

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,

Petitioner,

v.

PROXENSE, LLC,

Patent Owner.

Case No. IPR2024-00784
U.S. Patent No. 10,073,960
Filing Date: May 15, 2017
Issue Date: September 11, 2018

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

I.	Relief Requested.....	1
II.	The '960 Patent.....	2
	A. Overview	2
	B. Claim Construction.....	5
	C. Level of Ordinary Skill	7
III.	Overview of The Prior Art.....	7
	A. Dua	7
	B. Buer	10
	C. Giobbi157.....	12
	D. Nishikawa.....	14
IV.	Ground 1: Claims 1-6, 8-11, And 14-19 Would Have Been Obvious Over Dua In View Of Giobbi157	15
	A. Independent Claims.....	15
	1. Claim 14.....	15
	2. Claim 1.....	28
	B. Dependent Claims	31
	1. [2] “The device of claim 1, wherein at least one of the one or more of the application, the function, and the service is enabled, at least in part, on the device.” [15] “The method of claim 14, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on the device.”	31
	2. [3] “The device of claim 1, wherein at least one of the one or more of the application, the function, and the service is enabled, at least in part, external to the device using an	

- external, wireless communication interface, the device communicatively coupled to wirelessly communicate with the external, wireless communication interface.” [16] “The method of claim 14 further comprising: sending the enablement signal, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on a device external to the device and communicatively coupled to an external, wireless communication interface.”32
3. [4] “The device of claim 1, wherein the local, secured information includes biometric information for authenticating a user.” [17] “The method of claim 14, wherein the local, secured information includes biometric information for authenticating a user.”33
4. [5] “The device of claim 1, wherein the local, secured information includes biometric information based on a biometric scan of a finger, the biometric information for authenticating a user.”34
5. [6] “The device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information.” [18] “The method of claim 14, wherein the local, secured information includes financial information and wherein the one or more of the application, the function and the service completes a financial transaction.”35
6. [8] “The device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on an authorization of the financial information using an external authentication database, the financial information transmitted to the external authentication database.”35

[9]	“The device of claim 8, wherein the external authentication database is separate from a merchant providing a sale in the financial transaction.”	37
[10]	“The device of claim 1, wherein the one or more of the application, the function and the service enabled based on the local, secured information stored by the integrated, secure memory includes a first application, function or service based on a first subsets of local, secured information stored by the integrated, secure memory and a second application, function or service based on a second subset of local, secured information, the first and second subset of local, secured information having different accessibility.”	37
7.	[11] “The device of claim 1, wherein the device is a cell phone.” [19] "The method of claim 14, wherein the device is a cell phone."	39
V.	Grounds 2 and 3: Buer Renders Obvious Claims 1-7, 10-11, and 14-19 (Ground 2); Buer and Giobbi157 Render Obvious Claims 4, 8-10, 12, 13, 17, and 20 (Ground 3).....	39
A.	Independent Claims	39
1.	Claim 14.....	39
2.	Claim 1	56
B.	Dependent Claims	60
1.	[2] “The device of claim 1, wherein at least one of the one or more of the application, the function, and the service is enabled, at least in part, on the device.”	60
2.	[3] “The device of claim 1, wherein at least one of the one or more of the application, the function, and the service is enabled, at least in part, external to the device using an external, wireless communication interface, the device communicatively coupled to wirelessly communicate with the external, wireless communication interface.”	60

3. [4] “The device of claim 1, wherein the local, secured information includes biometric information for authenticating a user.”63
4. [5] “The device of claim 1, wherein the local, secured information includes biometric information based on a biometric scan of a finger, the biometric information for authenticating a user.”65
5. [6] “The device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information.”65
6. [7] “The device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on a signal received from the at least one external device by the integrated, wireless communication interface.”66
7. [8] “The device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on an authorization of the financial information using an external authentication database, the financial information transmitted to the external authentication database.”67
8. [9] “The device of claim 8, wherein the external authentication database is separate from a merchant providing a sale in the financial transaction.”69
9. [10] “The device of claim 1, wherein the one or more of the application, the function and the service enabled based on the local, secured information stored by the integrated, secure memory includes a first application, function or service based on a first subsets of local, secured information stored by the integrated, secure memory and a second application, function or service based on a second subset of

	local, secured information, the first and second subset of local, secured information having different accessibility.”69
10.	[11] “The device of claim 1, wherein the device is a cell phone.”71
11.	[12] “The device of claim 1, wherein the at least one external device is included in jewelry.”72
12.	[13] “The device of claim 1, wherein the at least one external device is a watch.”73
13.	[15] “The method of claim 14, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on the device.”73
14.	[16] “The method of claim 14 further comprising: sending the enablement signal, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on a device external to the device and communicatively coupled to an external, wireless communication interface.”73
15.	[17] “The method of claim 14, wherein the local, secured information includes biometric information for authenticating a user.”73
16.	[18] “The method of claim 14, wherein the local, secured information includes financial information and wherein the one or more of the application, the function and the service completes a financial transaction.”74
17.	[19] “The method of claim 14, wherein the device is a cell phone.”74
18.	[20] “The method of claim 14, wherein the external PDK is included in a watch.”74
VI.	Ground 4: Claim 4 Would Have Been Obvious Over Buer and Nishikawa76
VII.	Discretionary Denial Is Not Warranted78

A.	Discretionary Denial Is Not Warranted Under § 325(d).....	78
B.	Discretionary Denial Is Not Warranted Under <i>Fintiv</i>	79
C.	35 U.S.C. §314(a) – <i>General Plastic</i>	80
VIII.	Mandatory Notices.....	81
A.	Real Parties-in-Interest Under 37 C.F.R. §42.8(b)(1).....	81
B.	Related Matters Under 37 C.F.R. §42.8(b)(2)	81
C.	Counsel and Service Information Under 37 C.F.R. §42.8(b)(3).....	82
D.	Service Information Under 37 C.F.R. §42.8(b)(4).....	83
IX.	Standing	83
X.	Conclusion	83

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Advanced Bionics LLC v. MED-EL Elektromedizinische Gerate GmbH</i> , IPR2019-01469, Paper 6 (PTAB Feb. 13, 2020)	78
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020)	79, 80
<i>Fresenius USA, Inc. v. Baxter Int’l, Inc.</i> , 582 F.3d 1288 (Fed. Cir. 2009)	24, 51, 59
<i>Friskit, Inc. v. Real Networks, Inc.</i> , 306 F. App’x 610 (Fed. Cir. 2009)	<i>passim</i>
<i>Protect Animals with Satellites v. OnPoint Sys., LLC</i> , IPR2021-01483, Paper 11 (PTAB March 4, 2022)	79
<i>Realtime Data, LLC v. Iancu</i> , 912 F.3d 1368 (Fed. Cir. 2019)	7
<i>Samsung Elecs. Am., Inc. v. Proxense, LLC</i> , IPR2021-01438, Paper 12 (PTAB Feb. 28, 2022)	7
<i>Samsung Elecs. Am., Inc. v. Proxense, LLC</i> , IPR2021-01439, Paper 11 (PTAB Feb. 28, 2022)	7
Statutes	
35 U.S.C. §103	1
35 U.S.C. §314(a)	80
35 U.S.C. §315(d)	81
35 U.S.C. §325(d)	78
Regulations	
37 C.F.R. §42.8(b)(1)	81

37 C.F.R. §42.8(b)(2).....	81
37 C.F.R. §42.8(b)(3).....	81
37 C.F.R. §42.8(b)(4).....	82
37 C.F.R. §42.122(a)	83

TABLE OF EXHIBITS

Exhibit	Description
Ex-1001	U.S. Patent No. 10,073,960 to David L. Brown (“the ’960 patent”)
Ex-1002	Prosecution history of U.S. Patent No. 10,073,960
Ex-1003	Declaration of Andrew Wolfe, Ph.D., including his Curriculum Vitae
Ex-1004	U.S. Patent Application Publication No. 2006/0258289 to Dua (“Dua”)
Ex-1005	European Patent Application Publication No. EP 1536306 to Buer et al. (“Buer”)
Ex-1006	U.S. Patent Application Publication No. 2007/0245157 to Giobbi et al. (“Giobbi157”)
Ex-1007	U.S. Patent Application Publication No. 2004/0255139 to Giobbi (“Giobbi139”)
Ex-1008	PCT Application Publication No. WO 90/06633 to Lee et al. (“Lee”)
Ex-1009	Order, <i>Proxense, LLC v. Samsung Elecs. Co., Ltd.</i> , No. 6:21-cv-00210-ADA (W.D. Tex. Jan. 18, 2022)
Ex-1010	Memorandum in Support of Claim Construction Order, <i>Proxense, LLC v. Samsung Elecs. Co., Ltd.</i> , No. 6:21-cv-00210-ADA (W.D. Tex. Dec. 28, 2022)
Ex-1011	Scheduling Order, <i>Proxense, LLC v. Google LLC</i> , No. 6:23-cv-00320-ADA (W.D. Tex. March 18, 2024)
Ex-1012	U.S. Patent Application Publication No. 2005/0116050 to Jei et al. (“Jei”)
Ex-1013	PCT Application Publication No. WO 2005/104584 to Bella et al.

	("Bella")
Ex-1014	European Patent Application Publication No. EP 1600885 to Nishikawa et al. ("Nishikawa")
Ex-1015	Google's Proposed Constructions, <i>Proxense, LLC v. Google LLC</i> , No. 6:23-cv-00320 (W.D. Tex October 17, 2023)
Ex-1016	Proxense's Proposed Constructions, <i>Proxense, LLC v. Google LLC</i> , No. 6:23-cv-00320 (W.D. Tex October 17, 2023)
Ex-1017	U.S. Patent Application Publication No. 2004/0176032 to Kotola et al. ("Kotola")
Ex-1018	Preliminary Infringement Contentions Exhibit F, <i>Proxense, LLC v. Google LLC</i> , No. 6:23-cv-00320 (W.D. Tex)
Ex-1019	U.S. Patent Application Publication No. 2005/0151623 to Von Hoffmann ("Von Hoffmann")
Ex-1020	Claim Construction Order, <i>Proxense, LLC v. Google LLC</i> , No. 6:23-cv-00320-ADA (W.D. Tex. January 23, 2024)
Ex-1021	Bluetooth Specification, Profiles of the Bluetooth System, Version 1.0 B (December 1999)
Ex-1022	Comparison of District Courts (December 31, 2023)

LISTING OF CHALLENGED CLAIMS

Claim 1	
[1pre]	A device comprising:
[1a]	a battery;
[1b]	an integrated, secure memory storing local, secured information; and
[1c]	an integrated, wireless communication interface for communicating wirelessly with at least one external device within a proximity zone, the integrated, wireless communication interface communicatively coupled to the integrated, secure memory and coupled to draw power from the battery,
[1d]	wherein one or more of (a) the integrated, wireless communication interface communicating wirelessly with the at least one external device within the proximity zone enables one or more of an application, a function, and a service and (b) the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and a service.
Claim 2	
[2]	The device of claim 1, wherein at least one of the one or more of the application, the function, and the service is enabled, at least in part, on the device.
Claim 3	
[3]	The device of claim 1, wherein at least one of the one or more of the application, the function, and the service is enabled, at least in part, external to the device using an external, wireless communication interface, the device communicatively coupled to wirelessly communicate with the external, wireless communication interface.
Claim 4	
[4]	The device of claim 1, wherein the local, secured information includes biometric information for authenticating a user.

Claim 5	
[5]	The device of claim 1, wherein the local, secured information includes biometric information based on a biometric scan of a finger, the biometric information for authenticating a user.
Claim 6	
[6]	The device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information.
Claim 7	
[7]	The device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on a signal received from the at least one external device by the integrated, wireless communication interface.
Claim 8	
[8]	The device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on an authorization of the financial information using an external authentication database, the financial information transmitted to the external authentication database.
Claim 9	
[9]	The device of claim 8, wherein the external authentication database is separate from a merchant providing a sale in the financial transaction.
Claim 10	
[10]	The device of claim 1, wherein the one or more of the application, the function and the service enabled based on the local, secured information stored by the integrated, secure memory includes a first application, function or service based on a first subsets of local,

	secured information stored by the integrated, secure memory and a second application, function or service based on a second subset of local, secured information, the first and second subset of local, secured information having different accessibility.
Claim 11	
[11]	The device of claim 1, wherein the device is a cell phone.
Claim 12	
[12]	The device of claim 1, wherein the at least one external device is included in jewelry.
Claim 13	
[13]	The device of claim 1, wherein the at least one external device is a watch.
Claim 14	
[14pre]	A method comprising:
[14a]	creating a first wireless link between an integrated, wireless communication interface of a device and an external device, the device including a battery, an integrated, secure memory, and the integrated, wireless communication interface, wherein the integrated, secure memory stores local, secured information and the integrated, wireless communication interface is powered by the battery;
[14b]	receiving a first signal, at the integrated, wireless communication interface, via the first wireless link, from the external device; and
[14c]	generating an enablement signal enabling one or more of an application, a function and a service.
Claim 15	
[15]	The method of claim 14, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on the device.
Claim 16	

[16]	The method of claim 14 further comprising: sending the enablement signal, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on a device external to the device and communicatively coupled to an external, wireless communication interface.
Claim 17	
[17]	The method of claim 14, wherein the local, secured information includes biometric information for authenticating a user.
Claim 18	
[18]	The method of claim 14, wherein the local, secured information includes financial information and wherein the one or more of the application, the function and the service completes a financial transaction.
Claim 19	
[19]	The method of claim 14, wherein the device is a cell phone.
Claim 20	
[20]	The method of claim 14, wherein the external PDK is included in a watch.

I. Relief Requested

Google LLC (Petitioner) requests *inter partes* review of U.S. Patent No. 10,073,960 (“the ’960 patent,” Ex-1001) based on the following grounds:

Ground	Claim(s) Challenged	35 U.S.C. §	Reference(s)
1	1-6, 8-11, and 14-19	103	Dua, Giobbi157
2	1-7, 10-11, and 14-19	103	Buer
3	4, 8-10, 12, 13, 17, and 20	103	Buer, Giobbi157
4	4	103	Buer, Nishikawa

The ’960 patent generally relates to the use of keys and readers, such as RFID tags and RFID readers, Ex-1001, 1:51-2:17, and refers to a key as a “personal digital key (PDK)” and to a reader as a “receiver-decoder circuit (RDC).” *Id.*, 1:51-57. The ’960 patent is directed to a “hybrid device” (e.g., a cellular phone) with both an integrated, secure memory storing local, secured information (PDK) and an RDC, which can respectively communicate with external RDCs and PDKs that are in proximity with the hybrid device.

