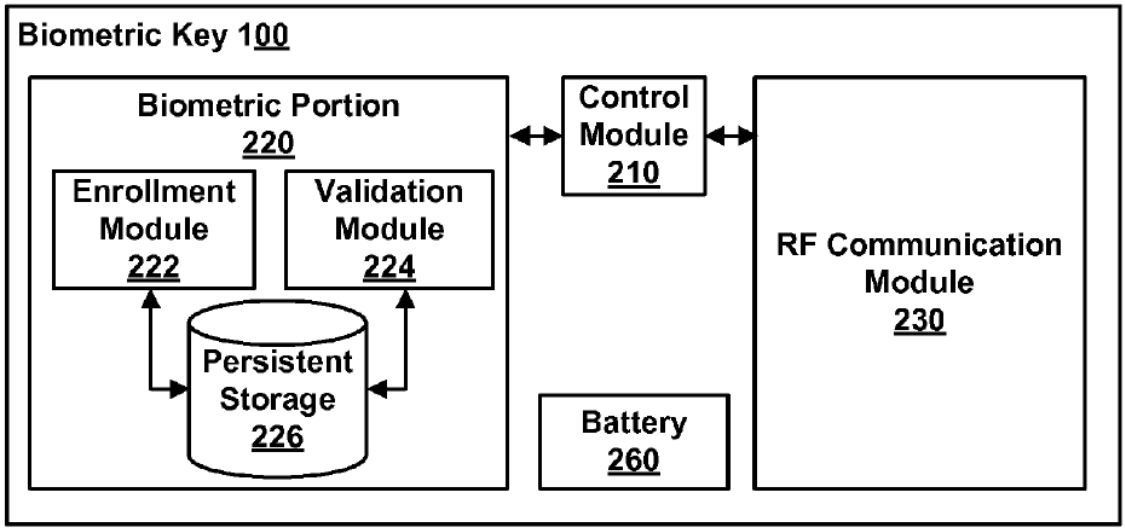


FIG. 2

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.

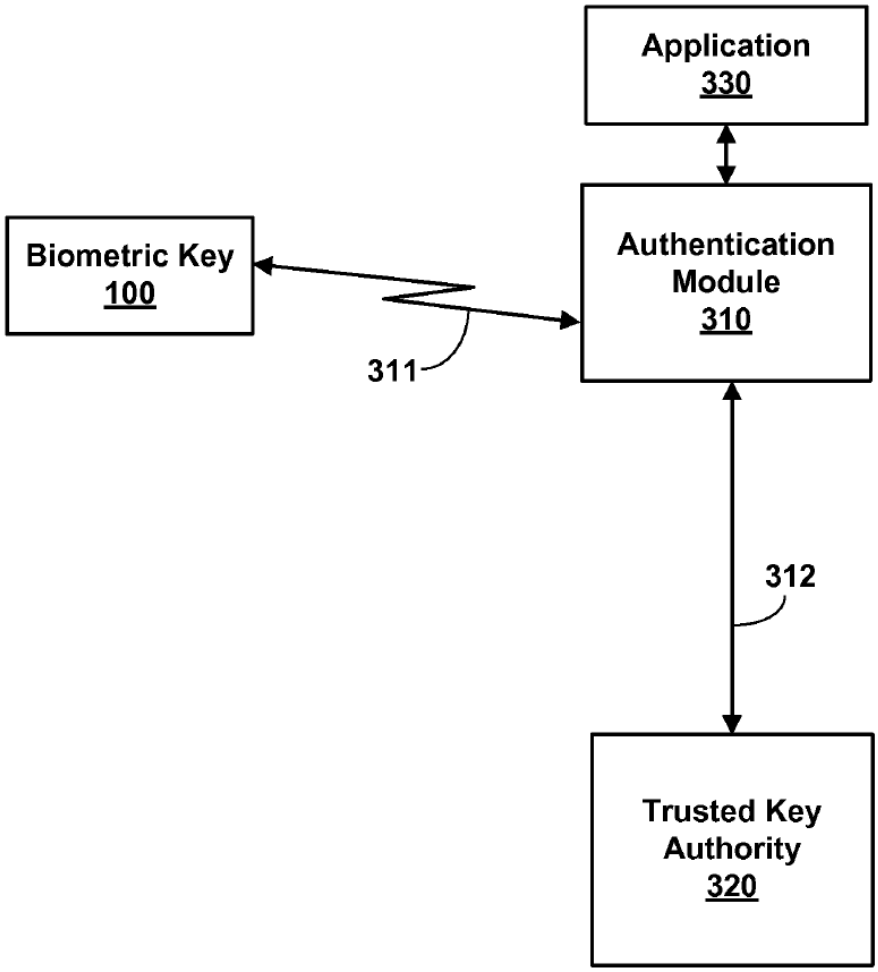


FIG. 3

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,[2] is illustrative of the claimed subject matter:

> 1. A method comprising:
>
> [1ai] persistently storing biometric data of a user and [1aii] a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and [1aiii] a secret decryption value in a tamper proof format written to a storage

[2] We add bracketed alphanumeric characters corresponding to those Petitioner uses in the Petition.

element on the integrated device that is not capable of being subsequently altered;

[1b] responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;

[1c] comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

[1d] 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

[1e] 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.
Ludtke	US 7,188,110 B1	Mar. 6, 2007 (filed Dec. 11, 2000)	1005
Kon	US 2002/0046336 A1	Apr. 18, 2002	1006

Petitioner also relies on the Declaration of Stephen Gray (Ex. 1003) and the Reply Declaration of Stephen Gray (Ex. 1026).

Patent Owner relies on the Declaration of Troy Carrothers (Ex. 2018).

E. The Asserted Grounds of Unpatentability

We instituted a trial under the following grounds:

Reference(s)	35 U.S.C. §	Claim(s) Challenged
Ludtke	103(a)[3]	1, 2, 4–7, 10, 12, 13, 15, 16, 18, 19, 22–27
Ludtke, Kon	103(a)	3, 14, 17

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.

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

[3] 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.

1. Third party that operates a trusted authority

Independent claims 1, 12, 16, and 22 each recite "a third party that operates a trusted authority."[4] In the Institution Decision, we preliminarily construed this term to mean "a trusted authority that is an entity separate from the parties to a transaction." Inst. Dec. 9–12.

Petitioner "agrees with the Board's construction, and submits that no further interpretation of third party trusted authority is warranted." Reply 5.

"Patent Owner agrees with this construction but challenges its application in the Petition, in particular the finding that the 'parties to a transaction' of the Patent (relative to the claimed third party trusted authority) can be a user and a vendor or merchant." PO Resp. 6. Instead, Patent Owner argues, "the parties could be either a user and an application (where a user is utilizing the claimed device or method) or, in another embodiment, a vendor and an application (where a vendor is utilizing the claimed device or method as a type of user)." *Id.* at 6–7. According to Patent Owner, "the specification and claim language at issue requires that at least one of the parties to the claimed transaction must be the application being accessed." *Id.* at 7.

[4] The parties also refer to this term as "third party trusted authority." The '730 patent, a parent of the '954 patent, was the subject of *Samsung Electronics America, Inc. v. Proxense LLC*, IPR2021-01444 (PTAB) (institution denied). *See* Ex. 1007 (IPR2021-01444, Paper 11 (PTAB Feb. 28, 2022) ("Samsung DDI")). In the Samsung DDI, the Board construed "third-party trusted authority" to mean "a trusted authority that is an entity separate from the parties to a transaction." Ex. 1007, 15. Patent Owner appears to contend that "third party that operates a trusted authority," recited in the '954 patent claims, has the same meaning as "third-party trusted authority," recited in the '730 patent claims. Petitioner does not appear to dispute this. We treat these terms as equivalent.

The language of claim 1 does not expressly identify the parties to a transaction. Claim 1 recites storing and processing biometric data of "a user." This suggests that a user could be a party to a transaction within the scope of claim 1. Claim limitation 1e recites "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." Independent claims 12, 16, and 22 have similar language. Patent Owner argues that "for all independent claims, the access message must be *received* from the 'trusted authority' and thus that 'trusted authority' **cannot be the same entity as the application under these claims**." PO Resp. 12–13. This language does not specify, one way or the other, whether "an application" is the second party to a transaction and Patent Owner cites no evidence to suggest that it does. Patent Owner cites *SIMO Holdings* for the proposition that an embodiment in the specification might not be included in a claim where there is probative evidence to the contrary. *Id.* (citing *SIMO Holdings Inc. v. Hong Kong uCloudlink Network Tech. Ltd.*, 983 F.3d 1367, 1378 (Fed. Cir. 2021)). However, that case does not support Patent Owner's overly narrow reading of the plain language of the claims.[5] Thus, the plain language of claim 1 does not limit the parties to a transaction between the user and an application, or require that one of the parties to a transaction be the application ultimately accessed.

[5] Patent Owner introduces and discusses new Exhibit 2034 in the Sur-reply, at 6–7. This exhibit violates Rule 42.23(b), which provides "[a] sur-reply may only respond to arguments raised in the corresponding reply and may not be accompanied by new evidence other than deposition transcripts of the cross-examination of any reply witness." We do not consider this new exhibit.

"We depart from the plain and ordinary meaning in only two instances," namely, "when a patentee acts as his own lexicographer," and "when the patentee disavows the full scope of the claim term in the specification or during prosecution." *Poly-Am., L.P. v. API Indus., Inc.*, 839 F.3d 1131, 1136 (Fed. Cir. 2016) (citing *Hill–Rom Servs., Inc. v. Stryker* Corp., 755 F.3d 1367, 1371 (Fed. Cir. 2014)). "Disavowal can be effectuated by language in the specification or the prosecution history. In either case, the standard for disavowal is exacting, requiring clear and unequivocal evidence that the claimed invention includes or does not include a particular feature." *Id.* (citing *Phillips*, 415 F.3d at 1316–17). According to the Federal Circuit, "disavowal requires that 'the specification [or prosecution history] make[ ] clear that the invention does not include a particular feature.'" *GE Lighting Sols., LLC v. AgiLight, Inc.*, 750 F.3d 1304, 1309 (Fed. Cir. 2014) (quoting *SciMed Life Sys. Inc. v. Advanced Cardiovascular Sys., Inc.*, 242 F.3d 1337, 1341 (Fed. Cir. 2001) (alterations in *GE Lighting*)).

As to the specification, Patent Owner argues that the '954 patent "only discloses embodiments where the parties to the transaction are a user and an application being accessed by that user." PO Resp. 10. In particular, Patent Owner cites to the examples of '954 patent Figures 3, 4, and 7. *Id.* at 10–12 (citing Ex. 1001, 2:35–48, 5:65–67, 6:8–34, 6:45–55, 6:64–66, 8:12–16, Figs. 3, 4, 7).

In one example cited by Patent Owner, describing Figure 3, the '954 patent states that "[s]ystem 300 comprises an authentication module 310 in communication with biometric key 100, a trusted key authority 320, and an application 330." Ex. 1001, 5:65–67. This passage does not state

that application 330 is a party to the transaction. The specification continues:

> Application 330 is a resource that can be accessed by a verified and authenticated user. 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, a financial account (e.g. a savings account, checking account, brokerage account, credit card account, credit line, etc.) and the like. In one embodiment, a file includes medical information such as a medical record, insurance information or other healthcare information.

Id. at 6:18–26. Petitioner argues that "an ATM is not a party to a transaction—the parties are the user and the bank, and the ATM is the mechanism through which the bank's accounts are accessed." Reply 5–6 (citing Ex. 1026 ¶ 13). Similarly, Petitioner argues, a file "is not a principal party to a transaction—rather the user and the provider of the file (e.g., a vendor) are the parties." *Id.* at 6 (citing Ex. 1026 ¶ 13). Petitioner makes similar arguments for financial accounts, savings accounts, medical records, and insurance information. *Id.* (citing Ex. 1001, 6:18–26; Ex. 1026 ¶ 14). We agree with Petitioner. The specification, here, gives several examples where the application being accessed is not, itself, a party to the transaction, but rather an asset of one of the parties or the mechanism by which the parties transact.

Patent Owner (PO Resp. 10) cites another example in which the '954 patent states "[i]n one embodiment, authentication can be required prior to allowing access to an application (e.g., application 330)." Ex. 1001, 6:64–66. However, the specification continues: "For example, a user can be standing proximate to a slot machine in a casino which requires that a user be over the age of 21. The slot machine can detect the biometric key in the

user's pocket, and, in response, spawn a conspicuous pop-up window on the slot machine requesting age verification." *Id.* at 6:66–7:4. Here, the parties are the user and a casino, and the slot machine is the mechanism for the transaction, not itself a party.

In another example, the '954 patent describes an "open system" in which "users can attempt authentication (e.g., in a public grocery store)." Ex. 1001, 6:48–51. The specification contrasts this with "a closed system," where "only known users are legitimate (e.g., owners of a home)." *Id.* at 6:51–55. Patent Owner argues that the grocery store example is only referring to the location of the application being accessed, and is not a transaction between a merchant and a user. PO Resp. 11–12. We disagree, and find that the '954 patent describes authentication of a transaction between a customer and a grocery store. Ex. 1001, 6:48–51. But even if Patent Owner's reading is correct, this example does not support limiting the claims to transactions in which one of the parties to the transaction is the application being accessed.

In short, Patent Owner points to no language in the specification limiting the claims to transactions in which the application being accessed is, itself, a party to the transaction and Petitioner points to several examples in which the application being accessed is not a party to the transaction. Thus, Patent Owner has provided no persuasive basis to depart from the plain and ordinary meaning of the claims.

In the Sur-reply, Patent Owner argues that, even if the specification supports a transaction having principal parties other than a user and the application being accessed, the language of the claims is limited to the parties being the user and the application being accessed; thus, the language of the claims controls and the unclaimed subject matter in the specification

should be disregarded. Sur-reply 7–8 (citing *Rolls-Royce, PLC v. United Technologies Corp.*, 603 F. 3d 1325, 1334 (Fed. Cir. 2010); *TIP SYSTEMS, LLC v. Phillips & Brooks/Gladwin*, 529 F. 3d 1364, 1373 (Fed. Cir. 2008)). However, as explained above, the plain language of the claims does not limit the parties to a transaction to the user and an application. Thus, Patent Owner's argument is unpersuasive.

Patent Owner also argues that Petitioner improperly applies "third-party trusted authority" in IPR2024-00232 (challenging the '730 patent). Sur-reply 8–9. In this proceeding, we evaluate whether Petitioner has shown that the challenged claims of the '954 patent are unpatentable, using the language of the claims of the '954 patent. Thus, Patent Owner's argument is inapposite and unpersuasive. Moreover, Patent Owner has admitted that the claims of the '730 patent, at issue in IPR2024-00232, are unpatentable and requested (and received) adverse judgment against itself. IPR2024-00232, Papers 29, 33; *see also* IPR2024-00775, Papers 14 (requesting adverse judgment as to claims 1–17 of the '730 patent), 15 (granting adverse judgment).

We maintain our construction of "a third party that operates a trusted authority," namely, "a trusted authority that is an entity separate from the parties to a transaction." Such a transaction is not limited to those in which the application being accessed is a party.

2. "access message"

Claim limitation 1e recites "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*." Independent claims 12, 16, and 22 recite similar language.

Petitioner notes that a District Court has construed "access message" to mean "[a] signal or notification enabling or announcing access." Pet. 4 (citing Ex. 1009, 3; Ex. 1010, 15, 20). However, Petitioner "maintains that the Board need not construe the term 'access message.'" Reply 6.

Patent Owner states that it "agree[s] on the construction of the term 'access message' to mean 'a signal or notification enabling or announcing access.'" PO Resp. 7. However, Patent Owner argues that applying "access message" to Ludtke's transaction confirmation "fails to account for the claim term 'access to an application.'" *Id.* at 7–8. Rather, Patent Owner argues, a transaction confirmation "is a message announcing that a transaction has been completed." *Id.* at 8. Patent Owner contends that "[t]he plain and ordinary meaning of 'access message' is a message enabling entry to, communication with, or use of an object wherein the object is the claimed application." *Id.* (citing *access*, MERRIAM-WEBSTER DICTIONARY (available at https://www.merriam-webster.com/dictionary/access)). Here, Patent Owner appears to retreat on its agreement that "access message" can include a signal "announcing" access, and suggests that we limit "access message" to a signal "enabling" access. However, Patent Owner then returns to its agreement, stating that "[i]t would be improper to construe 'access message' as something other than a signal or notification enabling or announcing a user's access to (ability to enter, communicate with, or make use of) an application." *Id.*

What Patent Owner appears to be arguing is that "access message" should be construed to mean "a signal or notification enabling or announcing

access," but that we should be further cognizant of the additional language in claim limitation 1e, "allowing the user access to the application."

We see no basis to depart from the District Court's construction of "access message," on which the parties appear to agree. However, we evaluate below Ludtke's applicability to the full scope of claim limitation 1e, including the language "allowing the user access to the application."

3. Remaining claim terms

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, 4–7, 10, 12, 13, 15, 16, 18, 19, and 22–27 over Ludtke

Petitioner contends that claims 1, 2, 4–7, 10, 12, 13, 15, 16, 18, 19, and 22–27 would have been obvious over Ludtke. Pet. 8–58. For the reasons given below, Petitioner has made a sufficient showing.

A claim is unpatentable under 35 U.S.C. § 103 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.[6] *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

1. Level of skill in the art

Petitioner contends that a person of ordinary skill in the art "would have had at least a bachelor's degree in Computer or Electrical Engineering or an equivalent engineering discipline, and at least three years of experience in the field of encryption and security, or the equivalent," and that "[a]dditional education could substitute for professional experience, and significant work experience could substitute for formal education." Pet. 4 (citing Ex. 1003 ¶¶ 31–32, 53–55). Patent Owner does not challenge Petitioner's proposed level of skill or propose an alternative in its papers.

Nevertheless, at the oral argument, Patent Owner argued that the level of skill we find should depend on how we construe the claims, namely, if we construe the claims broadly enough to encompass settlement of financial transactions where funds are transferred, then the level of skill should be found to include expertise in financial transactions. Tr. 38:21–41:10. We dismiss this argument as untimely. *See Dell Inc. v. Acceleron, LLC*, 884 F.3d 1364, 1369 (Fed. Cir. 2018) (noting that the "Board was obligated to dismiss [the petitioner's] untimely argument . . . raised for the first time during oral argument"). In any case, Patent Owner has pointed to no authority, and we are aware of no authority, in support of its position that the

[6] The complete record does not include allegations or evidence of objective indicia of nonobviousness.

level of skill in the art for a patent can change based on how the claims of the patent are construed.

Petitioner's proposal is consistent with the technology described in the specification and the cited prior art. On the complete record, we adopt Petitioner's proposed level of skill.

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

Ludtke describes techniques for identifying an authorized user with a biometric device and enabling the authorized user to access private information over a voice network. Ex. 1005, Abstract. Figure 4 of Ludtke, reproduced below, illustrates an example:

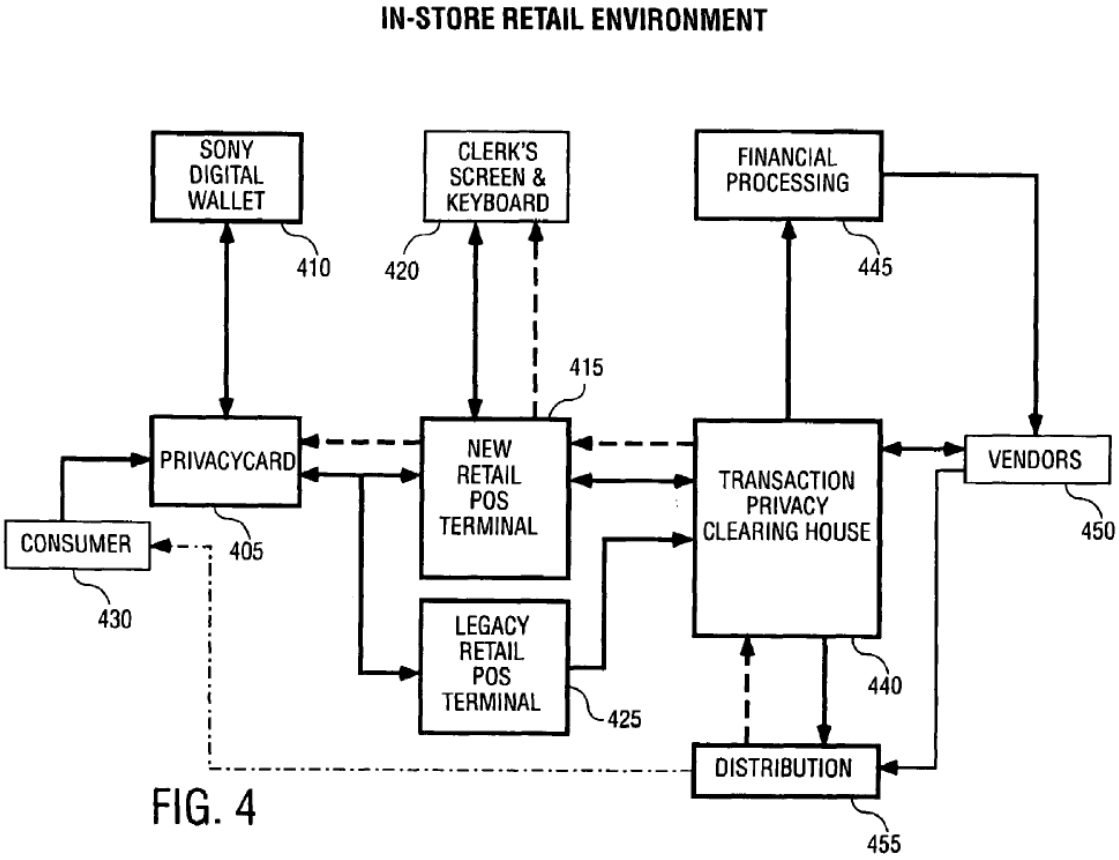


Figure 4 is a block diagram of an in-store retail system. *Id.* at 2:8–9.

