

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION,

Petitioner,

v.

PROXENSE, LLC,

Patent Owner

Case No. IPR2024-01326

U.S. Patent No. 8,352,730

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

I.	Relief Requested	1
II.	The '730 Patent	1
A.	Overview.....	1
III.	Claim Construction	3
IV.	Level of Ordinary Skill	4
V.	Ground 1: Claims 1, 2, 4-6, 8, 9, 11-12, and 14-17 Are Obvious Over Ludtke.	5
A.	Overview of Prior Art Ludtke.....	5
B.	Claims	8
1.	Independent claim 1.....	8
a.	[1preamble]: “A method for verifying a user during authentication of an integrated device, comprising the steps of:”	8
b.	[1ai]: “persistently storing biometric data of the user [in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered]” .	10
c.	[1aii]: “[persistently storing] a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device [in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered]”	13
d.	[1aiii]: “[persistently storing] a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;” .	15
e.	[1b]: “wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;”	22

f.	[1c]: “responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;”	22
g.	[1d]: “comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;”	24
h.	[1e]: “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 by an agent that is a third-party trusted authority possessig a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and”	24
i.	[1f]: “responsive to authentication of the one or more codes and the other data values by the agent, receiving an access message from the agent allowing the user access to an application, wherein the application is selected from a group consisting of a csino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.”	31
2.	Claim 2: “The method of claim 1, wherein the one or more codes and the other data values are transmitted to the agent over a network.” ..	35
3.	Claim 4: “The method of claim 1, wherein the one or more codes and the other data values indicate that the biometric verification was successful.”	35
4.	Claim 5: “The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.”	37
5.	Claim 6: “The method of claim 1, further comprising: establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication”	37
6.	Independent Claim 8.....	38
a.	[8preamble]: “An integrated device for verifying a user during authentication of the integrated device, comprising:”.....	38

- b. [8ai]: “a memory stores biometric data of a user, and” 38
- c. [8aii]: “a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device, and” 38
- d. [8aiii]: “a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered;” 38
- e. [8b]: “wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;” 38
- f. [8c]: “a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and the other data values includes the device ID code; and” 39
- g. [8d]: “responsive to the agent authenticating the one or more codes and the other data values, a radio frequency communicator, receives an access message from the agent allowing the user access to an 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.” 40
- 7. Claim 9: “The integrated device of claim 8, wherein the one or more codes and the other data values are transmitted to the agent over a network.” 41
- 8. Claim 11: “The integrated device of claim 8, wherein the verifier comprises: an LED to be activated for requesting the biometric scan.” 41

9.	Independent Claim 12.....	44
a.	[12preamble]: “A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:”	44
b.	[12a]: “receiving one or more codes from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and the other data values comprises the device ID code uniquely identifying the integrated device and a secret encryption value associated with a biometrically verified user, the device ID code being registered with an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices”	45
c.	[12b]: “requesting authentication of the one or more codes and the other data values by the agent, wherein the authentication determines whether the one or more codes and the other data values are legitimate;”	48
d.	[12c]: “receiving an access message from the agent; and;”	48
e.	[12d]: “in response to a positive access message, allowing the biometrically verified user access to an 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.”	49
10.	Claim 14: “The method of claim 12, further comprising: establishing a secure communications channel with a biometric key, wherein the one or more codes and the other data values associated with the biometrically verified user is received from the biometric key.....	49
11.	Independent claim 15.....	50
a.	[15preamble]: “A system, comprising:”	50
b.	[15ai]: “a biometric key stores biometric data of a user”.....	50
c.	[15aii]: “and a plurality of codes and other data values	

- comprising a device ID code uniquely identifying the biometric key” 51
- d. [15aiii]: “and a secret decryption value in a tamper proof format written to a storage element on the biometric key that is unable to be subsequently altered,” 51
 - e. [15aiv]: “and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending, one or more codes from the plurality of codes and other data values wherein the one or more codes and the other data values include the device ID code,” 51
 - f. [15av]: “and the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition; and” 51
 - g. [15b]: “an authentication unit receives the plurality of codes and the other data values and send the plurality of codes and the other data values to agent for authentication to determine whether the one or more codes and the other data values are legitimate, wherein the agent is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices,” 51
 - h. [15c]: “and responsive to the device ID code being authenticated, the authentication unit receiving an access message from the agent allowing the user to access an 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.” 54
- 12. Claim 16: “The system of claim 15, wherein the biometric key receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate the scan data.” 54
 - 13. Claim 17: “The system of claim 15, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the one or more codes and the other data values.” 56

VI.	Ground 2: Claims 3, 10, and 13 are Obvious Over Ludtke and Kon.	58
A.	Kon	58
B.	Claims	62
1.	Claim 3: “The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code.”	62
2.	Claim 10: “The integrated device of claim 9, wherein an age verification is registered in association with the device ID code.” ...	67
3.	Claim 13: “The method of claim 12, further comprising: registering a date of birth or age with the agent.”	67
VII.	Discretionary Denial Is Not Warranted	67
A.	Discretionary Denial Is Not Warranted Under <i>Fintiv</i>	67
B.	Discretionary Denial Is Not Warranted Under <i>General Plastics</i>	68
C.	Discretionary Denial is Not Warranted under § 325(d).	70
VIII.	Mandatory Notices	72
A.	Real Parties-in-Interest Under 37 C.F.R. § 42.8(b)(1)	72
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2).....	72
C.	Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3).....	73
D.	Service Information Under 37 C.F.R. § 42.8(b)(4)	74
IX.	Standing	74
X.	Conclusion	74

LIST OF EXHIBITS

Exhibit	Description
Ex. 1001	U.S. Patent No. 8,352,730 (“the ’730 patent”)
Ex. 1002	File History of U.S. Patent No. 8,352,730
Ex. 1003	Declaration of Stephen Gray (Decl.)
Ex. 1004	Curriculum Vitae of Stephen Gray
Ex. 1005	U.S. Patent No. 7,188,110 to Ludtke et al. (“Ludtke”)
Ex. 1006	U.S. Patent Application Publication No. 2002/0046336 to Kon et al. (“Kon”)
Ex. 1007	<i>Samsung Electronics America, Inc. v. Proxense, LLC</i> , IPR2021-01444, Paper 11 (PTAB Feb. 28, 2022).
Ex. 1008	<i>Proxense, LLC v. Google LLC</i> , Case No. 6:23-cv-00320, Dkt. No. 31, Scheduling Order (W.D. Tex Aug. 18, 2023)
Ex. 1009	<i>Proxense, LLC v. Samsung Electronics Co., Ltd.</i> , Case No. 6:21-cv-00210, Dkt. No. 43, Claim Construction Order (W.D. Tex. Jan. 18, 2022).
Ex. 1010	<i>Proxense, LLC v. Samsung Electronics Co., Ltd.</i> , Case No. 6:21-cv-00210, Dkt. No. 149, Memorandum in Support of Claim Construction Order (W.D. Tex. Dec. 28, 2022).
Ex. 1011	Request for Reexamination, No. 90/015,052 (June 6, 2022).
Ex. 1012	<i>Proxense, LLC v. Google LLC</i> , Case No. 6:23-cv-00320, Dkt. No. 1, Complaint (W.D. Tex. May 2, 2023)
Ex. 1013	<i>Proxense, LLC v. Google LLC</i> , Case No. 6:23-cv-00320, Preliminary Infringement Contentions (W.D. Tex. July 24, 2023).
Ex. 1014	<i>CERTIFICATION REPORT No. P165: Sony FeliCa Contactless Smart Card RC-S860</i> , UK IT Security Evaluation and Certification Scheme (Mar. 2002).

Exhibit	Description
Ex. 1015	U.S. Patent Application Publication No. 2002/0049806 to Gatz et al. (“Gatz”)
Ex. 1016	U.S. Patent Application Publication No. 2006/0034492 to Siegel et al. (“Siegel”)
Ex. 1017	U.S. Patent Application Publication No. 2001/0036297 to Ikegami et al. (“Ikegami”)
Ex. 1018	<i>Proxense, LLC v. Google LLC</i> , Case No. 6:23-cv-00320, Dkt. No. 45, Proxense’s Responsive Claim Construction Brief (W.D. Tex. Dec. 1, 2023).
Ex. 1019	<i>Proxense, LLC v. Google LLC</i> , Case No. 6:23-cv-00320, Dkt. No. 45, Proxense’s Expert Transcript (W.D. Tex. Dec. 18, 2023).
Ex. 1020	Decision on Petition, Ex Parte Reexamination No. 90/015,052 (Jan. 3, 2024).
Ex. 1021	Order Granting Request for Ex Parte Reexamination, Ex Parte Reexamination No. 90/015,052 (Aug. 2, 2022).
Ex. 1022	<i>Proxense, LLC v. Google LLC</i> , Case No. 6:23-cv-00320, Dkt. No. 50, Proxense’s Sur-Reply Claim Construction Brief (W.D. Tex. Jan. 5, 2024).
Ex. 1023	U.S. District Courts—National Judicial Caseload Profile, <i>available at</i> https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_dis_tcomparison0930.2023.pdf (retrieved Jan. 15, 2024).
Ex. 1024	Microsoft Stipulation dated August 20, 2024

I. Relief Requested

Microsoft Corporation (“Microsoft” or “Petitioner”) requests *inter partes* review of claims 1-6 and 8-17 of U.S. Patent No. 8,352,730 (“the ’730 patent”) based on the following grounds (Decl., 70-71):

Ground	Claim(s) Challenged	35 U.S.C. §	Reference(s)
1	1, 2, 4-6, 8, 9, 11-12, and 14-17	103	Ludtke
2	3, 10, 13	103	Ludtke and Kon

II. The ’730 Patent

A. Overview

The ’730 patent was filed on December 20, 2005 and claims priority to provisional applications filed on December 20, 2004 and February 14, 2005. Ex. 1001, cover page. The ’730 patent generally relates to “authentication responsive to biometric verification.” Ex. 1001, 1:16-19.

Figure 6 illustrates a process for “verifying a subject” using a biometric key. Ex. 1001, 6:65-67, FIG. 6. As shown in Figure 6, the device receives biometric scan data, such as a fingerprint scan, from the user (step 620). Ex. 1001, FIG. 6. If the scan data matches “previously-stored biometric data,” (step 630), the user is “verified” (step 640), at which point a “code” is sent to a trusted key authority (step 650). Ex. 1001, 7:3-14, FIG. 6.

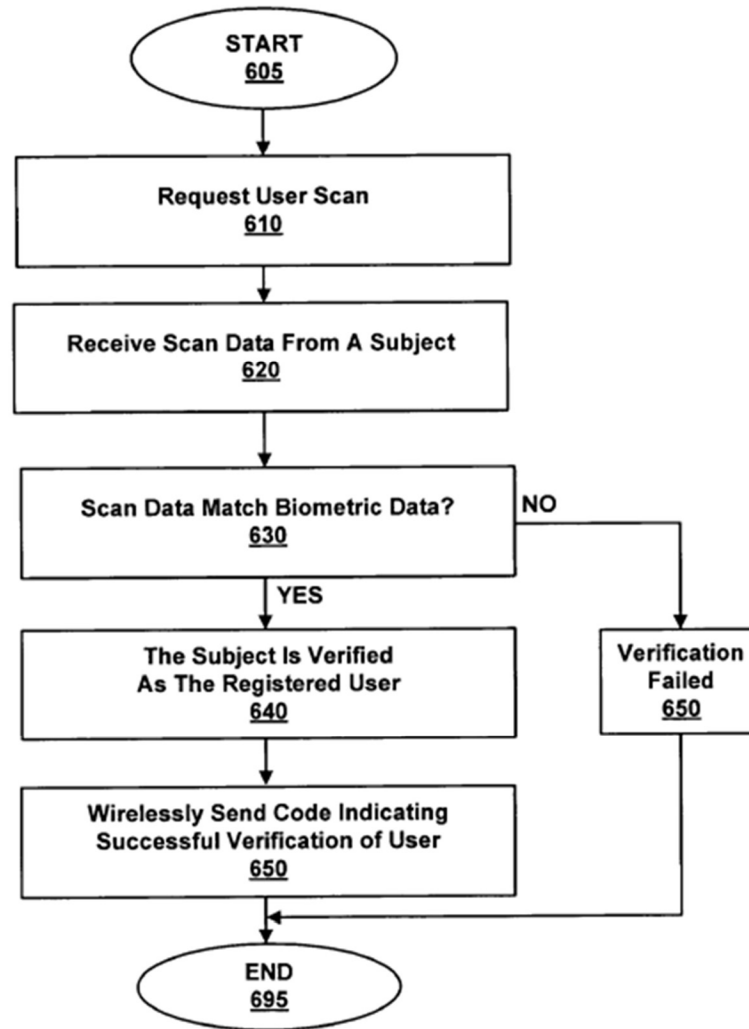


FIG. 6

Ex. 1001, FIG. 6.

Once the code is received, as illustrated in Figure 7, the trusted key authority determines whether the code is “authentic” (step 730). Ex. 1001, 7:15-18, FIG. 7. “If authentication is successful, the trusted key authority sends an access message to [an] application to allow user access and/or provide additional information from the profile” (step 740). Ex. 1001, 7:18-21, FIG. 7. If authentication is not successful, authentication fails (step 750) and “the message to the application

indicates that the user should be denied access.” Ex. 1001, 7:21-23, FIG. 7; Decl., 46-48.

