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.

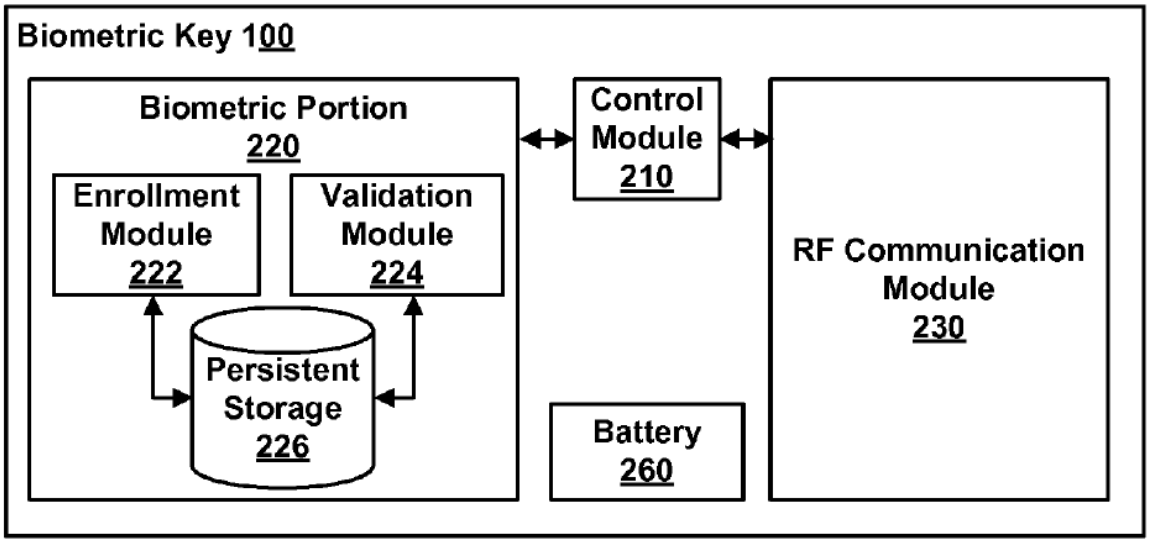

FIG. 2

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.

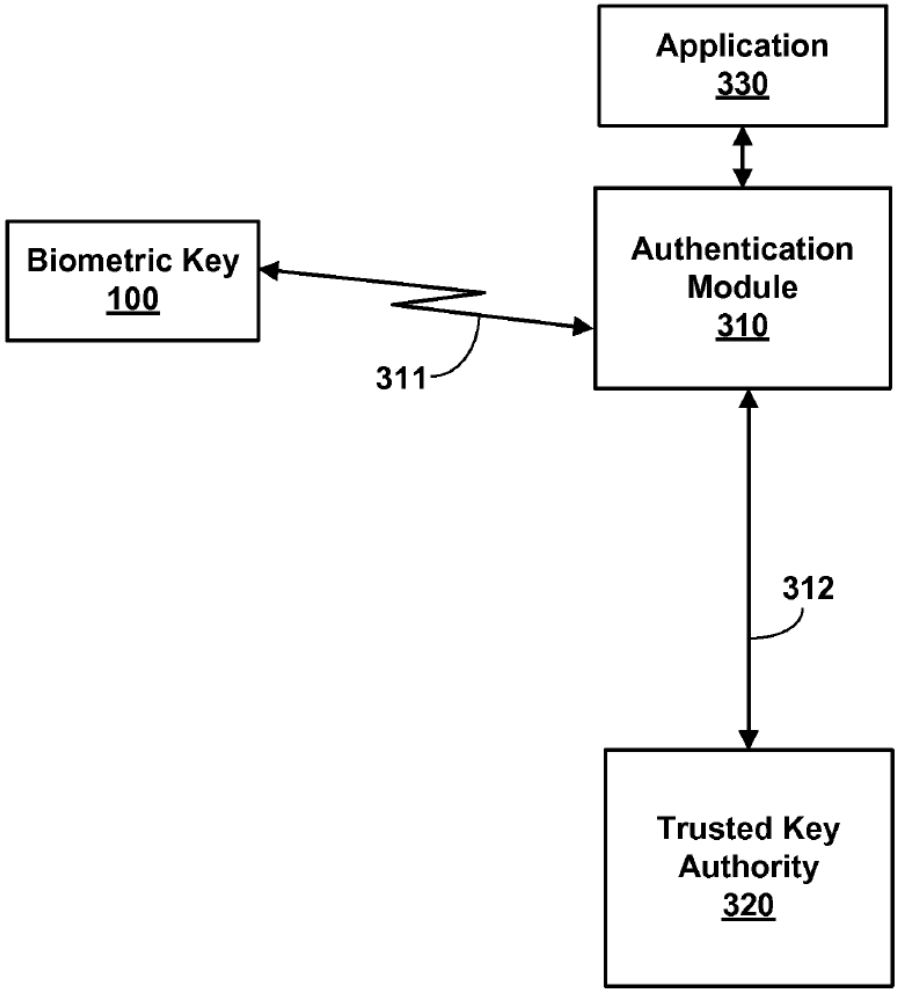

FIG. 3

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:

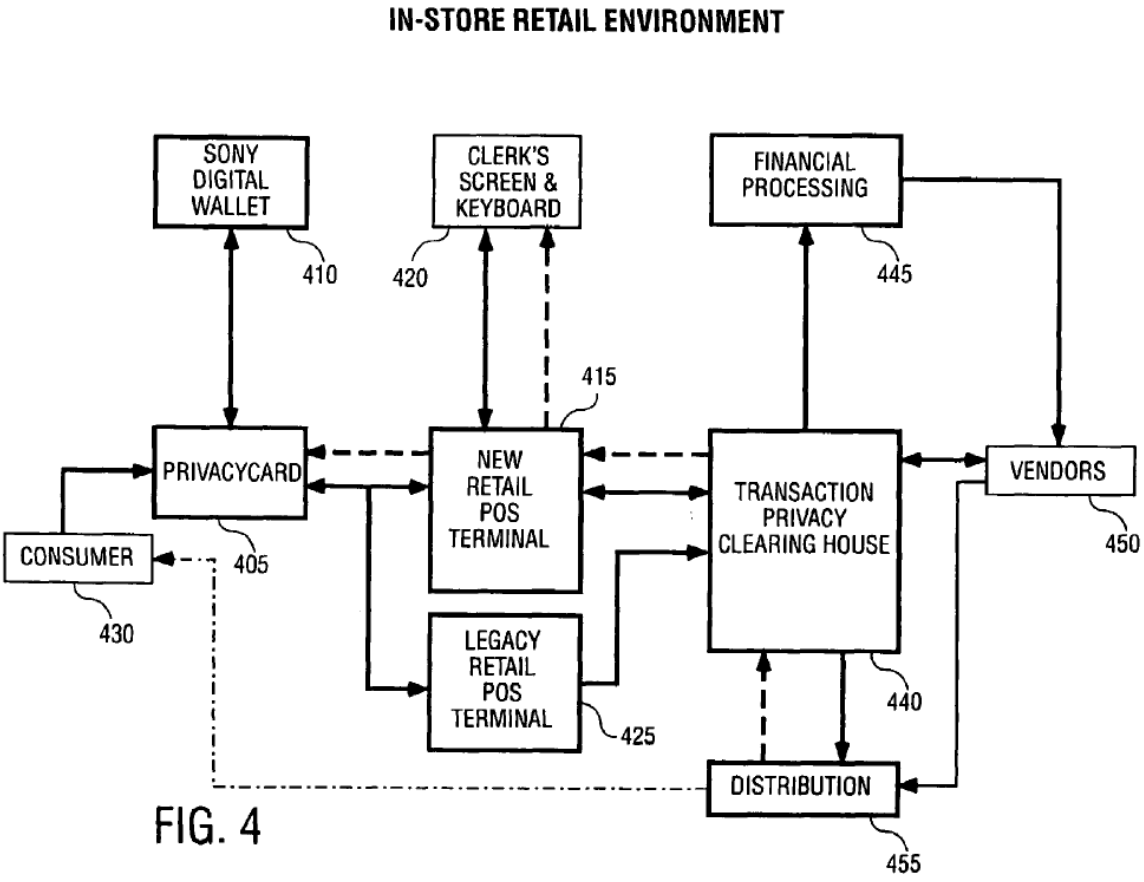

Figure 4 is a block diagram of an in-store retail system. *Id.* at 2:8–9.

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:

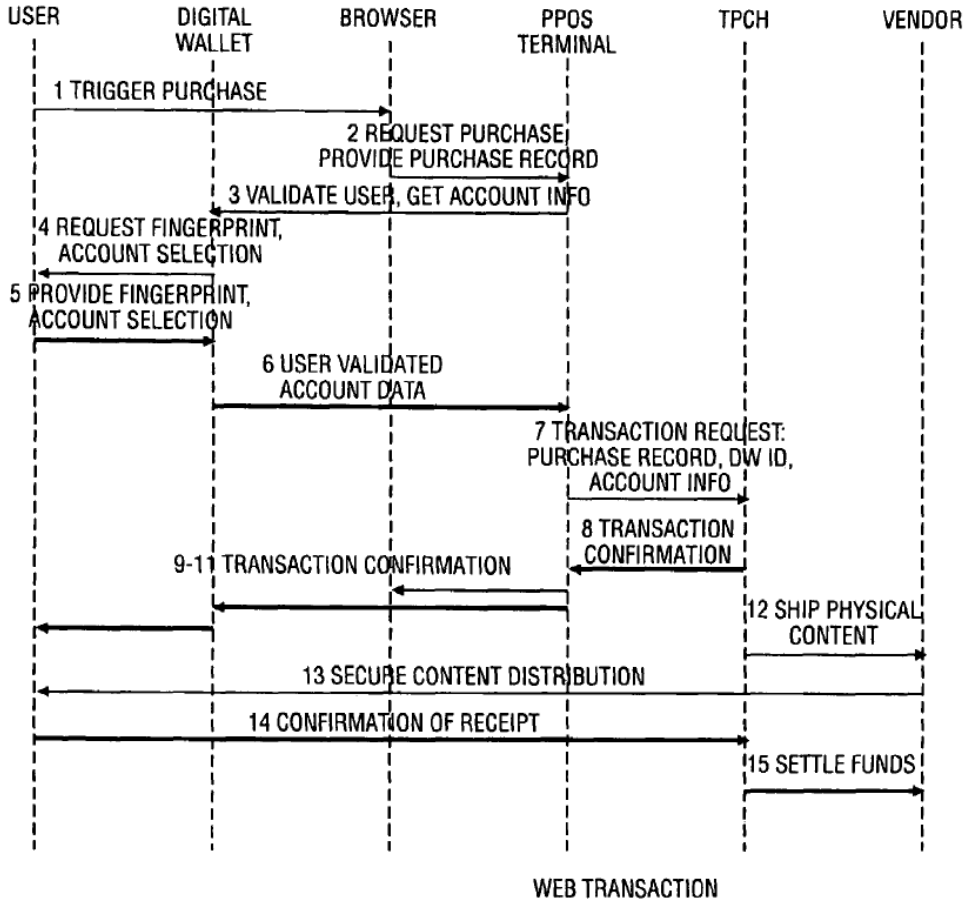

FIG. 17

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