In the retail environment of Figure 4, privacy card 405 interfaces with digital wallet 410 and retail point of sale (POS) terminal 415. *Id.* at 8:53–56. User 430 provides privacy card 405 and digital wallet 410 to POS terminal 415 or legacy retail POS terminal 425. *Id.* at 8:59–67. Transaction privacy clearing house (TPCH) 440 receives user 430's privacy card identification and determines whether the user has sufficient funds to perform the transaction. *Id.* at 9:1–3.

> In one embodiment, the transaction device(s), POS terminals and/or TPCH may function to verify the authenticity of each other. For example, a privacy card and digital wallet may be configured to verify the legitimacy of each other. Similarly, the transaction device may be configured to verify the legitimacy of the POS terminal and/or TPCH. A variety of verification techniques may be used. For example[,] lists of devices with account and/or access issues may be maintained. For example, in one embodiment, the public key infrastructure (PKI) may be used to verify legitimacy.

Id. at 5:11–20. "One means of authentication is some kind of PIN code entry. Alternately, authentication may be achieved by using more sophisticated technologies such as a biometric solution (e.g., fingerprint recognition)." *Id.* at 4:65–5:1. TPCH 440 interfaces with financial processing system 445, vendors 450, and distribution systems 455 to complete the transaction. *Id.* at 9:4–6.

Figure 17 of Ludtke is reproduced below:

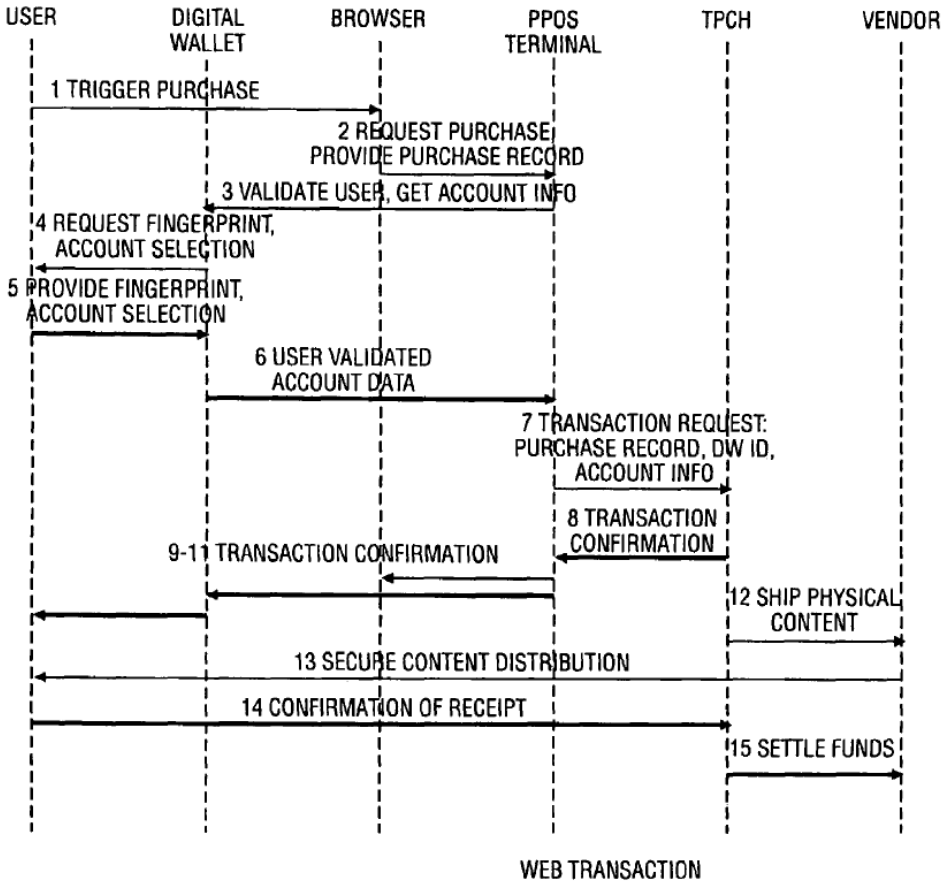


FIG. 17

Figure 17 is a flowchart of a process for performing a web-based transaction. *Id.* at 2:37–38. In this example,

> the user may be at home with a PC, cable, satellite or digital television device, a web browser, and a personal POS terminal device as described herein. The user has selected items to be purchased and is ready to trigger a purchase. The user may either navigate to a web page by using the facilities of the web browser, or by triggering a shopping activity using the transaction device.

Id. at 28:19–25.

The user triggers a purchase by clicking on a "Buy!" button in a web browser (step 1). *Id.* at 28:34–35. The browser, via a plug-in that allows it to communicate with a personal POS (PPOS) terminal integrated into the host personal computer (PC), communicates with the PPOS to initiate the

transaction and provide a record to the vendor (step 2). *Id.* at 28:35–40, 28:50–56. The PPOS terminal asks the transaction device to validate the user and get payment information from the user (step 3). *Id.* at 28:57–62. The user confirms the transaction and shows he or she is authorized by providing a fingerprint recognition sample to the transaction device (steps 4–5). *Id.* at 28:64–29:4. The transaction device validates that the user is authorized and the PPOS terminal sends to the TPCH the transaction record and the unique ID of the transaction device (steps 6–7). *Id.* at 29:5–14. The TPCH validates the transaction device, determines that the selected financial account has sufficient funds, and issues a transaction confirmation to the PPOS terminal (step 8). *Id.* at 29:15–18. The PPOS terminal sends the transaction confirmation to the web browser and transaction device (steps 9–11). *Id.* at 29:18–20. Secure distribution of physical or electronic content to the user is performed once the transaction is authorized (steps 12–13). *Id.* at 29:29–30. The TPCH then receives confirmation that content was delivered to the user and the TPCH processes settlement of funds. *Id.* at 29:31–34.

Ludtke describes various alternatives for the TPCH's involvement in funds settlement:

> The settlement of funds involves the transfer of the appropriate financial credit into the vendor's account. For the purposes of this example, it is assumed that the account is managed completely by the TPCH, and thus the funds transfer is handled completely inside of the TPCH. The vendor is not given any user identity information regarding the transaction; rather, the user is represented only by the transaction device identification information.
>
> In an alternative embodiment, the TPCH may issue a funds settlement request to a third party financial institution on behalf of the user, causing the necessary funds to be transferred to the vendor from the user's account. In yet another alternative

> embodiment, the TPCH may act as a proxy for the user, whereby the TPCH takes the funds from the user's account as managed by a third party financial institution, and then issues a funds transfer from the TPCH account to the vendor's account. This embodiment further preserves the user's identity by not linking it with the funds transfer into the vendor's account.

Id. at 29:35–53.

3. Differences, if any, between claims 1, 2, 4–7, 10, 12, 13, 15, 16, 18, 19, and 22–27 and Ludtke; reasons to modify

Regarding claim limitations 1ai, 1aii, and 1aiii, Petitioner argues that Ludtke teaches persistently storing, in a user identity/account information block of the transaction device, biometric information (e.g., fingerprint, retinal scan, voice, DNA, hand profile, face recognition), a plurality of codes and other values comprising a device ID code uniquely identifying the transaction device (e.g., globally unique silicon ID (GUID), magnetic strip, bar codes), and a secret decryption value (e.g., public key infrastructure (PKI) public keys and private keys). Pet. 9–21 (citing Ex. 1005, 5:11–20, 8:63–67, 9:18–25, 10:64–67, 11:1–5, 13:27–29, 13:39–41, 14:13–21, 19:9–14, 19:29–40, 23:11–19, 30:18–27, 37:39–45, 38:1–3, 38:9–21, 38:25–29, 38:40–61, 39:7–18, 40:5–26, Figs. 7B–7C, 27, 33; Ex. 1003 ¶¶ 73–94). Patent Owner does not contest Ludtke's applicability to these aspects of claim 1. Based on Petitioner's evidence, we find that Ludtke teaches claim limitations 1ai, 1aii, and 1aiii. More particularly, we find that Ludtke's fingerprint, retinal scan, etc., are "biometric data"; that Ludtke's GUID, magnetic strip, etc., are examples of "a device ID code uniquely identifying an integrated device"; and that PKI keys are examples of "a secret decryption value."

Regarding claim limitation 1b, Petitioner argues that Ludtke's transaction device requests and receives a fingerprint sample or other biometric data. *Id.* at 21–22 (citing Ex. 1005, 14:33–42, 14:40–46, 16:47–50; Ex. 1003 ¶¶ 95–96). As to claim limitation 1c, Petitioner argues that Ludtke's transaction device compares the fingerprint sample to stored authorized samples to determine a match. *Id.* at 22 (citing Ex. 1005, 14:40–46; Ex. 1003 ¶ 97). Patent Owner does not contest Ludtke's applicability to these aspects of claim 1. We agree with Petitioner and find that Ludtke teaches claim limitations 1b and 1c.

Claim limitation 1d recites:

> responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes from the plurality of codes and the 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 Ludtke describes the transaction device sending, over a wireless network, to the TPCH, a communication including a unique transaction device ID. Pet. 22–23 (citing Ex. 1005, 5:63–64, 7:46–48, 9:26–30, 9:35–42, 9:51–59, 28:50–29:12, 30:23–27; Ex. 1003 ¶¶ 98–106).

As to whether Ludtke teaches a determination of whether the scan data matches the biometric data, Petitioner points to Ludtke's description of the transaction device (digital wallet or privacy card) prompting the user to supply a fingerprint recognition sample, comparing the sample to stored fingerprints, and determining that the user is authorized if the supplied sample is recognized. *Id.* at 23–25 (citing Ex. 1005, 1:22–31, 1:37–38, 4:62–5:1, 14:33–46, 18:45–50, 18:52–55, 27:12–13, 28:13–18, 28:26–45, 28:50–29:12, 34:25–27; Ex. 1003 ¶¶ 99–103). As to whether Ludtke teaches wirelessly sending one or more codes for authentication, Petitioner points to

Ludtke's description of its transaction device sending the unique transaction device ID to the TPCH using wireless or cellular signals. *Id.* at 25 (citing Ex. 1005, 9:26–42; Ex. 1003 ¶ 103). Patent Owner does not contest Ludtke's applicability to these aspects of claim limitation 1d. We agree with Petitioner, and find that Petitioner's evidence shows that Ludtke teaches these aspects of claim limitation 1d.

Petitioner contends that Ludtke's TPCH is a third party that operates a trusted authority because it is an entity that is separate from the parties to the transaction. *Id.* at 25. Specifically, Petitioner contends that the parties to the transaction are the user (using the transaction device) and the external retailers and vendors that complete the transaction. *Id.* at 25–26 (citing Ex. 1005, 7:46–48 ("This allows the TPCH 110 to retain user privacy by not exposing addressing information and possibly email addresses to third parties."), 9:26–30, 9:35–39, 9:43–59, Fig. 6. As Ludtke states, "[i]n one embodiment of electric distribution, the TPCH 110 functions as the middleman of the distribution channel." Ex. 1005, 7:44–46.

Patent Owner contests Petitioner's identification of the user and the retailer as the parties to the transaction, and contends, instead, that the TPCH is both the application being accessed and a party to the transaction and, therefore, is not a third party that operates a trusted authority, as recited in claim limitation 1d. We address those arguments below with our analysis of Patent Owner's arguments for claim limitation 1e.

As to claim limitation 1e, Petitioner argues that, after the TPCH authenticates the transaction device ID, a webpage receives from the TPCH an indication of an approval of the transaction to be performed, and that the indication allows the user to access content or a reference to content on a

webpage. Pet. 28–29 (citing Ex. 1005, 24:17–32, 28:26–40, 29:15–20, 29:29–30, 31:41–52; Ex. 1003 ¶¶ 107–114). For example, Ludtke states:

> After validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction, the TPCH issues a transaction confirmation back to the personal POS terminal. The personal POS terminal reflects the transaction confirmation back to the web browser and the transaction device. The transaction device may display a transaction confirmation to the user and may additionally record the transaction in its local storage.
>
> . . .
>
> Secure distribution of physical (or electronic) content to the user is performed once the transaction is authorized.

Ex. 1005, 29:15–30. Mr. Gray testifies that "[t]he distributed content includes the content itself or a reference to that content, such as a 'web URL.'" Ex. 1003 ¶ 110. In this example, Petitioner contends that the "transaction confirmation" is an "access message" and that the content the user is allowed to access on the webpage is an "application." Pet. 30 (citing Ex. 1005, 29:15–22, 29:29–30; Ex. 1003 ¶ 110).

Petitioner relies on specific examples from Ludtke of new functionality and software that a user can download to the transaction device. *Id.* at 30–31 (citing Ex. 1005, 31:11–16, 19:45–50, 31:11–52; Ex. 1003 ¶¶ 112–113). For example, Ludtke states:

> In one embodiment, the transaction device can adapt to new services and functionality, either automatically by the transaction device or manually by the user. For example, on a web site the user might click a button that causes new functionality to be downloaded to the transaction device for access at a future time.

Ex. 1005, 31:12–16. In a specific example, "when arriving at a new airport, the transaction device might download a new service that provides

instructions for how to buy a train ticket to certain destinations." *Id.* at 31:30–33. Or, "if the transaction device finds itself in the presence of a service that is managed by an alternate system, it can download not only the service software, but also the necessary underlying 'transaction system' software. This might include new security protocols, etc." *Id.* at 31:35–40. Mr. Gray testifies that "[t]he downloaded functionality and software/service is an 'application' within the meaning of the '954 patent, which defines 'application' as 'a resource that can be accessed by a verified and authenticated user.'" Ex. 1003 ¶ 113 (citing Ex. 1005, 18:45–50, 31:11–52; Ex. 1001, 6:18–24).

Patent Owner argues that Ludtke's TPCH is the application being accessed in Ludtke's transactions and, therefore, that the TPCH cannot be a third party that operates a trusted authority because the trusted authority must not be the same entity as the application being accessed. PO Resp. 13. Patent Owner argues that "[t]he TPCH of Ludtke authenticates the transaction device, and confirms the transaction and authorizes it, [but] it does not split these steps up like the claims of the Patent at Issue require." *Id.* Patent Owner then points to examples in Ludtke where Patent Owner contends Ludtke confirms a transaction, and concludes that "[i]n all of the foregoing embodiments, TPCH both authenticates the device and confirms the transaction and the merchant accepts the confirmation as payment." *Id.* at 13–14 (citing Ex. 1005, 27:13–16, 29:15–34; Ex. 2018 ¶¶ 20–22). Patent Owner does not offer any persuasive support for its argument that the claims require that the third party that operates a trusted authority must not split up confirming and authorizing a transaction. If Patent Owner is arguing for a claim construction here, Patent Owner has not explained why the language of the claims, the specification, or the prosecution history support

this limitation, and we see no such evidence. Thus, Patent Owner's attempt to divide up the transaction in order to assign the TPCH the role of party rather than middleman is not persuasive.

Patent Owner argues that "the TPCH is being accessed to provide a payment to the merchant via a confirmation message (i.e., authorization), which completes the transaction," and that "[t]he TPCH of Ludtke is thus the application that the user is trying to access -- the ability to pay the vendor with the user's account (the private information) is the application." *Id.* at 14 (citing Ex. 2018 ¶¶ 20, 21, 30, 31). As we explained in our Institution Decision, however, the fact that "the TPCH is capable in certain embodiments of settling funds does not make it a 'party' to the transaction because it remains independent of the user, POS, and 'external' vendors." Inst. Dec. 21 (quoting Pet. 28). Rather, as we explained when preliminarily construing "third party that operates a trusted authority," active participation in a transaction, by itself, does not make an entity a party to that transaction. *Id.* at 11. Patent Owner offers no persuasive evidence suggesting that it does. Instead, we agree with Petitioner (Pet. 25–26) and find that the parties to the transactions described in Ludtke are the user of the transaction device (who seeks to purchase a good or service) and the retailer or vendor of that good or service.

Patent Owner further argues that "[i]n an attempt to establish an 'application' that is separate from the TPCH and the user, the Petition points to the disclosures of Ludtke that deal with settlement (the actual transfer of funds at some point after the transaction has been completed) rather than either authorization or transaction confirmation." PO Resp. 15 (citing Ex. 2018 ¶¶ 20–28); *see also* Sur-reply 11 ("Petitioner's rationale for why the TPCH is a 'third-party trusted authority' is that the TPCH processes

payments for 'web transactions.'"), 12 ("Thus, the rationale asserted in the Petition and reiterated in the Reply is that the online vendor completes the transaction by distributing the purchased items to the user after the user has provided payment via the TPCH."), 13 ("However, just because the user may engage in one transaction to fulfill their obligations in a second does not mean that the parties to the first transaction also become third parties with respect to the second. Rather, the web transaction is a separate and distinct transaction between the user and the vendor that is ***completed by the vendor***."). Patent Owner then discusses four examples in Ludtke and concludes that "[a]ll four of these settlement methods taught by Ludtke occur after the merchant has accepted the transaction confirmation (transaction authorization) issued by the TPCH as payment and has tendered the goods or services." PO Resp. 15–17 (citing Ex. 1005, 6:51–55, 7:12–20, 29:35–39, 29:43–46; Ex. 2018 ¶¶ 24–30).

Petitioner responds that the TPCH is not an "application," as claimed, because "it is not accessed by a *verified and authenticated user of the transaction device*—it 'functions as the middleman of the distribution channel.'" Reply 7–8 (quoting Ex. 1005, 7:44–48). We agree. Claim limitation 1e, for example, recites "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." Thus, according to the claim language, the claimed "application" is the application that receives an access message that indicates that the information received by the trusted authority from the user is authentic. Because the TPCH does not receive such an access message (the information it receives has not yet been authenticated), it is not the claimed application.

And, contrary to Patent Owner's arguments, we do not understand Petitioner to be arguing that issuance of payment (be it by the TPCH or by some other entity, such as a bank) is the transaction for purposes of identifying the parties and the application. Rather, Petitioner identifies the delivery of electronic content, new functionality, software, and services (e.g., electronic train tickets) to Ludtke's transaction device or to the user's web browser, in response to the transaction confirmation sent by the TPCH. Pet. 30–32; Reply 10–12. According to Mr. Gray, "Ludtke discloses receiving at the downloaded software/functionality (application) a transaction confirmation (access message) that allows the user to access the services prescribed by the downloaded software/functionality (application)." Ex. 1003 ¶ 114.

As to such additional software and services, Patent Owner argues that "the Petition does not identify an access message enabling or announcing access to these additional functionalities." Sur-reply 13. However, as Petitioner observes, Ludtke describes:

> After validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction, the TPCH issues a transaction confirmation back to the personal POS terminal. The personal POS terminal reflects the transaction confirmation back to the web browser and the transaction device. The transaction device may display a transaction confirmation to the user and may additionally record the transaction in its local storage. . . .
>
> Secure distribution of physical (or electronic) content to the user is performed once the transaction is authorized.

Ex. 1005, 29:15–23, 29:29–30. Mr. Gray testifies that "Ludtke discloses receiving at a web browser webpage (application) a transaction confirmation (access message) that allows the user to access electronic content on the web

browser (application)." Ex. 1003 ¶ 110 (citing Ex. 1005, 29:15–23, 29–30). Thus, Ludtke describes a webpage receiving a message that both enables and announces access to the additional functionality, software, and services. We find that this is an example of receiving, at an application (web browser or webpage), an access message (transaction confirmation) from the trusted authority (TPCH) indicating that the trusted authority successfully authenticated the codes from the transaction device and allowing the user access to the application (new electronic content available on the webpage).

Patent Owner further argues that each challenged claim "requires that the access message allow access to or announce access to an application" and that Petitioner "fails to account for this claim term." PO Resp. 17–18. Patent Owner argues that "Ludtke only discloses confirming a transaction," and "only provides a confirmation once the transaction has been fully completed." *Id.* at 18 (citing Pet. 29–31, 41–42, 54; Ex. 1005, 29:10–23; Ex. 1003 ¶ 112). Similarly, Patent Owner argues that

> Ludtke does not disclose a signal or notification enabling or announcing access to the digital content; Ludtke only discloses the delivery of that digital content to the user following the completion of a transaction. Thus, even if a vendor could be considered the application being accessed, the only thing disclosed in Ludtke is that a vendor can determine whether to deliver physical or digital goods to a user based on whether or not the vendor gets payment or a promise to pay **not** a signal enabling or announcing access.

Id. at 21–22 (citing Ex. 1005, 28:15–18, 28:26–40; 29:15–20, 31:41–50). Patent Owner misunderstands Ludtke. In the example of Figure 17, "[s]ecure distribution of physical (or electronic) content to the user is performed once the transaction is authorized," the TPCH then receives confirmation that the content was shipped to the user, and "[o]nce the

confirmation is received, the TPCH processes the settlement of funds." Ex. 1005, 29:29–34.

Patent Owner argues that Ludtke's transaction confirmation does not allow access to various entities that Patent Owner argues Petitioner identifies as applications. PO Resp. 18–22. For example, Patent Owner argues that Ludtke's transaction confirmation does not allow access to the POS terminals discussed in the examples of Figures 12–14 and 17. *Id.* at 18–20 (citing Ex. 1005, 21:51–57, 23:50–55, 25:34–58, 28:58–62, 29:6–14). This argument is inapposite, as Petitioner does not argue that the POS in these examples is the application being accessed. Pet. 30–32.

As to the example of Figure 17, Patent Owner argues that "the transaction confirmation received from the TPCH of Ludtke does not allow access to a website; the user already has access to the website at the beginning of a transaction." PO Resp. 20 (citing Ex. 1005, 28:34–35, 28:50–52). Here, Patent Owner refers to Ludtke's user clicking a "Buy!" button on a webpage in a web browser and the web browser communicating with the PPOS terminal to request that it initiate a transaction (steps 1 and 2 of Fig. 17). *Id.*; *see* Ex. 1005, 28:34–35, 28:50–52. Petitioner, however, does not argue that a user first opening a webpage corresponds to allowing access to an application. Rather, Petitioner argues that the transaction confirmation from Ludtke's TPCH allows the user to access new functionality, software, and services corresponding to an application, either on the webpage or the transaction device (steps 8–11 and 13 of Fig. 17). Pet. 30 (citing Ex. 1005, 29:15–22, 29:29–30). Patent Owner's argument is not directed to Petitioner's allegations and, thus, is not persuasive.