But hybrid devices having both an internal key and reader were known years before the ’960 patent was filed. Dua discloses a cellular phone with an integrated Radio Frequency Identification (RFID) Tag-Reader Module with both an RFID tag (PDK) and an RFID reader (RDC) to automatically set up and establish a wireless connection with an external device in its proximity. Ex-1004, [0011]-[0016]. Buer

also teaches a cellular phone with both an internal authentication component (PDK) and a proximity reader (RDC) to secure access to various services using external RFID tokens (keys) and readers in its proximity. Ex-1005, [0014], [0010], [0130], [0163]. In fact, numerous prior art patents teach the same concept of using a digital key and reader to secure data or a service. *See, e.g.*, Exs. 1006-1008, 1012-1014. Thus, the challenged claims merely recite the well-known concept of enabling applications, functions, or services with digital keys and readers that were well known in the art. Accordingly, the challenged claims should be held unpatentable.

II. The '960 Patent

A. Overview

The '960 patent generally relates to the use of keys and readers, such as RFID tags and RFID readers. Ex-1001, 1:51-2:17. The '960 patent is directed to a “hybrid device” (**red**) with both an integrated personal digital key (PDK) (“integrated, secure memory,” **blue**) and an integrated receiver-decoder circuit (RDC) (“integrated, wireless communication interface,” **yellow**) that communicate with each other via a signal line. *Id.*, 2:32-37. The '960 patent discloses that the hybrid device may be part of a cell phone.

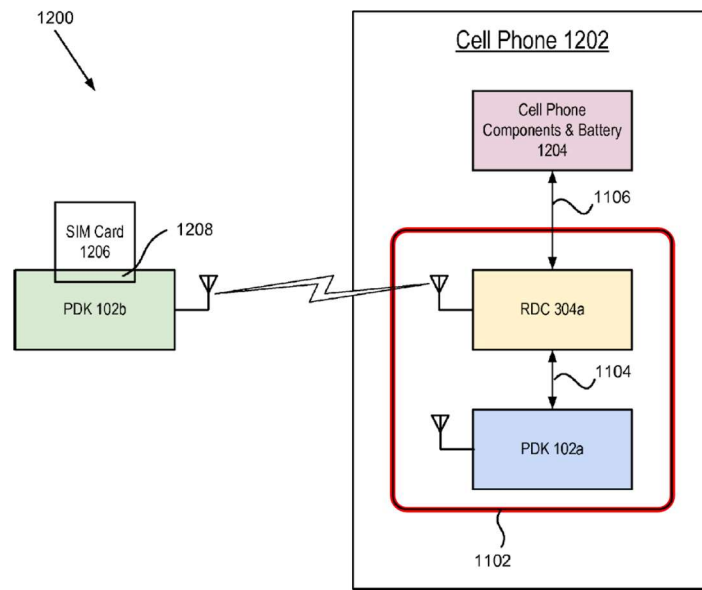


FIG. 12

Id., Fig. 12 (annotated). Additional cell phone components and a battery (pink) may be coupled to the integrated RDC by a signal line. *Id.*, 14:53-15:5. The integrated RDC may communicate wirelessly with an external PDK. *Id.*, 14:67-15:2.

The hybrid device may interconnect with other external devices, as shown below, so that the integrated PDK (blue) communicates wirelessly with the external device (RDC; purple), and the integrated RDC (yellow) communicates wirelessly with an external PDK (green) within its proximity zone.

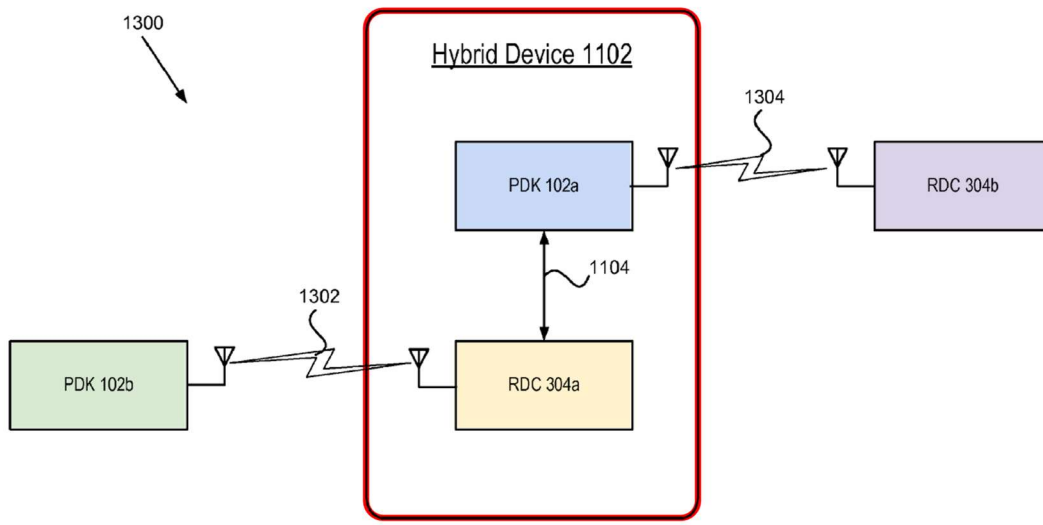


FIG. 13

Id., Fig. 13 (annotated), 16:55-17:4, 22:43-60.

The purpose of the integrated PDK and RDC is to enable various applications, functions, or services either on an external device or on the hybrid device using information stored on the integrated or external PDKs (e.g., (1) financial information such as bank information, credit/debit card information, and account information; (2) biometric information such as a fingerprint, palm print, retinal scan; or (3) personal identification information such as a name, address, phone number). *Id.*, 4:44-54, 7:14-25, 17:5-12. When the hybrid device may be used to access or enable a Wi-Fi service, an external PDK 102b “provides...information to the [integrated] RDC 304a,” and the hybrid device “then communicates with the [external] RDC 304b to access the Wi-Fi service.” *Id.*, 20:12-35. In this example, the hybrid device

and the external PDK may belong to different users, and the hybrid device may thus use another user's information stored on the external PDK. *Id.* As another example, the hybrid device may use the credit card information stored on the integrated PDK to provide authorization to the external RDC to make a purchase using the cell phone, and in this way, "to enable a service associated with the...[external] RDC." *Id.*, 17:5-12. The purchase authorization may depend on the presence of an external PDK being in proximity to the hybrid device. *Id.*, 17:12-19, 17:25-50. The external PDK first "authorizes the hybrid device," which "in turn authorizes" the external RDC, such that a user can only make a purchase when the external PDK is in proximity to the hybrid device *Id.*, 17:12-19, 17:25-28. In other words, the external PDK may be "used to enable specific features in the hybrid device." *Id.*, 17:18-19.

B. Claim Construction

In the previous district court litigation, *Proxense, LLC v. Samsung Elecs. Co., Ltd.*, No. 6:21-cv-00210-ADA (W.D. Tex.), the court construed the following terms in family members of the '960 patent:

- "hybrid device" means "[a] device comprising an integrated personal digital key (PDK) and an integrated receiver-decoder circuit."
- "personal digital key" means "[a]n operably connected collection of elements including an antenna and a transceiver for communicating

with a RDC and a controller and memory for storing information particular to a user.”

- “biometric information” is given its “plain and ordinary meaning.”
- “financial information” is given its “plain and ordinary meaning.”
- “receiver-decoder circuit” means “[a] component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing.”
- “inheritance information” means “[i]nformation passed from a first device to a second device for use by the second device.”
- “enablement signal” requires no construction.

Ex-1009, 3-4; Ex-1010, 25, 27, 32, 34, 36, 38, 40. In the pending district court litigation,¹ captioned *Proxense, LLC v. Google LLC*, No. 6:23-cv-00320 (W.D. Tex.) (“the pending litigation”), the court has adopted its prior constructions for “personal digital key” and “receiver-decoder circuit.”² Ex-1020. Because the prior art in this

¹ Google agreed to certain constructions, Ex-1015, 1, and Proxense contends no other terms “beyond what the Court had previously construed in the *Samsung* case” need to be construed. Ex-1016, 1.

² Google proposed alternative constructions for personal digital key” and “receiver-decoder circuit” in the pending litigation. Ex-1015, 1.

Petition renders obvious all claims regardless of the construction, the Board need not construe terms to resolve unpatentability in this Petition.³ *Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019).

C. Level of Ordinary Skill

A person of ordinary skill in the art (“POSITA”) at the time of the purported invention would have had a bachelor’s degree in computer or electrical engineering or an equivalent degree, and at least three years of experience in the field of encryption and security or equivalent experience. Additional education could substitute for professional experience, and significant work experience could substitute for formal education. Ex-1003, ¶38.

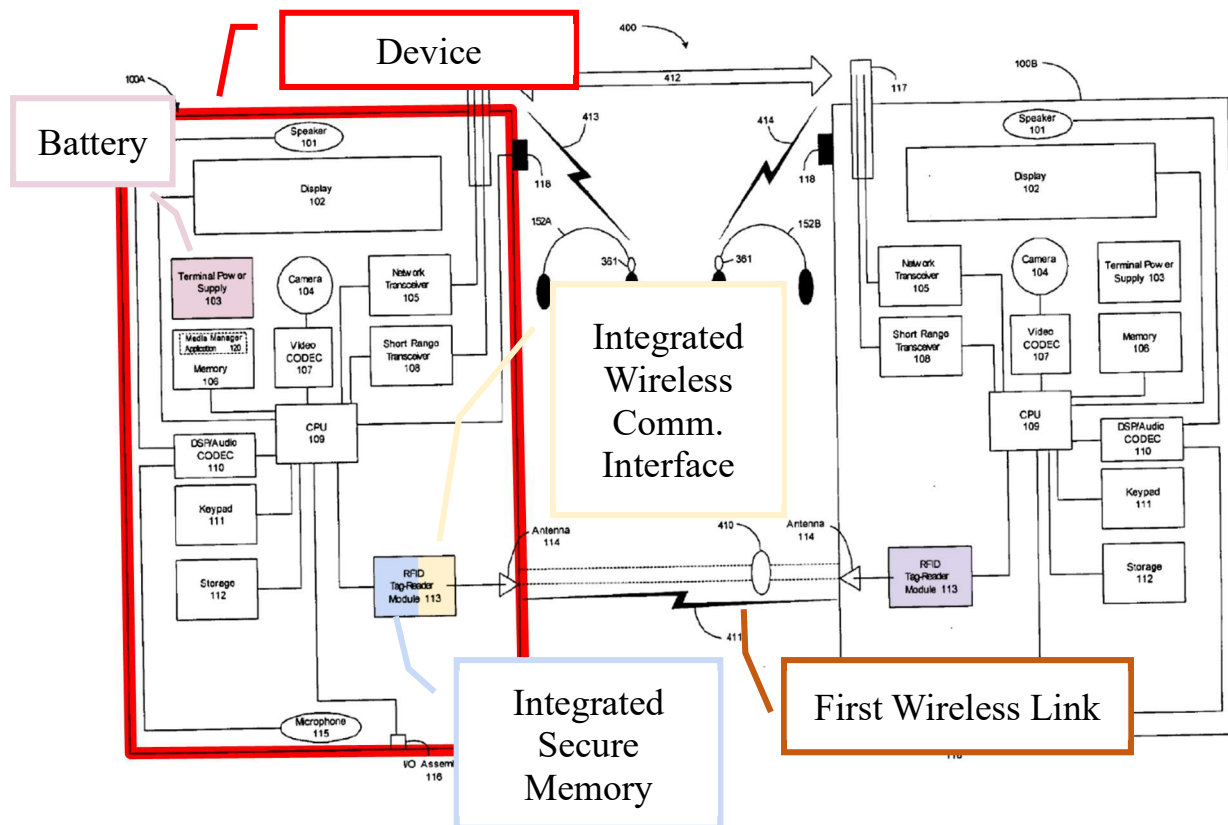
III. Overview of The Prior Art

A. Dua

Dua, U.S. Patent Application Publication No. 2006/0258289, published on November 16, 2006, qualifies as prior art under pre-AIA 35 U.S.C. §102(b). Dua’s

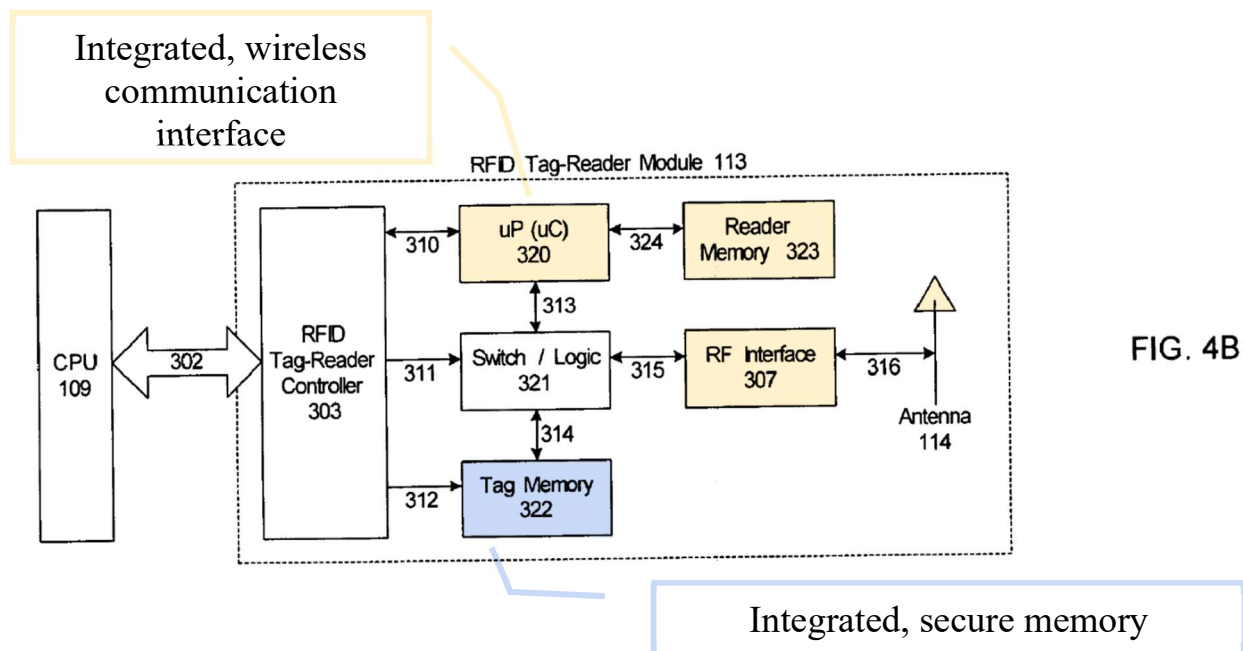
³ The Board previously determined that only “personal digital key” warranted construction for the purposes of institution. *See e.g., Samsung Elecs. Am., Inc. v. Proxense, LLC*, IPR2021-01438, Paper 12 at 16 (PTAB Feb. 28, 2022); *Samsung Elecs. Am., Inc. v. Proxense, LLC*, IPR2021-01439, Paper 11 at 16 (PTAB Feb. 28, 2022)

hybrid device (“cellular phone”) contains “both an RFID tag and an RFID reader” that establishes wireless connections with other devices to enable functions and to exchange data, Ex-1004, [0015], [0070], using an “RFID Tag-Reader Module” to “rapidly exchange information with an electronic device that is in close proximity.” *Id.*, [0070].