700

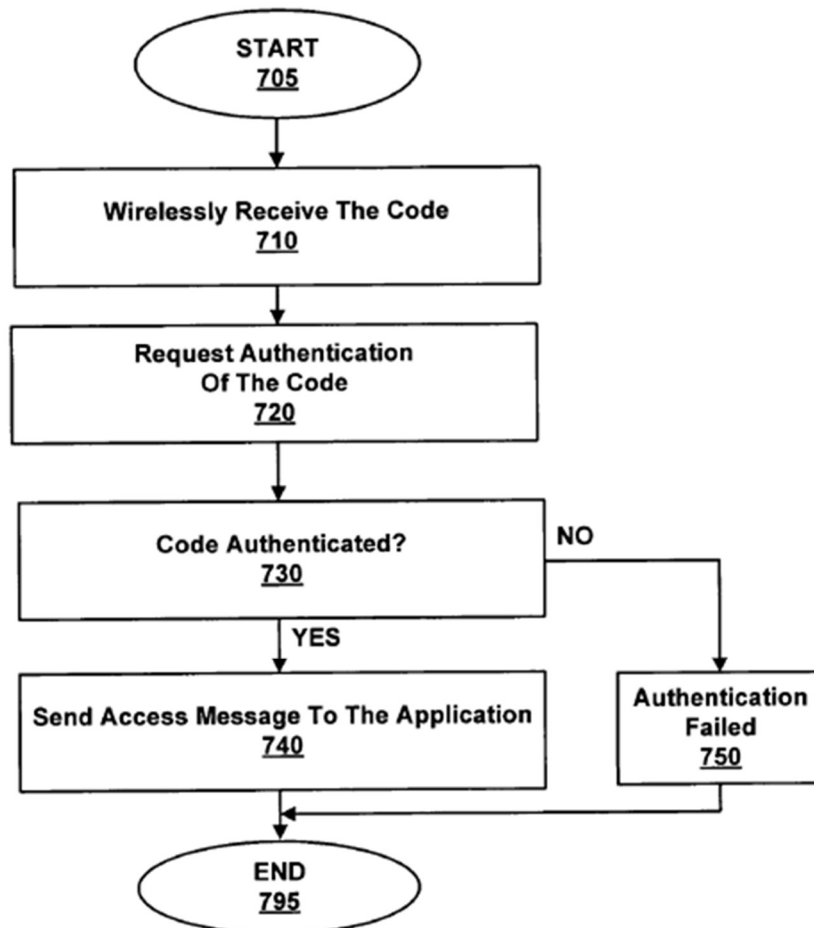


FIG. 7

Ex. 1001, FIG. 7.

III. Claim Construction

In a previous institution decision, the Board “interpreted” the term “third-party trusted authority” as recited in the ’730 patent “to mean a trusted authority that is an entity separate from the parties to a transaction.” Ex. 1007 at 15.

In the previous district court litigation, *Proxense, LLC v. Samsung Electronics Co., Ltd.*, Case No. 6-21-cv-00210, two terms from the '730 patent were construed by the court (Exs. 1009-1010):

- Device ID Code – “[a] unique code identifying a device”
- Access Message – “[a] signal or notification enabling or announcing access.”

Ex. 1009, 3; Ex. 1010, 15, 20; Decl., 49-53.

Because the prior art in this Petition discloses each of these prior constructions, and the plain and ordinary meaning of all terms, Petitioner submits that no claim terms need to be construed to resolve unpatentability in this Petition¹ (*Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019)).

IV. Level of Ordinary Skill

A person of ordinary skill in the art (“POSITA”) at the time of the purported invention 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. Decl., 31-32,

¹ Additional claim terms were construed in other proceedings relating the '730 patent, but the Board need not resolve those terms because the Grounds relied on in this petition render the challenged claims obvious under either the plain and ordinary or alternate construction.

54-56. Additional education could substitute for professional experience, and significant work experience could substitute for formal education. Decl., 55.

V. Ground 1: Claims 1, 2, 4-6, 8, 9, 11-12, and 14-17 Are Obvious Over Ludtke.

A. Overview of Prior Art Ludtke

Ludtke, filed December 11, 2000, is prior art under at least 35 U.S.C. § 102(e). Ludtke, cover page. Ludtke discloses systems and methods of authorizing a user to conduct a transaction using a “biometric device” (also called a “transaction device”) such as a privacy card and/or digital wallet. Ludtke, Abstract, 3:32-36, 6:36-44. The transaction device includes a processor, memory, and fingerprint recognition technology. Ludtke, 5:60-64, FIG. 7A. Ludtke stores “authorized fingerprint recognition samples,” a device ID corresponding to the privacy card, and a public key infrastructure (“PKI”) on the transaction device. Ludtke, 11:66-12:7, 14:19-21, 38:26-29. Ludtke also indicates that the biometric device can use other techniques, such as a “retinal scan, voice, DNA, hand profile, face recognition, etc.,” instead of or in addition to fingerprints. Ludtke, 35:61-64.

When an authorized user attempts to use the transaction device, e.g., at a point of sale (“POS”) terminal, or other “service,” the user is “prompted to supply a fingerprint recognition sample,” as an initial security measure. Ludtke, 1:22-31, 1:37-38, 14:33-42, 18:45-50, 18:52-55. The sample is compared to stored fingerprints and if the sample is recognized, the user is authorized. Ludtke, 14:40-

46.

In one embodiment, “the transaction device is used to trigger shopping activity” such as a “web-based transaction using a transaction device such as a privacy card and/or digital wallet and a personal POS terminal” by “clicking on a ‘Buy!’ or similar button in the web browser.” Ludtke, 28:15-18, 28:26-40, 28:34-35. The POS asks the transaction device to “validate the user” and the user is “prompted to supply a fingerprint recognition sample,” as an initial security measure. Ludtke, 1:22-31, 1:37-38, 14:33-42, 18:45-50, 18:52-55, 28:57-62. The sample is compared to stored fingerprints and if the sample is recognized, the user is authorized. Ludtke, 14:41-46. Once the transaction device authorizes the user based on the matching biometric information, the personal POS terminal “opens a secure communications session to the TPCH, requesting a transaction,” and “provides the transaction record that it received from the web browser *and the unique ID of the transaction device*.” Ludtke, 29:5-12 (emphasis added); *see also* Ludtke, 27:12-13 (“Privacy card information is provided to TPCH, step 1510.”), 34:25-27 (explaining that “necessary secure transaction communication with the TPCH” includes “providing the transaction data *and its device ID*” (emphasis added)). The TPCH is a trusted third-party agent, separate from the transaction device, personal POS terminal and the back-end transacting entity (e.g., vendor). Ludtke, 7:42-48, 9:26-34, FIG. 6.

Ludtke also discloses an alternate embodiment in which the POS

“functionality of providing secure communication and transactions with the Transaction Privacy Clearing House (TPCH)” described above “can be integrated into the digital wallet directly.” Ludtke, 28:41-45. Thus, Ludtke also discloses communicating the device ID directly from the transaction device to the TPCH responsive to a “match” between the scanned biometric data (e.g., fingerprint or other biometric data) and stored data.

Next, “[t]he TPCH uses the unique ID of the transaction device to process the transaction. 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” that “reflects the transaction confirmation back to . . . the transaction device. The transaction device may display a transaction confirmation to the user and may additionally record the transaction in its local storage.” Ludtke, 29: 12-23, FIG. 15.

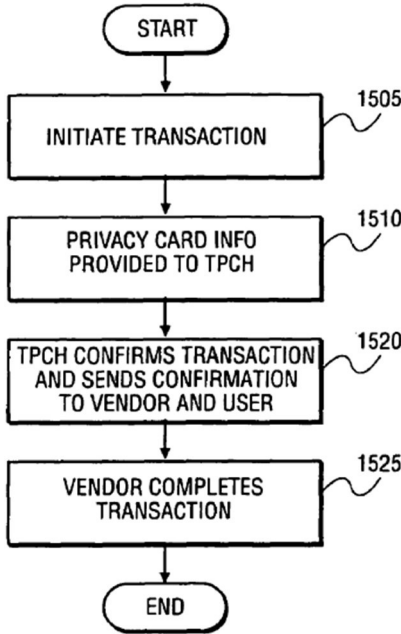


FIG. 15

Ludtke, FIG. 15.

Ludtke is analogous art to the '730 patent because it is directed to the same technical field: user authentication methods and systems. *Compare* Ex. 1001, 1:16-19, *with* Ludtke, 1:59-61; Decl., 33, 57-64.

B. Claims

1. Independent claim 1

- a. [1preamble]: “A method for verifying a user during authentication of an integrated device, comprising the steps of:”

To the extent limiting, Ludtke discloses [1preamble] because Ludtke discloses “identifying an authorized user” (verifying a user) “with a biometric device and enabling the authorized user to access private information” using a

“transaction device” such as a privacy card and/or digital wallet (integrated device). Ludtke, Abstract, 3:32-36; Decl., 72-74. Ludtke explains that “[t]he user connects to and performs transactions with [an] eCommerce system through a transaction device which has a unique identifier (ID)” such as “a privacy card is used” or “a digital wallet” (integrated devices). Ludtke, 3:32-36.

The ’730 patent describes a “biometric key” including the elements recited in [1ai]-[1aii]. Ex. 1001, 1:57-67. Patent Owner indicated in its Responsive Claim Construction Brief (Ex. 1018) that “an ‘integrated device’ is a ‘device’ that is integrated with a biometric key.” Ex. 1018, 4. Patent Owner’s Sur-Reply Claim Construction Brief also states that “‘integrated device’ integrates or includes a biometric key component” Ex. 1022, 2. Ludtke’s transaction devices (such as a digital wallet and/or privacy card) likewise include a biometric key and constitute an integrated device under Patent Owner’s construction, as explained below. Decl., 73-74.

Petitioner’s indefiniteness challenge in the district court proceeding does not preclude institution of an IPR. *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 801, 813 (Fed. Cir. 2021) (“The indefiniteness of a limitation ... precludes a patentability determination only when the indefiniteness renders it logically impossible for the Board to reach such a decision.”); *Zillow Grp., Inc. v. Int’l Bus. Machs. Corp.*, IPR2020-01656, Paper 8 at 11 (PTAB Mar. 15, 2021) (“Patent Owner cites no

authority nor are we aware of any authority for the proposition that we may not assess the patentability of claims in an *inter partes* review because the Petitioner also challenges those claims as indefinite in District Court.”); *Target Corp. v. Proxicom Wireless, LLC*, IPR2020-00931, Paper 10 at 9 (PTAB Nov. 10, 2020) (noting that “[a]lternative pleading before a court is common practice”); *Alcon Inc. v. AMO Dev., LLC*, IPR2021-00843, Paper 15 at 16 (PTAB Nov. 12, 2021) (instituting review despite petitioner’s allegation before the district court that the claim is indefinite when the Board was “able to construe the disputed claim term with sufficient precision to address the obviousness arguments”).

b. [1ai]: “persistently storing biometric data of the user [in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered]”

Ludtke discloses [1ai] because its transaction device, like a privacy card and/or digital wallet, (integrated device) stores “authorized fingerprint recognition samples” or other “biometric identification” e.g., “retinal scan, voice, DNA, hand profile, face recognition, etc.” (biometric data of the user) in a “user identity/account information block 760” or “write-once memory” (persistent storage). Ludtke, 13:27-29, 14:19-21, 19:9-14, 19:29-40, 35:61-64, FIGS. 7B-7C, Decl., 75-78.

Ludtke’s privacy card (integrated device) has a “user identity/account information block 760 [that] *stores data* about the user and accounts that are

accessed by the card” including “the authorized fingerprint recognition samples.”

Ludtke, 13:27-29, 14:19-21, 14:13-18 (emphasis added) (explaining that the privacy card embodied in Figure 7C “may include those functions set forth in FIG. 7b, referred to herein as first generation privacy card technology block 775 and FeliCa² Technology block 774”); Decl., 76.

Although Ludtke’s exemplary explanations relate to fingerprint data, Ludtke discloses that the biometric information used could also comprise “retinal scan, voice, DNA, hand profile, face recognition, etc.” using the same process for identification. Ludtke, 35:61-64. At very least, a POSITA would have understood that the same process would apply to any of Ludtke’s disclosed user biometric information. Ludtke, 35:61-64. Ludtke explains that “[t]he fingerprint data entry process may be performed at least twice, to confirm that the user has entered the correct data (using the correct fingerprint). If confirmation succeeds, “the device writes the fingerprint image data *into write-once memory* ” (persistent storage). Ludtke, 19:9-14, 19:29-40 (emphasis added); Decl., 77.

² FeliCa is a “contactless (wireless) card execution platform.” Ludtke, 11:1-5.

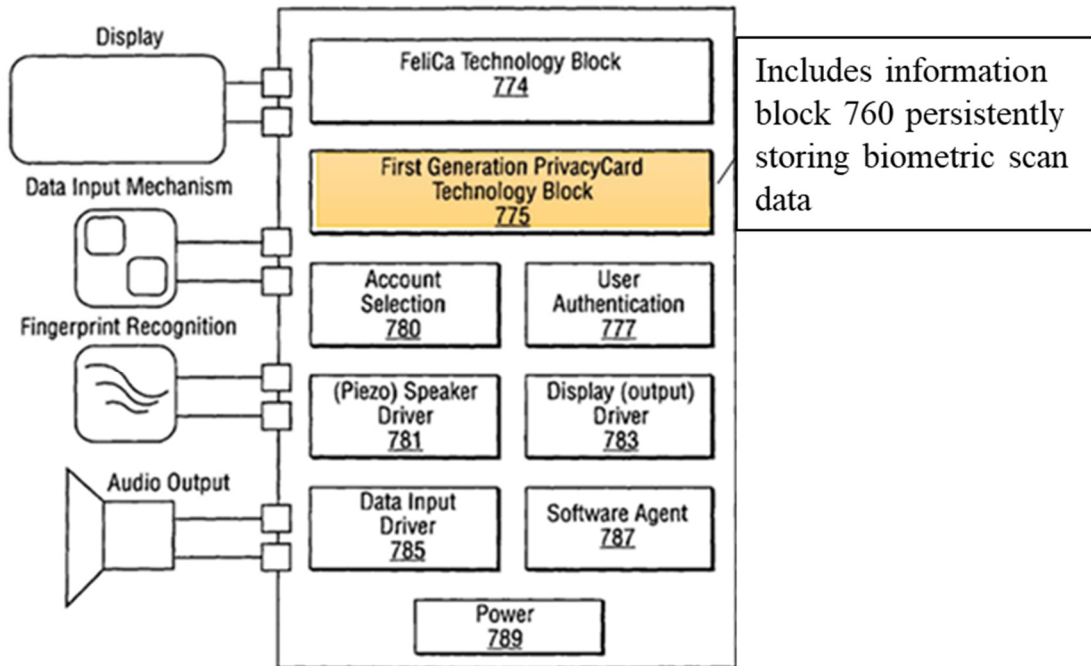


FIG. 7C

Ludtke, FIG. 7C (annotated).