Similarly, Patent Owner argues that "the transaction confirmation of Ludtke does not allow access to the functions of the transaction

device/digital wallet; the user already has access to all of those functions." PO Resp. 20. Petitioner, however, does not argue that a user first accessing the transaction device corresponds to allowing access to an application. Rather, Petitioner argues that the transaction confirmation from Ludtke's TPCH allows the user to access new functionality, software, and services corresponding to an application on the transaction device. Pet. 30 (citing Ex. 1005, 29:15–22, 29:29–30). We find that it does, as Ludtke describes electronic delivery of content to the user after the transaction is authorized. Ex. 1005, 29:29–30; *see also id.* at 31:11–16 (new functionality to be downloaded to the transaction device), 31:19–52 (examples including electronic train tickets and other digital content).

Patent Owner argues that "[a]s seen in figure 17 above, and in the teaching of Ludtke, the only reference to a 'signal' that Petitioner points to is the access message is **the signal whereby the user initially requests the content**, not the delivery of the content." PO Resp. 23. Here, Patent Owner "refers to step 1 of figure 17, wherein the signal relates only to the user **triggering the purchase**," and argues that "Figure [17] above and Ludtke's teachings make clear that the transaction confirmation to the transaction device is an independent step from the delivery of goods (whether physical or digital) to the user." *Id.* It is unclear what contention of Petitioner Patent Owner refers to here. In any case, Petitioner identifies signals 8–11 of Figure 17, not signal 1, as the access message. Pet. 30 (citing Ex. 1005, 29:12–22, 29:29–30; Ex. 1003 ¶ 110). We find that signals 8–11 correspond to an access message received by an application (e.g., a webpage with new content). Thus, Patent Owner's argument is not persuasive.

In sum, we find that the parties to the transactions described in Ludtke are the user of the transaction device and the retailer or vendor of the good

or service (e.g., web content, electronic train ticket, software) the user seeks to buy; and we further find that the TPCH, which merely acts as a middleman to facilitate the transaction, is not a party to the transactions described in Ludtke. Ex. 1005, 9:35–39, 28:34–56; Ex. 1003 ¶¶ 105–106. The web content, electronic train ticket, software, etc., is the application accessed. Ex. 1003 ¶ 113. We find that the TPCH sends (and the application receives) an access message (Ludtke's transaction confirmation) that indicates that the TPCH successfully authenticated codes from the transaction device and that allows the user access to the train ticket, software, etc. Ex. 1005, 29:15–31, 31:11–52; Ex. 1003 ¶¶ 110–114. Accordingly, Ludtke teaches claim limitations 1d and 1e.

Therefore, Ludtke teaches each limitation of claim 1.

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 to, and largely incorporate, its arguments and evidence for claim 1. Pet. 38–42, 45–54. Patent Owner presents its arguments for claims 1, 12, 16, and 22 together, and only as to the terms "third party that operates a trusted authority," "access message," and "application" appearing in each of these claims. PO Resp. 1–2. For the reasons given for claim 1, Petitioner has shown that Ludtke teaches each limitation of claims 12, 16, and 22.

Claim 2 depends from claim 1; claim 13 depends from claim 12. As to claims 2 and 13, we find that the device ID of Ludtke's transaction device is transmitted to the TPCH over a wireless or cellular network. Ex. 1005,

9:35–42, 5:63–64; Ex. 1003 ¶ 116; Pet. 32, 42. Thus, Ludtke teaches the additional limitation of claims 2 and 13.

Claim 4 depends from claim 1. We find that Ludtke teaches the transaction device sending a device ID to the TPCH when biometric scan data from the user matches stored biometric data. Ex. 1005, 14:33–46, 28:57–62, 29:5–6; Ex. 1003, 117–121; Pet. 32–34. Thus, Ludtke teaches the additional limitation of claim 4.

Claim 5 depends from claim 1; claim 26 depends from claim 22. We find that Ludtke teaches various examples of biometric data, including fingerprint and retinal scan data. Ex. 1005, 35:61–64; Ex. 1003 ¶ 122; Pet. 34, 58. Thus, Ludtke teaches the additional limitation of claims 5 and 26.

Claim 6 depends from claim 1; claim 25 depends from claim 22. We find that Ludtke teaches various examples of transaction devices, including pagers and cellular phones. Ex. 1005, 9:39–41, 11:66–12:7, 15:65–16:8, 17:65–18:4, 26:56–57, 33:49–54, Figs. 7A, 9A; Ex. 1003 ¶¶ 124–125; Pet. 35–36, 58. Thus, Ludtke teaches the additional limitation of claims 6 and 25.

Claim 7 depends from claim 1; claim 19 depends from claim 16; claim 27 depends from claim 22. We find that one example of an application accessed in Ludtke's transactions is a website. Ex. 1005, 29:15–20, 29:29–30, 31:41–52; Ex. 1003 ¶ 129; Pet. 37, 50, 58. Thus, Ludtke teaches the additional limitation of claims 7, 19, and 27.

Claim 10 depends from claim 1; claim 18 depends from claim 16. We find that Ludtke's description of establishing a secure connection to a back-end system teaches the additional limitation of claims 10 and 16. Ex. 1005,

37:39–45; Ex. 1003 ¶ 130; Pet. 37, 50. Thus, Ludtke teaches the additional limitation of claims 10 and 18.

Claim 15 depends from claim 12. We find that Ludtke's verification unit includes a liquid crystal display (LCD) screen that, conventionally, would have been back-lit using LEDs, and that the LCD screen requests a biometric scan. Ex. 1005, 11:37–41, 14:54–63, 16:53–56, 28:63–9:4; Ex. 1017 ¶ 41; Ex. 1018 ¶¶ 24, 108, 110, 135, 141, 154, 187; Ex. 1003 ¶¶ 142–145; Pet. 42–44. Thus, Ludtke teaches the additional limitation of claim 15.

Claim 23 depends from claim 22. We find that Ludtke teaches that its transaction device (an integrated hardware device) receives a validation request from a POS terminal and, upon receiving the request, prompts the user to scan their fingerprint. Ex. 1005, 14:33–46, 16:47–49, 28:57–62, 29:5–6; Ex. 1003 ¶¶ 171–173; Pet. 55–56. Thus, Ludtke teaches the additional limitation of claim 23.

Claim 24 depends from claim 23. We find that when Ludtke's integrated device cannot verify a fingerprint scan from the user, it does not send a device ID or other information to the TPCH. Ex. 1005, 4:62–5:1, 12:23–25, 14:40–46, 18:23–31, 29:5–6, 39:50–56 ("If a match does not occur, then at 3110 an error message is output and the DW [digital wallet] returns to checking to see if a fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes."); Ex. 1003 ¶¶ 174–177. Thus, Ludtke teaches the additional limitation of claim 24.

Patent Owner does not present separate arguments for the dependent claims.

In sum, Ludtke teaches each limitation of claims 1, 2, 4–7, 10, 12, 13, 15, 16, 18, 19, and 22–27.

4. Conclusion of obviousness

As detailed above, we find that Ludtke teaches each limitation of claims 1, 2, 4–7, 10, 12, 13, 15, 16, 18, 19, and 22–27. The record does not contain evidence of objective indicia of nonobviousness. Upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claims 1, 2, 4–7, 10, 12, 13, 15, 16, 18, 19, and 22–27 would have been obvious over Ludtke.

C. Obviousness of Claims 3, 14, and 17 over Ludtke and Kon

Petitioner contends that claims 3, 14, and 17 would have been obvious over Ludtke and Kon. Pet. 58–68. 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.

Kon describes examples of identifying a person using a person identification certificate (IDC) which can include information such as fingerprints, retina patterns, voice, etc. Ex. 1006 ¶¶ 173, 241. The IDC can include the age of the user. *Id.* ¶ 234, Fig. 5 (Subject Directory Attributes, including "Personal information . . . used to authenticate subject Age, sex, etc."). The user registers personal information with a person identification certificate authority (IDA), which issues the IDC to the user. *Id.* ¶ 178. Service providers verify the authenticity of the user based on the IDC. *Id.*

Petitioner contends that Kon describes registering and storing a user's age in association with a user device's device ID. Pet. 63–67 (citing

Ex. 1006 ¶¶ 194, 234, 241, 265–266, Figs. 5, 9; Ex. 1003 ¶¶ 184–185). Petitioner argues that "[t]he user's age, like the biometric information, provides another data point for identifying the user," and would have been especially useful when a transaction has an age minimum, such as purchasing alcohol or cigarettes. *Id.* at 68 (citing Ex. 1003 ¶¶ 186–187). Accordingly, Petitioner argues, a skilled artisan would have registered a user's age, as taught by Kon, with Ludtke's device ID to facilitate age-prohibitive transactions. *Id.* Petitioner makes the same arguments for claims 10 and 13. Pet. 69 (citing Ex. 1003 ¶ 188). Patent Owner does not provide separate arguments for claims 3, 14, and 17.

On the complete record, for the reasons articulated by Petitioner, we find that Kon teaches the additional limitations of claims 3, 14, and 17, and that a skilled artisan would have had reasons, with rational underpinning, for combining Ludtke and Kon. The record does not contain evidence of objective indicia of nonobviousness. Upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claims 3, 14, and 17 would have been obvious over Ludtke and Kon.

D. Patent Owner's Declaration Testimony and Sur-reply Exhibits

Patent Owner offers the declaration testimony of Troy Carrothers (Ex. 2018). Specifically, Patent Owner offers Mr. Carrothers' testimony to show that Ludtke's system, in particular the TPCH, implemented steps according to a standard credit card transaction. PO Resp. 13–17 (citing Ex. 2018 ¶¶ 20–31).

Petitioner argues that Mr. Carrothers' testimony should be given no weight because he does not have the education or experience required of a

person of ordinary skill in the art. Reply 2–4 (citing *Kyocera Senco Indus. Tools Inc. v. Int'l Trade Comm'n*, 22 F.4th 1369, 1376–77 (Fed. Cir. 2022)).

The Federal Circuit has made clear that:

> To offer expert testimony from the perspective of a skilled artisan in a patent case—like for claim construction, validity, or infringement—a witness must at least have ordinary skill in the art. Without that skill, the witness' opinions are neither relevant nor reliable. The opinions would not be based on any specialized knowledge, training, or experience that would be helpful to the factfinder. In fact, "[a]dmitting testimony from a person . . . with no skill in the pertinent art serves only to cause mischief and confuse the factfinder." That testimony would "amount[ ] to nothing more than advocacy from the witness stand."

Kyocera, 22 F.4th at 1376–77 (quoting *Sundance, Inc. v. DeMonte Fabricating Ltd.*, 550 F.3d 1356, 1362, 1364–65 (Fed. Cir. 2008) (alterations in *Kyocera*)).

As explained above, a person of ordinary skill in the art would have had at least a bachelor's degree in Computer or Electrical Engineering or an equivalent engineering discipline, and at least three years of experience in the field of encryption and security, or the equivalent, while additional education could substitute for professional experience, and significant work experience could substitute for formal education. Mr. Carrothers claims to be "a financial services and retail leader with approximately thirty years of experience working in a variety of leadership roles in retail payments." Ex. 2018 ¶ 1. He lists professional and consulting experience with retail payments, operational and risk management of a credit card portfolio, and payment insurance and acceptances in stores and online. *Id.* ¶¶ 1–5. His Curriculum Vitae (Ex. 2018, Appendix A) lists education including a Bachelor of Business Administration and a Master of Business

Administration. Mr. Carrothers does not claim to, or demonstrate that, he has either the technical education or the technical experience to be a person of ordinary skill in the art.

In response to Petitioner's challenge to Mr. Carrothers' qualifications, Patent Owner does not contend that Mr. Carrothers is at least a person of ordinary skill in the art.[7] Rather, Patent Owner argues that "[t]o put the asserted portions of Ludtke in context, Mr. Carrothers provided testimony regarding the processing of credit and debit card payments with respect to online transactions based on his expertise and experience with retail payments." Sur-reply 1.

Patent Owner uses Mr. Carrothers' testimony to support arguments regarding the timing and parties to the communications generated by Ludtke's system, and to support arguments that the TPCH is a party to Ludtke's transactions. PO Resp. 13–17 (citing Ex. 2018 ¶¶ 20–31). We find that Mr. Carrothers testifies on technical details regarding unpatentability, and that a declarant testifying as to such subject matter should have at least ordinary skill in the art. Thus, Mr. Carrothers' testimony is entitled to no weight. *See Kyocera*, 22 F.4th at 1376–77.

In the Sur-reply, Patent Owner contends that we should consider Mr. Carrothers' testimony because his testimony "can be corroborated by independent sources." Sur-reply 1. Patent Owner then introduces, and argues the contents of, several new exhibits not introduced into the record before the Sur-reply was filed. *Id.* at 1–5 (discussing Exhibits 2029–2033). Patent Owner's introduction of new exhibits violates our rules. 37 C.F.R.

[7] As noted above, we dismiss Patent Owner's belated attempt at oral hearing to challenge Petitioner's statement of the level of skill in the art (which we adopt).

§ 42.23(b) (emphasis added) provides that "[a] sur-reply may only respond to arguments raised in the corresponding reply and *may not be accompanied by new evidence* other than deposition transcripts of the cross-examination of any reply witness." According to our Trial Practice Guide, "[w]hile replies and sur-replies can help crystalize issues for decision, a reply or sur-reply that raises a new issue or belatedly presents evidence may not be considered." Consolidated Trial Practice Guide[8] at 974; *see also* 84 Fed. Reg. 64,280 (Nov. 21, 2019). Patent Owner's new evidence (Exhibits 2029–2033) and the argument that discusses the new evidence (Sur-reply 1–5) are improper and will not be considered.

E. The '052 Reexam

As noted above, the '730 patent, a patent related to the '954 patent, is the subject of the co-pending '052 reexam. Patent Owner argues that the Examiner in the '052 reexam has rejected arguments substantially the same as those presented by Petitioner in this proceeding. Setting aside whether the prosecution of a co-pending reexamination of a different patent is relevant to this proceeding, Patent Owner's characterization of the Examiner's position in the '052 reexam is incorrect and, therefore, unpersuasive.

Patent Owner argues that the Request for the '052 reexam was based on Ludtke's TPCH being a third-party trusted authority because Ludtke's TPCH processes a financial transaction.[9] Sur-reply 14–15 (citing Ex. 2023, 65, 69). Patent Owner argues that it explained to the Examiner that the

[8] Available at https://www.uspto.gov/TrialPracticeGuideConsolidated.
[9] As explained above, this is not Petitioner's allegation in this proceeding.

TPCH was the application being accessed by the user to tender payment to the vendor and reiterated (and expanded upon) that argument in response to a first office action. *Id.* at 15 (citing Ex. 2024, 5–10; Ex. 2025, 11–14; Ex. 2020,[10] 12–17). Patent Owner further argues that the '052 reexam "has addressed—and refuted—the argument that Ludtke's TPCH is a 'third-party trusted authority' due to processing a financial transaction." *Id.* (citing Ex. 2021, 27–28). However, the Examiner did not accept Patent Owner's argument; rather, the Examiner issued new grounds of rejection and determined that "[t]his argument is moot in view of the updated rejections." Ex. 2021, 27–28; *see also* moot, BLACK'S LAW DICTIONARY, 1099 (9th ed. 2009) ("Having no practical significance; hypothetical or academic <the question on appeal became moot once the parties settled their case>"). Thus, the '052 reexam record does not reflect that Patent Owner refuted an argument that Ludtke's TPCH is a third-party trusted authority because it processes a financial transaction.

Patent Owner also argues that the first Office Action in the '052 reexam "asserted that an access message received from Ludtke's TPCH enabled or announced access to additional functionalities, including access to the digital wallet itself." Sur-reply 15–16 (citing Ex. 2025, 15). Patent Owner argues that it "responded by detailing why Ludtke fails to disclose the TPCH sending an 'access message' allowing the user to access additional functionalities," and that "[t]he CRU found Patent Owner's arguments persuasive" and the '052 reexam "addressed -- and refuted -- the

[10] Patent Owner cites to Exhibit 2026, which is a December 6, 2024, Interview Summary and, therefore, not the correct exhibit. Sur-reply 15. Exhibit 2020 is an October 9, 2024, Response to Office Action, and appears to be the exhibit to which Patent Owner intended to cite.

argument that Ludtke's TPCH sends an access message allowing access to additional functionalities." *Id.* at 16 (citing Ex. 2020, 17–19; Ex. 2021, 28). However, the Examiner did not accept Patent Owner's argument; rather, the Examiner issued new grounds of rejection and determined that "[t]his argument is moot in view of the updated rejections." Ex. 2021, 28.

Finally, Patent Owner argues that it refuted, in a Response to Office Action, that Ludtke's TPCH provides an access message permitting access to a webpage and that "[t]he CRU found the Patent Owner's remarks persuasive." Sur-reply 16–17 (citing Ex. 2020, 19; Ex. 2021, 28). However, the Examiner did not accept Patent Owner's argument; rather, the Examiner issued new grounds of rejection and determined that "[t]his argument is moot in view of the updated rejections." Ex. 2021, 28.

Thus, the '052 reexam does not reflect that the Examiner was persuaded by the arguments Patent Owner presents in this proceeding.

In a December 17, 2024, Interview Summary, the "Examiner notes the claims [of the '730 patent] are silent as to where the access message is sent," and "[w]ere the claims [of the '730 patent] to recite the access message being sent to/received by the application . . ., the claims would be allowable over Ludtke," and that "[a]n Examiner's Amendment could achieve this." Ex. 2027, 4. The Examiner followed this up with a March 3, 2025, Final Rejection proposing an amendment. Ex. 2035, 31. Although Patent Owner did not address it in its briefs, at the oral argument Patent Owner attempted to belatedly argue that we should defer to the Examiner's statements as to language Patent Owner considers substantially similar in the claims of the '954 patent. Tr. 44:3–46:17. In the bulk of its Estoppel Brief, Patent Owner argued that we are bound, under the Administrative Procedures Act, to follow this "final determination" by the Examiner, that we "cannot

overrule the Examiner," and that we allegedly "ceded jurisdiction to the Examiner" and "lack[] jurisdiction" over the '052 reexamination. PO Estoppel Br. 2–6. These arguments are untimely, and we give them no weight. *See Dell*, 884 F.3d at 1369.

Moreover, the Examiner in the '052 reexam has withdrawn the Final Rejection, including the proposed amendment, on which Patent Owner's belated argument relies. Ex. 3003 (May 20, 2025, Office Action), 3 ("This is a Non-Final Office Action addressing amended claims 1–17. The previous rejection under Ludtke is withdrawn."). The Examiner gave no reason for withdrawing the rejection, and instead proceeded to reject claims 1–17 of the '730 patent over Burger[11] (US 2005/0050367 A1). We treat the Examiner's decision to withdraw the rejection involving Ludkte as a determination that that rejection is moot (and not an assessment of the merits), and her proposed amendment as withdrawn and, thus, of no relevance to this proceeding.

Even if we consider the '052 reexam, we see little relevance of its record to this proceeding.

III. ESTOPPEL

Because we conclude that Petitioner has proved on the merits that claims 1–7, 10, 12–19, and 22–27 of the '954 patent are unpatentable, we need not address Petitioner's argument (Pet. Estoppel Br.) that Patent Owner is collaterally estopped from arguing the patentability of the claims of the '954 patent.

[11] Burger is part of the challenges raised in IPR2024-00775 and IPR2024-00846.

IV. CONCLUSION[12]

Petitioner has proved by a preponderance of the evidence that claims 1–7, 10, 12–19, and 22–27 of the '954 patent are unpatentable.

The outcome for the challenged claims of this Final Written Decision follows. In summary:

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
1, 2, 4–7, 10, 12, 13, 15, 16, 18, 19, 22–27	103(a)	Ludtke	1, 2, 4–7, 10, 12, 13, 15, 16, 18, 19, 22–27	
3, 14, 17	103(a)	Ludtke, Kon	3, 14, 17	
Overall Outcome			1–7, 10, 12–19, 22–27	

[12] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

V. ORDER

It is hereby:

ORDERED that 1–7, 10, 12–19, and 22–27 of the '954 patent are unpatentable;

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:

Erika Arner
Kara Specht
Cory Bell
Safiya Aguilar
Shawn Chang
FINNEGAN, HENDERSON, FARABOW, GARRETT, & DUNNER LLP
erika.arner@finnegan.com
kara.specht@finnegan.com
cory.bell@finnegan.com
safiya.aguilar@finnegan.com
shawn.chang@finnegan.com

Philip W. Woo
D. Stuart Bartow
Monte T. Squire
Paul Belnap
DUANE MORRIS LLP
pwwoo@duanemorris.com
dsbartow@duanemorris.com
mtsquire@duanemorris.com
phbelnap@duanemorris.com

PATENT OWNER:

David L. Hecht
James Zak

HECHT PARTNERS LLP
dhecht@hechtpartners.com
jzak@hechtpartners.com

Trials@uspto.gov
571-272-7822

Paper 32
Date: October 17, 2025

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*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

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."). The Board instituted an *inter partes* review of the challenged claims pursuant to 35 U.S.C. § 314. Paper 8 ("Inst. Dec.").

After institution, Patent Owner filed a Patent Owner Response (Paper 10, "PO Resp."), Petitioner filed a Reply (Paper 14, "Reply"), and Patent Owner filed a Sur-reply (Paper 17, "Sur-reply"). The parties then presented oral arguments via a (video) Hearing (August 18, 2025), and the Board entered a Hearing transcript into the record (Paper 31, "Tr.").

For the reasons set forth in this Final Written Decision pursuant to 35 U.S.C. § 318(a), we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 1–29 are unpatentable.

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"); terminated after Patent Owner request for adverse judgment) and IPR2024-00776 and IPR2024-01335 (both challenging U.S. Patent No. 9,298,905 B1 ("the '905 patent"); both dismissed or terminated after Patent Owner's request for adverse judgment). The '730 patent also was the

subject of *Samsung Electronics America, Inc. v. Proxense LLC*, IPR2021-01444 (PTAB) (institution denied). The '954 patent also was the subject of *Google LLC v. Proxense, LLC*, IPR2024-00233 (PTAB) (final written decision determining all challenged claims unpatentable), *Microsoft Corp. v. Proxense, LLC*, IPR2024-01327 (PTAB) (institution denied), and *Apple Inc. v. Proxense, LLC*, IPR2024-01334 (PTAB) (petitioner joined to IPR2024-00233). Pet. 107; Paper 5, 2. The '730 patent also was the subject of *Apple Inc. v. Proxense, LLC*, IPR2024-00232 (terminated after Patent Owner's request for adverse judgment).