Id., Fig. 6 (annotated).

The RFID Tag-Reader Module, as shown below, includes specific circuit components for “RFID tag functionality” and circuit components for “RFID reader functionality.” *Id.*, [0106].



Id., Fig. 4B (annotated).

The components for “RFID tag functionality” (blue) store confidential information and encryption keys in “tamper resistant” internal tag memory for gaining access to an external device. *Id.*, [0108]-[0109]. This stored information may be encrypted. *Id.*, [0109], [0152]. Dua discloses transmitting this information to an external reader to establish a secure connection. *Id.*, [0092], [0100]-[0101], [0139].

The components for “RFID reader functionality” (yellow) are capable of communicating with external RFID tags. Ex-1004, [0071]. The RFID reader may also receive and decode encrypted data using an encryption key. *Id.*, [0152]. Dua discloses enabling services, such as “transmission of media assets to other devices in proximity via short-range RF,” and other additional functionalities, including

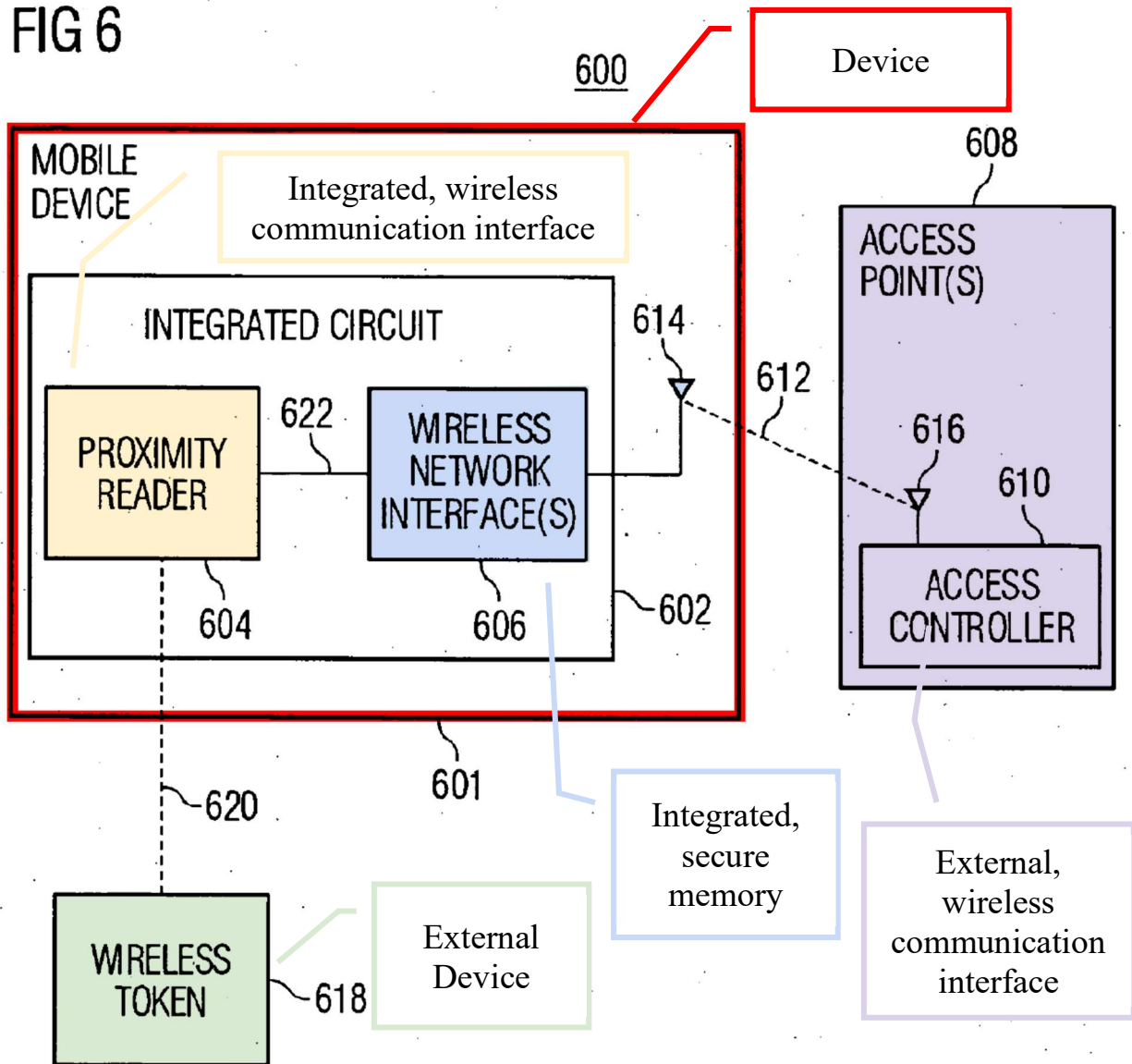
“transacting at a point-of-sale location using a digital wallet application and the RFID capability.” Ex-1004, [0058]; *see also id.*, [0070], [0089]; Ex-1003, ¶¶49-59.

B. Buer

Buer, European Patent Application Publication No. EP 1536306, published on September 30, 2004, qualifies as prior art under pre-AIA 35 U.S.C. §102(b). Buer discloses that “[a]ccess to secured services may be controlled based on the proximity of a wireless token to a computing device.” Ex-1005, Abstract. “An authorized user may be provided access to a service only when a wireless token assigned to the user is in...proximity.” *Id.* The computing device (access device) may be implemented as a mobile device (cellular phone). *Id.*, [0163], [0195]. When implemented as a mobile device, Buer’s access device could be used to enable various applications, functions, or services, including the following two embodiments: (1) “embodiments of a wireless proximity and authentication system that controls access to one or more data networks,” as disclosed in Figures 5-7, and (2) “embodiments of security processing systems (i.e., key management systems) that include wireless proximity and authentication,” as disclosed in Figures 8-11. *Id.*, [0155], [0176].

In the first embodiment, the mobile device may be enabled “to access one or more wireless networks (e.g., a cellular network, an 802.11 network, a Bluetooth network, etc.)”:

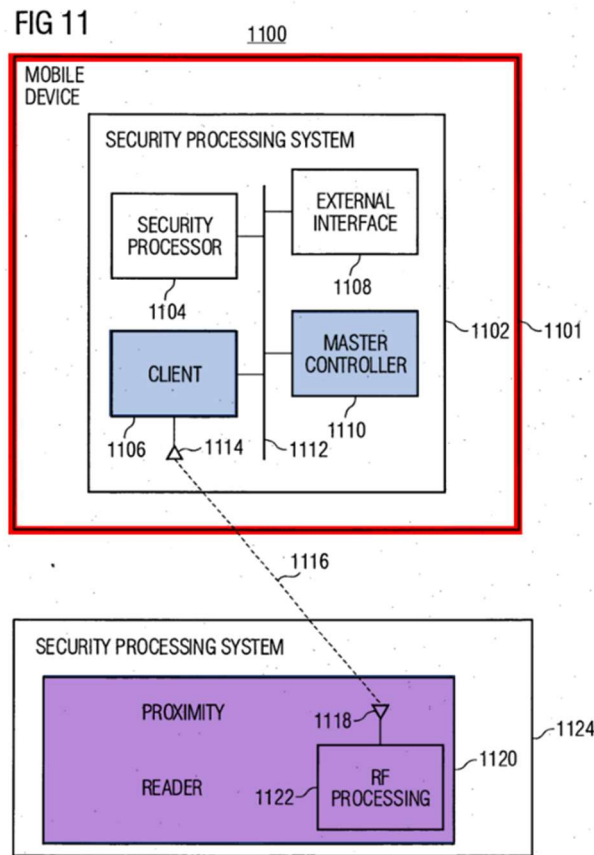
FIG 6



Id., Fig. 6 (annotated), [0163]. The mobile device receives authentication information from the wireless token via RF signals 620 and communicates with the access points wirelessly via RF signals 612. *Id.*, [0164]-[0165].

In the second embodiment, the mobile device (**red**) may also “be used to authenticate a user to another processing system,” such as an external proximity

reader 1120 or a computer with “point-of-sale components” (not shown) to “perform a sales transaction” (e.g., “credit card transactions”), as shown below.



Id., Fig. 11 (annotated), [0194]-[0196]; Ex-1003, ¶¶60-66.

C. Giobbi157

Giobbi157, U.S. Patent Application Publication No. 2007/0245157, published on October 18, 2007, qualifies as prior art under pre-AIA 35 U.S.C. §102(a). Giobbi157 “provide[s] efficient, secure, and highly reliable authentication for transaction processing and/or access control applications.” Ex-1006, Abstract.

Giobbi157 discloses a personal digital key (PDK) (“integrated, secure memory”) that “stores one or more profiles (e.g., a biometric profile) in a tamperproof memory that is acquired in a secure and trusted process.” *Id.* Giobbi157 teaches that the PDK may be integrated into a hybrid device, “such as a cell phone,” as shown below. *Id.*, [0035], [0011].

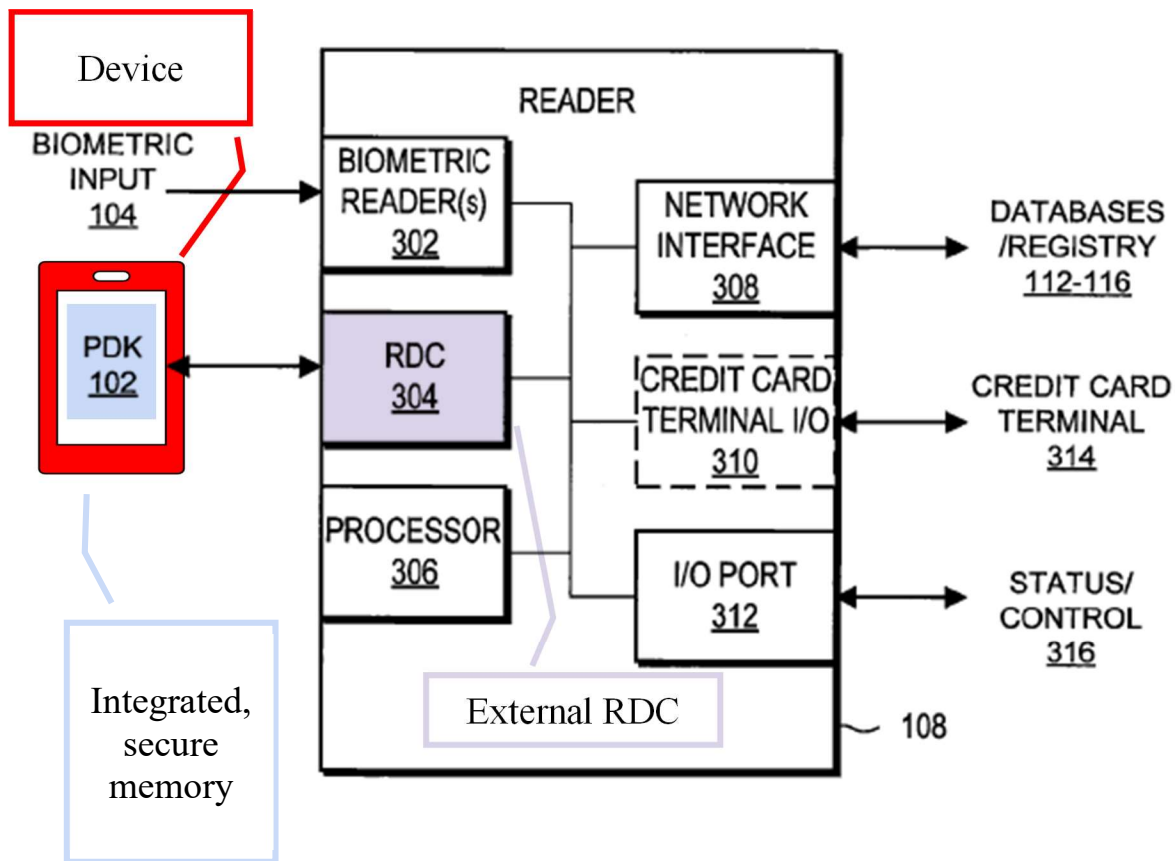


FIG. 3

Id., Fig. 3 (annotated). Giobbi157’s integrated PDK wirelessly communicates with an external receiver-decoder circuit (RDC), such that information stored on the integrated PDK is transmitted to the external RDC located on a “Reader 108.” *Id.*,

[0012], [0026]. The external RDC is communicatively coupled to an external database that is used for enabling an application, function, or service. *Id.*, [0053]. Giobbi¹⁵⁷ teaches that its hybrid device, which contains the PDK, enables an application, function, or service to take place by enabling a financial transaction, such as an ATM withdrawal. *Id.*, [0011], [0065]; Ex-1003, ¶¶67-73.

D. Nishikawa

Nishikawa, European Patent Application Publication No. EP 1600885, published on November 30, 2005, qualifies as prior art under pre-AIA 35 U.S.C. §102(b). Nishikawa discloses an improved e-token (e.g., “key holder type ID module”) that acts as “a SIM reader/writer...having contact and noncontact interfaces.” Ex-1014, [0001], [0017]. Nishikawa teaches “ways to improve the convenience of the key holder type ID module by combining the IC chip of the SIM with contact and noncontact interfaces to provide the key holder type ID module with noncontact communication function, and by combining a coil antenna and a display with a reader/writer to be used in combination with the SIM to provide the reader/writer with a short-distance communication function and a fingerprint sensing function.” *Id.*, [0017]. In Nishikawa, the SIM card is “loaded with multiple applications, such as electronic money, an electronic ticket, a fingerprint template, a fingerprint collating engine and a personnel ID card.” *Id.*, [0111]. In doing so, Nishikawa provides the key holder type ID module with a “noncontact

communication function and the short-distance communication means” for use “as an electronic ticket and as electronic money for various noncontact transactions,” and with a “fingerprint sensor” for authentication “on the basis of biometric data.” *Id.*, [0113]-[0114]; Ex-1003, ¶¶79-85.

IV. Ground 1: Claims 1-6, 8-11, And 14-19 Would Have Been Obvious Over Dua In View Of Giobbi157

A. Independent Claims

Independent claim 14 is the broadest independent claim and is asserted in the pending litigation. Dua alone, or in view of Giobbi157, however, renders obvious asserted independent claim 14. Ex-1003, ¶¶101-104.