A POSITA would have understood that Ludtke's fingerprint data is persistently stored in a tamper proof format that is unable to be subsequently altered because it is stored in "write-once memory." Ludtke, 19:9-14, 19:29-40; Decl., 78. This is consistent with the '730 patent which explains that "*at least some of persistent storage 226 is a memory element that can be written to once but cannot subsequently be altered.*" Decl., 78. Persistent storage 226 can include, for example, a ROM element, a flash memory element, or any other type of non-volatile storage element. Decl., 78. Persistent storage 226 is itself, and stores data in, a tamper proof format to prevent any changes to the stored data. Decl., 78. Tamper proofing 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).” Ex. 1001, 4:29-42 (emphasis added); Decl., 78.

- c. **[1aii]: “[persistently storing] a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device [in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered]”**

Ludtke discloses and renders obvious [1aii] because its transaction device (integrated device) stores a “unique transaction device ID value[.]” (device ID code) in its “permanent memory.” Ludtke, 30:20-23; Decl., 79.³

Ludtke’s stored device ID, like “globally unique silicon ID (GUID) 764[,] is used to identify the privacy card among other existing transaction cards,” and thus uniquely identifies the integrated device. Ludtke, 13:39-41. Even if the claim language is interpreted to require storing additional codes besides the “device ID

³ Patent Owner indicated in its Sur-Reply Claim Construction Brief that “the plain and ordinary meaning of the claim term, that within this stored area are (1) codes and values uniquely identifying an integrated device or biometric key; and (2) a secret decryption value.” Ex. 1022, 8. Ludtke’s transaction devices likewise store a device ID and a secret decryption value, as explained below.

code,” Ludtke discloses that the device ID is stored along with other codes and data values, e.g., magnetic stripe and bar codes, that allow the transaction device to interface with a POS terminal. Ludtke, 8:63-67, 9:18-25, 23:11-19; Decl., 80.

A POSITA would have understood that the transaction device ID is stored in a tamper proof format unable to be subsequently altered because it is intended to *uniquely* identify the corresponding device and “contain[s] an identification that maintains the confidentiality of the user’s identity” Ludtke, 10:64-67, 30:20-23; Decl., 81. Storing the device ID in a tamper proof format unable to be subsequently altered would have comported with Ludtke’s goal of ensuring that the device is authorized to perform certain transactions and ensuring the integrity of the confidential information. Ludtke, 30:18-27; Decl., 81. Ludtke’s use of FeliCa technology further suggests storing information in a tamper proof format because contactless smart cards implementing FeliCa were known to be tamper resistant. Ex. 1014, 21, 25; Decl., 81.

To the extent Patent Owner disputes that the transaction device ID is stored in a tamper proof format unable to be subsequently altered, a POSITA would have been motivated and found it obvious to store the device ID in “write-once memory” to prevent modification of the transaction device ID and ensure that the ID is associated with the correct device. Decl., 82. Ludtke uses write once memory to store other kinds of sensitive information (e.g., biometric data as explained in

[1ai], *supra*) in a tamper proof format unable to be subsequently altered, and a POSITA would have had a reasonable expectation of success in using the same type of memory to store the keys as well. Indeed, because Ludtke’s device ID “contain[s] an identification that maintains the confidentiality of the user’s identity” (Ludtke, 10:64-67), a POSITA would have understood the importance of ensuring the integrity of the device ID and would have been motivated to store it in the same format as Ludtke’s fingerprint data—tamper proof and unable to be subsequently altered—to preserve its integrity. Decl., 82.

d. [1aiii]: “[persistently storing] a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;”

Ludtke discloses and renders obvious [1aiii] because the transaction device uses a public key infrastructure (“PKI”) to verify the user, and the PKI requires the transaction device to store either a public key and/or a private key (secret decryption value) to decrypt encrypted data. Ludtke, 5:11-20, 38:9-14; Decl., 83-94. The disclosure of Ludtke makes clear that both Ludtke’s public key and private key are “secret values” that are used for decryption. Decl., 83-94.

Ludtke discloses that the “sensitive nature of the information being transferred, such as access codes, PINs, etc.,” make it “desir[able] to use a secure communication means and/or encryption to lessen the possibility of unauthorized

use of the information.” Ludtke, 37:39-45. So, to ensure the integrity of sensitive information, Ludtke uses a PKI system to encrypt and decrypt transmitted data. Ludtke, 5:11-20, 38:9-14; Decl., 84.

Public Key Decryption

In one example, the transaction device stores a secret decryption value configured as a public key. While public keys were traditionally known to various parties (and therefore not secret), Ludtke discloses using a public decryption key that is only known to the communicating parties for the purposes of exchanging sensitive data, like a password, in a one-to-one configuration where a single “public key” is distributed to correspond to a single “private key”; therefore, *both* public and private keys of Ludtke comprise a “secret” value. Ludtke, 38:1-3 (“[T]here may be a *one-to-one* relationship between a password and a public key”) (emphasis added), 38:12-14 (“[D]ata that is encrypted with a private key [is] only. . . capable of being decrypted with the public key . . .”), 38:25-29 (“The back-end distributes *one public key with each password* and *the biometric device stores and associates these back-end public keys with the associated password and data . . .*” (emphasis added)). This is also consistent with Patent Owner’s expert’s representations in the district court that “something that is secret is typically referred to as something that’s not known to the adversary” (Ex. 1019, 45:16-22), or in other words, secret values “are not available to anyone who hasn’t been

explicitly given the secret value.” Ex. 1019, 46:11-18; *see also* Ex. 1019, 50:11-14

(“The idea behind these protocols is that only the parties that the designer of the protocol wants would know the secret keys, and the bad guys wouldn’t.”); Decl., 85.

Ludtke’s secret public decryption key is used by the transaction device to decrypt data encrypted by the back end’s private key. More specifically, “the back-end select[s] an *unused* PKI key pair (one public, one private) from its internal database of keys” then “combines the selected public key with the password data structure, adds a password ID, and encrypts this entire combination with its private session key. It then, at 2710, transmits this to the device.” Ludtke, 38:45-53 (emphasis added). When the device receives the encrypted information (e.g., a Password ID), “the device *decrypts* and authenticates the incoming data *using the public session key* of the back-end system and other elements of the PKI system that are well known to those skilled in the art.” Ludtke, 38:49-61 (emphases added). In this way, the back-end system can assign passwords to the transaction device that the transaction device can decrypt “for later use.” Ludtke, 38:66-39:2. Accordingly, a POSITA would have understood that Ludtke stores a secret public decryption key, i.e., a secret decryption value. Decl., 86.

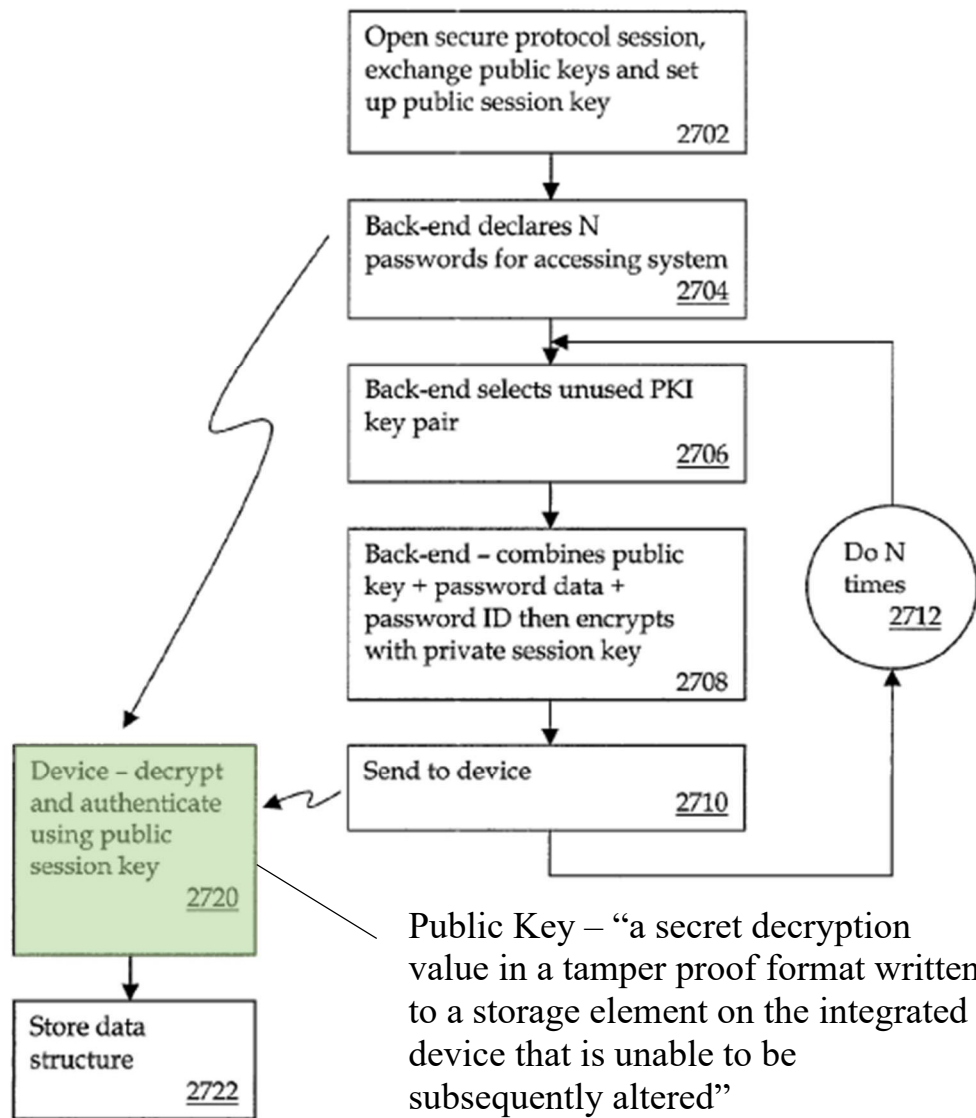


FIG. 27

Ludtke, FIG. 27 (annotated).

Furthermore, a POSITA would have been motivated and found it obvious to store the key in a tamper proof format unable to be subsequently altered to comport with Ludtke’s goal of generally preserving the integrity and confidentiality of sensitive information, like the key. Ludtke, 38:9-21, 38:40-46; Decl., 87. Because the key itself is considered sensitive and confidential information, since it grants

access to additional sensitive and confidential information, if the key could be modified or tampered with, its integrity would be compromised. Decl., 87. Indeed, the integrity of the system at large, which is intended to secure sensitive and confidential information, would also be compromised if the secret key cannot be secured. Decl., 87.

Specifically, a POSITA would have been motivated and found it obvious to store the key in “write-once memory,” i.e., in a tamper proof format that is unable to be subsequently altered, to prevent tampering and modification, thereby enhancing the security of the system generally and ensuring that sensitive data, like the key itself, remains secure. Decl., 88. Ludtke uses write once memory to store other kinds of sensitive information (e.g. biometric data as explained in [1ai], *supra*), in a tamper proof format unable to be subsequently altered, and a POSITA would have had a reasonable expectation of success in using the same type of memory to securely store the key as well. Decl., 88.

Private Decryption Key

Ludtke also discloses storing one or more private keys (secret decryption values) on the transaction device. Decl., 89.

Because information that is encrypted using a public key is decrypted with a private key (Ludtke, 38:9-14), a POSITA would have also understood that the private key stored at the transaction device is used to decrypt data encrypted using

a public key—and therefore constitutes a secret decryption value. Decl., 90. A POSITA would have been motivated and found it obvious to store the key in “write-once memory,” i.e., in a tamper proof format that is unable to be subsequently altered, to prevent modification and thereby enhance the security of the system, as discussed above. Decl., 91.

Private Encryption Key

Patent Owner in its complaint and infringement contentions identifies a private encryption key as a “secret decryption value.” Ex. 1012, ¶ 75 (“Android phones must contain a secret[] decryption value (i.e., the encryption key only accessible on the user’s own device)”; Ex. 1013, 15, 54. Ludtke also discloses storing a private encryption key on its transaction device. Decl., 92.

For example, Ludtke explains that the transaction device transmits a password encrypted with the device’s private encryption key to the back-end for decryption. As explained in column 39, the transaction device may “choose the PKI key pairs associated” with passwords, and “inform the back-end system about this key/password relationship, passing a ‘security mechanism public key’ and password to the back-end.” Ludtke, 39:7-12. Then, “[w]hen the back-end issues a challenge for a password with a given ID, *the device encrypts the password with its corresponding private key* and transmits [both] to the back-end” for decryption. Ludtke, 39:13-18 (emphasis added). In another example, the digital wallet

(transaction device) sends the “DW[(Digital Wallet)] identification (ID) plus an *encrypted message using the DW private key*” so the access site (back-end) “will decrypt the message with the DW public key.” Ludtke, 40:5-26; Decl., 93.