Patent Owner states that patents related to the '954 patent are the subject of *ex parte* reexaminations in Application No. 90/015,052 ("the '052 reexam"), reexamining the '730 patent (currently pending), Application No. 90/015,053, reexamining the '905 patent (reexamination certificate cancelling all claims), and Application No. 90/015,054, reexamining U.S. Patent No. 10,698,989 (reexamination certificate cancelling all claims). Paper 24, 3–4.

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.

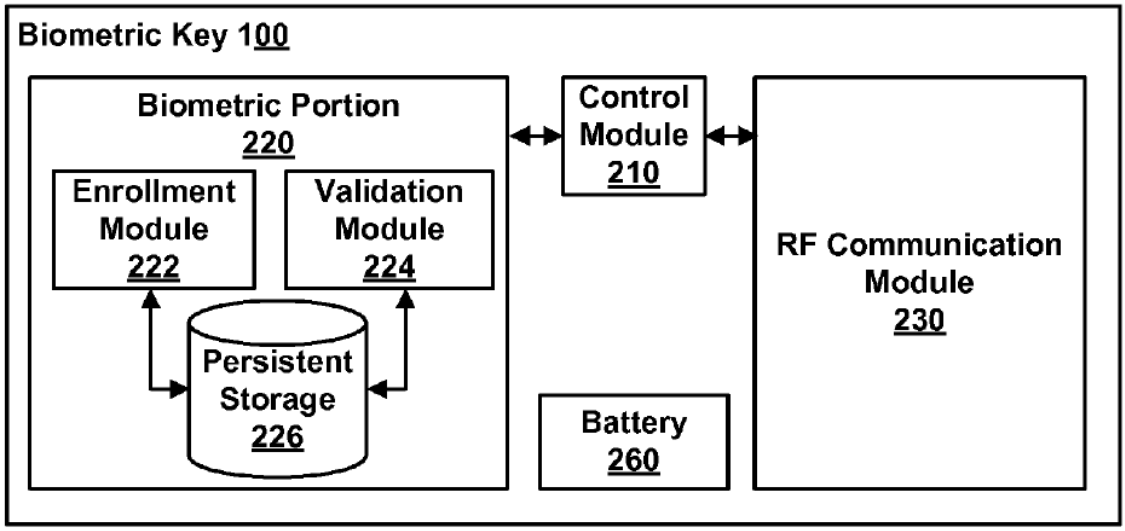


FIG. 2

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.

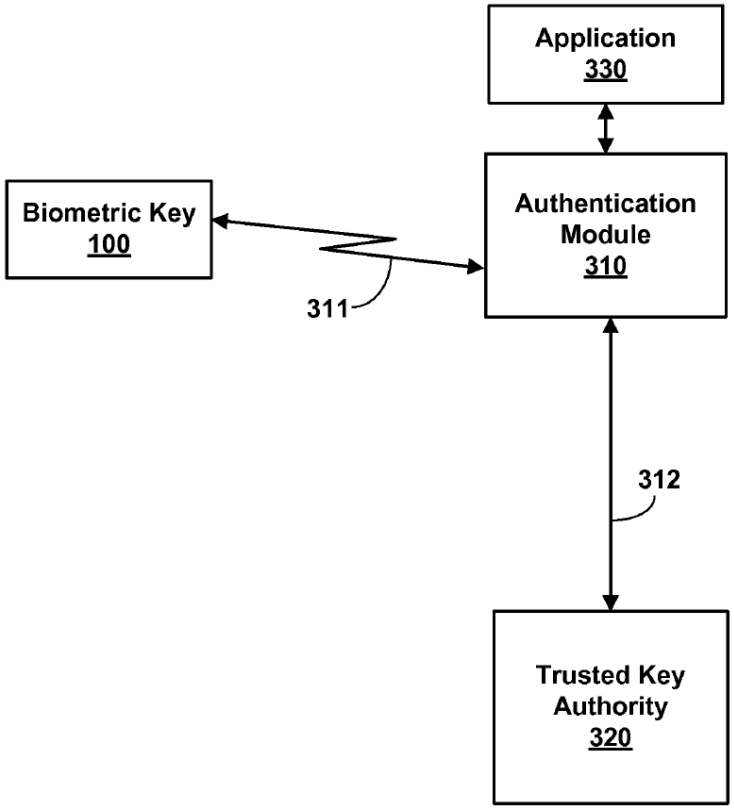


FIG. 3

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. 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.

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

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
Orsini	US 2004/0049687 A1	Mar. 11, 2004	1021

Petitioner also relies on the Declaration of Patrick Traynor, Ph.D. (Ex. 1003) and the Supplemental Declaration of Dr. Traynor (Ex. 1033).

E. The Asserted Grounds of Unpatentability

We instituted a trial under the following grounds (Inst. Dec. 8):

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),

[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.

> 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.

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

Independent claims 1, 12, 16, and 22 each recite "a third party that operates a trusted authority."[3] In our Institution Decision, we preliminarily construed this term "based on the ordinary meaning . . ., namely, 'a trusted authority that is an entity separate from the parties to a transaction.'" Dec. 11. We declined to construe any other terms, including "access message." *Id.* at 11–12.

As to our construction of "third party that operates a trusted authority," "Patent Owner does not dispute this construction," but does "dispute[] the implicit construction of the ***transaction*** and the ***principal parties*** thereto." PO Resp. 2. Patent Owner argues that, rather than challenging our construction of "third party that operates a trusted authority," "Patent Owner is merely attempting to construe the ***transaction*** and the ***principal parties*** thereto, which limit the scope of 'third-party

[3] The parties also refer to this term as "third party trusted authority." The '730 patent, a parent of the '954 patent, was the subject of *Samsung Electronics America, Inc. v. Proxense LLC*, IPR2021-01444 (PTAB) (institution denied). *See* Ex. 1007 (IPR2021-01444, Paper 11 (PTAB Feb. 28, 2022) ("Samsung DDI")). In the Samsung DDI, the Board construed "third-party trusted authority" to mean "a trusted authority that is an entity separate from the parties to a transaction." Ex. 1007, 15. Patent Owner appears to contend that "third party that operates a trusted authority," recited in the '954 patent claims, has the same meaning as "third-party trusted authority," recited in the '730 patent claims. Petitioner does not appear to dispute this. We treat these terms as equivalent.

trusted authority.'" *Id.* Specifically, Patent Owner argues, "[t]he claims . . . require a ***transaction*** of allowing a user access to an application, in which the ***principal parties*** are the user being allowed access and the application being accessed." *Id.* at 3; *accord id.* at 5 ("'Third-party trusted authority,' therefore, cannot be construed to encompass third parties to transactions other than those in which the principal parties are a user being allowed access and an application being accessed, and the underlying transaction is allowing a user access to an application."), 7 ("[T]he 'third-party trusted authority' is limited to a third-party with respect to a user being allowed access to an application and the application being accessed.").

In our Final Written Decision in IPR2024-00233 (Paper 35, "'233 FWD"), we "maintain[ed] our construction of 'a third party that operates a trusted authority,' namely, 'a trusted authority that is an entity separate from the parties to a transaction,'" and made clear that "[s]uch a transaction is not limited to those in which the application being accessed is a party." '233 FWD, 15. In reaching this conclusion, we found that "the plain language of claim 1 does not limit the parties to a transaction between the user and an application, or require that one of the parties to a transaction be the application ultimately accessed." *Id.* at 11. We further found nothing in the intrinsic evidence that departed from the ordinary meaning, either through lexicography or disavowal of the full claim scope. *Id.* at 12–14 (citing Ex. 1001[4], 2:35–48, 5:65–67, 6:8–34, 6:45–55, 6:64–7:4, 8:12–16, Figs. 3, 4, 7). Thus, in IPR2024-00233, we essentially rejected the modifications to our construction that Patent Owner advances in the Patent Owner Response.

[4] The '954 patent is Exhibit 1001 in both this proceeding and in IPR2024-00233.

In the Sur-reply, which post-dated the '233 FWD, Patent Owner states that "[t]he claims at issue have been construed in [the '233 FWD]" and, "[w]ithout forfeiting any right of appeal, Patent Owner believes that construction is binding upon these proceedings." Sur-reply 1.

For the same reasons, and based on the same evidence, given in the '233 FWD, we maintain our construction of "a third party that operates a trusted authority," namely, "a trusted authority that is an entity separate from the parties to a transaction," and make clear that such a transaction is not limited to those in which the principal parties are the user being allowed access and the application being accessed.

Based on the complete 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.[5] *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

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:

[5] The record does not include allegations or evidence of objective indicia of nonobviousness.

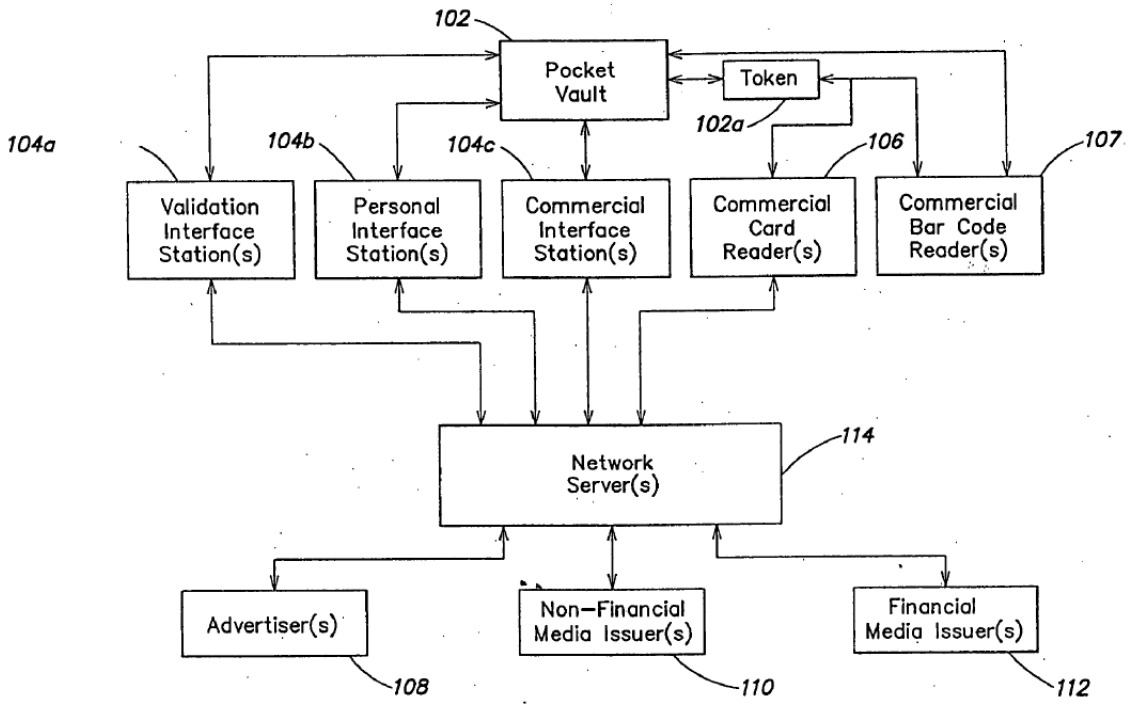


FIG. 1

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 media 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:

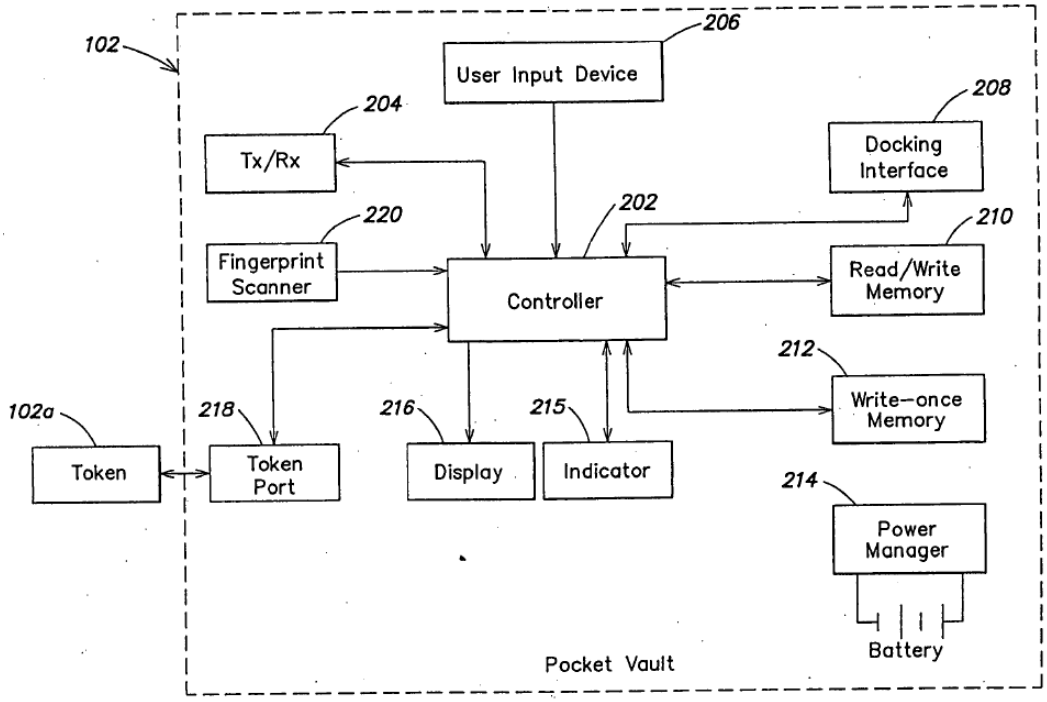


FIG. 2

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.[6] *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

[6] Burger contemplates other forms of biometric data, such as "retina scan, a speech pattern analysis, keystroke rhythm, etc." *Id.* ¶ 112.

fingerprint from scanner 220 to the fingerprint stored in fingerprint memory 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 104*a*–104*c*. *Id.* ¶¶ 186, 474, Figs. 7A, 8A, 19.

Figures 24 and 25 are reproduced below:

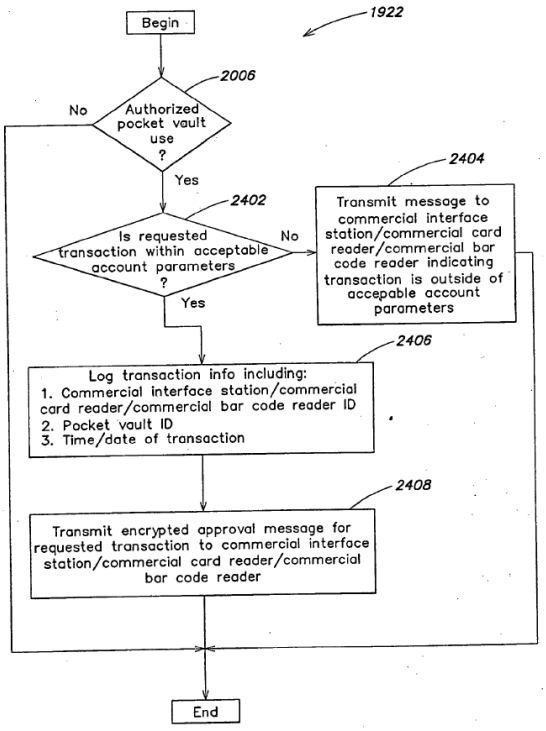


FIG. 24

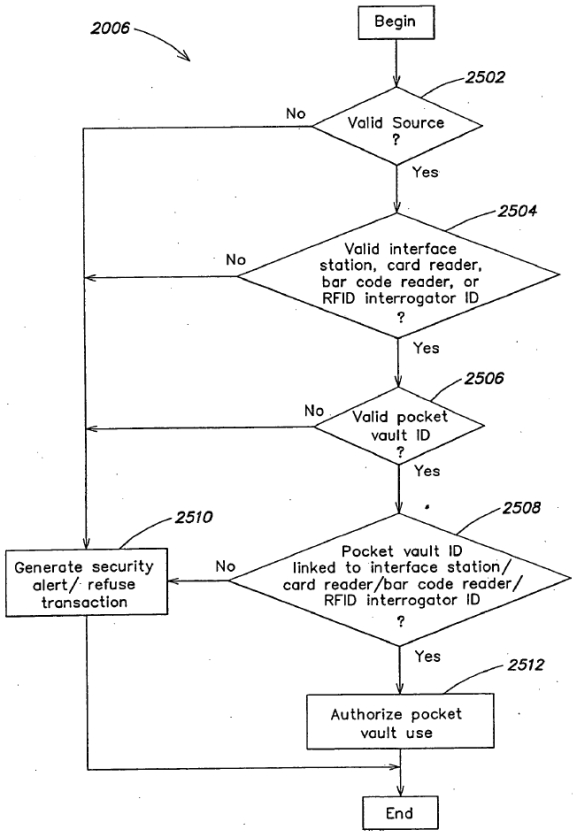


FIG. 25

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, network server 114 may serve as a repository for information regarding advertisers 108, and may serve as a conduit for advertisers to target particular classes of pocket vault holders and channel information to them. *Id.* ¶ 117. Figure 10A, reproduced below, illustrates an example:

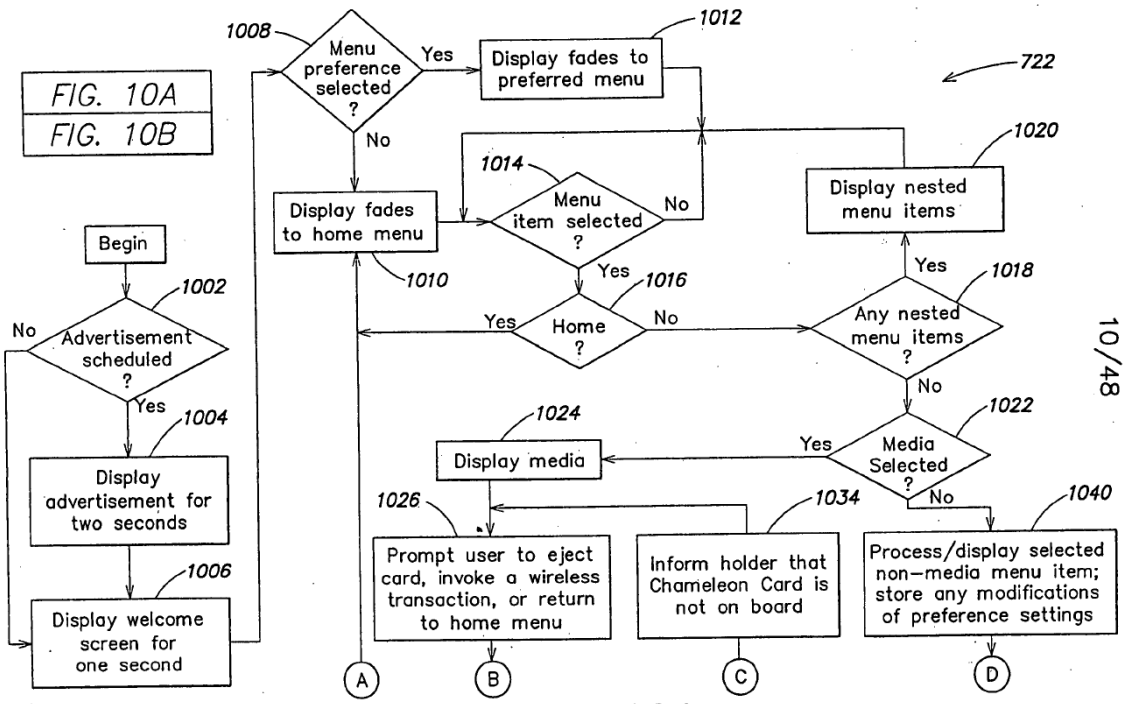


FIG. 10A

10/48

Figure 10A is a flow diagram of an authorized holder routine executed by controller 202 of pocket vault 102. *Id.* ¶¶ 57, 60, Fig. 2. Advertiser 108 can make arrangements with the company operating network server 114 to have certain advertisements uploaded to pocket vault 102 when it interfaces with personal interface station 104b. *Id.* ¶ 237. When it is determined that an advertisement is scheduled for display on pocket vault 102 (step 1002), the scheduled advertisement is displayed (e.g., for two seconds) (step 1004). *Id.* ¶¶ 237–238, Fig. 26I.

In another 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 102*a* 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

a) Claim 1: uncontested limitations

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). We agree.

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,

we agree with Petitioner and find 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). We also agree with Petitioner and find 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 uncontroverted testimony.

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," we agree with Petitioner and find 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. Pet. 28–30 (citing Ex. 1005 ¶¶ 112, 135, 178–182, Figs. 2, 7A; Ex. 1003 ¶¶ 99–100).

We agree with Petitioner and find that 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 teaches claim limitation 1.3, "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data." *Id.* at 30–31 (citing Ex. 1005 ¶¶ 182–184, Figs. 2, 7A; Ex. 1003 ¶ 101).

Patent Owner does not contest that Burger teaches limitations 1.1–1.3 of claim 1.

b) Claim 1: "third party that operates a trusted authority" and "application"

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). We find that Petitioner's evidence shows that Burger teaches these aspects of claim limitation 1.4, and Patent Owner does not contest this.

Petitioner argues that network server 114 acts as a third party that operates a trusted authority in three example transactions described in Burger, a credit card transaction, an advertisement displayed at the pocket vault, and an electronic hotel room key. For each of these examples, the parties' disagreement centers around an identification of the application to be accessed and the party, beyond the user, who is the other primary party to the transaction. Because the parties' disputes are as to the transactions as wholes, we evaluate claim limitation 1.4 along with 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."