1. Claim 14

a. [14pre] “A method comprising:”

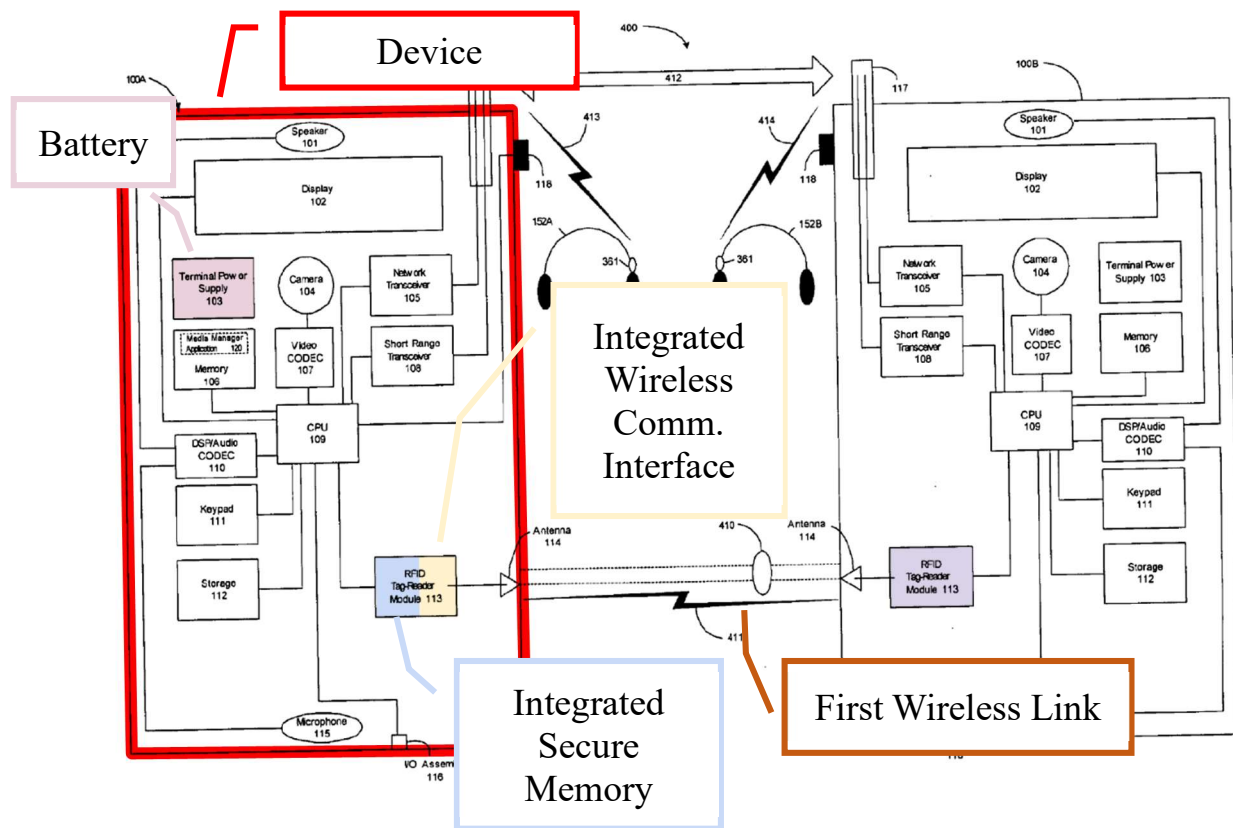
To the extent the preamble for claim 14 is limiting, Dua discloses the preamble because it discloses a method to automatically set up and establish a wireless connection between two devices based on the proximity of the devices. Ex-1004, [0013]; Ex-1003, ¶105.

- b. [14a] “creating a first wireless link between an integrated, wireless communication interface of a device and an external device, the device including a battery, an integrated, secure memory, and the integrated, wireless communication interface, wherein the integrated, secure memory stores local, secured information and the integrated, wireless communication interface is powered by the battery;”

Dua discloses [14a].

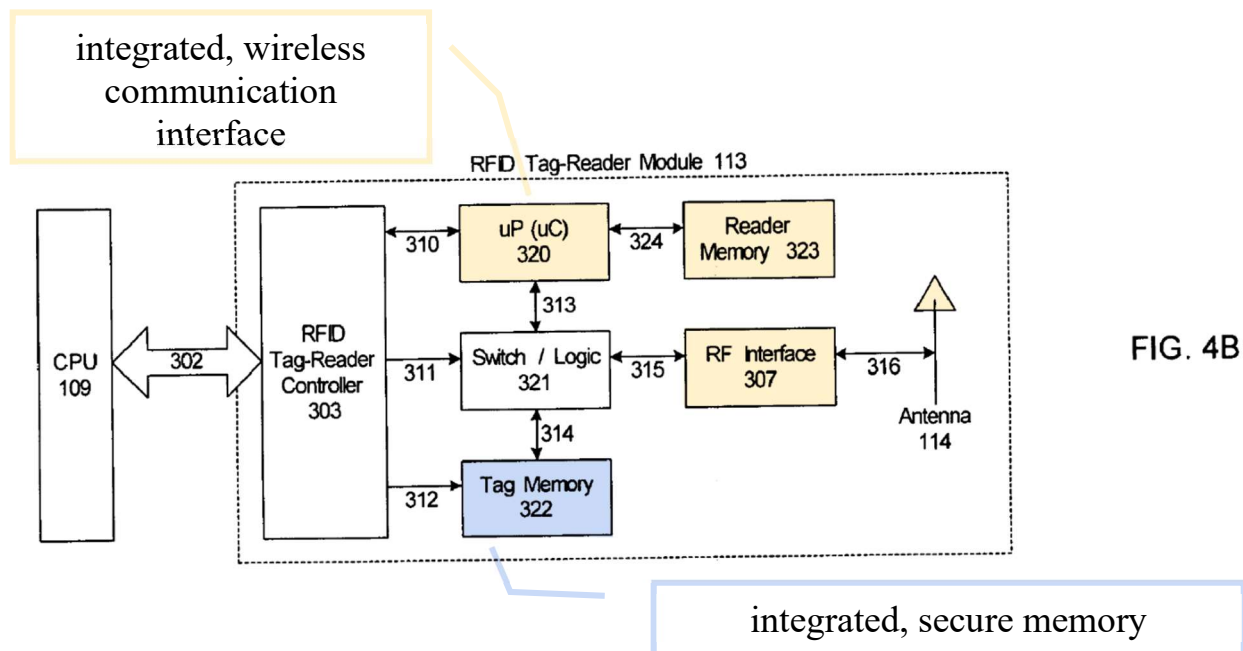
(1) A device including a battery, an integrated, secure memory, and the integrated, wireless communication interface:

Dua discloses the device in [14a] because it discloses a media player (cellular phone) with a power supply and an RFID Tag-Reader Module, as shown below. Ex-1004, [0057], [0070]; Ex-1003, ¶¶106-107.



Ex-1004, Fig. 6 (annotated). Dua’s media player (“device,” **red**) includes a battery (**pink**), such as “a rechargeable power supply 103 (e.g., rechargeable lithium polymer battery).” *Id.*, [0059].

Dua’s RFID Tag-Reader Module 113 (e.g., “integrated, secure memory,” **blue**; “integrated, wireless communication interface,” **yellow**) enables the device to “rapidly exchange information with an electronic device [with RFID] that is in close proximity.” *Id.*, [0057], [0070], Figs. 1, 6. Dua’s RFID Tag-Reader Module, as shown below, includes “both an RFID tag [(the claimed ‘integrated, secure memory,’ **blue**)] and an RFID reader [(the claimed ‘integrated, wireless communication interface,’ **yellow**)].” *Id.*, [0089].



Id., Fig. 4B (annotated).

Dua’s Tag-Reader Module (**blue**), as shown, is an integrated, secure memory, because it includes a Tag Memory 322 for storing tag data, where the Tag Memory 322 may be a “non-volatile configurable memory” and “tamper resistant” to prevent hackers from retrieving “confidential information and encryption keys.”

Id., [0105], [0109]. The stored information may include a “user identifier” or “other attributes (e.g., a complete calling card containing the contact information for the device owner such as f[u]ll name, title, company, mailing address, E.164 number, e-mail address, etc.).” *Id.*, [0133], Fig. 7. The RFID tag component may also store information to enable “electronic payments at the point-of-sale and secure key access to buildings, cars, etc.” *Id.*, [0070], [0089]. Tag Memory 322 thus stores information particular to a user. The integrated Tag Memory is an

integrated, tamper-resistant memory that securely stores information therein.

Ex-1003, ¶¶108-109.

In Dua, when enhanced security is desired, encryption keys are used and shared between the devices. Ex-1004, [0152]. A POSITA would have understood that the encryption keys provide enhanced security by encrypting “sensitive” information using those keys. *Id.*; Ex-1003, ¶110. It would have been obvious to encrypt the “confidential information” stored in the tag memory to enhance security. Ex-1004, [0109]; Ex-1003, ¶110. A POSITA would have been motivated to use an encryption key to improve RFID security so that the transfer between a tag and reader could be encrypted so that “hackers” could not access the confidential information. Ex-1004, [0108]-[0109], [0152]; Ex-1003, ¶111. A POSITA would have had a reasonable expectation of success in using encryption to enhance security because Dua’s encryption key is stored in the tag memory, and the tag could transfer the encryption key to an RFID reader for decrypting the encrypted data. Ex-1004, [0109], [0152]; Ex-1003, ¶111. The integrated, secure memory thus would store local, encrypted “confidential information” in an integrated, tamper-resistant memory. Ex-1003, ¶111.

Dua’s Tag-Reader Module (**yellow**), as shown, is an “integrated, wireless communication interface” because it comprises operably-connected components that include a reader logic 320 that is implemented as a microcontroller (μC) and a

microprocessor (μ P), Ex-1004, [0106]. *Id.* The RFID “reader component” is used for “transmitting interrogation signals via its antenna to an external electronic device’s RFID tag when in close proximity.” *Id.*, [0071], [0100]. The RFID Tag-Reader Module’s reader component uses the “internal power supply 103 as a power source for transmitting interrogation signals to a target device.” *Id.*, [0071], [0094]. Dua discloses that the RFID reader component is an integrated, wireless communication interface that is powered by a battery, as claimed.

Dua explains that, after transmitting the interrogation signals, the RFID reader component receives “a response signal from the external device’s RFID tag.” *Id.*, [0071], [0100]. The response signal includes “RFID transmission data.” *Id.*, [0130]-[0143]. Furthermore, a reader memory 323 may also be used as a buffer storage for communication with media player 100, as well as with an RFID tag or another RFID tag reader device. *Id.*, [0107]. Ex-1003, ¶¶112-113.

To the extent Patent Owner contends that the integrated, wireless communication interface must receive encrypted data and decode the encrypted data, Dua renders this obvious. In Dua, when “enhanced security is desired” for RFID transmission, encryption keys are used and shared between the external device and the device to facilitate the sharing of “sensitive” information between the devices. *Id.*, [0152]. A POSITA would have understood that the encryption keys provide “enhanced security” by enabling the devices to stored encrypted,

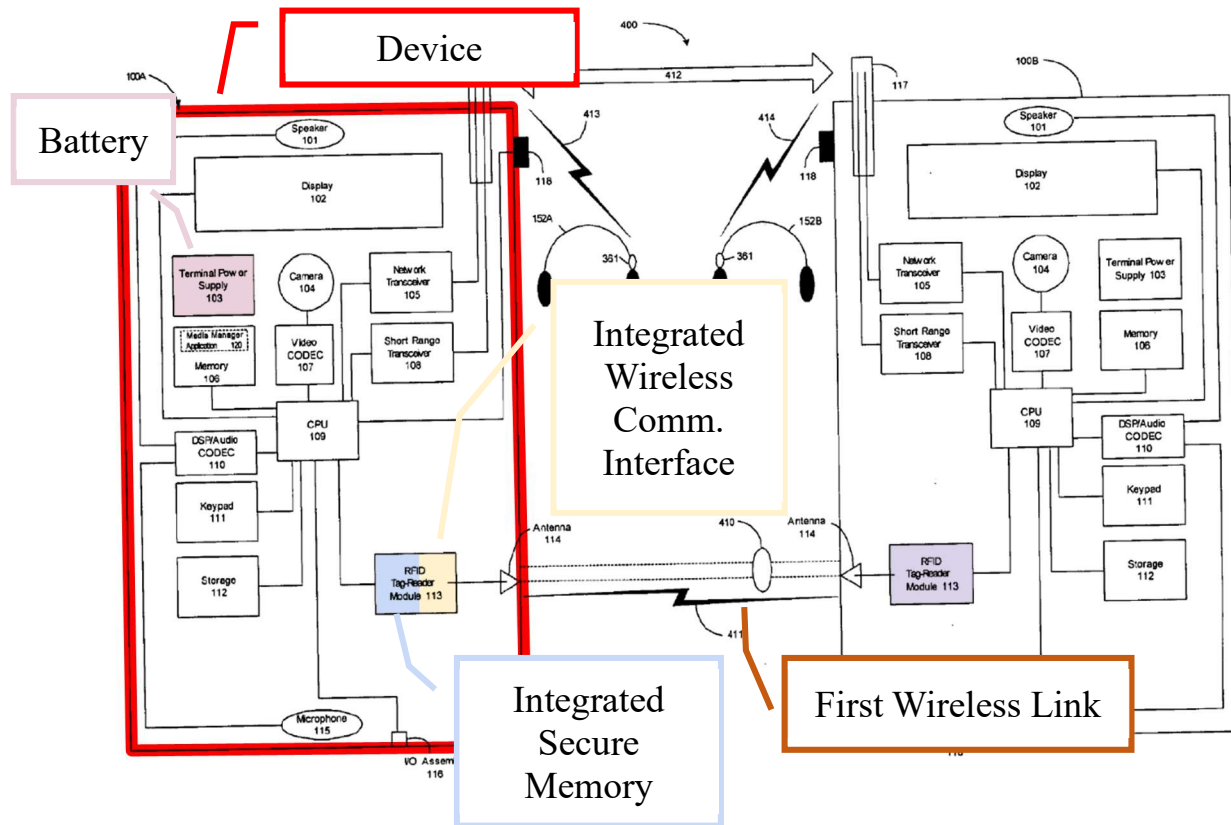
“sensitive” information. *Id.*; Ex-1003, ¶¶114-115. It would have been obvious to store encrypted “confidential information” in the external device’s tag memory and transfer encrypted information to enhance security during the data transfer to the device. Ex-1004, [0109]; Ex-1003, ¶115. A POSITA would have been motivated to use an encryption key to improve RFID security “hackers” could not access the encrypted, confidential information during any data transfer from the external device to the device, as Dua suggests. Ex-1004, [0109], [0152]; Ex-1003, ¶116; *see also* Ex-1006, [0047] (“[T]he data can be encrypted by the transceiver...and transmitted over a secure link.”), [0050] (“Encrypting data transmitted between the PDK 102 and Reader 108 minimizes the possibility of eavesdropping or other fraudulent activity.”). A POSITA would have had a reasonable expectation of success in encrypting the RFID transmissions because Dua explains that the encryption key is stored in the external tag memory (in the external device), and the external tag could transfer the encryption key to an RFID reader (integrated, wireless communication interface) for decrypting the encrypted data. Ex-1004, [0108]-[0109], [0152]; Ex-1003, ¶117. The RFID reader (integrated, wireless communication interface) thus would receive any confidential data in an encrypted format and decode the encrypted data using the encryption key. Ex-1003 ¶117.