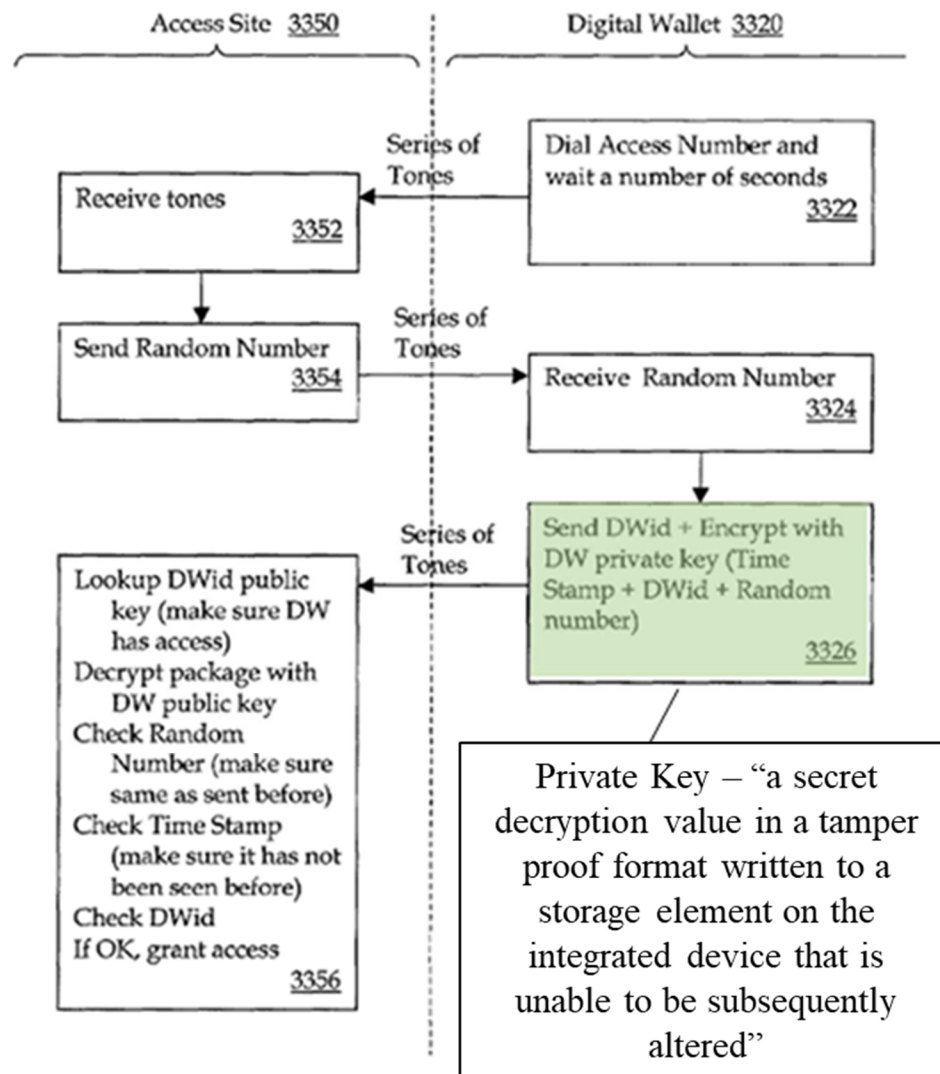


FIG. 33

Ludtke, FIG. 33 (annotated).

Thus, the private encryption key stored on Ludtke’s transaction device is also a “secret decryption value” within the meaning prescribed by Patent Owner in

its infringement contentions and construction. As explained for the private decryption key above, a POSITA would have been motivated and found it obvious to store the key in “write-once memory,” i.e., in a tamper proof format that is unable to be subsequently altered, to prevent modification, thereby enhancing the security of the system, as discussed above. Decl., 94.

- e. **[1b]: “wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;”**

Ludtke discloses [1b] because as explained for [1ai], the biometric data expressly includes a “fingerprint” as well as a “retinal scan, voice, DNA, hand profile, face recognition, etc.” Ludtke, 35:61-64; Decl., 95-96.

Ludtke states, “[t]he identification by the biometric device may be achieved in a variety of ways, as discussed above. For example, biometric identification[] may be [] [a] fingerprint, retinal scan, voice, DNA, hand profile, face recognition, etc.” Ludtke, 35:61-64; Decl., 96.

- f. **[1c]: “responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;”**

Ludtke discloses [1c] because Ludtke discloses “validating that the user interacting with the device is an authorized user” by prompting the user to “supply a fingerprint recognition sample” and receiving a fingerprint sample (scan data)

from a “fingerprint recognition pad” (a biometric scan) in response to the prompt (request for biometric verification). Ludtke, 14:33-42; Decl., 97-98. A POSITA would have understood that the disclosed fingerprint verification request is illustrative and that the same process is performed for each of the disclosed types of “biometric identification,” including the disclosed “retinal scan, voice, DNA, hand profile, face recognition, etc.” Ludtke, 35:61-64; Decl., 97.

In Ludtke, the privacy card user authentication⁴ block 777 “includes a biometric solution” such as a fingerprint recognition pad for “validating that the user interacting with the device is an authorized user.” Ludtke, 14:33-40. In operation, “the user is prompted to supply a fingerprint recognition sample,” after which the “block captures the sample[] and carries out a recognition algorithm against the authorized samples that are stored in the user identity block If a match is found, the user is authorized to access the data and functionality of the device. Ludtke, 14:40-46; Decl., 98; *see also* Ludtke, 16:47-49 (explaining that the digital wallet also receives biometric scan data after prompting).

⁴ The authentication block performs authorization that is distinct from the authentication performed by the third-party trusted authority described in [1e] below.

- g. [1d]: “comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;”**

Ludtke discloses [1d] because as explained in [1c], the transaction device uses a “recognition algorithm” to compare the fingerprint sample (scan data) “against the authorized samples that are stored in the user identity block” (biometric data) to determine “a match.” Ludtke, 14:40-46; Decl., 99. As explained above for [1ai], the fingerprint of Ludtke is illustrative, and Ludtke expressly discloses using other “biometric identification” e.g., “retinal scan, voice, DNA, hand profile, face recognition, etc.” for validation. Ludtke, 35:61-64; Decl., 99.

- h. [1e]: “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 by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and”**

Ludtke discloses [1e] because Ludtke discloses transferring (sending) the transaction device ID (one or more codes from the plurality of codes and the other data values) to a “single trusted” and “highly secured” transaction processing clearing house (TPCH) (third-party trusted authority) containing a “copy” of “unique transaction device ID[s]” (list of device ID codes uniquely identifying

legitimate integrated devices) over a wireless network connection using “wireless or cellular signals,” (wirelessly) once a biometric information match is identified (responsive to a determination that the scan data matches the biometric data).

Ludtke, 3:40-43, 4:48-50, 5:63-64, 7:46-48, 9:26-30, 9:35-42, 9:51-59, 28:50-29:12, 30:23-27; Decl., 100-109.

First, Ludtke determines whether the scan data matches the biometric data (as explained for [1c] and [1d]) and sends the transaction device ID responsive to a “match” between the scan data and stored data. Decl., 101.

In one embodiment, where “the transaction device is used to trigger shopping activity” such as a “web-based transaction using a transaction device such as a privacy card and/or digital wallet and a personal POS terminal,” “the user may tap on an on-screen icon being displayed by the transaction device, e.g., digital wallet; and the digital wallet transmits a signal” which “causes” a “web browser” for purchasing desired content (application) “to launch.” Ludtke, 28:15-18, 28:26-40. “Once a transaction has been triggered, the browser communicates with the personal POS terminal, requesting it to initiate a transaction” and “provides a transaction record, which includes all of the necessary data to support th[e] transaction, including a list of items being purchased, unit cost and quantity, the vendor who will provide the items, etc.” Ludtke, 28:13-18, 28:50-56; Decl., 102.

The POS asks the transaction device to “validate the user” and the user is “prompted to supply a fingerprint recognition sample,” as an initial security measure. Ludtke, 1:22-31, 1:37-38, 14:33-42, 18:45-50, 18:52-55, 28:57-62. The sample is compared to stored fingerprints and if the sample is recognized, the user is authorized. Ludtke, 14:41-46. As explained above, the fingerprint is illustrative and Ludtke expressly discloses using other “biometric identification” e.g., “retinal scan, voice, DNA, hand profile, face recognition, etc.” for validation. Ludtke, 35:61-64. After the transaction device receives the fingerprint recognition sample “*to confirm [an] entire transaction and that the user is authorized,*” the personal POS terminal “opens a secure communications session to the TPCCH, requesting a transaction” and “provides the transaction record that it received from the web browser *and the unique ID of the transaction device.*” Ludtke, 28:50-29:12 (emphases added); *see also* Ludtke, 27:12-13 (“Privacy card information is provided to TPCCH, step 1510.”), 34:25-27 (explaining that “necessary secure transaction communication with the TPCCH” includes “providing the transaction data and [the] device ID.”); Decl., 103.

The “confirmation that the user is authorized” is based on the match between the scan data and stored data, as explained for [1c] and [1d]. Ludtke, 14:40-46; *see also* Ludtke, 4:62-5:1 (“The transaction device enhances security by authenticating the user of the card *prior to usage* such that if a card is lost or stolen, it is useless in

the hands of an unauthorized person. ... [A]uthentication may be achieved by using more sophisticated technologies such as a biometric solution (e.g., fingerprint recognition)” (emphasis added)); Decl., 104.

Ludtke also discloses an alternate embodiment in which the POS “functionality of providing secure communication and transactions with the Transaction Privacy Clearing House (TPCH)” described above “can be integrated into the digital wallet directly.” Ludtke, 28:41-45. Thus, Ludtke also discloses communicating the device ID directly from the transaction device to the TPCH responsive to a “match” between the scan data and stored data. Decl., 105.

Second, Ludtke discloses sending the transaction device ID wirelessly. Decl., 106. More specifically, Ludtke discloses that “the TPCH is located at a secure location” and “embodied as a secure server.” Ludtke, 9:26-34. The TPCH receives incoming communications, including the transaction ID using an “incoming communications mechanism 605” using “wireless or cellular signals.” Ludtke, 9:35-42; Decl., 106.

Finally, Ludtke discloses that the TPCH is a trusted third-party possessing a list of legitimately integrated device ID codes. Decl., 107. As Ludtke explains, with respect to Figure 6, the TPCH is an entity separate from the parties to a transaction because it is distinct from the transaction device, the POS on which the user/transaction device is performing a transaction, and the “*external* retailers and

vendors” that complete the transaction. Ludtke, 9:35-39 (emphasis added), FIG. 6.

Indeed, as Ludtke explains, “[t]he incoming communications mechanism 605 and outgoing communications mechanism 610 are the means of communicating with *external* retailers and vendors, as well as the transaction device.” Ludtke, 9:36-39.

That the vendors and transaction device are “external” to the TPCCH confirms that the TPCCH is a third party, and not a party to the transaction itself.

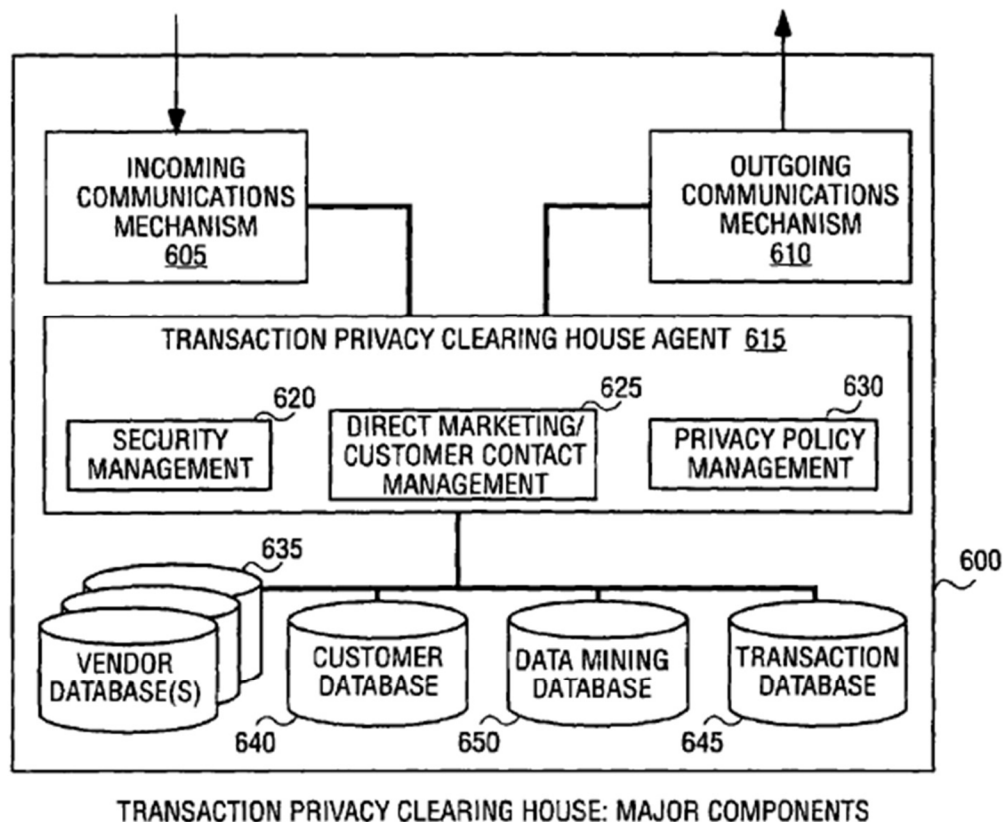


FIG. 6

Ludtke, FIG. 6.

This is consistent with Patent Owner's previous "agree[ment] that at a 'third-party trusted authority' is *an institution or entity that is outside of the multi-party system (user and application or vendor)* that is being authenticated" and the Board's construction that third-party trusted authority is a trusted authority that is an entity separate from the parties to the transaction," and one that is "separate from the principal parties to a transaction." Ex. 1007, 13-15 (emphases added). Indeed, the Board differentiated the prior art cited in the prior IPR2021-01447 because the purported third party authority was not a third party at all, stating "the DPC is the resource to be accessed, *but it is a party to the transaction, rather than a third party.*" Ex. 1007, 24.

Here, to the extent Patent Owner raises any argument that the TPCCH of Ludtke is similar to the mapping in the prior IPR, Patent Owner is wrong, particularly because Ludtke expressly identifies the TPCCH as external to the parties to the transaction, capable only of communication with the parties, as explained above. That the TPCCH 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. Moreover, Ludtke expressly discloses that the TPCCH "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" thus further confirming that the TPCCH is not the vendor/retailer, or

even the user's financial institution from which funds are withdrawn (not a principal party to the transaction, and therefore a third party). Ludtke, 29:43-46; Decl., 107-108.

Ludtke further discloses that the separation between the TPCCH, vendors, and the POS on which the user/transaction device is performing a transaction "ensures secure communications among the components internal to the TPCCH 600 and *the entities external to the TPCCH 600*" and "ensures that only authorized entities are allowed access to data and that only authorized transaction devices can execute transactions against a user's account," thereby allowing the TPCCH to function "as the middleman of the distribution channel." Ludtke, 7:44-48, 9:26-30, 9:52-59. Accordingly, the TPCCH is a trusted third party. Decl., 108.