(1) third party that operates a trusted authority; first theory (credit card transactions)

In Petitioner's first asserted example transaction, 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, 103, 125, 155–158, 189, 236–238, 320, Figs. 7B, 10A, 19; Ex. 1003 ¶ 114). Burger describes, for example, that "Pocket Vault 102 may be equipped to generate the token 102*a* such that the token 102*a* has transactional information regarding a media (e.g., an actual or simulated magnetic stripe or a bar code) produced thereon." Ex. 1005 ¶ 103. "[T]he token 102*a* may be used by the Pocket Vault holder to engage in a transaction wherein an entity swipes the magnetic stripe portion of the token 102*a* through a card reader 106 or scans the bar code on the token 102*a* using a bar code reader 107." *Id.* In cases where the retailer needs to see the credit or debit card number, "the holder may, for example, repeat the biometric input to the Pocket Vault 102 to reveal the card account number," and "[i]f placed in the personal interface station 104*c*, such account numbers may be automatically revealed." *Id.* ¶ 320; *see also id.* ¶¶ 157–158).

In this 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. Pet. 42–43 (citing Ex. 1005 ¶¶ 95, 155–158, 320; Ex. 1003 ¶ 114). 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 an "alternative mapping" of this 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 either mapping of 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. 52–53 (citing Ex. 1005 ¶¶ 94–96, 125–129, 155–158, 189, 242, 517–527, Figs. 7B, 10A, 19, 26H–26K). 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 Petitioner's first mapping of this example, the pocket vault presenting via magnetic stripe or displaying a credit card number to a retailer, Patent Owner argues that "[n]either the Petition nor Dr. Traynor offer anything more than a conclusory statement devoid of any articulated reasoning and rational underpinning" for why it would have been obvious for the pocket vault to receive an access message before displaying sensitive credit or debit card information to conduct a transaction. PO Resp. 7–8.

We find that, after Burger's network server 114 authenticates a user's pocket vault ID, the user is granted access to pocket vault 102 and can select a transaction from a displayed menu, including use of a credit card.

Ex. 1005 ¶ 242, Fig. 26H. It is straightforward and logical that the user's subsequent access to that credit card information, either by displaying it or through token 102a, is because network server 114 sent a communication to pocket vault 102 indicating that it successfully authenticated the pocket vault. Ex. 1003 ¶ 115. This is the obvious inference a skilled artisan would have drawn from Burger's description of authenticating the pocket vault and subsequently allowing credit card information to be used. Thus, we find that, in this example, the operator of network server 114 is a third party that operates a trusted authority, the principle parties to the transaction are the user of pocket vault 102 and the retailer, and a message from network server 114 to pocket vault 102 allowing the credit card to be used (displayed or encoded in the token) is an access message allowing the user access to the application (file with credit card information). Accordingly, we find that this example of Burger teaches claim limitations 1.4 and 1.5.

As to Petitioner's alternative mapping, network server 114 transmitting an encrypted approval message to an interface station (or to pocket vault 102 in Petitioner's modification of this example), Patent Owner argues that an approval message in the context of Burger is an indication that funds have been secured after an authorization process has been conducted and it is determined that the transaction is within acceptable parameters set by the issuing bank. PO Resp. 8–14 (citing Ex. 1005 ¶¶ 320, 473–474, 511, 514, 517–518, Fig. 24; Ex. 2010 (PayPal article, "How online payment processing works"); Ex. 2011 (Stripe article, "How credit card transaction processing works: A quick guide"); Ex. 2012 (PayPal article, "How PayPal helps sellers process and accept credit card payments"); Ex. 2013 (Stripe article, "Card authorization explained: How it works and what businesses need to know")). Thus, Patent Owner argues, "the transaction of 'obtaining

payment information or authorization for charging a credit card or bank account' solely is performed by the Pocket Vault and the Pocket Vault Server 114," and the financial media issuer is not a participant or party to the transaction. Sur-reply 4. In this example, Patent Owner argues, the transaction is between only two parties and lacks a third party. *Id.*

Petitioner responds by clarifying that, in this example, "the 'second party' is a financial media issuer 12, such as a bank or credit card company" and "the 'third party' is a party that operates the network server." Reply 10. Petitioner argues that Patent Owner "conflates the 'approval' for charging a financial account in a transaction, with an approval to use sensitive information to ultimately conduct a financial transaction—the latter of which was articulated in the Petition." *Id.* at 10–11 (citing Pet. 45). Here, it is Petitioner who is conflating its two separate mappings of this example. Patent Owner's argument is directed to Petitioner's alternative mapping, in which the network server 114 determines whether a "requested transaction [is] within acceptable account parameters" and, if so, transmits an "encrypted approval message for [the] requested transaction to commercial interface station/commercial card reader/commercial bar code reader." Ex. 2005 ¶¶ 514, 517–518, Fig. 24 (2402, 2408). We agree with Patent Owner that this appears to be a transaction in which network server 114 determines whether the transaction is within the financial institution's parameters and sends an authorization message to the pocket vault indicating that funds can be transferred. Petitioner does not explain persuasively why the financial institution is the second party to the transaction and the network server is a third party, since the network server appears to be playing the role of the financial institution. Thus, Petitioner has not shown that the alternative mapping of this example teaches claim limitations 1.4 and 1.5.

(2) third party that operates a trusted authority; second theory (advertising)

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). Burger states that "network server 114 may also serve as a repository for information regarding media issuers or advertisers" and "may serve as a conduit for advertisers to target particular classes of Pocket Vault holders, and channel information to them." Ex. 1005 ¶ 117. In Burger's example of Figure 7, after network server 114 has authenticated pocket vault 102 (Fig. 7A, steps 702–713), and the pocket vault user seeks to engage in a non-financial transaction (Fig. 7B, step 720), an authorized holder routine is executed (Fig. 7B, step 722, Fig. 10A). Ex. 1005 ¶¶ 178–186, 189, 194, 236. As shown in Figure 10A, reproduced above, if advertiser 108 makes arrangements with the company operating network server 114, advertising information can be uploaded to pocket vault 102 when the user interfaces pocket vault 102 with interface station 104*b*, after which the advertisement is displayed, e.g., for two seconds. *Id.* ¶¶ 237–238, Fig. 10A (steps 1002–1004).

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. We credit this testimony, as it is consistent with the process of Figures 7 and 10.

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).

Patent Owner argues that the claims require that, in a transaction allowing the user access to an application, the principal parties must be the user being allowed access and the application being accessed. PO Resp. 15. Because the parties to the advertising transaction in Petitioner's theory are the user and the advertiser, Patent Owner argues that this is not a transaction between the user and the application being accessed. *Id.* at 16. As we conclude in the above Claim Construction section, however, the claimed transaction is not limited to those in which the principal parties are the user being allowed access and the application being accessed. Thus, Patent Owner's argument is unpersuasive.

Patent Owner also argues that, even if the claims contemplate a transaction between a user and an advertiser (we determine that they do), Petitioner has equated the third party that operates a trusted authority and the application being accessed. *Id.* at 16–17. According to Patent Owner, Burger states that network server 114 may contract with the advertisers and may act as a conduit for advertisers by storing and delivering adds. *Id.* at 17–19 (citing Ex. 1005 ¶¶ 98, 104, 111, 117, 237, 538); *see also* Sur-reply 7–8 (citing Ex. 1005 ¶¶ 98, 117, 237, 538). Thus, Patent Owner argues, network server 114 is the application being accessed, and cannot also be the

third party that operates a trusted authority. PO Resp. 19–20. According to Patent Owner,

> advertisements are stored on Pocket Vault Server 114 and downloaded to Pocket Vault software on the Pocket Vault device. Accordingly, the transaction of accessing advertisements is performed only between the Pocket Vault Server 114 and the Pocket Vault. Therefore, there are only two participants in the transaction of accessing advertisement.

Sur-reply 8.

Petitioner responds that nothing in the '954 patent states that the third party that operates a trusted authority cannot be an active participant in the transaction. Reply 14–15. Thus, Petitioner argues, simply because network server 114 stores information to facilitate an advertising transaction between a user and an advertiser does not mean that network server 114 is a principal party to that transaction. *Id.* at 15. We have previously explained that active participation in a transaction, alone, does not make an entity a party to that transaction; instead, we evaluate a party's relationship to the transaction to determine whether it is a principal party or a third party. Dec. 10–11.

Petitioner also argues that it identifies different software, that running on pocket vault 102, as the application being accessed, and that Patent Owner's argument improperly conflates that software with software running on network server 114. Reply 15–16. Under Petitioner's theory, after the pocket vault is authenticated, and the pocket vault receives a message from the network server to that effect, the pocket vault displays (the user accesses) an advertisement that has been scheduled on the pocket vault. Pet. 39–40 ("[A]n advertiser may send information to the network server, which is then forwarded onto a Pocket Vault for display upon successful authentication of the user and Pocket Vault ID.") (citing Ex. 1005 ¶¶ 117, 146, 237, 541,

Fig. 1). Although acknowledging that software on the pocket vault should not be conflated with software on the network server, Patent Owner argues that "Pocket Vault Server 114 is still the application being accessed as well as the purported third party that operates a trusted authority." Sur-reply 9.

We agree with Petitioner. Petitioner has shown that Burger teaches an advertising transaction between advertiser 108 and the user of pocket vault 102, with the user accessing (viewing) the advertisement on the pocket vault after network server 114 authenticates pocket vault 102 and sends an access message to pocket vault 102 notifying it of the authentication. Pet. 39–40. We find that, in this transaction, the advertiser and the user of the pocket vault are the principal parties to the transaction and the operator of network server 114 is a third party that operates a trusted authority. Although network server 114 may store and transmit advertisements on behalf of advertiser 108 or otherwise act as a conduit for advertisements, witnessing and helping to facilitate the transaction does not make network server 114 a principal party to that transaction.

On the complete record, we find that Burger's advertising example teaches claim limitations 1.4 and 1.5.

(3) third party that operates a trusted authority; third theory (electronic hotel room key)

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).

With reference to Figure 1 of Burger, reproduced above, building access cards (e.g., electronic hotel room keys) is an example of media from

non-financial media issuers 110 stored on pocket vault 102 and requiring authentication to access. Ex. 1005 ¶¶ 128–129, 679. Information such as "building security ID" is added to pocket vault 102, e.g., when docked to personal docking station 104b, through a secure connection to network server 114. *Id.* ¶ 102. According to a "typical scenario involve[ing] distribution of hotel room key cards to hotel guests who make room reservations over the Internet," described in Burger,

> Using a hotel's secure web site, the prospective guest, who is also a Pocket Vault holder, may secure a room for a specific time period by providing a credit card number. . . . Next, 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 by the appropriate security mechanism such as a thumbprint for bio-metric ID verification). After downloading is complete, the display 216 of the Pocket Vault 102 may include an icon for the hotel room key (e.g., the hotel's logo) . . . . When the room key card icon is selected, the Pocket Vault 102 may encode the Chameleon Card with the magnetic stripe coding to unlock the guest's hotel room.

Id. ¶ 679.

Petitioner argues that, in this example, and pursuant to claim limitation 1.5, the "application" that is accessed is a keyless lock and the transaction is obtaining authorization to enter a secure building or facility. Pet. 52; Reply 16. 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 room key issuer), and the third party, a third party that operates a trusted authority, is network server 114 and the party that operates it. Pet. 35–36; Reply 16.

As noted above, claim limitation 1.5 recites (emphasis added) "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." Focusing on this language, in response, Patent Owner argues that, in Burger's hotel room key example, the hotel room key card is received/downloaded from the hotel's website and not network server 114. PO Resp. 20–21. According to Patent Owner, "[a]s the hotel key is not received from network server 114 acting as a third-party trusted authority, it cannot be equated to an access message without rendering the claim language requiring receipt of the access message ***from the third-party trusted authority*** meaningless." *Id.* at 21. In other words, Patent Owner argues that, because pocket vault 102 receives the hotel room key from the hotel's website, it does not receive it "from the trusted authority" as recited in claim limitation 1.5. *Id.*

Petitioner responds that Burger describes pocket vault 102 receiving the hotel room key from network server 114 along with an encrypted approval message indicating that pocket vault 102 has been authenticated. Reply 17–18 (citing Ex. 1005 ¶¶ 182–186, 517–527, 679, Figs. 24, 25).

We agree with Petitioner. Burger describes the hotel guest linking to network server 114 while staying within the hotel's website when obtaining a hotel room key card. Ex. 1005 ¶ 679. As with the advertising example, non-financial media issuers 110 may enlist network server 114 to store non-financial media (e.g., hotel keys) and upload the non-financial media to pocket vault 102 when the pocket vault next synchronizes with the network server. *Id.* ¶ 467. Moreover, as indicated above, Burger expressly states that a "building security ID" is added to pocket vault 102 "through a secure

connection to the network server 114." *Id.* ¶ 102. Thus, in accordance with Petitioner's arguments for the hotel key example, and contrary to Patent Owner's, we find that pocket vault 102 receives an electronic hotel room key and an encrypted approval message from network server 114.

In the Sur-reply, Patent Owner argues that, if pocket vault 102 receives the hotel room key card from network server 114, network server 114 would be both the application accessed and the third party that operates a trusted authority. Sur-reply 11. This argument is unpersuasive for the same reasons given above for Patent Owner's substantially similar argument regarding network server 114 storing and uploading advertisements.

On the complete record, we find that Burger's electronic hotel room key example teaches claim limitations 1.4 and 1.5.

In sum, in each of the three examples in Burger that Petitioner relies on, we find that Burger teaches claim limitations 1.4 and 1.5. Thus, on the complete record, Petitioner has shown that Burger teaches each limitation of claim 1.

c) Remaining claims

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 to, and largely incorporate, its arguments and evidence for claim 1. Pet. 62–65, 67–78, 80–83. Patent Owner presents its arguments for claims 1, 12, 16, and 22 together. PO Resp. 7, 17, 19, 21. For the reasons

given for claim 1, Petitioner has shown that Burger teaches each limitation of claims 12, 16, and 22.

Claim 2 depends from claim 1; claim 13 depends from claim 12. As to claims 2 and 13, we find that the pocket vault ID of Burger's pocket vault is transmitted to the network server over a wireless or cellular network. Ex. 1005 ¶¶ 99, 114, 122, 147, Fig. 7A; Ex. 1003 ¶ 120; Pet. 53, 65. Thus, Burger teaches the additional limitation of claims 2 and 13.

Claim 4 depends from claim 1. We find that Burger teaches the pocket vault sending an ID to the network server when biometric scan data from the user matches stored biometric data. Ex. 1005 ¶¶ 122, 135, 178–184, 349, 358, 553; Ex. 1003 ¶¶121–122; Pet. 54. Thus, Burger teaches the additional limitation of claim 4.

Claim 5 depends from claim 1; claim 26 depends from claim 22. We find that Burger teaches various examples of biometric data, including fingerprint and retinal scan data. Ex. 1005 ¶¶ 112, 135; Ex. 1003 ¶ 123; Pet. 55, 88. Thus, Burger teaches the additional limitation of claims 5 and 26.

Claims 7 and 9 depend from claim 1; claims 19 and 21 depend from claim 16; claims 27 and 29 depend from claim 22. We find that Burger describes keyless locks, financial accounts, and computer software as example applications. Ex. 1005 ¶¶ 3, 95–96, 105, 109, 127–129, 139, 149, 155–158, 182–186, 236–238, 242, 250, 255, 318–332, 511–529, 559, 679; Ex. 1003 ¶¶ 124–125; Pet. 56–58, 79, 89. Thus, Burger teaches the additional limitation of claims 7, 9, 19, 21, 27, and 29.

Claim 8 depends from claim 1. Claim 20 depends from claim 16. Claim 28 depends from claim 22. We find that Burger gives medical information cards as an example application. Ex. 1005 ¶¶ 3, 126–127;

Ex. 1003 ¶ 126; Pet. 57–58, 79, 89. Thus, Burger teaches the additional limitation of claims 8, 20, and 28.

Claim 10 depends from claim 1; claim 18 depends from claim 16. We find that Burger's description of establishing a trust relationship between network server 114 and pocket vault 102 over a secure Internet connection teaches the additional limitation of claims 10 and 16. Ex. 1005 ¶ 114; Ex. 1003 ¶ 128; Pet. 58, 78–79.

Claim 11 depends from claim 1. We find that Burger, in its description of the process of registering a pocket vault with network server 114, teaches the additional limitations of claim 11. Ex. 1005 ¶¶ 101, 462–464, 476–481, 562, 573, 585, Figs. 19, 20; Ex. 1003 ¶¶ 129–132; Pet. 59–62.

Claim 15 depends from claim 12. We find that it would have been obvious to include an LED in Burger's pocket vault to be activated for requesting a biometric scan, in light of Burger's description of LEDs for displaying information and a beep to indicate that a biometric scan is complete. Ex. 1005 ¶¶ 131, 204, 206, 232, 355, 384, 585, 598, Fig. 2; Ex. 1003 ¶ 143; Pet. 66–67. Thus, Burger teaches the additional limitation of claim 15.

Claims 23 and 24 depend from claim 22. We find that Burger teaches the additional limitations of claims 23 and 24. Ex. 1005 ¶¶ 101, 184, 185, 464, 476–482, 562, 573, 575, 585, Figs. 20, 32; Ex. 1003 ¶¶ 164–169; Pet. 83–88.

Patent Owner does not present separate arguments for the dependent claims.

In sum, Burger teaches each limitation of claims 2, 4, 5, 7–13, 15, 16, 18–24, and 26–29.

4. Conclusion of obviousness

As detailed above, we find that Burger teaches each limitation of claims 1, 2, 4, 5, 7–13, 15, 16, 18–24, and 26–29. The record does not contain evidence of objective indicia of nonobviousness. Upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claims 1, 2, 4, 5, 7–13, 15, 16, 18–24, and 26–29 would have been obvious over Burger.

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:

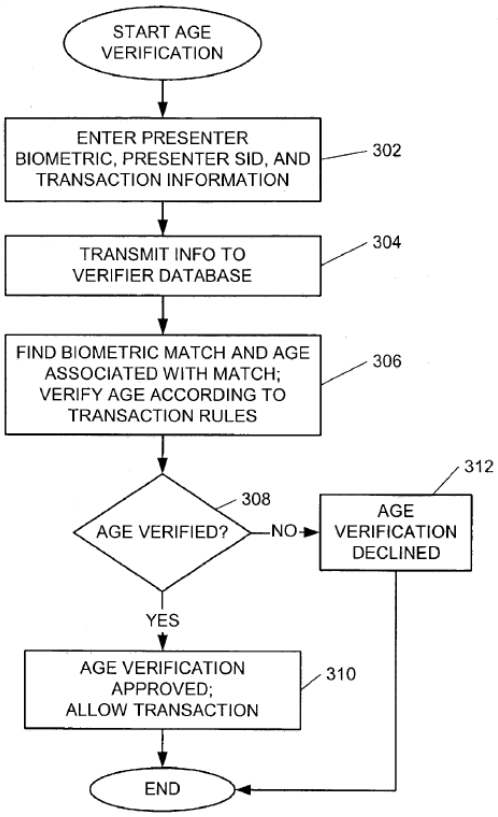


FIG. 3

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. We credit Dr. Traynor's uncontroverted testimony and find that a skilled artisan would have had reasons, with rational underpinning, to combine the teachings of Burger and Robinson.

As to claims 3, 14, and 17, Robinson describes 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). We find that a skilled artisan would have combined the teachings of Burger and Robinson, such that Robinson's age-verifying information would have been stored in the database of Burger's network server 114. *Id.* at 95 (citing Ex. 1003 ¶ 176). Patent Owner does not provide separate arguments for claims 3, 14, and 17. PO Resp. 22.

On the complete record, we find 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. The record does not contain evidence of objective indicia of nonobviousness. Upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claims 3, 14, and 17 would have been obvious over 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). Dr. Traynor testifies that this would have merely involved combining prior art elements according to known methods to yield predictable results. Ex. 1003 ¶¶ 84–88; Ex. 1005 ¶¶ 93–95, 118; Ex. 1021 ¶¶ 63, 65, 67; Pet. 99–101 (citing; Ex. 1003 ¶¶ 84–88). We credit Dr. Traynor's uncontroverted testimony and find that a skilled artisan would have had reasons, with rational underpinning, to combine the teachings of Burger and Orsini.

Patent Owner does not provide separate arguments for claims 6 and 25. PO Resp. 22.

On the complete record, for the reasons articulated by Petitioner, we find 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. The record does not contain evidence of objective indicia of nonobviousness. Upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claims 6 and 25 would have been obvious over Burger and Orsini.

E. The '052 Reexam[7]

As noted above, the '730 patent, a patent related to the '954 patent, is the subject of the co-pending '052 reexam. As noted above, Patent Owner requested (and was granted) adverse judgment in IPR2024-00232 and

[7] In IPR2024-00233, Patent Owner sought Director Review (Paper 36 in IPR2024-00233) of our '233 FWD, because our Final Written Decision allegedly was inconsistent with an Office Action in the '052 reexam (Ex. 2016 in this proceeding). Director Review was denied in that case. Paper 38 in IPR2024-00233. That Office Action has since been superseded. Ex. 2017.

IPR2024-00775, resulting in the cancellation of all original claims of the '730 patent. Patent Owner, however, amended the claims in the '052 reexam (cancelling claims 1–17 and adding claims 18–34[8]), and, according to the reexamination Examiner, "the '954 Patent claim 1 shares similar scope relating to the access message limitation with claim 18 of the '730 Patent." Ex. 2017 (July 29, 2025, Non-final Office Action in '052 reexam), 55[9]. The parties have entered papers from the '052 reexam as exhibits in this proceeding. *See* Exs. 1038, 2017, 2018.[10]

Although the current rejection of claims in the '052 reexam is non-final, and does not purport to be a final set of factual findings and conclusions, we nevertheless have considered the record from the '052 reexamination, in particular, the July 29, 2025, Non-final Office Action (Ex. 2017), and see no findings or conclusions inconsistent with our findings and conclusions in this Decision. The reexamination Examiner rejected then-pending claims 18–34 as anticipated by Burger, making findings similar to those we make here. Ex. 2017, 12–28. In fact, the reexamination

[8] June 30, 2025, Supplemental Amendment in '052 reexam (Ex. 3001). Claims 18–34 have since been cancelled and claims 35–51 have been added. Ex. 1038.

[9] We use the Examiner's page numbering in the upper right corners of the document.