Accordingly, Dua discloses a device, as claimed. Ex-1003 ¶117.

(2) Creating a First Wireless Link between an Integrated, Wireless Communication Interface of a Device and an External Device:

Dua discloses creating a first wireless link during an RFID discovery process as in [14a] because the RFID reader component generates and transmits interrogation signals to create an RFID link between the integrated RFID reader in the device and an external RFID tag in an external device, as shown below.

Ex-1004, [0122]; Ex-1003, ¶¶118-119.



Ex-1004, Fig. 6 (annotated). Because both components are labeled as “RFID Tag-Reader Module 113,” they both include the circuit components required for the claimed “integrated, secure memory” and “integrated, wireless communication

interface,” as addressed above. The “reader component” of the “RFID Tag-Reader Module 113” in device 100A (integrated, wireless communication interface) then communicates with the “tag component” of the “RFID Tag-Reader Module 113” in device 100B (external integrated, secure memory).⁴ *Id.*, [0071]-[0072], [0127]-[0128], Fig. 4. Moreover, as Dua explains, the “reader component” is used for transmitting interrogation signals to an external electronic device’s RFID tag when in close proximity. *Id.*, [0071]-[0072], [0127].

c. [14b] “receiving a first signal, at the integrated, wireless communication interface, via the first wireless link, from the external device; and”

Dua discloses [14b] because it discloses receiving “RFID transmission data” (a first signal) at the device’s reader component (the integrated, wireless communication interface) via the first wireless link from the external RFID tag (the external integrated, secure memory in the external device). *Id.*, [0127]; Ex-1003, ¶¶120-121. As Dua explains, during the RFID discovery process, after the external device’s RFID tag received the interrogation signals, the external device’s RFID

⁴ The “tag components” of the “RFID Tag-Reader Module 113” in device 100A (integrated, secure memory) also communicate with the “reader components” of the “RFID Tag-Reader Module 113” in device 100B (external RDC). Ex. 1004, [0071]-[0072], [0127]-[0128], Fig. 4.

tag transmits RFID transmission data to the device. Ex-1004, [0127]-[0144]. The transmitted RFID transmission data (first signal) includes information such as “communication settings, media processing capabilities, and other parameters” for establishing a wireless connection with the external device. Ex-1004, [0128].

d. [14c] “generating an enablement signal enabling one or more of an application, a function and a service.”

Dua discloses [14c] because it discloses that, after receiving the RFID transmission data from an external device with an RFID tag-reader module, the device automatically generates “a Bluetooth paging message” (an enablement signal) to enable an application, function, or service. Ex-1004, [0123], [0128]; Ex-1003, ¶¶122-123. [14c] is recited as allowing “mixed operations” involving several alternatives: what is being enabled (e.g., application, function, or service). Ex-1001, Abstract, 16:47-54. Because [14c] recites alternative events, “the entire element is disclosed by the prior art if one alternative...is in the prior art.” *Fresenius USA, Inc. v. Baxter Int’l, Inc.*, 582 F.3d 1288, 1298 (Fed. Cir. 2009). Because Dua discloses enabling an application, function, or service on either device with an RFID tag-reader module, Dua discloses this claim limitation. Ex-1003, ¶123.

The Integrated, Wireless Communication Interface Communicating Wirelessly with the External Device Enables an Application, Function, or Service:

To the extent that the enablement signal must be generated by the integrated RFID reader, Dua discloses this. Ex-1003, ¶¶124-125. As Dua explains, digital media may be playing on a device, and the user of the device may decide to transmit the digital media (music) to an external device. Ex-1004, [0126]. By bringing the external device into proximity with the device, the device's integrated RFID reader (integrated, wireless communication interface) wirelessly communicates interrogation signals to the external device's RFID tag, which in turn wirelessly communicates RFID transmission data to the integrated RFID reader (integrated, wireless communication interface). *Id.*, [0127]-[0142]. This RFID discovery/paging process causes the device to generate a Bluetooth paging message (enablement signal) to enable a service (e.g., wireless connection and transmission of media) on the external device. Dua's Bluetooth paging message causes the external device to perform a wireless connection set up, and upon completion, the device "automatically transmits" media content to the external device. *Id.*, [0128]. During the transmission of the media content, the media could be "automatically convert[ed]...into a format that is supported by" the external device. *Id.*, [0161], [0172]. Accordingly, the Bluetooth paging message may be used to enable wireless transmission of media that would not have otherwise been supported by the external device. *Id.*, [0161], [0172], [0123], [0128].

Alternatively, the Bluetooth paging message is generated to enable a function (e.g., wireless connection) between the hybrid device and external device. *Id.*, [0144]. As Dua explains, the device and target device may “conserve power by not always having their wireless interface turned on.” *Id.*, [0144], [0137]. Dua’s RFID transmission data helps “facilitate the automatic activation of a radio transceiver with an appropriate communications protocol,” such as exchanging Bluetooth paging messages, to enable wireless connectivity functions in the two devices. *Id.*, [0144]; Ex-1003, ¶126.

The Local, Secured Information Stored by the Integrated, Secure Memory Enables an Application, Function, or Service:

To the extent that the enablement signal must be generated by the integrated RFID tag (integrated, secure memory), Dua also discloses this. As Dua explains, its integrated RFID tag could establish “wireless communication between a diverse set of [external] devices” for various purposes, including “for electronic payments” at point-of-sale or to “secure key access to buildings.” Ex-1004, [0052], [0070]. In Dua, “a credit card profile or other payment information” may be stored on the device. *Id.*, [0224]. During electronic payments using RFID technology, the integrated RFID tag (integrated, secure memory) would generate RFID signal (enablement signal) to exchange financial information with the external point-of-

sale device that is in close proximity to enable electronic payments. Ex-1003 ¶¶127-128.

While Dua does not expressly disclose where the credit card profile or other payment information is stored, a POSITA would have been motivated to securely store the financial information in its tamper-resistant tag memory “to prevent hackers from retrieving confidential information.” *Id.*, [0105], [0109]. Indeed, as Giobbi¹⁵⁷ teaches, “credit/debit card information” used to complete financial transactions (e.g., “charging a credit card for a purchase”) would be stored in a “profile memory field 232” in the “physical access secured and tamperproof” memory. Ex-1006, [0036], [0042], [0063]. A POSITA would have been motivated and capable of storing the “credit card profile or other payment information” in Dua’s tag memory, because storing the “credit card profile or other payment information” in tag memory would require minimal modification without undue experimentation. Ex-1003, ¶¶129-130. Such a combination would have been no more than combining prior art elements using known methods to yield predictable results. Ex-1003, ¶130; *see, e.g., Friskit, Inc. v. Real Networks, Inc.*, 306 F. App’x 610, 616 (Fed. Cir. 2009). A POSITA would have had a reasonable expectation of success in storing a “credit card profile or other payment information” in Dua’s tamper-resistant tag memory. Ex-1003, ¶130.

2. Claim 1

a. [1pre] “A device comprising:”

To the extent the preamble is limiting, Dua discloses the device because it discloses a media player (e.g., cellular phone) with an RFID Tag-Reader Module.

Ex-1004, [0057], [0070]; Ex-1003, ¶131; §IV.A.1.b.

b. [1a] “a battery;”

Dua’s device includes a battery, such as “a rechargeable power supply 103 (e.g., rechargeable lithium polymer battery).” Ex-1004, [0059]; Ex-1003, ¶132. §IV.A.1.b.

c. [1b] “an integrated, secure memory storing local, secured information; and”

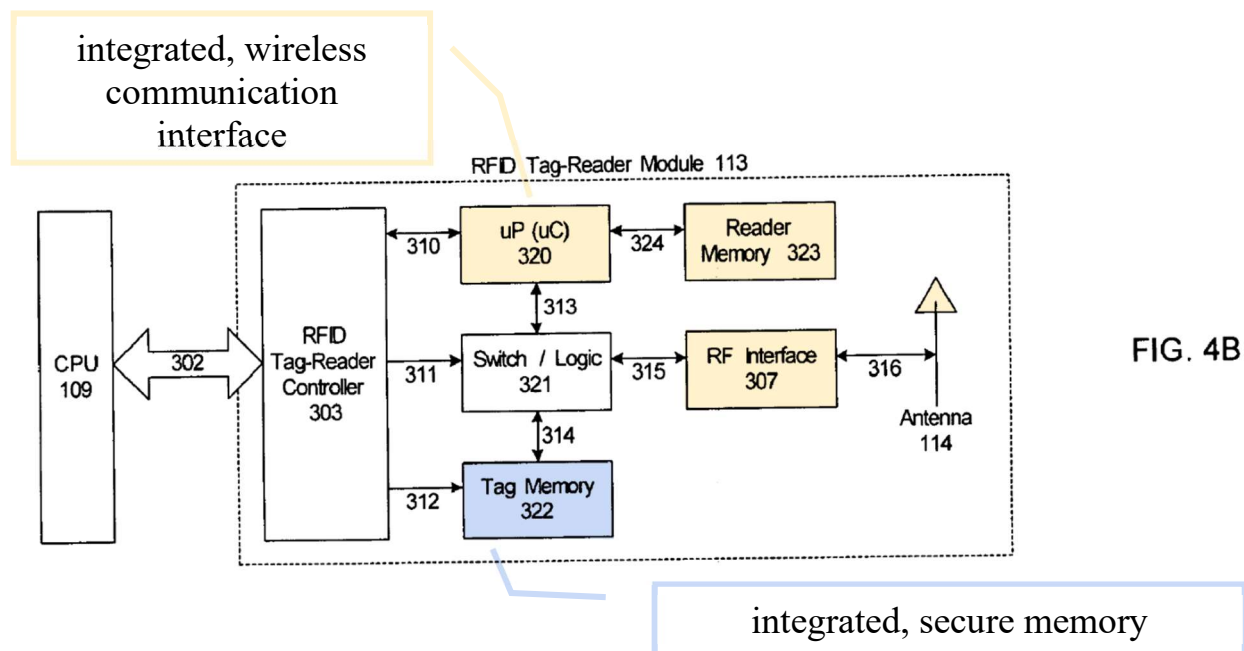
Dua’s device renders obvious an integrated, tamper-resistant memory storing local, encrypted information. Ex-1004, [0105], [0109], [0152]; Ex-1003, ¶¶133-134; §IV.A.1.b.

d. [1c] “an integrated, wireless communication interface for communicating wirelessly with at least one external device within a proximity zone, the integrated, wireless communication interface communicatively coupled to the integrated, secure memory and coupled to draw power from the battery,”

Dua discloses “an integrated, wireless communication interface for communicating wirelessly with at least one external device within a proximity zone” because its RFID reader component (integrated, wireless communication

interface) communicates wirelessly with at least one external RFID tag when within a proximity zone. Ex-1004, [0071]-[0072], [0122], [0127]; Ex-1003, ¶¶135-136; §IV.A.1.b.

Dua further discloses that “the integrated, wireless communication interface [is] communicatively coupled to the integrated, secure memory” because Dua’s RFID reader component (integrated, wireless communication interface) is communicatively coupled to the integrated, secure tag memory for communication with the integrated, secure tag memory, as shown below. Ex-1003, ¶137.



Ex-1004, Fig. 4B (annotated). Dua’s RFID Tag-Reader Module includes “an integrated RFID Tag-Reader Controller 303 that manages all communication between CPU 109 and the functional components of RFID Tag-Reader Module 113,” and “tag logic” (switch/logic component 321). *Id.*, [0106], [0108]. Dua

explains that during cross-discovery, an RFID tag can be written with data received by an RFID reader. *Id.*, [0152]. Accordingly, the integrated, wireless communication interface is communicatively coupled to the integrated, secure memory to update the information stored in the RFID tag memory. *Id.*, [0151]-[0154].

Lastly, Dua discloses “the integrated, wireless communication interface [is] communicatively...coupled to draw power from the battery” because Dua’s RFID reader component is communicatively coupled to draw power from the battery to transmit interrogation signals. Ex-1004, [0094], [0071], [0094]; Ex-1003, ¶138; §IV.A.1.b.

- e. **[1d] “wherein one or more of (a) the integrated, wireless communication interface communicating wirelessly with the at least one external device within the proximity zone enables one or more of an application, a function, and a service and (b) the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and a service.”**

Dua discloses [1d] that either the integrated, wireless communication interface or the local, secured information stored by the integrated, secure memory enables an application, function, or service. Ex-1003, ¶¶139-140; §IV.A.1.d.

(a) The Integrated, Wireless Communication Interface Communicating Wirelessly with the External Device Within the Proximity Zone Enables an Application, Function, or Service:

Dua discloses that, when an external device is within a proximity zone of its integrated RFID reader (integrated, wireless communication interface), the integrated RFID reader (integrated, wireless communication interface) communicates wirelessly with the external device's RFID tag. Ex-1003, ¶141; §IV.A.1.d. Data received by the RFID reader is sent to the device's CPU for use by applications operating on the device to generate a Bluetooth paging message to enable wireless connection and transmission of media to the external device, as in [1d](a). Ex-1004, [0103], [0123], [0128], [0161], [0172]; Ex-1003, ¶142.

(b) The Local, Secured Information Stored by the Integrated, Secure Memory Enables an Application, Function, or Service:

Dua teaches that the local, encrypted financial information stored in the integrated, tamper-resistant memory enables “electronic payments” at point-of-sale, as in [1d](b). Ex-1004, [0052], [0070], [0109]; Ex-1003, ¶143; §V.A.1.d.

B. Dependent Claims

1. [2] “The device of claim 1, wherein at least one of the one or more of the application, the function, and the service is enabled, at least in part, on the device.”
[15] “The method of claim 14, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on the device.”

Dua discloses claims 2 and 15 because the application, service, or function that is enabled runs on the device itself. *See* [14c]; [1d]; Ex-1003, ¶¶144-145, 165.

Dua explains that the device may “conserve power by not always having their wireless interface turned on.” Ex-1004, [0144], [0137]. Dua explains that the device uses the RFID discovery/paging process to help “facilitate the automatic activation of a radio transceiver” in the device. *Id.*, [0144].

2. **[3] “The device of claim 1, wherein at least one of the one or more of the application, the function, and the service is enabled, at least in part, external to the device using an external, wireless communication interface, the device communicatively coupled to wirelessly communicate with the external, wireless communication interface.”**
[16] “The method of claim 14 further comprising: sending the enablement signal, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on a device external to the device and communicatively coupled to an external, wireless communication interface.”