Ludtke explains that the TPCCH can "maintain a copy" of "unique transaction device ID values" so that "whenever a transaction arrives with one of these values, the TPCCH knows *which transaction device*, and hence which user, the transaction it associated with." Ludtke 30:20-27. Thus, Ludtke discloses a TPCCH (trusted third-party authority) possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values include the device ID code. Decl., 109.

- i. **[1f]: “responsive to authentication of the one or more codes and the other data values by the agent, receiving an access message from the agent allowing the user access to an 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.”**

Ludtke discloses or renders obvious [1f]. Decl., 110-117.

Ludtke’s transaction device receives an indication of “approval of the transaction to be performed” from the TPOCH (receiving an access message from the agent allowing the user access to an application) after the codes are authenticated (responsive to authentication of the one or more codes and the other data values by the agent). Ludtke, 6:36-44, 29:5-23; Decl., 111.

After receiving the fingerprint recognition sample “to confirm [an] entire transaction and that the user is authorized,” the personal POS terminal “opens a secure communications session to the TPOCH, requesting a transaction” and “provides the transaction record that it received from the web browser *and the unique ID of the transaction device.*” Ludtke, 28:50-29:12 (emphasis added). “The TPOCH *uses the unique ID of the transaction device to process the transaction*” and “[a]fter validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction, the TPOCH *issues a transaction confirmation*” (access message) “*back to the personal POS terminal*”

where it is then reflected “back to the web browser and the transaction device” and displayed to the user. Ludtke, 29:10-23 (emphases added); Decl., 112.

Ludtke’s approval allows the user to access an application 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 because “[s]ecure distribution of physical (or electronic) content...is performed once the transaction is authorized”—that is, once the access message is sent “back to the *web browser*” webpage . Ludtke, 29:10-23, 29:29-30 (emphasis added); Decl., 113.

Ludtke’s transaction device is configured to access various types of “content” or “services.” Ludtke, 19:45-50 (explaining that the transaction device is “to be used for the initial set of services that the user requested during the registration process” and that “[o]nce the device has been initialized for secure transactions, additional services could be downloaded to the device.”). These services, as explained in the “Art Background” relate to “voice mail, *bank balances*, dialing cards, credit reports, paying for purchases, *depositing money*, *accessing stored messages*, *logging onto computers*, etc.” Ludtke, 1:22-31, 1:38-39 (emphases added); *see also* Ludtke, 18:52-55 (“existing financial accounts that will be accessed via this device [include] *credit/debit accounts*, savings/checking, loyalty cards, etc.” (emphasis added)). Decl., 114.

A POSITA would have understood that when the transaction device is

configured to access “stored messages” upon receiving an indication of “approval,” (access message) as described above, the transaction device accesses a file, as recited in [1f], because “stored messages” are files. Decl., 115. A POSITA would have also understood that when the transaction device is configured for “logging into [a] computer[.]” upon approval, the approval allows the user access to computer software on that computer and the computer itself (hardware), as recited in [1f]. Decl., 115. A POSITA would have also understood that a transaction device configured to access “bank balances” and “debit accounts” upon approval, at least suggests allowing the user access to an ATM machine, as recited in [1f], because ATMs allow users to access bank balances and debit accounts. Ludtke, 5:49-52 (“The transaction device may represent a single account such as a particular credit card, or it might represent multiple accounts such as a credit card, telephone card and debit card.”), 8:33-36 (“The user 240 uses the privacy card 205 to interface to the POS terminal in a manner similar to how credit cards and debit cards interface with POS terminals.”); Decl., 115. Thus, Ludtke discloses and renders obvious receiving an indication of approval (access message) allowing the user to access at least web sites, files, software, hardware, and an ATM (applications). Decl., 115.

Additionally, a POSITA would have been motivated and found it obvious to configure Ludtke’s transaction device to allow the user to access at least one of the

claimed applications (e.g., website, hardware, software, file, ATM) upon receiving the indication of approval (access message), because Ludtke expressly contemplates using the transaction device to conduct “secure transaction” services (Ludtke, 5:49-52, 8:32-35, 18:52-55, 19:45-50), which include access to computers (software/hardware), stored messages (a file), transactional websites, and debit accounts via a functional debit card (ATM). Ludtke, 1:22-31, 1:38-39, 5:49-52, 8:32-35, 18:52-55, 19:45-50; Decl., 116.

Such an implementation of Ludtke would have been within the purview of one skilled in the art and would have only required the use of known conventional components in accordance with their intended use. Decl., 117. Ludtke expressly discloses that the transaction device can be “adapt[ed] 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. The transaction device may also have wireless data transfer so it can detect the presence of a new service based on wireless data received.” Ludtke, 31:11-18. Accordingly, to the extent not expressly disclosed or suggested, a POSITA would have been motivated to configure Ludtke’s transaction device to access applications including an ATM, software, hardware, and a file, and had a reasonable expectation of success in doing so. Decl., 117.

2. Claim 2: “The method of claim 1, wherein the one or more codes and the other data values are transmitted to the agent over a network.”

Ludtke discloses claim 2. Decl., 118-119.

As explained for [1e], the device ID and other codes are sent to the external server TPCN over a wireless network connection using e.g., “wireless or cellular signals.” Ludtke, 9:35-42, 5:63-64 (“Furthermore, the privacy card may have a wireless communication mechanism for input and output.”); Decl., 119.

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

Ludtke discloses claim 4 because, as discussed in [1e], sending the transaction device ID (one or more codes and the other data values) indicates that the scan data matches the biometric data (the biometric verification was successful). *See* [1e]; Decl., 120-124. This is consistent with the ’730 patent, which explains that the act of sending the device ID indicates that biometric verification was successful. Ex. 1001, FIG. 6 (“Wirelessly Send Code Indicating Successful Verification of User”), 6:23-25 (“If the biometric verification of the user is successful, the key provides its code over the secure communications channel.”); Decl., 120.

As explained for [1c]-[1d], biometric information recognition is a security

measure “that limits access to the card 705 to authorized users.” Ludtke, 12:23-25, 4:62-5:1 (“The transaction device enhances security by authenticating the user of the card prior to usage such that if a card is lost or stolen, it is useless in the hands of an unauthorized person. . . . [A]uthentication may be achieved by using more sophisticated technologies such as a biometric solution (e.g., fingerprint recognition).”); Decl., 121.

And as explained for [1e], when the “personal POS terminal receives the transaction request, it communicates with the transaction device, *asking the transaction device to validate the user*, confirm that the user wants to make this transaction, and get the appropriate information for which account the user wants to use for payment.” Ludtke, 28:57-62 (emphasis added); [1e]. Upon receiving the request, the transaction device “validat[es] that the user interacting with the device is an authorized user” by prompting the user to “supply a fingerprint recognition sample” and receiving a fingerprint sample (biometric scan) from the “fingerprint recognition pad” in response to the prompt to generate the scan data. Ludtke, 14:33-42; [1c]; Decl., 122.

The transaction device user authentication block “captures the sample[], and carries out a recognition algorithm against the authorized samples that are stored in the user identity block.” Ludtke, 14:40-46. Then, “[i]f a match is found, the user is authorized to access the data and functionality of the device” and “validates that

the user is authorized” to conduct their transaction at the POS terminal. Ludtke, 14:40-46, 29:5-6; Decl., 123; *see also* Ludtke, 16:47-49 (explaining that the digital wallet also receives biometric scan data after prompting).

Thus, communicating the device ID code responsive to the fingerprint (or other biometric scan) recognition, as disclosed by Ludtke, indicates that the biometric verification was successful. Decl., 124.

4. Claim 5: “The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.”

Ludtke discloses claim 5 because, as explained for [1ai] and [1c], Ludtke’s stored fingerprint samples (biometric data) and received fingerprint sample (scan data) are both based on the authorized user’s fingerprint scan. Ludtke, 14:33-46; Decl., 125.

5. Claim 6: “The method of claim 1, further comprising: establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication”

Ludtke discloses claim 6 because, as explained for [1aiii], Ludtke discloses “establish[ing] a secure connection to a back-end system” prior to transferring (sending) the “access codes, PINs, etc.,” using a public key infrastructure. Ludtke, 37:39-45; Decl., 126.

6. Independent Claim 8

- a. [8preamble]: “An integrated device for verifying a user during authentication of the integrated device, comprising:”**

Ludtke discloses [8preamble] because, as explained for [1preamble], Ludtke discloses “a biometric device” (also called a transaction device), such as a privacy card and/or digital wallet (integrated device), for “enabling the authorized user to access private information over a voice network” (verifying a user during authentication). Ludtke, Abstract, 3:32-36; Decl., 127.

- b. [8ai]: “a memory stores biometric data of a user, and”**

Ludtke discloses [8ai] for the reasons explained for [1ai]. Decl., 128.

- c. [8aii]: “a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device, and”**

Ludtke discloses [8aii] for the reasons explained for [1aii]. Decl., 129.

- d. [8aiii]: “a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered;”**

Ludtke discloses [8aiii] for the reasons explained for [1aiii]. Decl., 130.

- e. [8b]: “wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;”**

Ludtke discloses [8b] for the reasons explained for [1b]. Decl., 131.

- f. **[8c]: “a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and the other data values includes the device ID code; and”**

Ludtke discloses [8c] for the reasons explained for [1c] and [1e]. Decl., 132-134.

As explained for [1c], the privacy card includes a user authentication block 777 (verification unit) for “validating that the user interacting with the device is an authorized user.” Ludtke, 14:33-40. In operation, “the user is prompted to supply a fingerprint recognition sample,” after which the “block captures the sample[] and carries out a recognition algorithm against the authorized samples that are stored in the user identity block. If a match is found, the user is authorized to access the data and functionality of the device.” Ludtke, 14:40-46; Decl., 133; *see also* Ludtke, 16:47-49 (explaining that the digital wallet also receives biometric scan data after prompting).

And as explained for [1e], the transaction device ID (one or more codes

from the plurality of codes and the other data values) is sent to a “single trusted” and “highly secured” TPOCH (third-party trusted authority) containing a “copy” of “unique transaction device ID[s]” (list of device ID codes uniquely identifying legitimate integrated devices) using e.g., “wireless or cellular signals” once the fingerprint match is identified. Ludtke, 3:40-43, 4:48-50, 5:63-64, 7:46-48, 9:26-30, 9:35-42, 9:52-59, 28:50-29:12, 30:23-27; Decl., 134.

- g. [8d]: “responsive to the agent authenticating the one or more codes and the other data values, a radio frequency communicator, receives an access message from the agent allowing the user access to an 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.”**

Ludtke discloses or renders obvious [8d] for the reasons explained for [1f]. Decl., 135-137.

As explained for [1f], the transaction device receives an indication of “approval of the transaction to be performed” from the TPOCH after the codes are authenticated, and the approval allows the user to access e.g., a computer (software/hardware), stored messages (a file), and/or debit accounts (ATM). Ludtke, 1:22-31, 1:38-39, 5:49-52, 8:32-35, 18:52-55, 19:45-50; Decl., 136. In one embodiment, the TPOCH “issues a transaction confirmation” (access message)

“back to the personal POS terminal” where it is then reflected “*back to the web browser and the transaction device*” and displayed to the user. Ludtke, 29:15-23 (emphases added). Alternatively, where the communication functions of the POS are integrated into the transaction device, the confirmation may be delivered to the transaction device. Ludtke, 28:41-45; Decl., 136.

Ludtke discloses that the transaction device uses a “wireless communication mechanism for input and output,” including for receiving “cellular signal” communication output from the TPC. Ludtke, 5:63-64, 9:39-42, 17:3-10, 33:46-49. Because Ludtke’s transaction device communicates using cellular technology, a POSITA would have understood that the wireless communication mechanism is a radio frequency communicator. Decl., 137.

7. Claim 9: “The integrated device of claim 8, wherein the one or more codes and the other data values are transmitted to the agent over a network.”

Ludtke discloses claim 9 for the reasons explained for claim 2. Decl., 138.

8. Claim 11: “The integrated device of claim 8, wherein the verifier comprises: an LED to be activated for requesting the biometric scan.”

Ludtke discloses or renders obvious claim 11 because Ludtke’s verification unit (verifier) includes a “high resolution color” or “black & white” “LCD screen” that is activated when the user “interacts with the device” for fingerprint

recognition. Ludtke, 11:37-41, 14:54-63, 16:53-56; Decl., 139-143.

Ludtke discloses that the “fingerprint recognition, on-card display technology” of the transaction device authentication block verification unit (verifier) “may be *enabled* via thin LCD technologies.” Ludtke, 11:37-41 (emphasis added). The LCD is configured such that when “the user interacts with the device” the LCD generates (displays) “the appropriate images.” Ludtke, 14:54-63. Moreover, “[w]hen the user has selected an account, *the transaction device asks the user to confirm the entire transaction and that the user is authorized, for example, by entering a PIN or providing a fingerprint recognition sample*” and “request[s] the user’s attention, either via audio *or video signals, or both.*” Ludtke, 28:63-29:4 (emphases added); Decl., 140.

A POSITA would have understood that an LCD that asks the user to “provid[e] a fingerprint recognition sample” using “video signals” and “appropriate images” does so using its display, which is conventionally backlit using an LED. Ludtke, 14:54-63, 28:63-29:4; Siegel, [0041] (“[M]ost LCD panels are backlit with fluorescent tubes or arrays of light-emitting diodes (LEDs) that are built into the sides or back of the panel.”); Ikegami, [0024], [0108], [0110], [0135], [0141], [0154], [0187] (describing an “authenticating apparatus” including “an instruction unit for prompting the person to be authenticated to input data” such as “biometrics information” and wherein the instruction unit prompts the user with “a

light emitting element such as an LED or the like.”); Decl., 141.

Thus, Ludtke discloses activating the LCD when a fingerprint scan (biometric scan) is needed (for requesting the biometric scan), and therefore at least suggests activating an LED as part of the process because LCDs typically use LEDs to backlight their display. Siegel, [0041]; Ikegami, [024], [0108], [0110], [0135], [0141], [0154], [0187]; Decl., 142.