[10] *See* C. Stewart, *Memorandum: PTAB consideration of prior findings of fact and conclusions of law* (Sept. 16, 2025) ("[I]f the Board reaches an initial or final decision on a finding of fact or conclusion of law that is different than the prior finding or conclusion of the Office, district court, or the ITC, the Board shall explain in the institution or final written decision why a different outcome is warranted. . . . To help make its assessment, the Board shall consider relevant materials submitted by the parties from the other proceeding (e.g., an opinion, a judgment, trial testimony, or other evidence) . . . .").

Examiner "adopts the PTAB's rationale from IPR2024-00846 for Granting Institution of Inter Partes Review [Paper 8] of related ['954 patent] dated November 18, 2024." Ex. 2017, 55. Patent Owner admits that the Examiner "adopted specifically the rationale from the institution decision of this proceeding." Tr. 26:3–5. For example, the Examiner concludes that

> The claims do not require the parties to be a user and an application. Rather, claim 18 requires a third party trusted authority, where the access message is sent to the application from the agent (of the third party trusted authority). The parties could be the user and the application or could be, for example, the user and vendors, advertisers, non-financial media issuers and financial media issuers.

Ex. 2017, 56. With this understanding, the Examiner finds:

> Burger discloses the network server is the third-party trusted authority between the user of the Pocket Vault (where the user utilizes the Pocket Vault to conduct the transaction) and advertisers, non-financial media issuers and financial media issuers as shown in Fig. 1. Thus, Burger can be viewed as having the parties be a user and the advertisers, non-financial media issuers and financial media issuers; or the user and the Pocket Vault (i.e., the application).

Id. at 57. Here, we see no material inconsistencies between our findings and conclusions and those of the Examiner.

At the hearing, Patent Owner admitted that "[t]he examiner in the CRU have adopted the Board's claim construction," and "didn't see them make any inconsistent claim construction with the Board." Tr. 26:10–12. Patent Owner further admits that "with regards to what Burger discloses, . . . the CRU hasn't made any inconsistencies." *Id.* at 26:17–18. Instead (for the first time at the oral argument) Patent Owner sought to argue that, in light of principles of compact prosecution, the Examiner's decision to reject the pending claims under an anticipation ground, and not an obviousness

ground, implies that the Examiner determined that the claims were not obvious. *Id.* at 26:18–27:9. "Under the principles of compact prosecution, the examiner should review each claim for compliance with every statutory requirement for patentability in the initial review of the application and identify all of the applicable grounds of rejection in the first Office action to avoid unnecessary delays in the prosecution of the application." Manual of Patent Examining Procedure (MPEP) § 2173.06(I). However, we see no requirement that the Examiner, when concluding that Burger discloses each limitation of claims 18–34, was required to make back-up obviousness rejections based on what Patent Owner might argue in the future.

In any case, Patent Owner has since cancelled claims 18–34 and added new claims 35–51. Ex. 1038. Thus, even if there were inconsistencies between the Examiner's rejection of '730 patent claims 18–34 and our analysis of claims 1–29 of the '954 patent here (we see none), the Examiner's rejection of claims that have since been cancelled has little relevance to this proceeding.

III. CONCLUSION[11]

Petitioner has proved by a preponderance of the evidence that claims 1–29 of the '954 patent are unpatentable.

[11] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

The outcome for the challenged claims of this Final Written Decision follows. In summary:

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
1, 2, 4, 5, 7–13, 15, 16, 18–24, 26–29	103(a)	Burger	1, 2, 4, 5, 7–13, 15, 16, 18–24, 26–29	
3, 14, 17	103(a)	Burger, Robinson	3, 14, 17	
6, 25	103(a)	Burger, Orsini	6, 25	
Overall Outcome			1–29	

IV. ORDER

It is hereby:

ORDERED that 1–29 of the '954 patent are unpatentable;

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:

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

PATENT OWNER:

David Hecht
James Zak
HECHT PARTNERS LLP
dhecht@hechtpartners.com
jzak@hechtpartners.com
zakx0017@umn.edu

US008886954B1

(12) **United States Patent**
Giobbi

(10) **Patent No.: US 8,886,954 B1**
(45) **Date of Patent: *Nov. 11, 2014**

(54) **BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION**

(71) Applicant: **Proxense, LLC**, Bend, OR (US)

(72) Inventor: **John J. Giobbi**, Bend, OR (US)

(73) Assignee: **Proxense, LLC**, Bend, OR (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/710,109**

(22) Filed: **Dec. 10, 2012**

Related U.S. Application Data

(63) Continuation of application No. 11/314,199, filed on Dec. 20, 2005, now Pat. No. 8,352,730.

(60) Provisional application No. 60/652,765, filed on Feb. 14, 2005, provisional application No. 60/637,538, filed on Dec. 20, 2004.

(51) **Int. Cl.**
H04L 29/06 (2006.01)
G05B 1/00 (2006.01)

(52) **U.S. Cl.**
CPC ***G05B 1/00*** (2013.01)
USPC **713/186**; 713/153

(58) **Field of Classification Search**
CPC combination set(s) only.
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,759,060 A 7/1988 Hayashi et al.
4,993,068 A 2/1991 Piosenka et al.
5,187,352 A 2/1993 Blair et al.
5,296,641 A 3/1994 Stelzel
5,392,433 A 2/1995 Hammersley et al.
5,416,780 A 5/1995 Patel

(Continued)

FOREIGN PATENT DOCUMENTS

WO WO 00/62505 10/2000
WO WO 01/22724 3/2001

(Continued)

OTHER PUBLICATIONS

"Alliance Activities: Publications: Identity—Smart Card Alliance," Smart Card Alliance, 1997-2007, Retrieved on Jan. 7, 2007 from <URL:http://www.smartcardalliance.org/pages/publications-identity>, 3 pgs.

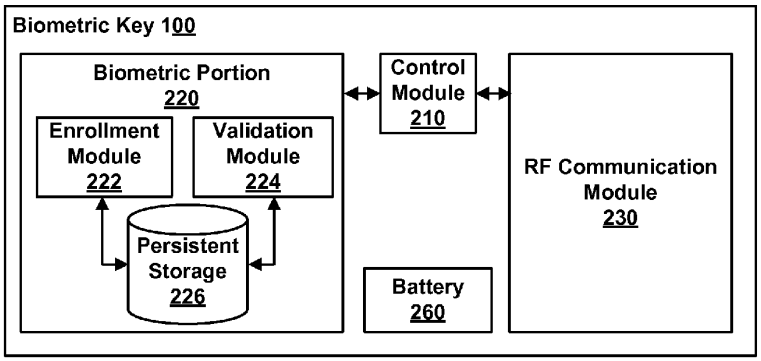
(Continued)

Primary Examiner — Eleni Shiferaw
Assistant Examiner — Phy Ahn Vu
(74) *Attorney, Agent, or Firm* — Patent Law Works LLP

(57) **ABSTRACT**

Systems and methods verifying a user during authentication of an integrated device. In one embodiment, the system includes an integrated device and an authentication unit. The integrated device stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format, and when scan data is verified by comparing the scan data to the biometric data, wirelessly sends one or more codes and other data values including the device ID code. The authentication unit receives and sends the one or more codes and the other data values to an agent for authentication, and receives an access message from the agent indicating that the agent successfully authenticated the one or more codes and other data values and allows the user to access an application.

29 Claims, 6 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

5,422,632	A		6/1995	Bucholtz et al.
5,450,489	A		9/1995	Ostrover et al.
5,619,251	A		4/1997	Kuroiwa et al.
5,629,980	A		5/1997	Stefik et al.
5,644,354	A		7/1997	Thompson et al.
5,666,412	A		9/1997	Handelman et al.
5,784,464	A		7/1998	Akiyama et al.
5,825,876	A		10/1998	Peterson, Jr.
5,857,020	A		1/1999	Peterson, Jr.
5,892,825	A		4/1999	Mages et al.
5,894,551	A		4/1999	Huggins et al.
5,898,880	A		4/1999	Ryu
5,917,913	A		6/1999	Wang
5,928,327	A		7/1999	Wang et al.
5,991,399	A		11/1999	Graunke et al.
5,991,749	A		11/1999	Morrill, Jr.
6,016,476	A		1/2000	Maes et al.
6,018,739	A		1/2000	McCoy et al.
6,035,038	A		3/2000	Campinos et al.
6,035,329	A		3/2000	Mages et al.
6,038,334	A		3/2000	Hamid
6,041,410	A	*	3/2000	Hsu et al. 713/186
6,042,006	A		3/2000	Van Tilburg et al.
6,055,314	A		4/2000	Spies et al.
6,070,796	A		6/2000	Sirbu
6,088,730	A		7/2000	Kato et al.
6,104,334	A		8/2000	Allport
6,121,544	A		9/2000	Petsinger
6,148,142	A		11/2000	Anderson
6,161,179	A		12/2000	Seidel
6,185,316	B1		2/2001	Buffam
6,209,089	B1		3/2001	Selitrennikoff et al.
6,219,109	B1		4/2001	Raynesford et al.
6,219,439	B1		4/2001	Burger
6,247,130	B1		6/2001	Fritsch
6,256,737	B1		7/2001	Bianco et al.
6,266,415	B1		7/2001	Campinos et al.
6,295,057	B1		9/2001	Rosin et al.
6,336,121	B1		1/2002	Lyson et al.
6,336,142	B1		1/2002	Kato et al.
6,363,485	B1		3/2002	Adams et al.
6,367,019	B1		4/2002	Ansell et al.
6,381,747	B1		4/2002	Wonfor et al.
6,385,596	B1		5/2002	Wiser et al.
6,392,664	B1		5/2002	White et al.
6,397,387	B1		5/2002	Rosin et al.
6,401,059	B1		6/2002	Shen et al.
6,411,307	B1		6/2002	Rosin et al.
6,424,715	B1		7/2002	Saito
6,425,084	B1		7/2002	Rallis et al.
6,434,535	B1		8/2002	Kupka et al.
6,446,130	B1		9/2002	Grapes
6,463,534	B1		10/2002	Geiger et al.
6,480,188	B1		11/2002	Horsley
6,490,443	B1		12/2002	Freeny, Jr.
6,510,350	B1		1/2003	Steen, III et al.
6,523,113	B1		2/2003	Wehrenberg
6,529,949	B1		3/2003	Getsin et al.
6,546,418	B2		4/2003	Schena et al.
6,550,011	B1		4/2003	Sims, III
6,563,805	B1		5/2003	Ma et al.
6,564,380	B1		5/2003	Murphy
6,628,302	B2		9/2003	White et al.
6,632,992	B2		10/2003	Hasegawa
6,647,417	B1		11/2003	Hunter et al.
6,667,684	B1		12/2003	Waggamon et al.
6,683,954	B1		1/2004	Searle
6,697,944	B1		2/2004	Jones et al.
6,709,333	B1		3/2004	Bradford et al.
6,711,464	B1		3/2004	Yap et al.
6,775,655	B1		8/2004	Peinado et al.
6,804,825	B1		10/2004	White et al.
6,806,887	B2		10/2004	Chernock et al.
6,850,147	B2		2/2005	Prokoski et al.
6,873,975	B1		3/2005	Hatakeyama et al.
6,950,941	B1		9/2005	Lee et al.
6,963,971	B1	*	11/2005	Bush et al. 713/153
6,973,576	B2		12/2005	Giobbi
6,975,202	B1		12/2005	Rodriguez et al.
6,983,882	B2		1/2006	Cassone
7,012,503	B2		3/2006	Nielsen
7,090,126	B2		8/2006	Kelly et al.
7,112,138	B2		9/2006	Hedrick et al.
7,137,012	B1		11/2006	Kamibayashi et al.
7,191,466	B1		3/2007	Hamid et al.
7,218,944	B2		5/2007	Cromer et al.
7,249,177	B1		7/2007	Miller
7,305,560	B2		12/2007	Giobbi
7,529,944	B2		5/2009	Hamid
7,574,734	B2		8/2009	Fedronic et al.
7,587,611	B2		9/2009	Johnson et al.
7,617,523	B2	*	11/2009	Das et al. 726/5
7,644,443	B2		1/2010	Matsuyama et al.
7,715,593	B1		5/2010	Adams et al.
7,883,417	B2		2/2011	Bruzzese et al.
7,904,718	B2		3/2011	Giobbi et al.
2001/0044337	A1		11/2001	Rowe et al.
2002/0007456	A1		1/2002	Peinado et al.
2002/0013772	A1		1/2002	Peinado
2002/0014954	A1		2/2002	Fitzgibbon et al.
2002/0015494	A1		2/2002	Nagai et al.
2002/0023032	A1		2/2002	Pearson et al.
2002/0026424	A1		2/2002	Akashi
2002/0071559	A1		6/2002	Christensen et al.
2002/0073042	A1		6/2002	Maritzen et al.
2002/0098888	A1		7/2002	Rowe et al.
2002/0103027	A1		8/2002	Rowe et al.
2002/0104006	A1		8/2002	Boate et al.
2002/0108049	A1		8/2002	Xu et al.
2002/0109580	A1		8/2002	Shreve et al.
2002/0129262	A1	*	9/2002	Kutaragi et al. 713/193
2002/0138767	A1		9/2002	Hamid et al.
2002/0140542	A1		10/2002	Prokoski et al.
2002/0144117	A1		10/2002	Faigle
2002/0150282	A1		10/2002	Kinsella
2002/0152391	A1		10/2002	Willins et al.
2002/0158750	A1		10/2002	Almalik
2002/0174348	A1	*	11/2002	Ting 713/186
2002/0178063	A1		11/2002	Gravelle et al.
2002/0191816	A1		12/2002	Maritzen et al.
2003/0036425	A1		2/2003	Kaminkow et al.
2003/0046552	A1		3/2003	Hamid
2003/0054868	A1		3/2003	Paulsen et al.
2003/0054881	A1		3/2003	Hedrick et al.
2003/0055689	A1		3/2003	Block et al.
2003/0079133	A1		4/2003	Breiter et al.
2003/0115474	A1	*	6/2003	Khan et al. 713/186
2003/0127511	A1		7/2003	Kelly et al.
2003/0139190	A1		7/2003	Steelberg et al.
2003/0149744	A1	*	8/2003	Bierre et al. 709/217
2003/0172037	A1		9/2003	Jung et al.
2003/0176218	A1		9/2003	LeMay et al.
2003/0186739	A1		10/2003	Paulsen et al.
2004/0127277	A1		7/2004	Walker et al.
2004/0128162	A1	*	7/2004	Schlotterbeck et al. 705/2
2004/0129787	A1	*	7/2004	Saito et al. 235/492
2004/0209690	A1		10/2004	Bruzzese et al.
2004/0209692	A1		10/2004	Schober et al.
2004/0215615	A1		10/2004	Larsson et al.
2004/0230488	A1		11/2004	Beenau et al.
2005/0074126	A1	*	4/2005	Stanko 380/279
2005/0081040	A1		4/2005	Johnson et al.
2005/0109836	A1	*	5/2005	Ben-Aissa 235/380
2005/0229007	A1		10/2005	Bolle et al.
2005/0251688	A1		11/2005	Nanavati et al.
2005/0253683	A1		11/2005	Lowe
2006/0022046	A1		2/2006	Iwamura
2006/0113381	A1		6/2006	Hochstein et al.
2006/0156027	A1		7/2006	Blake
2007/0220272	A1		9/2007	Campisi et al.
2008/0019578	A1		1/2008	Saito et al.
2008/0188308	A1		8/2008	Shepherd et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2009/0328182	A1	12/2009	Malakapalli et al.
2010/0117794	A1	5/2010	Adams et al.
2011/0126188	A1	5/2011	Bernstein et al.

FOREIGN PATENT DOCUMENTS

WO	WO 01/75876	10/2001
WO	WO 01/77790	10/2001
WO	WO 2005/050450	6/2005
WO	WO 2005/086802	9/2005

OTHER PUBLICATIONS

"Applying Biometrics to Door Access," Security Magazine, Sep. 26, 2002, Retrieved on Jan. 7, 2007, from <URL:http://www.securitymagazine.com/CDA/Articles/technologies/3ae610eaa34d8010VgnVCM100000f932a8c0__>, 5 pgs.

Van Winkle, William, "Bluetooth, the King of Connectivity," Laptop Buyer's Guide and Handbook, Jan. 2000, pp. 148-153.

Yoshida, Junko, "Content Protection Plan Targets Wireless Home Networks," www.eetinnes.com, Jan. 11, 2002, 2 pgs.

Debow, Yvette, "Credit/Debit Debuts in Midwest Smart Card Test," Computers in Banking, v6, n11, Nov. 1989, 4 pgs.

Dennis, Sylvia, "Digital Passports Need Not Infringe Civil Liberties," Newsbytes, Dec. 2, 1999, 2 pgs.

Blum, Jonathan, "Digital Rights Management May Solver the Napster "Problem"," Technology Investor Industrysector, Oct. 2000, pp. 24-27.

Lake, Matt, "Downloading for Dollars," Sound & Vision, Nov. 2000, pp. 137-138.

Sapsford, Jathon, "E-Business: Sound Waves Could Help Ease Web-Fraud Woes," Wall Street Journal, Aug. 14, 2000, 2 pgs.

"Firecrest Shows How Truly Commercially-Minded Companies Will Exploit the Internet," Computergram International, Jan. 18, 1996, 2 pgs.

"Frequently Asked Questions (FAQs) About BioPay," BioPay, LLC, 2007, Retrieved on Jan. 7, 2007, from <URL: http://www.biopay.com/faqs-lowes.asp>, 5 pgs.

McIver, R. et al., "Identification and Verification Working Together," Bioscrypt, Aug. 27, 2004, Retrieved on Jan. 7, 2007, from <URL:http://www.ibia.org/membersadmin/whitepapers/pdf/15/Identification%20and%20%20Verification%20Working%20-Together.pdf>, 5 pgs.

Weber, Thomas E., "In the Age of Napster, Protecting Copyright is a Digital Arms Race," Wall Street Journal, Jul. 24, 2000, 3 pgs.

PCT International Search Report, PCT/US04/38124, Apr. 7, 2005, 10 pgs.

PCT International Search Report, PCT/US05/43447, Feb. 22, 2007, 7 pgs.

PCT International Search Report, PCT/US05/46843, Mar. 1, 2007, 10 pgs.

PCT International Search Report, PCT/US07/11102, Oct. 3, 2008, 11 pgs.

PCT International Search Report, PCT/US07/11103, Apr. 23, 2008, 9 pgs.

PCT International Search Report, PCT/US07/11104, Jun. 26, 2008, 9 pgs.

PCT International Search Report, PCT/US07/11105, Oct. 20, 2008, 10 pgs.

Nilsson, J. et al., "Match-On-Card for Java Cards," Precise Biometrics, White Paper, Apr. 2004, Retrieved on Jan. 7, 2007, from <URL:http://www.ibia.org/membersadmin/whitepapers/pdf/17/Precise%20Match-on-Card%20for%20Java%20Cards.pdf>, 5 pgs.

Nordin, B., "Match-On-Card Technology," Precise Biometrics, White Paper, Apr. 2004, Retrieved on Jan. 7, 2007, from <URL:http://www.ibia.org/membersadmin/whitepapers/pdf/17/Precis%20Match-on-Card%20technology.pdf>, 7 pgs.

"Micronas and Thomson Multimedia Showcase a New Copy Protection System that Will Drive the Future of Digital Television," www.micronas.com, Jan. 8, 2002, 3 pgs.

Pope, "Oasis Digital Signature Services: Digital Signing without the Headaches," Internet Computing—IEEE, vol. 10, Oct. 2006, pp. 81-84.

"SAFModuleTM: A Look Into Strong Authentication," saflink Corporation, Retrieved on Jan. 7, 2007, from <URL: http://www.ibia.org/membersadmin/whitepapers/pdf/6/SAFmod_WP.pdf>, 8 pgs.

"Say Hello to Bluetooth," Bluetooth Web site, Jun. 2000, 4 pgs.

"Smart Cards and Biometrics White Paper," Smart Card Alliance, May 2002, Retrieved on Jan. 7, 2007, from <URL: http://www.securitymanagementcom.library/smartcard_faqtech0802.pdf>, 7 pgs.

Lewis, Peter H., "Sony and Visa in On-Line Entertainment Venture," New York Times, v145, Nov. 16, 1995, 1 pg.

Fasca, Chad, "The Circuit," Electronic News, vol. 45 Iss. 45, Nov. 8, 1999, 2 pgs.

Wallace, Bob, "The Internet Unplugged," InformationWeek.com, Dec. 13, 1999, pp. 22-24.

Paget, Paul, "The Security Behind Secure Extranets," Enterprise Systems Journal, Dec. 1999, 4 pgs.

Kontzer, Tony, "Thomson Bets on Smart Cards for Video Encryption," www.informationweek.com, Jun. 7, 2001, p. 1.

Press Release, "Thomson Multimedia Unveils Copy Protection Proposal Designed to Provide Additional Layer of Digital Content Security," www.thompson-multimedia.com, May 30, 2001, 2 pgs.

Wade, Will, "Using Fingerprints to Make Payments at POS Slowly Gaining Popularity," Credit Union Journal, International Biometric Group, Apr. 21, 2003, Retrieved on Jan. 7, 2007, from <URL:http://www.biometricgroup.com/in_the_news/04.21.03.html>, 3 pgs.

Antonoff, Michael, "Visiting Video Valley," Sound & Vision, Nov. 2001, pp. 116, 118-119.

"What is a File?," Apr. 30, 1998, URL: http://unixhelp.ed.ac.uk/editors/whatisafile.html, accessed Mar. 11, 2010 via http://waybackmachine.org/1998061500000* /http://unixhelp.ed.ac.uk/editors/whatisafile.html, 1 pg.

Farouk, "Authentication Mechanisms in Grid Computing Environment; Comparative Study", 2012, IEEE, p. 1-6.