Dua discloses claims 3 and 16 that an application, function, or service that is enabled runs externally to the device using an external, wireless communication interface. *See* [1d], [14c]; Ex-1003, ¶¶146-147, 166. Dua explains that its integrated RFID tag could establish “wireless communication between a diverse set of [external] devices” for various purposes, including “for electronic payments” at point-of-sale or to “secure key access to buildings.” Ex-1004, [0052], [0070]. Dua’s device uses RFID to wirelessly communicate with the external RF 13.56 MHz readers. *Id.*, [0089]. Credit card information stored in the device is sent via the integrated RFID Tag-Reader Module to the external RFID reader at the point-of-sale device for enabling electronic payments. *Id.*, [0070], [0224].

3. [4] **“The device of claim 1, wherein the local, secured information includes biometric information for authenticating a user.”**
[17] **“The method of claim 14, wherein the local, secured information includes biometric information for authenticating a user.”**

Dua and Giobbi157 render obvious claims 4 and 17 because the information stored locally on its integrated tag is secured biometric information for authenticating a user. Ex-1003, ¶¶148-150, 167. Dua discloses that its device may include “an integrated biometric fingerprint reader [to] provide[] enhanced security for protecting...against unauthorized use.” Ex-1004, [0058]. Giobbi157 teaches storing a “biometric profile” in a local, secured memory, so that a user would use “a matching biometric input” obtained from the device to “unlock” the tag memory. Ex-1006, [0043]. Giobbi157 teaches that the biometric input would be used to compare “stored biometric information” to authenticate the user (e.g., fingerprint authentication). *Id.*, [0028], [0037]-[0038], [0048]. A POSITA would have been motivated to include biometric information for authenticating a user in Dua’s local, tamper-resistant tag memory, because doing so would promote Dua’s purpose of “enhanc[ing] security for protecting...against unauthorized use.” Ex-1004, [0058]; Ex-1003, ¶149. A POSITA would have been capable of storing “biometric information for authenticating a user” in Dua’s tag memory, as Giobbi157 teaches, because storing “biometric information for authenticating a user” in tag memory

would require minimal modification without undue experimentation. Ex-1003, ¶150. Such a combination would have been no more than combining prior art elements using known methods to yield predictable results. Ex-1003, ¶150; *see, e.g., Friskit*, 306 F. App'x at 616. A POSITA would have had a reasonable expectation of success in storing “biometric information for authenticating a user” in Dua’s tamper-resistant tag memory. Ex-1003, ¶150.

4. [5] **“The device of claim 1, wherein the local, secured information includes biometric information based on a biometric scan of a finger, the biometric information for authenticating a user.”**

Dua and Giobbi157 render obvious claim 5 because the biometric information is based on a biometric scan of a finger. Ex-1006, [0037]; Ex-1003, ¶¶151-152; §IV.B.3. Giobbi157 explains that in the “case of fingerprint authentication,” “the biometric profile sample may represent only [a] small portion area of the full fingerprint image,” “the fingerprint profile sample...[may] describe[] an arc of one or more lines of the fingerprint,” or “the fingerprint profile sample can be data representing color information of the fingerprint.” Ex-1006, [0038]; Ex-1003, ¶152.

5. **[6] “The device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information.”**
[18] "The method of claim 14, wherein the local, secured information includes financial information and wherein the one or more of the application, the function and the service completes a financial transaction."

Dua and Giobbi157 render obvious claims 6 and 18 because Dua discloses that the local, secure information may be “credit card profile or other payment information” used to complete financial transactions (e.g., “electronic payments” at point-of-sale). Ex-1004, [0052], [0070], [0224]; Ex-1003, ¶¶153-154; §IV.A.1.d. Dua does not expressly disclose where the credit card profile or other payment information is stored, but Dua in view of Giobbi157 renders obvious that the credit card profile or other payment information would have been stored in its tamper-resistant tag memory. *Id.*, [0105], [0109]; Ex-1003, ¶¶154, 168.

6. **[8] “The device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on an authorization of the financial information using an external authentication database, the financial information transmitted to the external authentication database.”**

Dua and Giobbi157 render obvious claim 8. Dua discloses that its RFID Tag-Reader Module “can also be used in connection with other applications...such as electronic payments at the point-of-sale.” Ex-1004, [0070]; Ex-1003, ¶¶155-156.

Giobbi157 discloses that its external reader is communicatively coupled “to receive and/or transmit information to remote databases for remote authentication.” Ex-1006, [0031], [0053]. The remote databases include a “validation database...for authorizing a transaction to be processed.” *Id.*, [0033]. In Giobbi157, “the process involves transmitting credit card (or other purchasing information) to a validation database 112 to authorize the purchase and receive the status of the card.” *Id.*, [0074]. A POSITA would have been motivated to use an external validation database, as Giobbi157 teaches, because the validation database would provide protection to ensure that “the card is active and not reported lost or stolen and that sufficient funds are present to execute the purchase,” *id.*, when Dua’s RFID Tag-Reader Module is used for “electronic payments at the point-of-sale.” Ex-1004, [0070]. A POSITA would have been motivated to use an external validation database, as Giobbi157 teaches, because doing so would require minimal modification without undue experimentation. Ex-1003, ¶156. Such a combination would have been no more than combining prior art elements using known methods to yield predictable results. Ex-1003, ¶156; *see, e.g., Friskit*, 306 F. App’x at 616. A POSITA would have had a reasonable expectation of success in using a validation database to complement the financial transaction. Ex-1003, ¶156.

[9] “The device of claim 8, wherein the external authentication database is separate from a merchant providing a sale in the financial transaction.”

Dua and Giobbi157 render obvious claim 9. As discussed with respect to claim 8, Giobbi157 discloses an external validation database. Giobbi157 discloses that “in purchase transactions, the validation database 112 is a credit card validation database that is separate from the merchant providing the sale.” Ex-1006, [0033]. Ex-1003, ¶¶157-158.

[10] “The device of claim 1, wherein the one or more of the application, the function and the service enabled based on the local, secured information stored by the integrated, secure memory includes a first application, function or service based on a first subsets of local, secured information stored by the integrated, secure memory and a second application, function or service based on a second subset of local, secured information, the first and second subset of local, secured information having different accessibility.”

Dua and Giobbi157 render obvious claim 10 because its integrated RFID tag could establish “wireless communication between a diverse set of devices,” including “for electronic payments” at point-of-sale or to “secure key access to buildings.” Ex-1004, [0052], [0070].

As the '960 patent explains, a device may have two applications, each of which can access a different local, secured information stored on an integrated, secure memory. Ex-1001, 9:48-54. A first application (e.g., “auto login/logoff”) may be “enabled” based on a first local, secured information (e.g., “username and

password”), Ex-1001, 9:54-57, while a second application (e.g., “credit card transaction”) uses a second local, secured information (e.g., biometric information” or “credit card information,” etc.), 1001, 9:57-62, 9:20-26. It would have been obvious that the information for “electronic payments” is different from information for “secure key access to buildings.” Ex-1003, ¶161. Indeed, Giobbi157 discloses storing multiple user profiles, such as biometric profile, PIN profile, picture profile, registry profile, credit cards, and personal information, in its secured and tamperproof memories. Ex-1006, [0037]-[0042], [0058]. Each of the profiles provides a different accessibility to certain application, function, or service. One profile may be used to enable “access to secure physical or digital assets,” and another may be used for completing a purchase transaction. *Id.*, [0063]. A POSITA would have been motivated to store multiple subsets of local, secured information, as Giobbi157 teaches, so the device can access different applications, functions, or services. A POSITA would have been motivated to store a credit card information in one subset of local, secured information for credit card processing, and a biometric profile or PIN profile in another subset of local, secured information for accessing physical assets, such as gaining access to buildings. Ex-1003, ¶162. A POSITA would have been motivated to use multiple profiles, as Giobbi157 teaches, because doing so would require minimal modification without undue experimentation. Ex-1003, ¶162. Such a combination would have been no more than combining prior

art elements using known methods to yield predictable results. Ex-1003, ¶162; *see, e.g., Friskit*, 306 F. App'x at 616. A POSITA would have had a reasonable expectation of success in using multiple profiles. Ex-1003, ¶162.

7. [11] **"The device of claim 1, wherein the device is a cell phone."**
[19] **"The method of claim 14, wherein the device is a cell phone."**

Dua discloses claims 11 and 19 because the device may be a device such as a cell phone. Ex-1004, [0057], [0070]; *see* claims 1, 14; Ex-1003, ¶¶163-164, 169.

V. Grounds 2 and 3: Buer Renders Obvious Claims 1-7, 10-11, and 14-19 (Ground 2); Buer and Giobbi¹⁵⁷ Render Obvious Claims 4, 8-10, 12, 13, 17, and 20 (Ground 3).

A. Independent Claims

Buer renders obvious each of independent claims 1 and 14. Ex-1003, ¶¶170-171. Independent claim 14 is representative.

1. Claim 14

a. [14pre] "A method comprising:"

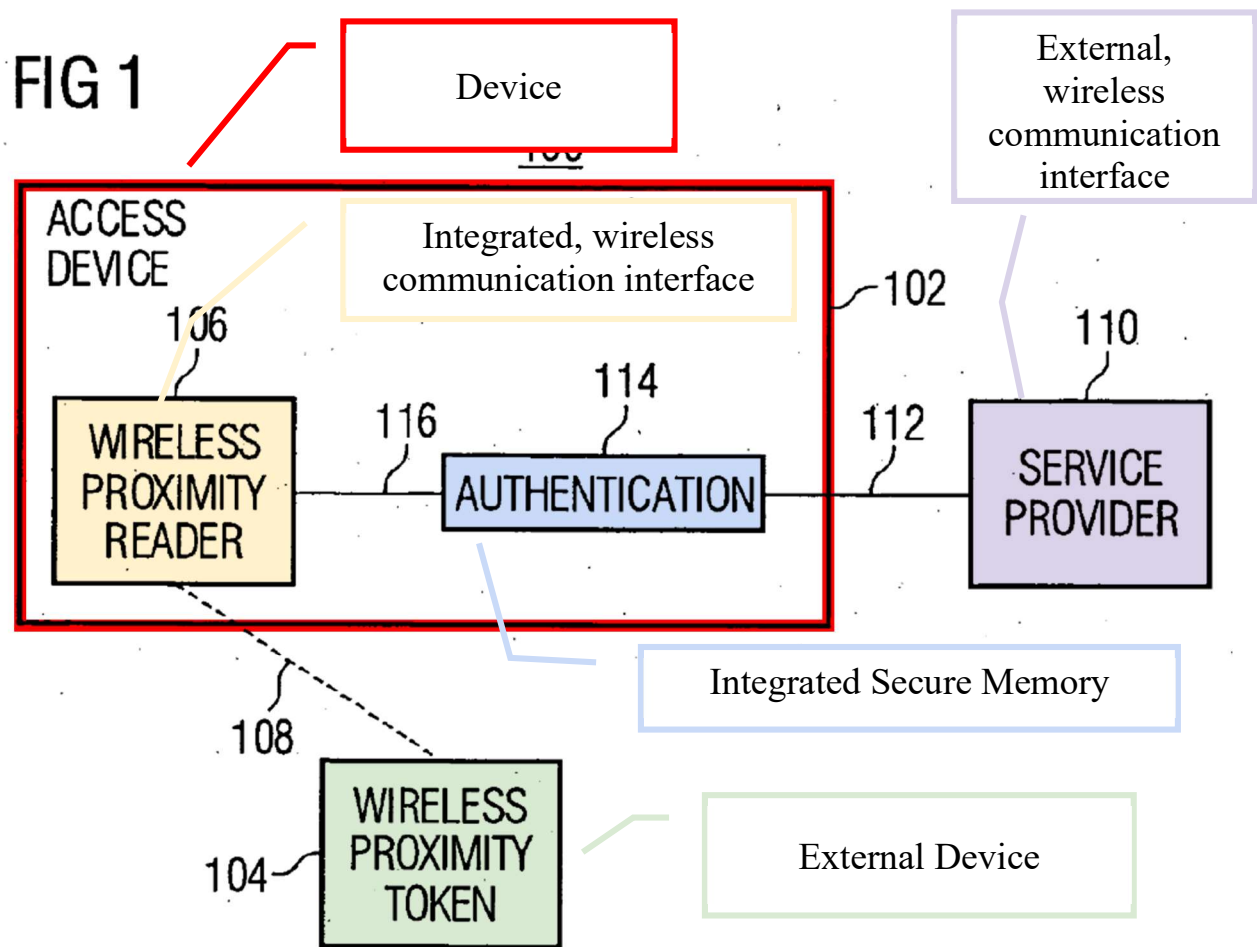
To the extent the preamble for claim 14 is limiting, Buer discloses the preamble because it discloses a method for an access device to access a secured service. Ex-1003, ¶172.

- b. **[14a] “creating a first wireless link between an integrated, wireless communication interface of a device and an external device, the device including a battery, an integrated, secure memory, and the integrated, wireless communication interface, wherein the integrated, secure memory stores local, secured information and the integrated, wireless communication interface is powered by the battery;”**

Buer discloses [14a].

(1) A device including an Integrated, Secure Memory and an Integrated, Wireless Communication Interface:

Buer discloses the device in [14a] because it discloses an access device that combines an authentication circuitry (an integrated, secure memory) and a wireless proximity reader (an integrated, wireless communication interface) within a device, as shown below. Ex-1003, ¶174.