To the extent it is disputed that Ludtke’s LCD is at least suggestive of an LED, a POSITA would have been motivated and found it obvious to backlight Ludtke’s LCD using LEDs because “liquid crystals do not emit light” and “most LCD panels are backlit with fluorescent tubes or arrays of light-emitting diodes (LEDs) that are built into the sides or back of the panel” to achieve the desired lighting. Siegel, [0041]; Decl., 143. A POSITA would have had a reasonable expectation of success in backlighting the LCD with LEDs since such a modification would have only required the use of routine components (LEDs) in accordance with their known and conventional use (backlighting an LCD) as taught by Siegel, and further because it was known in the art to use LEDs to prompt a user’s attention for the purposes of inputting biometric information in an authentication device. Ikegami, [0024], [0108], [0110], [0135], [0141], [0154], [0187]; Decl., 143.

9. Independent Claim 12

- a. [12preamble]: “A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:”**

Ludtke discloses [12preamble] because, as explained for [1e], Ludtke discloses a method of authenticating a verified user using a POS terminal (a device with a computer processor to execute steps). Ludtke, 28:57-29:20; Decl., 144-146.

As illustrated in Figure 14, Ludtke’s POS terminal includes a processor configured to execute software, including “internal driver software that executes locally to drive the wireless transceiver, software to store incoming data into memory and to control input/output to a computer (e.g., PC) coupled to the personal POS terminal,” “[h]ost application software,” and “user application” software stored on the POS terminal. Ludtke, 25:34-58, FIG. 14. “The personal POS terminal may also include software that is configured to communicate with the PC and the eCommerce system to perform the transaction.” Ludtke, 26:23-26; Decl., 145.

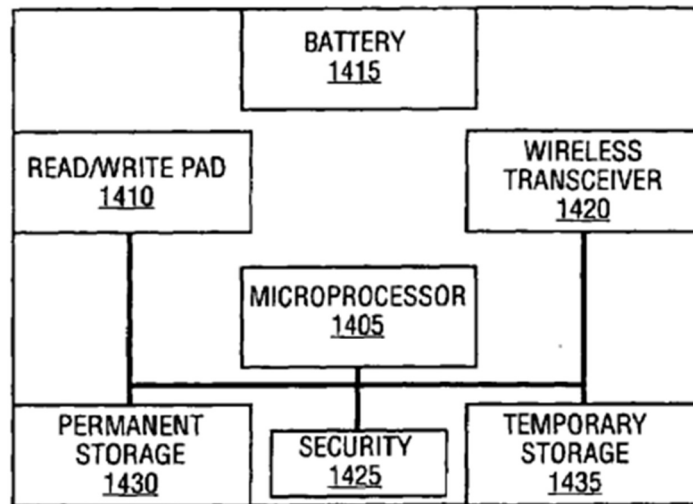


DIAGRAM OF THE MAJOR COMPONENTS OF THE
PERSONAL POS, SHOWING THE DATA/ADDRESS
BUS INTERCONNECT

FIG. 14

Ludtke, FIG. 14.

Executing the software causes the steps recited in each of [12a]-[12d] to be executed, as explained below. Decl., 146.

- b. [12a]: “receiving one or more codes from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and the other data values comprises the device ID code uniquely identifying the integrated device and a secret decryption value associated with a biometrically verified user, the device ID code being registered with an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices”

Ludtke discloses [12a] because the POS terminal receives the transaction

device's device ID, as explained for [1e]. Decl., 147-151.

When Ludtke's "personal POS terminal receives the transaction request, it communicates with the transaction device, *asking the transaction device to validate the user*, confirm that the user wants to make this transaction, and get the appropriate information for which account the user wants to use for payment." Ludtke, 28:57-62 (emphasis added). The POS terminal then receives the validating information, including the transaction device's transaction device ID, so that it can "provide[] the transaction record that it received from the web browser *and the unique ID of the transaction device*" to the TPC, as explained for [1e]. Ludtke, 28:50-29:12 (emphasis added). The transaction device ID uniquely identifies the transaction device and is one of one or more codes from a plurality of codes and other data values (such as bar codes and magnetic strip information), as also explained for [1aii]. Ludtke, 3:49-53; Decl., 148-149. The transaction device ID is also registered with a TPC (third-party trusted authority) which maintains a "copy" of transaction device IDs as explained for [1e]. Ludtke, 30:23-27; Decl., 149. Thus, Ludtke discloses receiving *one* or more codes from a plurality of codes and other data values including a device ID code.

Ludtke also discloses that the transaction devices include a plurality of codes and the other data values, including a secret decryption value configured as a public decryption key or private encryption key, as discussed in [1aiii]. The secret

decryption value may also be received during the secure communication exchange between the transaction device and back-end system associated with the POS terminal. Ludtke, 37:39-45, FIGS. 5A-5B, 17; Decl., 150.

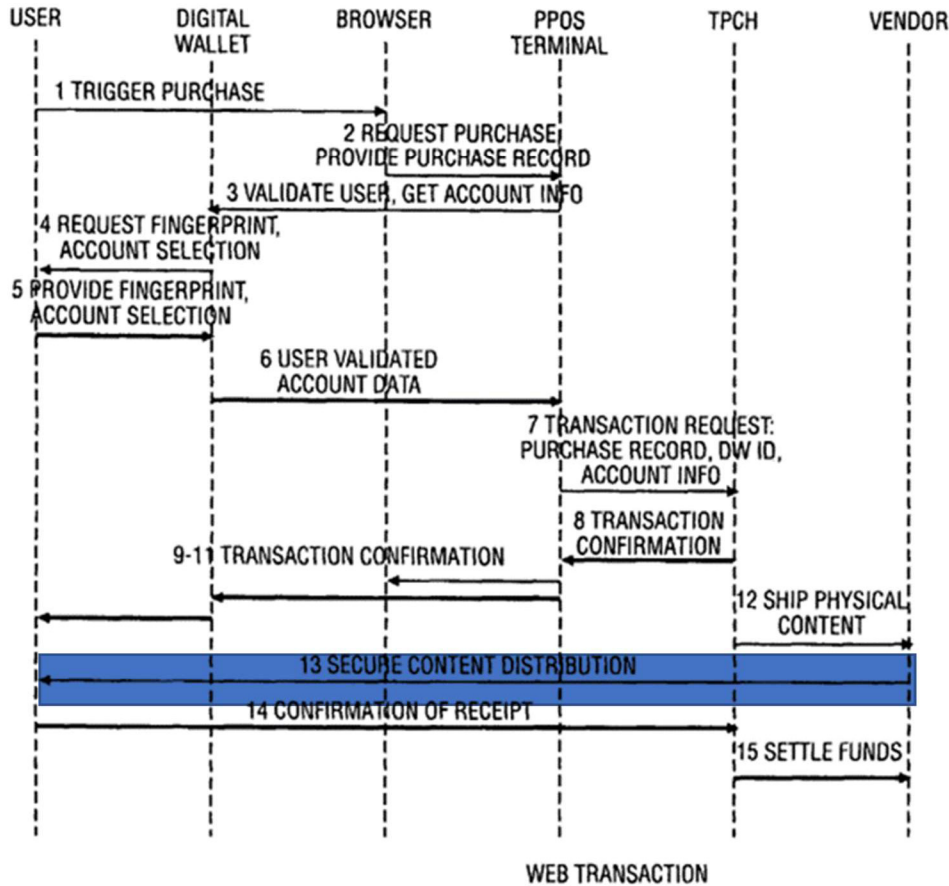


FIG. 17

Ludtke, FIG. 17 (annotated).

For example, when the transaction device generates one or passwords associated with the data to be transmitted, the device “choose[s] the PKI key pairs associated with those passwords” and “inform[s] the back-end system about this key/ password relationship, passing a ‘security mechanism public key’ and

password to the back-end.” Ludtke, 39:7-12. The back-end then “utilizes the corresponding ‘security mechanism public key’ to decrypt and authenticate the password.” Ludtke, 39:16-18. The secret decryption value is also associated with the verified user of the transaction device, as discussed in [1aiii]. Decl., 151

c. [12b]: “requesting authentication of the one or more codes and the other data values by the agent, wherein the authentication determines whether the one or more codes and the other data values are legitimate;”

Ludtke discloses [12b] for the reasons explained for [1e]. Decl., 152-153.

After receiving a fingerprint recognition sample “to confirm [an] entire transaction and that the user is authorized,” Ludtke’s personal POS terminal “opens a secure communications session to the TPCB, requesting a transaction” to request authentication of the transaction device ID (one or more codes) and “provides the transaction record that it received from the web browser and the unique ID of the transaction device. Ludtke, 28:50-29:12. The authentication “validat[es] that the transaction device is in good standing and that the selected account has sufficient funds for the transaction” and thus determines whether the transaction device ID is legitimate Ludtke, 29:15-18; Decl., 153.

d. [12c]: “receiving an access message from the agent; and;”

Ludtke discloses [12c] for the reasons explained for [1f]. Decl., 154-155.

After the transaction device ID is authenticated as discussed in [12b], “the TPCB

issues a transaction confirmation” (access message) “*back to the personal POS terminal*” where it is then reflected “back to the web browser and the transaction device” and displayed to the user. Ludtke, 29:15-23 (emphasis added); Decl., 155.

- e. **[12d]: “in response to a positive access message, allowing the biometrically verified user access to an 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.”**

Ludtke discloses or renders obvious [12d] for the reasons explained for [1f]. Decl., 156.

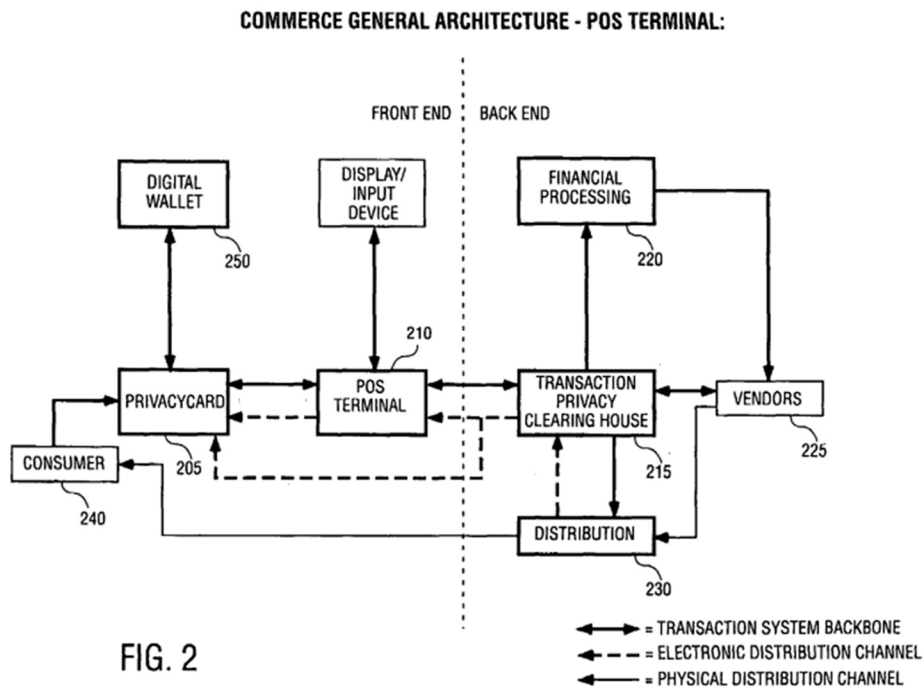
- 10. **Claim 14: “The method of claim 12, further comprising: establishing a secure communications channel with a biometric key, wherein the one or more codes and the other data values associated with the biometrically verified user is received from the biometric key.**

Ludtke discloses claim 14 for the same reasons discussed for claim 6. Decl., 157. Although claim 6 does not recite a biometric key, claim 6 is written in the form of a method performed by the integrated device. Ludtke’s transaction device (integrated device) of claim 1 includes a biometric device (key). Ludtke, Abstract, 3:32-36; Decl., 157. Therefore, the secure communication channel of Ludtke is formed between the biometric key and the POS terminal, as claimed. Decl., 157.

11. Independent claim 15

a. [15preamble]: “A system, comprising:”

Ludtke discloses [15preamble] because, as illustrated in Figure 2, Ludtke discloses a system. Ludtke, Abstract, FIG. 2; Decl., 158-159. Ludtke’s system includes the elements recited in [15ai]-[15c], such as a biometric integrated device (privacy card) and a POS terminal (authentication unit), for communication with a TPC (third-party trusted authority) for reasons explained below. Decl., 159.



Ludtke, FIG. 2.

b. [15ai]: “a biometric key stores biometric data of a user”

Ludtke discloses [15ai] for the reasons explained for [1ai]. Decl., 160-161.

Ludtke’s transaction device (integrated device) of claim 1 is a biometric

device (key). Ludtke, Abstract, 3:32-36; Decl., 161.

- c. **[15aii]: “and a plurality of codes and other data values comprising a device ID code uniquely identifying the biometric key”**

Ludtke discloses [15aii] for the reasons explained for [1aii]. Decl., 162.

- d. **[15aiii]: “and a secret decryption value in a tamper proof format written to a storage element on the biometric key that is unable to be subsequently altered,”**

Ludtke discloses [15aiii] for the reasons explained for [1aiii]. Decl., 163.

- e. **[15aiv]: “and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending, one or more codes from the plurality of codes and other data values wherein the one or more codes and the other data values include the device ID code,”**

Ludtke discloses [15aiv] for the reasons explained for [1e]. Decl., 164.

- f. **[15av]: “and the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition; and”**

Ludtke discloses [15av] for the reasons explained for [1b]. Decl., 165.

- g. **[15b]: “an authentication unit receives the plurality of codes and the other data values and send the plurality of codes and the other data values to agent for authentication to determine whether the one or more codes and the other data values are legitimate,**

wherein the agent is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices,”

Ludtke discloses [15b] for the reasons explained for [12a]-[12b]. Decl., 166-169.

After receiving a fingerprint recognition sample “*to confirm [an] entire transaction and that the user is authorized,*” a personal POS terminal (an authentication unit) “opens a secure communications session to the TPCCH, requesting a transaction” and “provides the transaction record that it received from the web browser *and the unique ID of the transaction device.*” Ludtke, 28:50-29:12 (emphases added); Decl., 167.