* cited by examiner

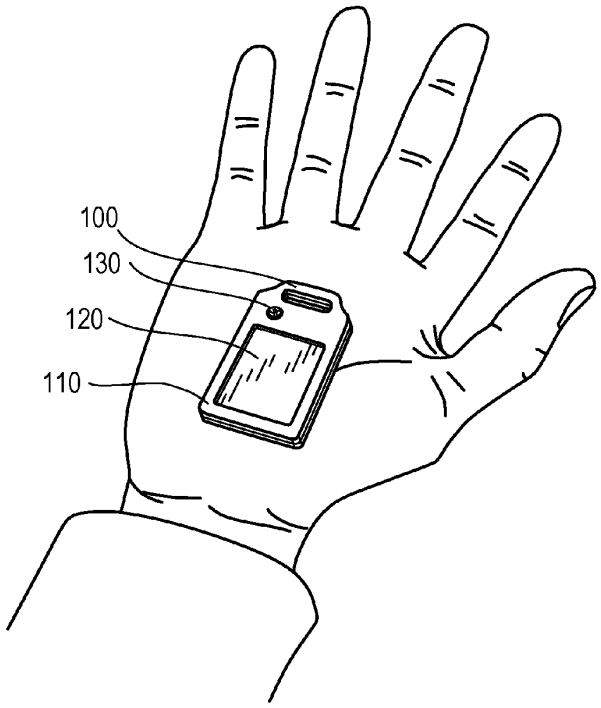

100
130
120
110

FIG. 1

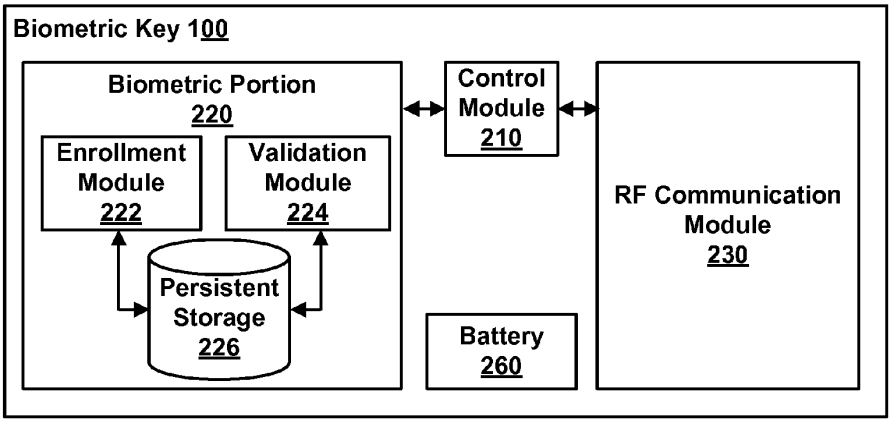

Biometric Key 100
Biometric Portion 220
Enrollment Module 222
Validation Module 224
Persistent Storage 226
Control Module 210
Battery 260
RF Communication Module 230

FIG. 2

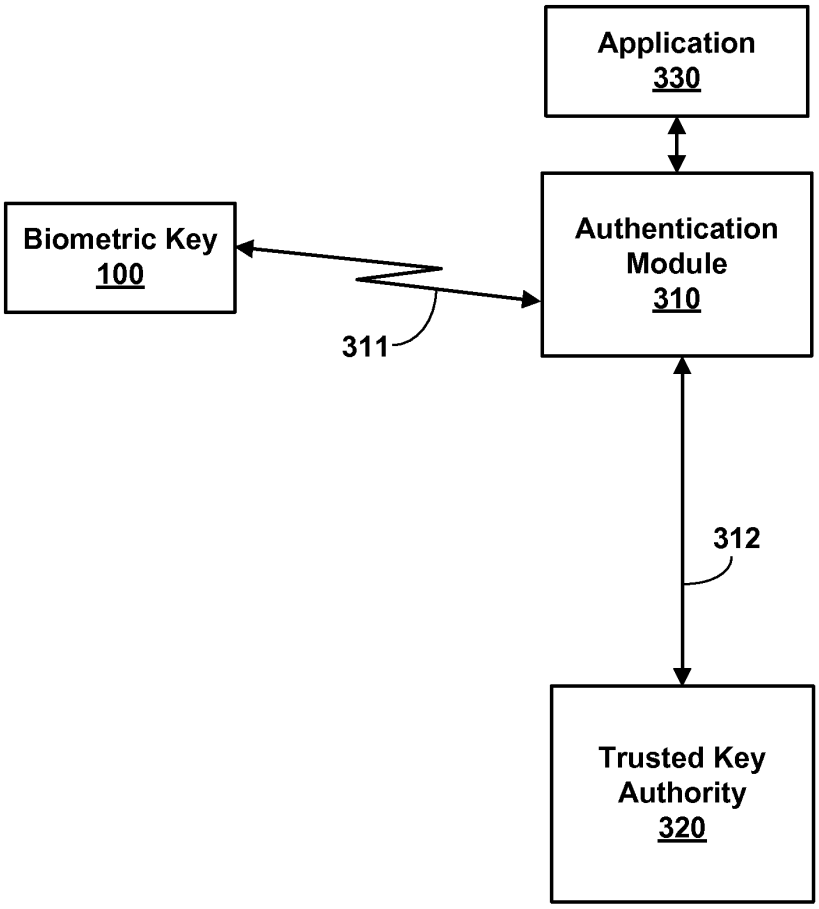

Application
330
Authentication
Module
310
Biometric Key
100
311
312
Trusted Key
Authority
320

FIG. 3

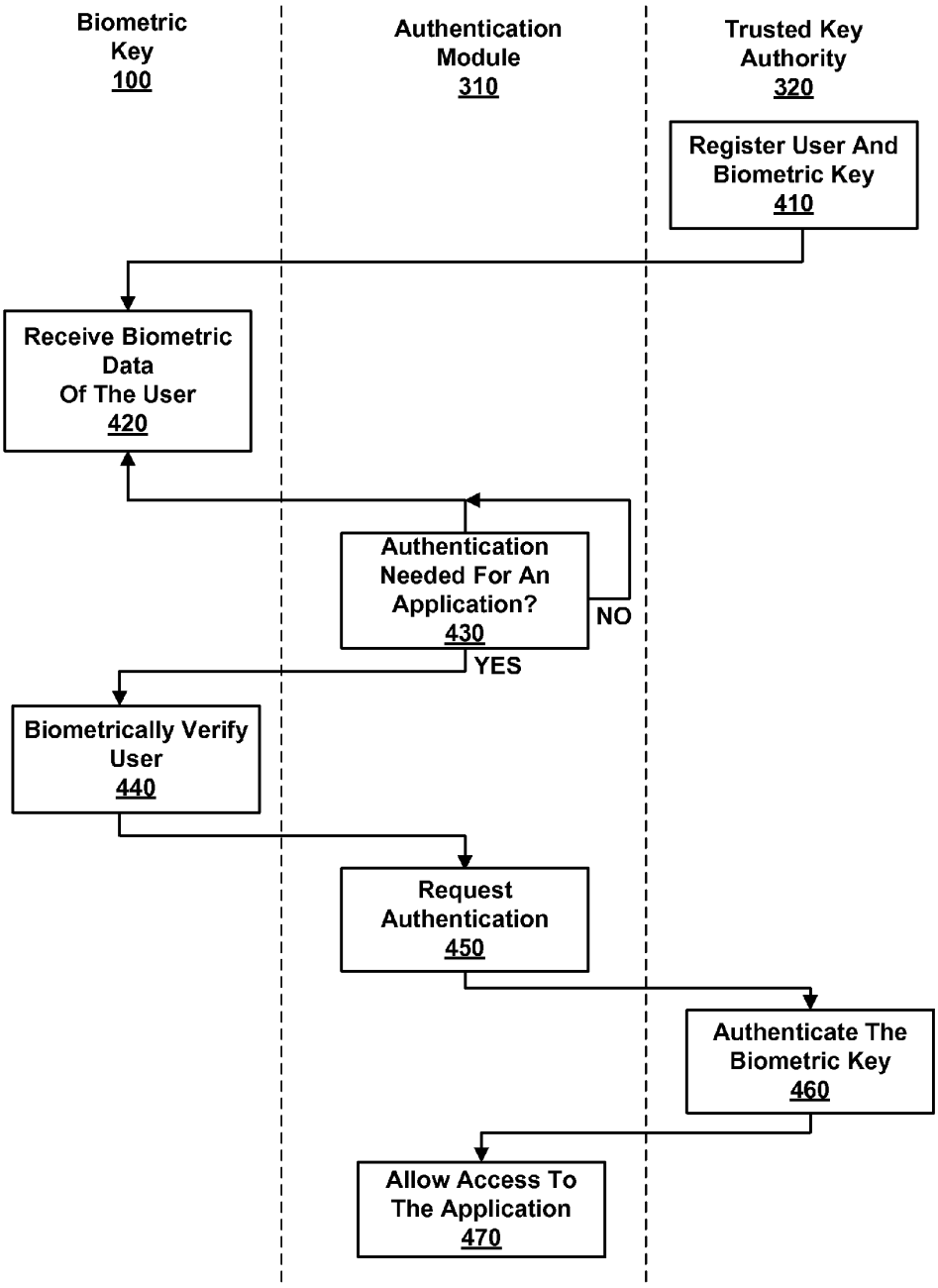

Biometric Key 100
Authentication Module 310
Trusted Key Authority 320
Register User And Biometric Key 410
Receive Biometric Data Of The User 420
Authentication Needed For An Application? 430
NO
YES
Biometrically Verify User 440
Request Authentication 450
Authenticate The Biometric Key 460
Allow Access To The Application 470

FIG. 4

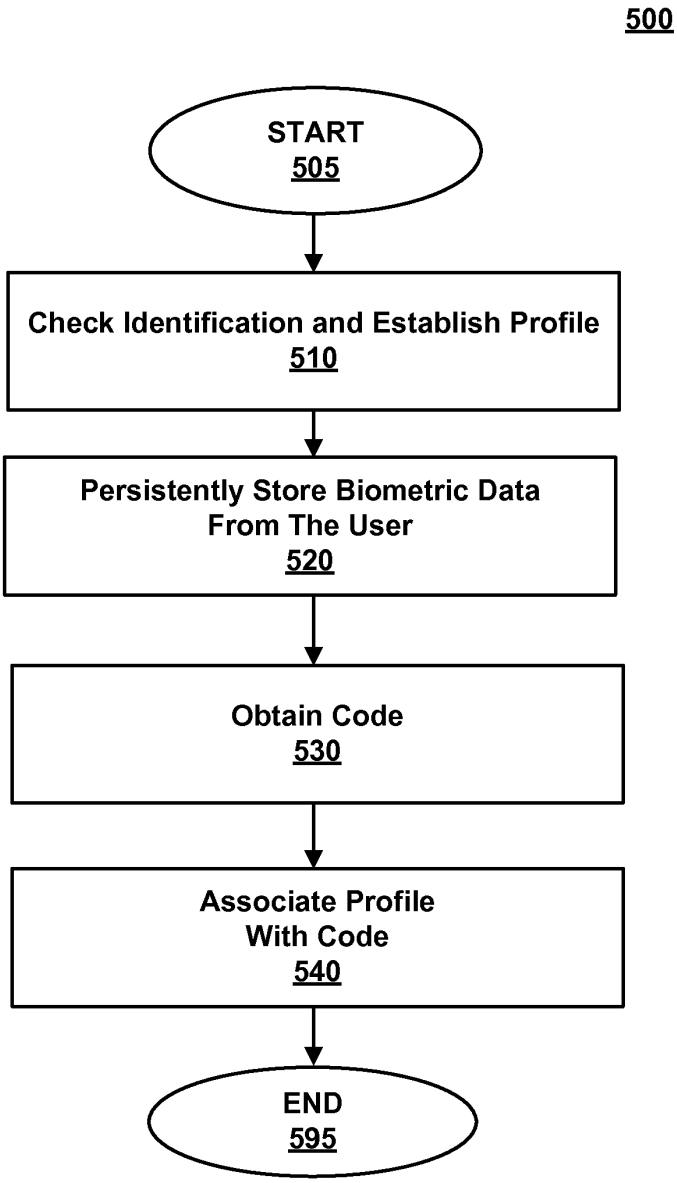

500
START
505
Check Identification and Establish Profile
510
Persistently Store Biometric Data From The User
520
Obtain Code
530
Associate Profile With Code
540
END
595

FIG. 5

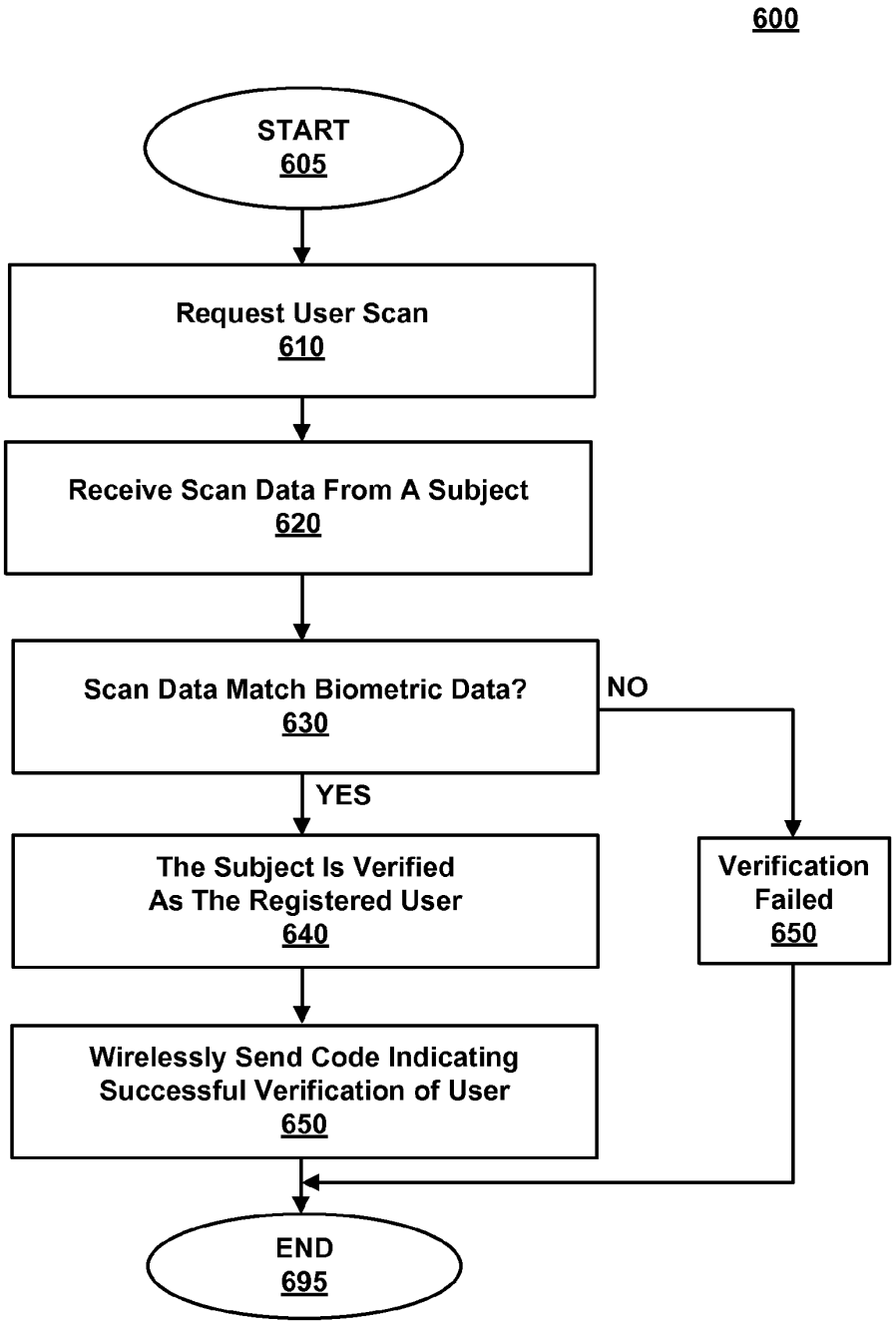

600
START
605
Request User Scan
610
Receive Scan Data From A Subject
620
Scan Data Match Biometric Data?
630
NO
YES
The Subject Is Verified
As The Registered User
640
Verification
Failed
650
Wirelessly Send Code Indicating
Successful Verification of User
650
END
695

FIG. 6

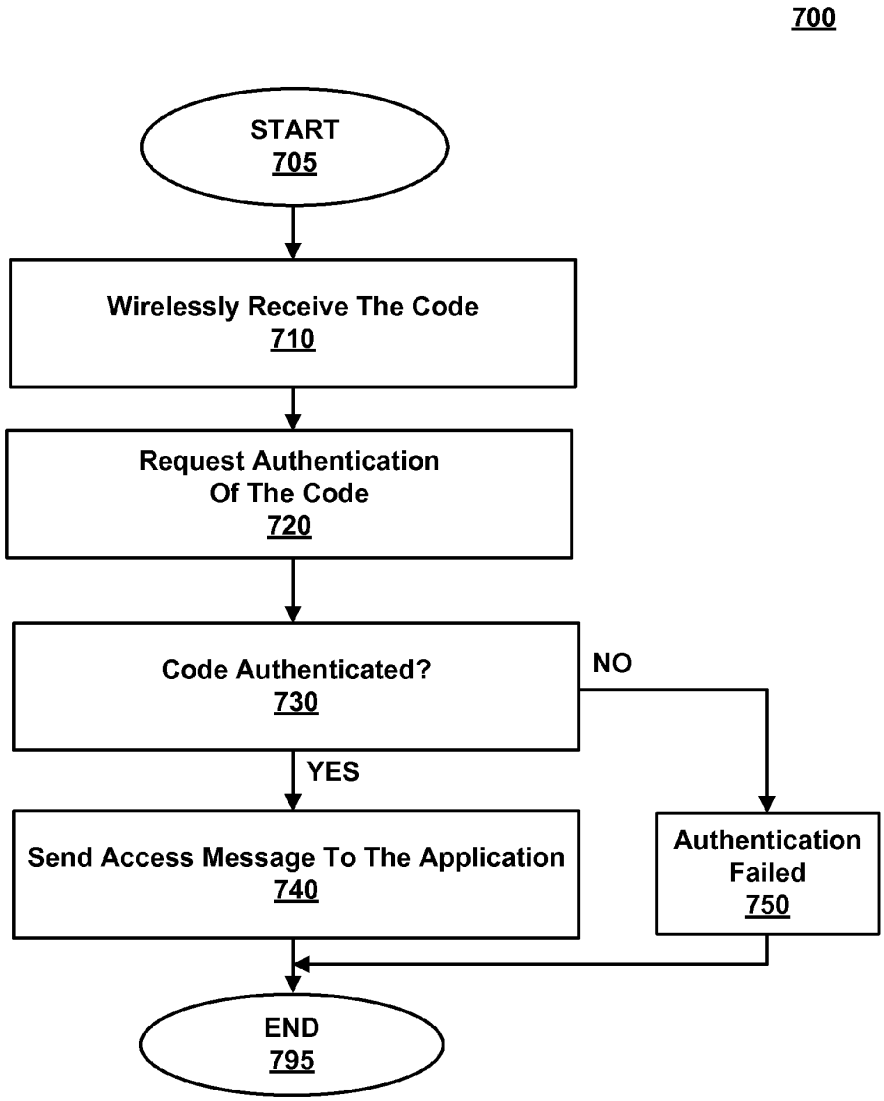

700
START
705
Wirelessly Receive The Code
710
Request Authentication
Of The Code
720
Code Authenticated?
730
NO
YES
Send Access Message To The Application
740
Authentication
Failed
750
END
795

FIG. 7

BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application claims priority, under 35 U.S.C. §120, to U.S. patent application Ser. No. 11/314,199, filed Dec. 20, 2005 and entitled "Biometric Personal Data Key (PDK) Authentication," which claims the benefit of U.S. Provisional Application No. 60/637,538, filed on Dec. 20, 2004, and of U.S. Provisional Application No. 60/652,765, filed on Feb. 14, 2005, the entire contents of which are hereby incorporated by reference.

FIELD OF THE INVENTION

The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated.

BACKGROUND

Conventional user authentication techniques are designed to prevent access by unauthorized users. One technique is to require a user being authenticated to provide secret credentials, such as a password, before allowing access. Similarly, a PIN number can be required by an ATM machine before allowing a person to perform automated bank transactions. A difficulty with this technique is that it requires the user to memorize or otherwise keep track of the credentials. A uses often has multiple sets of credentials (e.g., passwords and PINs) and it can be quite difficult to keep track of them all.

Another technique that does not require the user to memorize credentials is to provide the user with an access object such as a key (e.g., an electronic key) that the user can present to obtain access. For example, a user can be provided with a small electronic key fob that allows access to a building or other secured location. A difficulty with using access objects is that authentication merely proves that the access object itself is valid; it does not verify that the legitimate user is using the access object. That is, illegitimate user can use a stolen access object to enter a secured location because the user's identity is never checked.

Some hybrid authentication techniques require the user to provide both an access object and credentials. The user is authenticated only upon providing both items. Of course, this solution does not resolve the problem of making the user memorize credentials.

Therefore, there is a need for systems and methods for verifying a user that is being authenticated that does not suffer from the limitations described above. Moreover, the solution should ease authentications by wirelessly providing an identification of the user.

SUMMARY

The present invention addresses the above needs by providing systems and methods for authentication responsive to biometric verification of a user being authenticated. In one embodiment, an integrated device includes a persistent storage to persistently stores a code such as a device identifier (ID) and biometric data for a user in a tamper-resistant format, and a verification module, in communication with the persistent storage, to receive scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sending a code for authentication.

In one embodiment, a method for verifying a user during authentication of an integrated device, includes persistently storing biometric data for the user in a tamper-resistant format; responsive to receiving a request for biometric verification of the user, receiving scan data from a biometric scan; comparing the scan data to the biometric data to determine whether the data match; and responsive to a determination that the scan data matches the biometric data, wirelessly sending a code for authentication.

Other embodiments include corresponding systems, apparatus, and computer programming products, configured to perform the actions of the methods, encoded on computer storage devices. These and other embodiments may each optionally include one or more of the following features. For instance the operations further include registering an age verification for the user in association with the code. For instance the operations further include establishing a secure communication channel prior to sending the code for authentication. For instance the operations further include receiving a request for the code without a request for biometric verification, and responsive to receiving the request for the code without a request for biometric verification, sending the code without requesting the scan data. For instance, the features include: the code is registered with a trusted authority, and the code can be authenticated to a third party by the trusted authority; the code uniquely identifies the integrated device; the code indicates that the biometric verification was successful; persistently storing biometric data includes permanently storing biometric data; the biometric data and the scan data are both based on a fingerprint scan by the user, an LED to be activated for requesting the biometric scan.