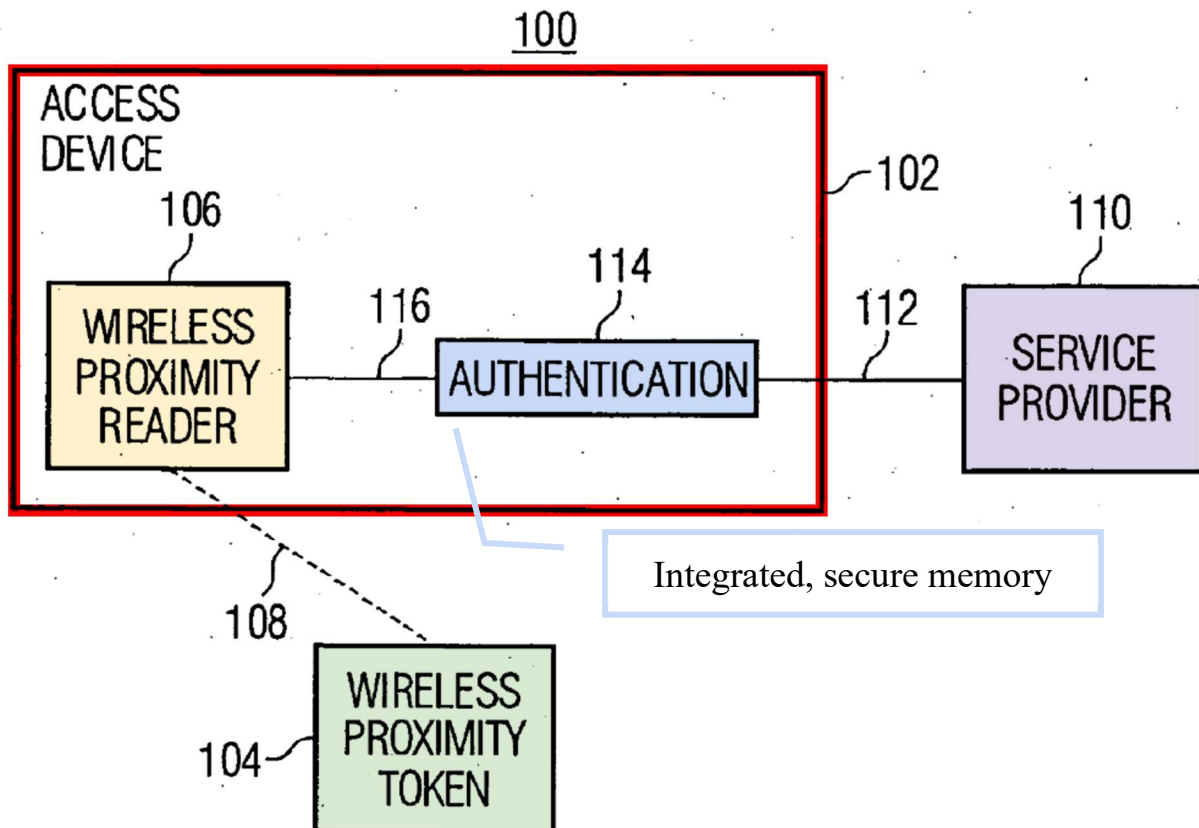


Ex-1005, Fig. 1 (annotated). Buer's authentication system provides access to a secured service, where the access is controlled based on the proximity of a wireless token to an access device. Ex-1003, ¶¶. In Figure 1, Buer's access device 102 ("device," **red**) includes two components: an authentication component 114 ("integrated, secure memory," **blue**) and a wireless proximity reader 106 ("integrated, wireless communication interface," **yellow**). Ex-1005, Fig. 1. The authentication component 114 is configured to process (e.g., encrypt or sign) the information before sending it to the service provider 110 (**purple**). *Id.*, [0118], Fig.

1. The wireless proximity reader 106 is configured to receive information from a wireless proximity token 104 (“external, secure memory,” **green**) when the token is proximate to the access device. *Id.*, [0111]-[0112], Fig. 1.

In Buer’s access device, as shown below, the authentication component discloses the integrated secure memory. Ex-1003, ¶175.

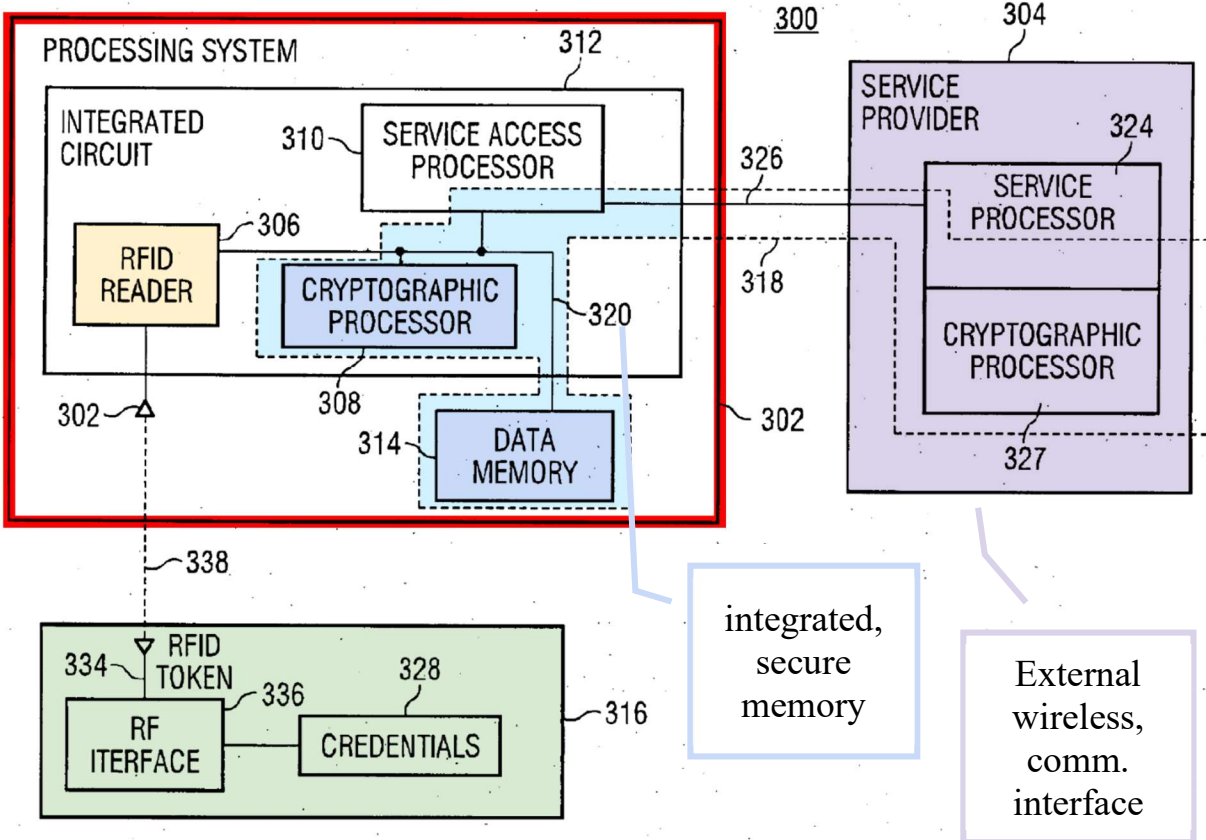
FIG 1



Ex-1005, Fig. 1 (annotated). In Buer, the authentication component is implemented as a cryptographic processing system, *id.*, Figs. 3, 6, and, as shown below, is an operably connected collection of circuit components (**blue**) that include a

cryptographic processor and data memory (“integrated, secure memory”). *Id.*, [0137].

FIG 3

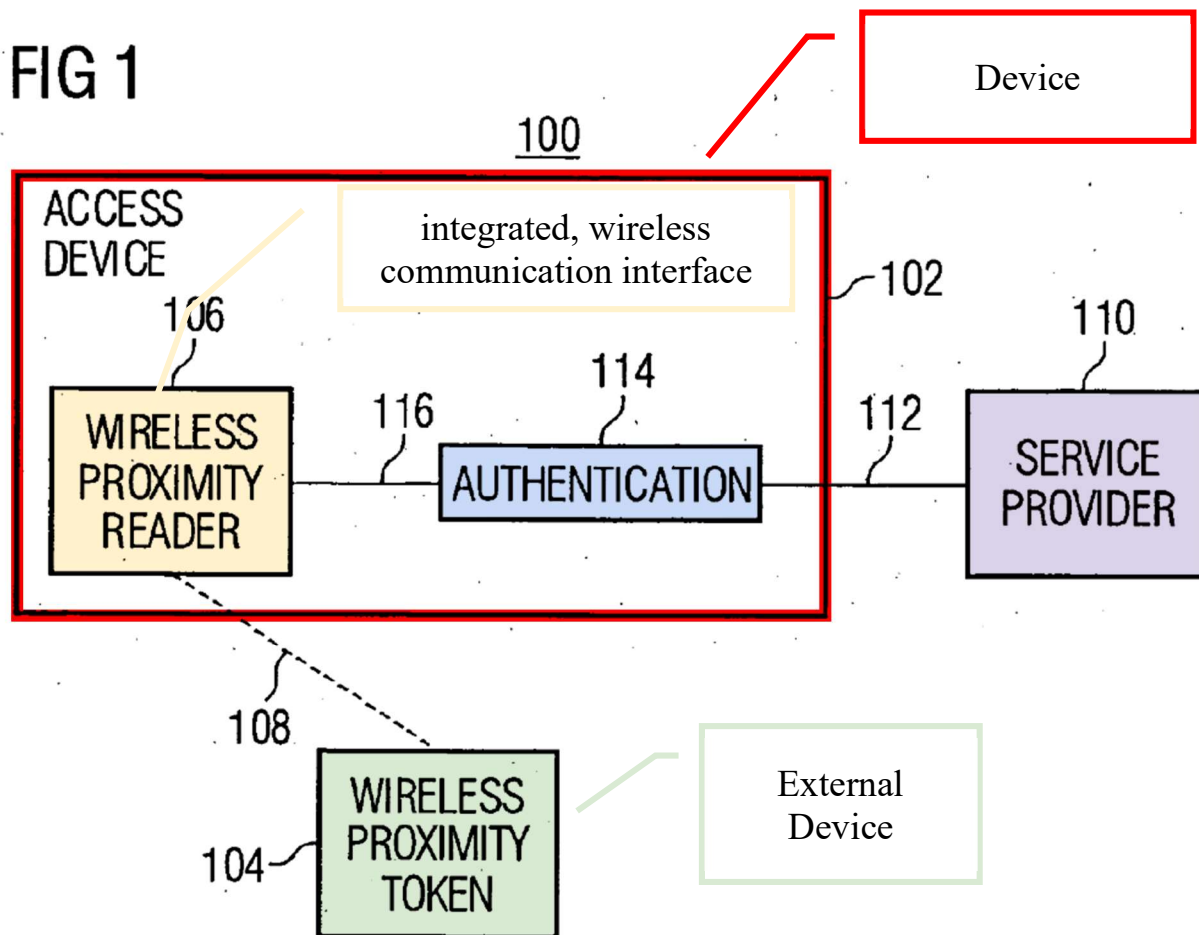


Id., Fig. 3 (annotated). Buer’s cryptographic processor 308 acts as a controller for encrypting any important information, such as a user’s credentials (“information particular to a user”), received from the external token. *Id.*, [0119], [0135]-[0137], [0141], [0150]. The encrypted information (and credentials) is stored in data memory 314 within the cryptographic boundary 318 (light blue). *Id.*, [0135], [0137]. As Buer explains, the memory may use “tamper resistant and/or tamper evident hardware.” *Id.*, [0013], [0134]. The information is encrypted when stored in data

memory 314 within the cryptographic boundary. *Id.*, [0135], [0137]. Accordingly, Buer discloses an integrated, tamper-resistant memory storing local, encrypted information. Ex-1003, ¶175.

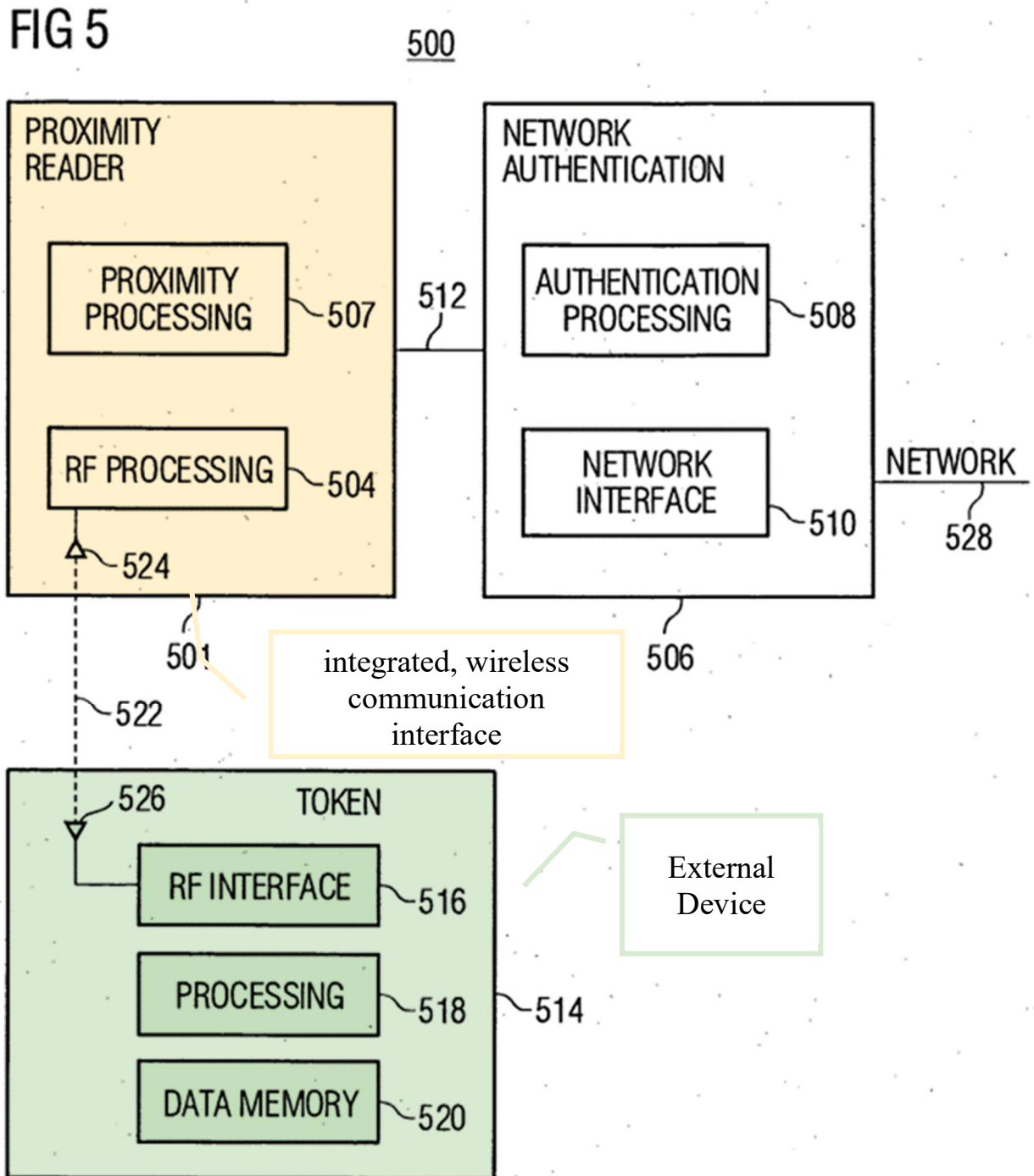
Buer's wireless proximity reader discloses the integrated, wireless communication interface in [14a] because Buer's wireless proximity reader 106 ("integrated, wireless communication interface," yellow), as shown below, is a component that is "configured to receive signals 108 (e.g., RF signals)" from at least one wireless proximity token 104 ("external device," green) when the token 104 is "proximate to the access device 102." Ex-1005, [0111]; Ex-1003, ¶176.

FIG 1



Ex-1005, Fig. 1 (annotated). Buer's proximity reader 501 may include a collection of circuit components, including an antenna 524, an RF processing component 504, and a proximity processing component 502, 507,⁵ as shown below. *Id.*, [0157].

⁵ There appears to be a typographical error in Figure 5 because the proximity processing component should be labeled 502. See Ex. 1005, [0157].



Id., Fig. 5 (annotated).