As explained for [12b], Ludtke’s personal POS terminal “opens a secure communications session to the TPCCH, requesting a transaction” to request authentication of the transaction device ID (one or more codes) and “provides the transaction record that it received from the web browser and the unique ID of the transaction device.” Ludtke, 28:50-29:12. The authentication “validat[es] that the transaction device is in good standing and that the selected account has sufficient funds for the transaction” and thus determines whether the transaction device ID is legitimate. Ludtke, 29:15-18; Decl., 168. The transaction device ID is also registered with the TPCCH (third-party trusted authority) which maintains a “copy” of transaction device IDs as explained for [1e]. Ludtke 30:23-27; Decl., 169. For

example, Ludtke indicates that “the TPOCH maintains secure information linking a user to a particular *transaction card identification* and interfaces among the transaction device, vendor and any financial systems to provide the user authorization to perform and complete a transaction” Ludtke, 11:8-12 (emphasis added). And Ludtke indicates that “[t]he TPOCH agent 615 handles system management and policy control, and forms the core functionality of the TPOCH 600. In one embodiment, within the entire system, there is one clearing house agent, which resides permanently at the clearing house. Among the responsibilities handled by the agent include internal system management functions such as data mining, financial settlement and allocation of payments to internal and external accounts, and registration of new users joining the system.” Ludtke, 9:43-51. Since the TPOCH maintains a transaction device ID for each user it handles, and since it can register new users, a POSITA would have understood that the TPOCH possesses “a list of device ID codes uniquely identifying legitimate integrated devices.” Decl., 169.

- h. [15c]: “and responsive to the device ID code being authenticated, the authentication unit receiving an access message from the agent allowing the user to access an 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.”**

Ludtke discloses or renders obvious [15c] for the reasons explained for [1f].

Decl., 170-171.

After the transaction device ID is authenticated as discussed in [15b], the TPOCH *issues a transaction confirmation*” (access message) “*back to the personal POS terminal*” (authentication unit) where it is then reflected “back to the web browser and the transaction device” and displayed to the user. Ludtke, 29:15-23 (emphases added); Decl., 171.

- 12. Claim 16: “The system of claim 15, wherein the biometric key receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate the scan data.”**

Ludtke discloses claim 16 because, as explained for [1c] and [1e], Ludtke’s transaction device (which includes a biometric key) receives a validation request from the POS terminal (authentication request from the authentication unit) and prompts the user to scan their fingerprint (requests a biometric scan) to validate the

user. Decl., 172-174.

When the “personal POS terminal receives the transaction request, it communicates with the transaction device, *asking the transaction device to validate the user*, confirm that the user wants to make this transaction, and get the appropriate information for which account the user wants to use for payment.” Ludtke, 28:57-62 (emphasis added); [1e]. Upon receiving the request, Ludtke’s transaction device “validat[es] that the user interacting with the device is an authorized user” by prompting the user to “supply a fingerprint recognition sample” and receiving a fingerprint sample (biometric scan) from the “fingerprint recognition pad” in response to the prompt to generate the scan data. Ludtke, 14:33-42; [1c]. Ludtke’s transaction device’s user authentication block “captures the sample[] and carries out a recognition algorithm against the authorized samples that are stored in the user identity block.” Ludtke, 14:40-46; Decl., 173.

Then, “[i]f a match is found, the user is authorized to access the data and functionality of the device” and “validates that the user is authorized” to conduct their transaction at the POS terminal. Ludtke, 14:40-46; 29:5-6; Decl., 174; *see also* Ludtke, 16:47-49 (explaining that the digital wallet also receives biometric scan data after prompting).

13. Claim 17: “The system of claim 15, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the one or more codes and the other data values.”

Ludtke discloses or renders obvious claim 17. Decl., 175-179.

As explained for claim 16, Ludtke’s “user is prompted to supply a fingerprint recognition sample,” after which the “block captures the sample[] and carries out a recognition algorithm against the authorized samples that are stored in the user identity block” to determine “if . . . the user is authorized to access the data and functionality of the device” and whether to “validate[] that the user is authorized” to conduct the transaction at the POS terminal. Ludtke, 14:40-46, 29:5-6; Decl., 176.

A POSITA would have understood that the transaction device does not send the one or more codes if it cannot verify that the scan data is from the user because the biometric scan data “is used as a security mechanism that limits access to the card 705 to authorized users” and the user is only authorized/validated “[i]f a match is found” between the scan data and “stored” “authorized samples.” Ludtke, 12:23-25, 14:40-46; Decl., 177. Indeed, a transaction device that cannot be authenticated/validated as being from the user is “useless.” Ludtke, 4:62-65, 66-5:1; *see also* Ludtke, 39:50-56 (“At 3104 the DW checks to see if a fingerprint has been detected. If not then the DW loops back looking for a fingerprint. If a

fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. *If a match does not occur, then at 3110 an error message is output* and the DW returns to checking to see if a fingerprint has been detected 3104.”) (emphasis added); Decl., 177.

Additionally, a POSITA would have been motivated and found it obvious to configure Ludtke’s transaction device to not send the one or more codes and other data values if the transaction device (biometric key) cannot verify the scan data as being from the user, to prevent unauthorized use of the transaction device when “lost or stolen.” Ludtke, 4:62-5:1, 18:23-31; Decl., 178.

Such a modification would have been within the purview of one skilled in the art, and would have only required the use of known conventional components in accordance with their known use—for example, configuring Ludtke’s authorization block to output an “error” or “authentication failure” message upon failing to detect a fingerprint match, as was well known in the art. *See e.g.*, Ludtke, 39:50-56; Kon, [0007]-[0010] (describing a “a conventional process of identifying a person using biometric information” wherein a comparator transmits an “authentication failure message” “[i]f it is determined that the input data does not match with the registered information.”); Decl., 179. Accordingly, a POSITA would have been motivated to make such a modification and had a reasonable expectation of success in doing so. Decl., 179.

VI. Ground 2: Claims 3, 10, and 13 are Obvious Over Ludtke and Kon.

Dependent claims 3, 10, and 13 require an age or birthdate verification.

While Ludtke does not expressly disclose age or birthdate verification, Kon does, and it would have been obvious to add Kon's age and birthdate verification to Ludtke. Decl., 180.

A. Kon

Kon, filed August 31, 2001 and published April 18, 2002, is prior art under 35 U.S.C. § 102(b). Kon, cover page.

Kon discloses authenticating a user transaction “in response to a request from a user device.” Kon, [0174]. Like Ludtke, Kon uses the user's biometric information, which includes “fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information,” and “the ID of a user device” (device ID) to authorize a user and their corresponding device to conduct a transaction. Kon, [0060], [0174], [0178], [0194] (explaining that a public key certificate (“PKC”) includes the ID of the user device), [0226]-[0229] (explaining that a person identification certificate (“IDC”) includes the PKC).

Kon's authenticating information is stored in the IDC, illustrated in Figure 5. Kon, FIG. 5, [0194] (explaining that the PKC “Subject” field includes the ID of the user device), [0217] [0226]-[0229] (explaining that the IDC includes “Subject

Template Info” where “data representing biometric information such as a fingerprint of the user is stored,” and “Subject PKC info” containing the PKC information).

FIG. 5

	Item	Description
Indispensable Items	Version	Version
	Serial Number	Identification Number
	signature algorithm Identifier	Signature algorithm
	algorithm parameters	Algorithm Parameters
	Issuer	Name of the identification authority (in the form of a distinguished name)
	Validity notBefore notAfter	Period during which the certificate is valid Start date Expiration date
Extended Items	Subject	Name of the subject to be certificated (in a DN form)
	subject Template Info	Template information
	encrypt Type	• encrypt Type
	encrypt Unique ID	• The unique ID or the certificate number of a public key certificate used for encryption
	encryption Algorithm parameter	• Algorithm
	validity	• parameter
	subject Template Source	• Validity period (start date, expiration date)
	subject Template	• Type of the template
	Subject PKC info	• Template
	subject PKC serial Number	Information about the public key certificate of the subject
	subject PKC Unique ID	• Certificate number of the subject public key certificate
	Issuer Unique ID	• Unique ID of the subject of the subject public key certificate
	Subject Unique ID	Unique ID of the issuer
	Public Key Certificate	Unique ID of the subject
	Issuer Alt Name	Public key certificate
	subject Directory Attributes	Alternative name of the issuer
		Personal information (encrypted as required) information used to authenticate subject Age, sex, etc.

Kon, FIG. 5 (annotated, excerpted).

Kon further discloses that the user’s personal information, including the user’s age, is registered for incorporation in the IDC (e.g., in the “Extended” field section) in association with the device ID (located in the Subject field). Kon,

[0194] (“Subject is a field in which the name of a subject or a user is described.

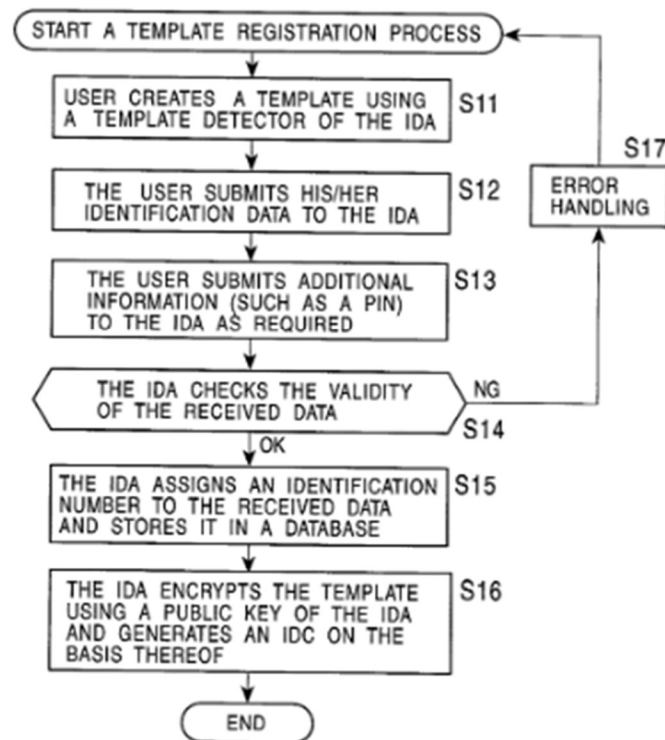
More specifically, for example, *the ID of a user device* or the ID of a subject which supplies services is described.” (emphasis added)), [0234] (“[A]n arbitrary attribute of [a] user, such as an *age*, sex, address, [or] telephone number, is encrypted *as required to identify the user*.” (emphases added)), [0241] (“The person identification certificate (IDC) described above includes information (template information) used to identify a person. An example of template information is biometric information. . . . Personal identification information other than biometric information is also usable. Specific examples of such personal identification information includes a seal, *a passport, a driver’s license*, and a card.” (emphasis added)), [0264] (“To effectively *register* a person identification certificate (IDC), a person to be certified with a person identification certificate (IDC) first presents sampling information to register his/her template.” (emphasis added)), [0265] (“FIG. 9 illustrates a flow in terms of registration of a template and creation of an IDC. Registration of a template is performed on the basis of information (sampling information) acquired using an apparatus capable of acquiring personal information in one of the various forms described earlier.”), FIGS. 5 and 9.

FIG. 5

	Item	Description
Indispensable Items	Version	Version
	Serial Number	Identification Number
	signature algorithm Identifier algorithm parameters	Signature algorithm Algorithm Parameters
	Issuer	Name of the identification authority (in the form of a distinguished name)
	Validity notBefore notAfter	Period during which the certificate is valid Start date Expiration date
	Subject	Name of the subject to be certificated (in a DN form)
Extended Items	subject Template Info encrypt Type encrypt Unique ID encryption Algorithm parameter validity subject Template Source subject Template	Template information • encrypt Type • The unique ID or the certificate number of a public key certificate used for encryption • Algorithm • parameter • Validity period (start date, expiration date) • Type of the template • Template
	Subject PKC info	Information about the public key certificate of the subject
	subject PKC serial Number	• Certificate number of the subject public key certificate
	subject PKC Unique ID	• Unique ID of the subject of the subject public key certificate
	Issuer Unique ID	Unique ID of the issuer
	Subject Unique ID	Unique ID of the subject
	Public Key Certificate	Public key certificate
	Issuer Alt Name	Alternative name of the issuer
	subject Directory Attributes	Personal information (encrypted as required) information used to authenticate subject Age, sex, etc.

Kon, FIG. 5 (annotated, excerpted) (illustrating registered user information).

FIG. 9



Kon, FIG. 9 (illustrating process for registering user identification information).

Kon is analogous art to the '730 patent because it is directed to the same technical field: user authentication methods and systems. *Compare* Ex. 1001, 1:16-19, *with* Kon, [0020], [0034]; Decl., 65-69.

B. Claims

- Claim 3: “The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code.”**

Ludtke in combination with Kon renders obvious claim 3. Decl., 181-186.

Kon discloses registering and storing a user’s personal information, including the user’s age, in association with the user device’s device ID—the

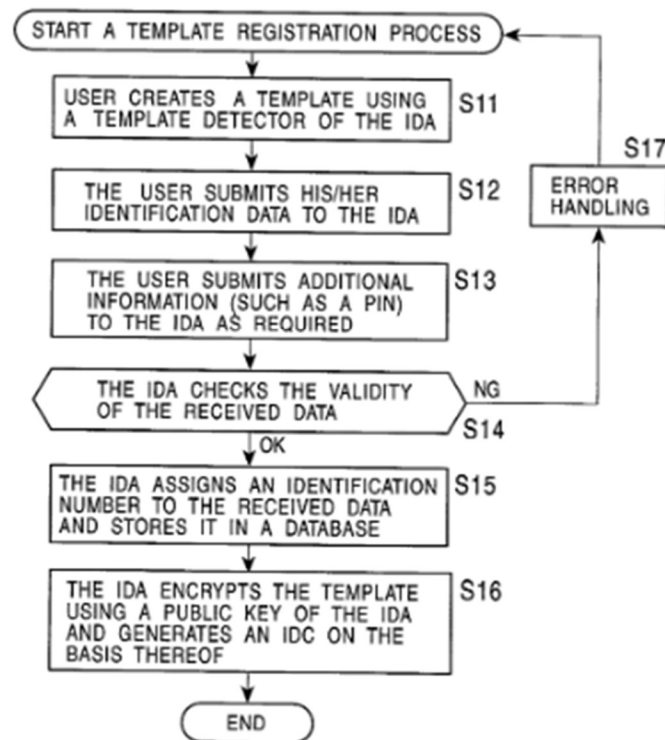
user's device ID is stored in a "Subject" field and the user's age is stored in a "Directory Attribute" field of a registered IDC certificate. Kon, [0194] ("Subject is a field in which the name of a subject or a user is described. . . , for example, *the ID of a user device*" (emphasis added)), [0234] ("[A]n arbitrary attribute of a[] user, such as an age, sex, address, [or] telephone number, is encrypted as required to identify the user." (emphases added)), [0265] ("FIG. 9 illustrates a flow in terms of registration of a template and creation of an IDC. Registration of a template is performed on the basis of information (sampling information) acquired using an apparatus capable of acquiring personal information in one of the various forms described earlier." (emphasis added)), FIGS. 5, 9; Decl., 182.