In one embodiment, a method for authenticating a verified user, includes receiving a code associated with a biometrically verified user; requesting authentication of the code; receiving an authentication result; and in response to the authentication result being positive, providing access to an application.

In one embodiment, a system includes an integrated device (e.g. a biometric key) to store biometric data for a user in a tamper resistant format, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending a code; and an authentication module to receive the code and send the code to a trusted authority for authentication, and responsive to the code being authenticated, allowing the user to access an application.

Other embodiments include corresponding systems, apparatus, and computer programming products, configured to perform the actions of the methods, encoded on computer storage devices. These and other embodiments may each optionally include one or more of the following features. For instance, the operations further include registering the code with a trusted authority, wherein requesting authentication of the code includes providing the code to the trusted authority and wherein receiving an authentication result comprises receiving the authentication result from the trusted authority. For instance the operations further include registering a date of birth or age with the trusted authority. For instance the operations further include establishing a secure communications channel with an integrated device, wherein the code associated with the biometrically verified user is received from the integrated device. For instance the features include: the integrated device receives an authentication request from the authentication module, and in response, requests a biometric scan from the user to generate the scan data; when the

integrated device cannot verify the scan data as being from the user, it does not send the code.

Advantageously, user authentication is bolstered with highly reliable biometric verification of the user in an integrated device. Furthermore, a keyless environment relieves authorized users from having to memorize credentials, and of having to physically enter credentials or keys. In addition, the integrated device can be authenticated for an application that is open to the public (i.e., in an open loop system).

The features and advantages described in the specification are not all inclusive and, in particular, many additional features and advantages will be apparent to one of ordinary skill in the art in view of the drawings, specifications, and claims. Moreover, it should be noted that the language used in the specification has been principally selected for readability and instructional purposes and may not have been selected to delineate or circumscribe the inventive matter.

BRIEF DESCRIPTION OF THE DRAWINGS

The teachings of the present invention can be readily understood by considering the following detailed description in conjunction with the accompanying drawings.

FIG. **1** is a schematic diagram illustrating a biometric key for providing authentication information for a biometrically verified user according to one embodiment of the present invention.

FIG. **2** is a block diagram illustrating functional modules within the biometric key according to one embodiment of the present invention.

FIG. **3** is a block diagram illustrating a system for providing authentication information for a biometrically verified user.

FIG. **4** is a flow chart illustrating a method for providing authentication information for a biometrically verified user.

FIG. **5** is a flow chart illustrating a method for enrolling biometric data of the user with the biometric key.

FIG. **6** is a flow chart illustrating a method for verifying a subject presenting the biometric key according to one embodiment of the present invention.

FIG. **7** is a flow chart illustrating a method for authenticating a verified user of the biometric key according to one embodiment of the present invention.

DETAILED DESCRIPTION

Systems and methods for authentication responsive to biometric verification of a user being authenticated are described. Generally, biometric verification uses biometric data to ensure that the user of, for example, a biometric key, is the person registered as an owner. Biometric data is a digital or analog representation of characteristics unique to the user's body. For example, a fingerprint of a subject can be compared against previously-recorded biometric data for verification that the subject is the registered owner of the biometric key. Then, the biometric key itself can be authenticated.

Although the embodiments below are described using the example of biometric verification using a fingerprint, other embodiments within the spirit of the present invention can perform biometric verification using other types of biometric data. For example, the biometric data can include a palm print, a retinal scan, an iris scan, hand geometry recognition, facial recognition, signature recognition, or voice recognition.

FIG. **1** is a schematic diagram illustrating an example of a biometric key **100** for providing authentication information for a biometrically verified user according to one embodiment of the present invention. In one embodiment, the biometric key **100** comprises a frame **110**, a scan pad **120**, and an LED **130**. In one embodiment, biometric key **100** has a small form factor (e.g., the size of an automobile remote control) such that it can be unobtrusively carried by a user. In one embodiment, the biometric key **100** is integrated into another object or device. A device having an integrated biometric key **100** is occasionally referred to herein as an "integrated device." For example, in one embodiment, the biometric key **100** is integrated into a mobile phone (e.g. a cellular phone or smartphone), tablet, laptop, mp3 player, mobile gaming device, watch, key fob or other mobile device, thereby making the biometric key **100** unobtrusive to carry.

Frame **110** can be formed by plastic, metal or another suitable material. Frame **110** is shaped to secure scan pad **120**, and includes a perforation for attachment to, for example a key chain or clip. In one embodiment, frame **110** is formed from a unitary molding to protect biometric data. Accordingly, frame **110** cannot be opened to expose the underlying components unless it is broken.

Scan pad **120** can be, for example, an optical scanner using a charge coupled device, or a capacitive scanner. Scan pad **120** can be sized to fit a thumb or other finger. Biometric key **100** of the present embodiment includes LED **130** that lights up to request a fingerprint scan from a user. In one embodiment, LED **130** can also confirm that user verification and/or authentication has completed.

Biometric key **100** can authenticate a user for various purposes. For example, biometric key **100** can allow keyless entry into homes and autos. In another example, biometric key **100** can log a user onto a computer system or point of sale register without typing in credentials. In still another example, biometric key **100** can verify that an enrolled user is above a certain age (e.g., before allowing access to a slot machine in a casino). In some embodiments, biometric key **100** operates without biometric verification, and request a fingerprint scan from a user only when biometric verification is needed for the particular use.

FIG. **2** is a block diagram illustrating biometric key **100** according to one embodiment of the present invention. Biometric key **100** comprises control module **210**, biometric portion **220**, RF communication module **230**, persistent storage **240**, and battery **250**. Biometric key **100** can be formed from a combination of hardware and software components as described above. In one embodiment, biometric key **100** comprises a modified key fob.

Control module **210** coordinates between several functions of biometric key **100**. In one embodiment, control module **210** provides a verification code upon successful verification of the user. More specifically, once biometric portion **220** indicates that a fingerprint scan matches biometric data that was collected during enrollment, control module **210** can trigger RF communication module **230** for sending a code indicating that the user was verified. In another embodiment, control module **210** can work in the opposite direction by detecting a request for verification from RF communication module **230**, and then requesting verification of the user from biometric portion **210**. Note that control module **210** of FIG. **2** is merely a grouping of control functions in a central architecture, and in other embodiments, the control functions can be distributed between several modules around biometric key **100**.

Biometric portion **220** comprises enrollment module **222**, validation module **224**, and biometric data base **226**. In one embodiment, enrollment module **222** registers a user with biometric key **100** by persistently storing biometric data asso-

ciated with the user. Further, enrollment module **222** registers biometric key **100** with a trusted authority by providing the code (e.g., device ID) to the trusted authority. Or conversely, the trusted authority can provide the code to biometric key **100** to be stored therein.

Validation module **224** can comprise scan pad **120** (FIG. **1**) to capture scan data from a user's fingerprint (e.g., a digital or analog representation of the fingerprint). Using the scan data, validation module **214** determines whether the user's fingerprint matches the stored biometric data from enrollment. Conventional techniques for comparing fingerprints can be used. For example, the unique pattern of ridges and valleys of the fingerprints can be compared. A statistical model can be used to determine comparison results. Validation module **224** can send comparison results to control module **210**.

In other embodiments, validation module **224** can be configured to capture biometric data for other human characteristics. For example, a digital image of a retina, iris, and/or handwriting sample can be captured. In another example, a microphone can capture a voice sample.

Persistent storage **226** persistently stores biometric data from one or more users which can be provided according to specific implementations. In one embodiment, at least some of persistent storage **226** is a memory element that can be written to once but cannot subsequently be altered. Persistent storage **226** can include, for example, a ROM element, a flash memory element, or any other type of non-volatile storage element. Persistent storage **226** is itself, and stores data in, a tamper-proof format to prevent any changes to the stored data. 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). Furthermore, data can be stored in an encrypted form.

In one embodiment, persistent storage **226** also stores the code that is provided by the key **100** responsive to successful verification of the user. As described above, in one embodiment the code is a device ID or other value that uniquely identifies biometric key **100**. In one embodiment, the code is providing during the manufacturing process and the biometric data are provided during an enrollment of the user. In other embodiments, the code is provided during enrollment and/or the biometric data are provided during manufacturing. Further, in some embodiments persistent storage **226** stores other data utilized during the operation of biometric key **100**. For example, persistent storage **226** can store encryption/decryption keys utilized to establish secure communications links.

Radio frequency (RF) communication module **230** is, for example, a transceiver or other mechanism for wireless communication. RF communication module **230** can send and receive data (e.g., the code) as modulated electromagnetic signals. In one embodiment, RF communication **220** can be optimized for low-power usage by, for example, using short-range transceivers. RF communication module **230** can actively send out connection requests, or passively detect connection requests.

Battery **260** can be a conventional power source suitable for the components of biometric key **100**. Battery **260** can be either replaceable or rechargeable. Alternatively, battery **260** can be embedded within key **100** such that the key must be discarded or recycled upon expiration of the battery.

FIG. **3** is a block diagram illustrating a system **300** for providing authentication information for a biometrically verified user. System **300** comprises an authentication module **310** in communication with biometric key **100**, a trusted key authority **320**, and an application **330**.

Authentication module **310** is coupled in communication with biometric key via line **311** (i.e., a wireless medium such as EM signals), and with trusted key authority **320** via line **312** (e.g., a secure data network such as the Internet, or a cell network). Authentication module **310** can include one or more of, for example, a computerized device, software executing on a computerized device, and/or a reader/decoder circuit. In one embodiment, authentication module **310** servers as a gatekeeper to application **330** by requiring the code indicating successful biometric verification of the user prior to allowing access to the application. Further, in one embodiment, authentication module **310** provides the code to trusted key authority **320** in order to verify that it belongs to a legitimate key (e.g., when application **330** is security-critical). Authentication module **310** can send a message to application **330**, or otherwise allow access to the application, responsive to a successful authentication by trusted key authority **320**.

Application **330** is a resource that can be accessed by a verified and authenticated user. 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, a financial account (e.g. a savings account, checking account, brokerage account, credit card account, credit line, etc.) and the like. In one embodiment, a file includes medical information such as a medical record, insurance information or other healthcare information. Application **330** can execute on the same system as authentication module **310** or on another system in communication with the system of the authentication module. In one embodiment, application module **330** allows access by a user after receiving a message from authentication module **310**. At that point, application **330** can allow direct use by the user, or require that communications continue to pass through authentication module **310** for continued authentication.

Trusted key authority **320** is a third-party authority that is present in some embodiments in order to provide enhanced security. 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. The list can be batched or updated each time a new user/key is enrolled. In one embodiment, trusted key authority **320** can also store a profile associated with a biometric key. The profile describes the user associated with the key, the key itself, the trusted key authority, and/or other relevant information. In one embodiment, the functionality of trusted key authority **320** is provided by a server or other computerized device.

In an open system, where unknown users can attempt authentication (e.g., in a public grocery store), trusted key authority **320** provides verification that a key presenting a certain code is legitimate. By contrast, in a closed system, only known users are legitimate (e.g., owners of a home), the trusted key authority **320** can be maintained locally and serves to verify that the key belongs to one of the limited number of users that can use the system.

FIG. **4** is a flow chart illustrating a method **400** for authenticating a biometrically verified user using a trusted key authority (e.g., authority **320**). A biometric key (e.g., biometric key **100**) is registered **410** with the trusted key authority. The code (e.g., device ID) of the key is stored by the trusted key authority. Additionally, a user is enrolled **420** with the biometric key as described below with reference to FIG. **5**.

In various situations, authentication of the key is needed **430** (e.g., by authentication module **310**). In one embodiment, authentication can be required prior to allowing access to an application (e.g., application **330**). For example, a user can be standing proximate to a slot machine in a casino which

requires that a user be over the age of 21. The slot machine can detect the biometric key in the user's pocket, and, in response, spawn a conspicuous pop-up window on the slot machine requesting age verification. Alternatively, the biometric key can blink an LED. In other embodiments, biometric verification is not necessary and only the key itself is authenticated.

The biometric key establishes communication with the authentication module using various techniques. In one embodiment, the key and authentication module engage in preliminary data exchanges to determine who and/or what they are (e.g., to ascertain that they belong to the same system). These data exchanges can include challenge-response dialogs, hashing algorithms, and the like in order to ensure that the biometric key and authentication module are themselves legitimate. Further, in one embodiment the key and authentication module establish a secure communications channel. The key performs the biometric verification of the user **440** as described below with reference to FIG. **6**. If the biometric verification of the user is successful, the key provides its code over the secure communications channel.

The code is utilized to authenticate the biometric key itself **450**, **460** as described below with reference to FIG. **7** and profile information is received. Responsive to successful authentication of the key, access is allowed 470 to the application. In the slot machine example, a new pop-up window can be spawned to indicate a successful age verification.

FIG. **5** is a flow chart illustrating a method **500** for enrolling biometric data of the user with the biometric key according to one embodiment of the present invention. An agent checks **510** an identification of the user and establishes a profile. The agent can be, for example, a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness. 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.

The profile describes the user and can include, for example, the user's name, date of birth, age, passwords, account numbers, preferences etc. In some embodiments, the profile stores no or only limited information about the user. For example, the agent might store the date of birth of the user in the profile, but not store any other information about the user. In addition, the profile describes the biometric key and/or key authority. For the biometric key, the profile can store a value indicating the status of the key, such as whether the key is in-service, out-of-service, abandoned, lost, stolen etc. For the key authority, the profile can store a value identifying the key authority.

The agent also collects and persistently stores **520** biometric data from the user. To do so, a fingerprint or eye retina can be scanned and converted to data which is then persistently stored in the biometric key. In one embodiment, the agent does not retain the biometric data. Since this step occurs under control of the agent, the agent can be certain that the biometric data stored within the key matches the user who presented the identification. The agent also obtains the code (e.g., device ID) from the biometric key in which the biometric data was stored. The agent associates the code and the profile using a table and/or other data structure.

FIG. **6** is a flow chart illustrating a method **600** for verifying a subject presenting the biometric key according to one embodiment of the present invention. In response to an authentication request, a user scan is requested **610** (e.g., by a blinking LED). Once the subject provides a fingerprint, scan data is received **620**. Scan data is compared for a match **630** to previously-stored biometric data. If there is no match, then verification fails **650**.

If there is a match, the subject is verified **640** as the user. The code indicating a successful verification is wirelessly sent **650** from the biometric key (e.g., by RF communication module **230**).

FIG. **7** is a flow chart illustrating a method **700** for authenticating a biometric key according to one embodiment of the present invention. The code is wirelessly received **710**. A request for authentication of the code is sent to the trusted key authority **720**. The trusted key authority determines whether the code is authentic **730** (i.e., it was created through an established enrollment process) and has a valid status (e.g., has not expired). If authentication is successful, the trusted key authority sends an access message to the application to allow user access and/or provide additional information from the profile **740** (such as the user's age). If authentication is not successful, authentication fails **750** and the message to the application indicates that the user should be denied access.

In some embodiments, the biometric key provides multiple codes and/or other data values. For example, the key can provide a device ID code that the authentication module can provide to the trusted key authority in order to authenticate the key, and the key can provide a secret decryption value that can be used to communicate with the biometric key. As used herein, the term "code" is intended to include one or more of these values, depending upon the specific embodiment.

The order in which the steps of the methods of the present invention are performed is purely illustrative in nature. The steps can be performed in any order or in parallel, unless otherwise indicated by the present disclosure. The methods of the present invention may be performed in hardware, firmware, software, or any combination thereof operating on a single computer or multiple computers of any type. Software embodying the present invention may comprise computer instructions in any form (e.g., source code, object code, interpreted code, etc.) stored in any computer-readable storage medium (e.g., a ROM, a RAM, a magnetic media, a compact disc, a DVD, etc.). Such software may also be in the form of an electrical data signal embodied in a carrier wave propagating on a conductive medium or in the form of light pulses that propagate through an optical fiber.

While particular embodiments of the present invention have been shown and described, it will be apparent to those skilled in the art that changes and modifications may be made without departing from this invention in its broader aspect and, therefore, the appended claims are to encompass within their scope all such changes and modifications, as fall within the true spirit of this invention.

In the above description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the invention. It will be apparent, however, to one skilled in the art that the invention can be practiced without these specific details. In other instances, structures and devices are shown in block diagram form in order to avoid obscuring the invention.

Reference in the specification to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the invention. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment.

Some portions of the detailed description are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art.

An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

The present invention also relates to an apparatus for performing the operations herein. This apparatus can be specially constructed for the required purposes, or it can comprise a general-purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program can be stored in a computer readable storage medium, such as, but is not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, and magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

The algorithms and modules presented herein are not inherently related to any particular computer or other apparatus. Various general-purpose systems can be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatuses to perform the method steps. The required structure for a variety of these systems will appear from the description below. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages can be used to implement the teachings of the invention as described herein. Furthermore, as will be apparent to one of ordinary skill in the relevant art, the modules, features, attributes, methodologies, and other aspects of the invention can be implemented as software, hardware, firmware or any combination of the three. Of course, wherever a component of the present invention is implemented as software, the component can be implemented as a standalone program, as part of a larger program, as a plurality of separate programs, as a statically or dynamically linked library, as a kernel loadable module, as a device driver, and/or in every and any other way known now or in the future to those of skill in the art of computer programming. Additionally, the present invention is in no way limited to implementation in any specific operating system or environment.

It will be understood by those skilled in the relevant art that the above-described implementations are merely exemplary, and many changes can be made without departing from the true spirit and scope of the present invention. Therefore, it is intended by the appended claims to cover all such changes and modifications that come within the true spirit and scope of this invention.

What is claimed is:

1. A method comprising:

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;

responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

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

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.

2. The method of claim **1**, wherein the one or more codes and other data values are transmitted to the trusted authority over a network.

3. The method of claim **1**, further comprising:

registering an age verification for the user in association with the device ID code.

4. The method of claim **1**, wherein the one or more codes and other data values indicate that the biometric verification was successful.

5. The method of claim **1**, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

6. The method of claim **1**, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

7. The method of claim **1**, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

8. The method of claim **1**, wherein the application includes a file including medical information.

9. The method of claim **1**, wherein the application includes a financial account.

10. The method of claim **1**, further comprising:

establishing a secure communication channel prior to sending the one or more codes and other data values for authentication.

11. The method of claim **1**, further comprising:

receiving a request for the one or more codes and other data values without a request for biometric verification; and

responsive to receiving the request for the one or more codes and other data values without a request for biometric verification, sending the one or more codes and other data values without requesting the scan data.

12. An integrated device comprising:

a persistent storage media that stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper

proof format written to the persistent storage media and not capable of being subsequently altered;

a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends one or more codes and other data values from the plurality of codes and other data values for authentication by a third party that operates a trusted authority, wherein the one or more codes and other data values includes the device ID code; and

a radio frequency communication module that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party and allowing the user access to an application.

13. The integrated device of claim **12**, wherein the one or more codes and other data values are transmitted to the trusted authority over a network.

14. The integrated device of claim **12**, wherein an age verification is registered in association with the device ID code.

15. The integrated device of claim **12** comprising:

an LED to be activated for requesting the biometric scan.

16. A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

wirelessly receiving one or more codes and other data values from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and other data values comprises the device ID code uniquely identifying an integrated device associated with a biometrically verified user, the device ID code being registered with a trusted authority for authentication, the trusted authority operated by a third party;

requesting authentication of the integrated device using the one or more codes and other data values by the trusted authority;

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 to the third party; and

in response to receiving the access message, allowing the biometrically verified user access to the application.

17. The method of claim **16**, further comprising:

registering a date of birth or age with the trusted authority.

18. The method of claim **16**, further comprising:

establishing a secure communications channel with the integrated device, wherein the one or more codes and other data values associated with the biometrically verified user is received from the integrated device.

19. The method of claim **16**, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

20. The method of claim **16**, wherein the application includes a file including medical information.

21. The method of claim **16**, wherein the application includes a financial account.

22. A system, comprising:

an integrated hardware device that stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated hardware device and a secret decryption value in a tamper proof format written to a storage element in the integrated hardware device that is not capable of being subsequently altered, and that wirelessly sends one or more codes and other data values from the plurality of codes and other data values, wherein the one or more codes and other data values include the device ID code; and

an authentication circuit that receives the one or more codes and other data values and sends the one or more codes and other data values to a third party that operates a trusted authority for authentication, and that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party and allows the user to access an application.

23. The system of claim **22**, wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from the user to generate scan data.

24. The system of claim **22**, wherein when the integrated hardware device cannot verify scan data as being from the user, the integrated hardware device does not send the one or more codes and other data values.

25. The system of claim **22**, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

26. The system of claim **22**, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

27. The system of claim **22**, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

28. The system of claim **22**, wherein the application includes a file including medical information.

29. The system of claim **22**, wherein the application includes a financial account.

* * * * *

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS, AND TYPE STYLE REQUIREMENTS

This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) or Fed. R. App. P. 28.1(e). The brief contains 10,383 words.

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) or Fed. R. App. P. 28.1(e) and the type style requirements of Fed. R. App. P. 32(a)(6). The brief has been prepared in a proportionally spaced typeface using Microsoft Word in Office 365 in 14-point Times New Roman font.

Dated: April 3, 2026

Respectfully Submitted,

/s/ David L. Hecht

David L. Hecht
Hecht Partners LLP
125 Park Avenue, 25th Floor
New York, NY 10017
Tel: (212) 851-6821
E: dhecht@hechtpartners.com

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing:

APPELLANT'S OPENING BRIEF

was filed with the Clerk of the United States Court of Appeals for the Federal Circuit via the CM/ECF SYSTEM. Counsel registered with the CM/ECF system have been served by operation of the Court's CM/ECF SYSTEM per Fed. R. App. P. 25 and Fed. Cir. R. 25(c) on the 3rd day of April, 2026.

Dated: April 3, 2026

/s/ David L. Hecht

David L. Hecht
Hecht Partners LLP
125 Park Avenue, 25th Floor
New York, NY 10017
Tel: (212) 851-6821
E: dhecht@hechtpartners.com