FIG. 5

	Item	Description
Indispensable Items	Version	Version
	Serial Number	Identification Number
	signature algorithm Identifier	Signature algorithm
	algorithm parameters	Algorithm Parameters
	Issuer	Name of the identification authority (in the form of a distinguished name)
	Validity notBefore notAfter	Period during which the certificate is valid Start date Expiration date
Extended Items	Subject	Name of the subject to be certificated (in a DN form)
	subject Template Info	Template information
	encrypt Type	• encrypt Type
	encrypt Unique ID	• The unique ID or the certificate number of a public key certificate used for encryption
	encryption Algorithm parameter	• Algorithm • parameter
	validity	• Validity period (start date, expiration date)
	subject Template Source	• Type of the template
	subject Template	• Template
	Subject PKC info	Information about the public key certificate of the subject
	subject PKC serial Number	• Certificate number of the subject public key certificate
	subject PKC Unique ID	• Unique ID of the subject of the subject public key certificate
	Issuer Unique ID	Unique ID of the issuer
	Subject Unique ID	Unique ID of the subject
	Public Key Certificate	Public key certificate
	Issuer Alt Name	Alternative name of the issuer
	subject Directory Attributes	Personal information (encrypted as required) information used to authenticate subject Age, sex, etc.

Kon, FIG. 5 (annotated, excerpted) (illustrating registered user information).

FIG. 9



Kon, FIG. 9 (illustrating process for registering user identification information).

As illustrated in Figure 9, user identification registration includes submitting, by a user, their identifying information (e.g., age) (step S12), and validating (verifying) the received information (step S14) before storing it in a database. Kon, [0265]-[0266], FIG.9. Documentation corroborating, i.e., verifying, the user's age may be supplied, including the user's passport or driver's license. Kon, [0241] ("The person identification certificate (IDC) described above includes information (template information) used to identify a person . . . Specific examples of such personal identification information include[] a seal, a *passport*, a *driver's license*, and a card." (emphasis added)). Thus, Kon discloses registering the user's

age verification in association with the user's device ID. Decl., 183.

The user's age, like the biometric information, provides another data point for identifying the user (Kon, [0241]); thus, a POSITA would have understood the benefit of using age as an identifying data point for authentication. Indeed, a POSITA would have considered age to be an especially useful identifier where, for example, a service or transaction implicates an age minimum (e.g., purchasing alcohol, cigarettes, or other age-restricted shopping content). Decl., 184-185 (citing Ex. 1015, [0005] ("As particular types of information or images contained in this uncontrolled information collection may not be suitable for certain users, it may be desirable to selectively restrict access to WWW resources."), [0078] (noting that if an account is designated to a child, it may be restricted from accessing "age-restricted shopping content" or require verification "that the associated account can access such shopping content"), [0082] (describing the need to control access to certain services, and explaining that age may be used to restrict user access), FIG. 14 (showing a user interface for accessing age-restricted shopping content)).

Accordingly, a POSITA would have been motivated and found it obvious to register the user's age, as taught by Kon, in association with Ludtke's device ID to facilitate age-prohibitive transactions. Decl., 186 (citing Ex. 1015).

2. **Claim 10: “The integrated device of claim 9, wherein an age verification is registered in association with the device ID code.”**

Ludtke in view of Kon renders obvious claim 10 for the reasons explained for claim 3. Decl., 187.

3. **Claim 13: “The method of claim 12, further comprising: registering a date of birth or age with the agent.”**

Ludtke in view of Kon renders obvious claim 13 for the reasons explained for claim 3. Decl., 188.

VII. Discretionary Denial Is Not Warranted

A. Discretionary Denial Is Not Warranted Under *Fintiv*

In *Apple Inc. v. Fintiv, Inc.*, the Board enumerated six factors to determine whether a petition should be discretionarily denied institution under §314(a). IPR2020-00019, Paper 11 at 2-3 (PTAB Mar. 20, 2020) (precedential) (“*Fintiv*”). In June 2022, the USPTO issued updated discretionary denial guidance in view of the *Fintiv* factors and expressly noted that ***the PTAB will not discretionarily deny institution if Petitioner presents a Sotera stipulation.*** Memorandum, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (USPTO June 21, 2022) (“Director’s Guidance”), 3, 7-8. Here, Petitioner has eliminated any risk of duplicated effort by voluntarily presenting a *Sotera* stipulation to Patent Owner. Ex-1024; *Sotera*

Wireless, Inc. v. Masimo Corp., Case IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020). For at least this reason, the Board should not discretionarily deny this petition.

**B. Discretionary Denial Is Not Warranted Under
*General Plastics***

The *General Plastic* factors weigh in favor of institution. *Gen. Plastic Indus. Co. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 (PTAB Sept. 6, 2017).

IPR2021-01444 (“the Samsung IPR”) does not preclude institution because Petitioner was not a party to the Samsung IPR and does not have a “significant relationship” with Samsung. This IPR relies on Grounds that were not presented in the Samsung IPR and was diligently prepared by Petitioner after Patent Owner filed a complaint in the Western District of Texas accusing Petitioner of infringing the ’730 patent in May 2023.

Factor 1 favors institution. Petitioner was not a party to the Samsung IPR and Petitioner does not have a “significant relationship” with Samsung.

Factors 2 and 5 have limited relevance or favor institution. Petitioner was not a party to the Samsung IPR, and was not aware of Patent Owner’s infringement allegations at the time of the Samsung IPR, which was filed on August 26, 2021, nearly two years before Patent Owner filed its complaint against Petitioner. IPR2021-01444, Paper 2. Petitioner had no reason to perform any prior art searches when the Samsung IPR was filed and did not perform any prior art

searches at that time. Nor did Petitioner have reason to challenge the '730 patent until Patent Owner alleged infringement in the district court.

Factor 3 favors institution. This Petition raises grounds relying on prior art that was not relied on in the Samsung IPR. There is no evidence of road mapping, and the mere fact that the preliminary patent owner response and decision denying institution of the Samsung IPR issued more than one year before the filing of this petition, is insufficient to establish otherwise.

Factor 4 favors institution. Petitioner conducted prior art searching and diligently prepared to file the instant petition shortly after receiving Patent Owner's allegations of infringement in the district court.

Factors 6-7 favor institution. The merits of this petition are strong, asserting obviousness grounds based on art not considered during prosecution and not previously presented to the Board. There is significant value for the Board to consider the invalidity grounds in this petition "to improve patent quality and restore confidence in the presumption of validity that comes with issued patents." *Code200, UAB v. Bright Data, Ltd.*, IPR2022-00861, Paper 18, 5 (PTAB Aug. 23, 2022) (citations omitted). Furthermore, because the Samsung petition was not instituted, a decision granting institution of this IPR would not hinder the Board's ability to issue a final determination not later than one year after granting such a decision.

C. Discretionary Denial is Not Warranted under § 325(d).

Neither Ludtke nor Kon were considered by the Examiner during prosecution or in the earlier-filed IPR. *See generally* Ex. 1002; Section VII.B, *supra*. Ludtke is currently cited in an *ex parte* reexamination request challenging the '730 patent, but in combination with various references that are not relied on in the instant petition:

SNQ 1: Ludtke in combination with Okereke renders obvious claims 1-2, 4-9, 11-12, and 14-17 under 35 U.S.C. §§ 102 (a) and (e) and 35 U.S.C. § 103;

SNQ 2: Ludtke in combination with Okereke and Robinson renders obvious claims 3, 10, and 13 under 35 U.S.C. § 102 (a) and (e) and 35 U.S.C. § 103;

SNQ 3: Ludtke in combination with Scott renders obvious claims 1-2, 4-9, 11-12, and 14-17 under 35 U.S.C. § 102 (b) and (e) and 35 U.S.C. § 103; and

SNQ 4: Ludtke in combination with Scott and Robinson renders obvious claims 3, 10, and 13 under 35 U.S.C. (a), (b), and (e) and 35 U.S.C. § 103.

Ex. 1011, 26.

Although the pending *ex parte* reexamination was filed on June 6, 2022, no rejection or action on the merits has issued. Thus, the Office has not yet substantively applied the cited prior art to the claims of the '730 patent.

Moreover, Patent Owner's Petition to the Director Under 1.181(a)(2) to Exercise Her Discretion Under § 325(d) and its respective request for rehearing on the same, were denied on January 3, 2024. The Office found that requester's

grounds based on Ludtke do not warrant denial under § 325(d) and confirmed that Ludtke raised substantial new questions of patentability that should be considered. Ex. 1020, 1021. That same reasoning applies even more so here where, unlike in the pending *ex parte reexamination*, Petitioner relies on Ludtke in a single reference obviousness challenge and in combination with new references. Ludtke presents a new and meritorious challenge to the claims of the '730 patent, and there is no basis for denial under § 325(d).

Additionally, Petitioner submits that the evidence and facts presented in the Petition warrant reconsideration of the prior art. Petitioner presents testimony from Mr. Gray, not reexamination expert Dr. Andrew Wolfe. Mr. Gray's declaration relates to grounds not previously presented in the reexamination and is not based on the opinions of Dr. Wolfe. If this proceeding is instituted, Mr. Gray, unlike Dr. Wolfe, will be subject to cross-examination—allowing the Board further opportunity to reach an accurate conclusion on the validity of the challenged claims over the prior art.

Petitioner further interprets the Ludtke reference in a new light that is materially different than the one articulated in the reexamination request. For example, the Petition asserts that Ludtke alone discloses or suggests all limitations of the challenged independent claims of the '730 patent; whereas the reexamination request states that “Ludtke does not explicitly disclose” “secret

information” (Ex. 1011, 47) or “transaction device information” (Ex. 1011, 48).

Requestor relies on secondary references for these limitations, and in doing so overlooks Ludtke’s express disclosure, teaching, and suggestion of these claim elements, as explained in this Petition. *See e.g.*, Sections V.B.1.c and V.B.1.d.

Finally, as 35 U.S.C. § 325(d) is discretionary, regardless of the *Advanced Bionics* factors, discretionary denial of this Petition in view of the pending *ex parte* reexamination is improper because Petitioner here has been accused of infringing the ’730 patent and should be entitled to challenge the claims asserted against it.

VIII. Mandatory Notices

A. Real Parties-in-Interest Under 37 C.F.R. § 42.8(b)(1)

Microsoft Corporation is the real party-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

To the best of Petitioner’s knowledge, the ’730 patent is/was involved in the following district court litigations/proceedings:

Name	Number	Court	Filed
<i>Microsoft Corp v. Proxense, LLC</i>	IPR2024-00775	PTAB	Apr. 19, 2024
<i>Google LLC v Proxense, LLC</i>	IPR2024-00232	PTAB	Jan. 17, 2024
<i>Proxense, LLC v. Apple, Inc</i>	6-24-cv-00143	WDTX	Mar. 18, 2024
<i>Proxense, LLC v. Microsoft Corp.</i>	6:23-cv-00319	WDTX	May 2, 2023
<i>Proxense, LLC v. Google LLC</i>	6:23-cv-00320	WDTX	May 2, 2023

<i>Samsung Electronics America, Inc. v. Proxense, LLC</i>	IPR2021-01444	PTAB	Aug. 26, 2021
<i>Proxense, LLC v. Samsung Electronics Co., Ltd.</i>	6:21-cv-00210	WDTX	Mar. 5, 2021
<i>In re Proxense, LLC</i>	90/015,052	USPTO	June 8, 2022

C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Lead Counsel	Backup counsel
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email: IPR42342-0136IP2@fr.com	Roberto J. Devoto, Reg. No. 55,108 Usman Khan, Reg. No. 70,439 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 PTABInbound@fr.com

D. Service Information Under 37 C.F.R. § 42.8(b)(4)

Please address all correspondence and service to the address listed above.

Petitioner consents to electronic service by email at IPR42342-0136IP2@fr.com (referencing No. 42342-0136IP2 and cc'ing PTABInbound@fr.com, axf-ptab@fr.com, devoto@fr.com and khan@fr.com).

IX. Standing

Petitioner certifies that the '730 patent is available for IPR, and Petitioner is not barred or estopped from requesting IPR on the grounds identified in this Petition.

X. Conclusion

Petitioner has established a reasonable likelihood of prevailing for the challenged claims and requests the Board institute IPR and cancel each challenged claim as unpatentable.

Respectfully submitted,

Dated 8-20-24

/ Roberto J. Devoto /
W. Karl Renner, Reg. No. 41,265
Roberto J. Devoto, Reg. No. 55,108
Usman Khan, Reg. No. 70,439
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2024-01326)

Attorneys for Petitioner

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 13,311 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated August 20, 2024

/ Roberto J. Devoto /

W. Karl Renner, Reg. No. 41,265

Roberto J. Devoto, Reg. No. 55,108

Usman Khan, Reg. No. 70,439

Fish & Richardson P.C.

60 South Sixth Street, Suite 3200

Minneapolis, MN 55402

T: 202-783-5070

F: 877-769-7945

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on August 20, 2024, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided by Federal Express, to the Patent Owner, by serving the correspondence address of record as follows:

Patent Law Works/Proxense
Greg Sueoka
4516 South 700 East, Suite 290
Salt Lake City, UT 84107

/Diana Bradley/
Diana Bradley
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(858) 678-5667