In Buer, the “wireless proximity reader and token may be implemented using one or more of a wide variety of wireless proximity techniques.” *Id.*, [0128]. As Buer

explains, the proximity reader and the external token communicate via RF signals when they are within proximity to one another. *Id.*, [0112], [0146], [0157], [0173]. In particular, the token stores encrypted authentication information that is provided to the proximity reader. *Id.*, [0130], [0158]. The reader receives the encrypted data and extracts any embedded information. *Id.*, [0097], [0184]. Accordingly, the proximity reader necessarily decodes the encrypted information for later processing (including for extracting the embedded information, as disclosed). Ex-1003, ¶177.

Because Buer's access device includes an integrated authentication component and a wireless reader, Buer discloses a device with both an integrated, secure memory and an integrated, wireless communication interface, as recited in [14a]; Ex-1003, ¶178.

(2) The device including a Battery:

Buer discloses that its access device may be implemented as a mobile device, such as a cellular phone. Ex-1005, [0163], [0195]. A POSITA would have understood that the mobile device would include, although not shown, a battery to power its internal components. Ex-1003, ¶179. A POSITA would have been motivated to include a battery within the mobile device, instead of relying on an external power source, because doing so would enable the mobile device to be untethered from the external power source, further enhancing mobility and promoting a better user experience. Ex-1003, ¶179. A POSITA would have been

capable of including a battery because it would require minimal modification without undue experimentation. Ex-1003, ¶180. Such a combination would have been no more than combining prior art elements using known methods to yield predictable results. Ex-1003, ¶180; *see, e.g., Friskit*, 306 F. App'x at 616. A POSITA would have had a reasonable expectation of success in integrating a battery into Buer's mobile device. Ex-1003, ¶180.

Although Buer does not expressly disclose that the integrated, wireless communication interface is powered by the battery, a POSITA would have understood that integrated wireless proximity reader draws its energy from the battery.⁶ Ex-1003, ¶181.

(3) Creating a First Wireless Link between an Integrated, Wireless Communication Interface of a Device and an External Device:

Buer discloses creating a first wireless link between the wireless proximity reader (integrated, wireless communication interface) and a wireless proximity token (external device) as in [14a]. Ex-1003, ¶¶182-183. As Buer explains, “an RFID

⁶ As Proxense also contends, mobile devices “necessary [sic] require energy to power their operations, which, unless received from a wall plug or a PC, will be provided by a battery.” Ex-1018, 3 (Ex. F, Preliminary Infringement Contentions). Proxense served Final Infringement Contentions, and its position remains the same.

signaling sequence” between the reader and the token includes creating a first set of RF signals that are “used to power and activate the token” before the token can send its information to the reader. Ex-1005, [0146]-[0149].

In Buer, the wireless token is an “external device” that acts as a physical authentication/verification mechanism (e.g., “what the user possesses”). *Id.*, [0114]. If the request was made without the token, access may be denied. *Id.*, [0011]. On the other hand, “after the system verifies that the user (e.g., the user’s token) is relatively close to the device,” access to various services, applications, or functions (e.g., access to data networks, applications, or financial transactions) may be enabled. *See, e.g., id.*, [0120]-[0122], [0155].

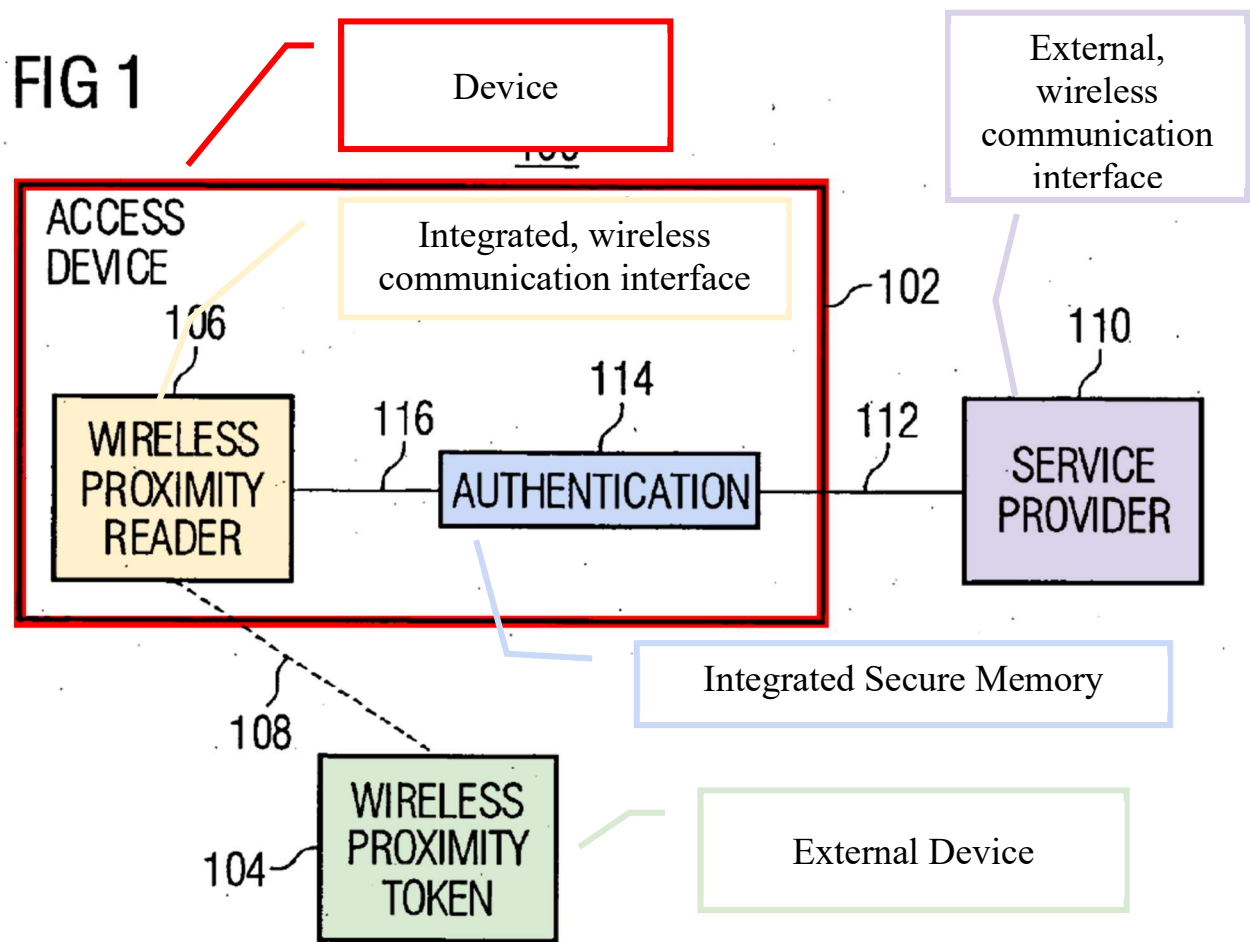
c. [14b] “receiving a first signal, at the integrated, wireless communication interface, via the first wireless link, from the external device; and”

Buer discloses receiving RF signals at the integrated, wireless communication interface from the external device as in [14b] because the integrated reader receives RFID signals, including proximity signaling and authentication information, during the RFID signaling from the external token. Ex-1003, ¶¶184-185. In particular, during the initial RFID signaling sequence, the token may perform proximity signaling by sending RF signals to the proximity reader for the proximity reader to verify that a particular token is within range. Ex-1005, [0157]-[0158]. The token generates additional RF signals to send the encrypted authentication information that

is stored in the token to the proximity reader. *Id.*, [0148]-[0150]; *see also id.*, [0097], [0130], [0158]-[0159], [0184]. The integrated reader receives the RFID signals that are broadcasted from the wireless token and extracts the encrypted authentication information (e.g., credentials) from the RFID signals. *Id.*, [0148]-[0150], Fig. 4; *see also id.*, Figs. 7, 9. Ex-1003, ¶185.

d. [14c] “generating an enablement signal enabling one or more of an application, a function and a service.”

Buer discloses the authentication component generating an enablement signal enabling a wide variety of applications, functions, or services, as in [14c] because it provides encrypted or signed credentials to a service provider to enable access to secured services, as shown below. Ex-1003, ¶¶186-188.



Ex-1005, Fig. 1 (annotated).

[14c] is recited as allowing “mixed operations,” Ex-1001, Abstract, 16:47-54, “the entire element is disclosed by the prior art if one alternative...is in the prior art.” *Fresenius*, 582 F.3d at 1298.

The Integrated, Wireless Communication Interface Communicating Wirelessly with the External Device Within the Proximity Zone Enables an Application, Function, or Service:

Buer discloses that information received wirelessly by the integrated proximity reader from the external token enables the application, service, or function on the device itself. Ex-1003, ¶¶189-190. In Buer, after a proximity reader verifies a user (via an external token), the authentication component generates an enablement signal (e.g., RF signal) providing the necessary authentication information (e.g., signed information) via its cryptographic processing system to a service provider via the service access processor 310, which sends the encrypted information via a communication link 326 to an external cryptographic processor 322, 327⁷ for decryption and/or authentication processing, as necessary and to enable a wide variety of applications, functions, or services on the device. Ex-1005, [0138], [0152]-[0153], [0174]. The service provide may enable access to the following requested service:

[S]ervice may include, for example, access to data and/or a data processing service. Thus, a service may enable an access device to, for example, read or write data in a data memory, access encrypted data, use cryptographic keys, gain access to

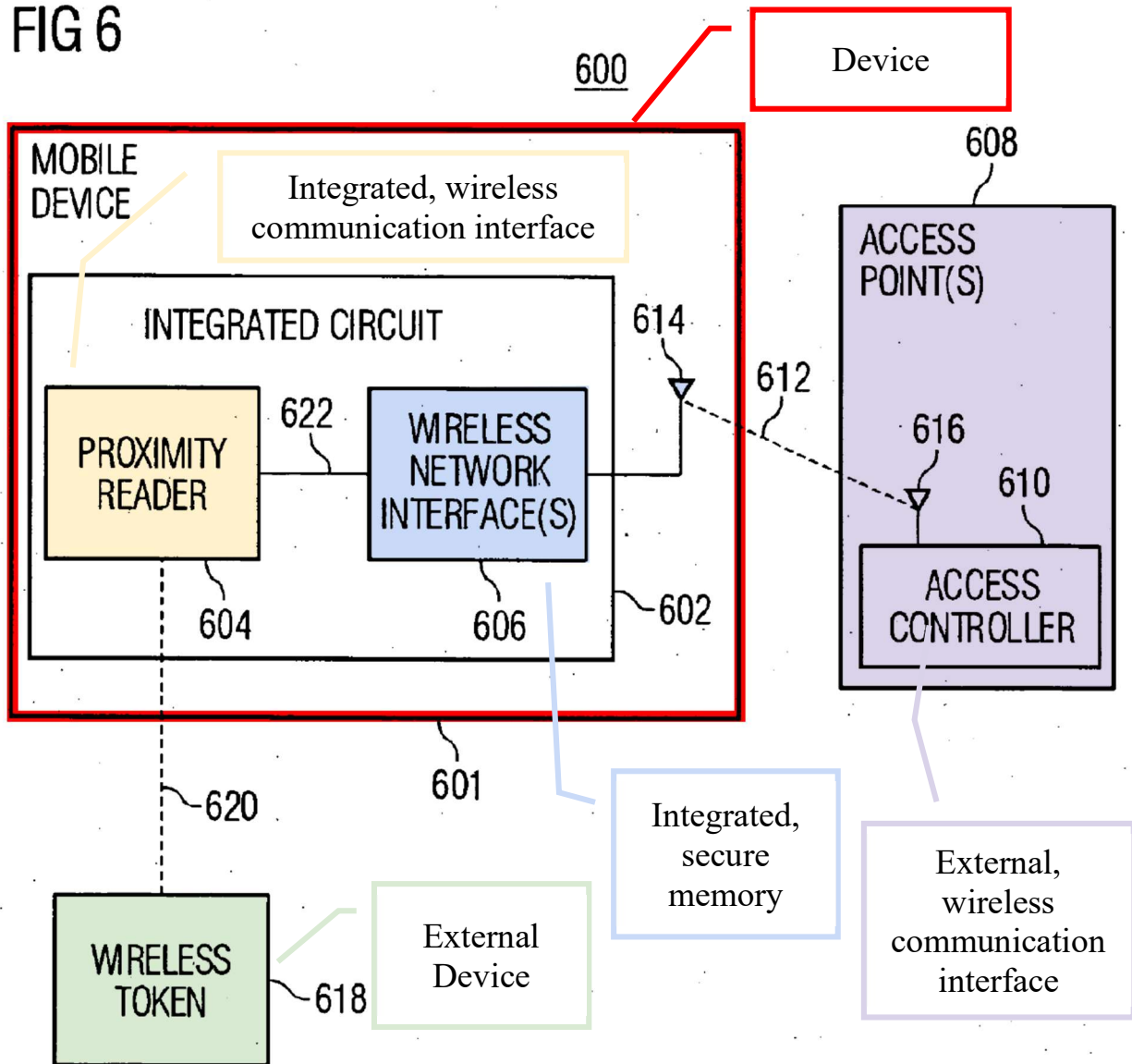
⁷ Figure 3 appears to include a typographical error.

cryptographic material such as security associations and keys,
access a web page, access a data network or access a processing
application.

Id., [0120]; *see also, e.g., id.*, [0122], [0155], [0162], [0193]-[0196]. Buer's application access may include "invoking, interacting with or using the application or loading the application onto the access device." *Id.*, [0122]. Data network access may include "sending and/or receiving data over the network." *Id.*

Like the '960 patent, Buer discloses enabling network access on a device. Buer discloses that the network interface 606 performs "network authentication and connection processing" by "communicating with a respective access controller 610 in one or more access point(s) 608 via RF signals 612" transmitted via antennas 614. *Id.*, [0165]. The RF signals generated by the wireless network interface are enablement signals that contain the encrypted or signed information that is sent to the "network access provider (e.g., access point 608)." *Id.*, [0165], [0174].

FIG 6



Id., Fig. 6 (annotated).

The network provider then verifies the credentials and provides access to the requested wireless network. *Id.*, [0175]. Thus, the service provider may “enable an access device to...access a data network.” *Id.*, [0120], [0122], Fig. 7. The network may include a cellular network, an 802.11 network, a Bluetooth network, etc. *Id.*, [0163], [0165], [0174].

The Local, Secured Information Stored by the Integrated, Secure Memory Enables an Application, Function, or Service:

Buer discloses that information stored by the integrated, secure memory, such as credit card information, may “be used to authenticate a user to another processing system” (external device) associated with an external proximity reader 1120 (external, wireless communication interface) with “point-of-sale components” to “perform a sales transaction,” such as “credit card transactions.” Ex-1005, [0193]-[0196]. As Buer explains, the mobile device may include a trusted platform module (TPM), which includes a proximity reader that is used to extract any user credential from a token. *Id.*, [0184], [0190]-[0191], [0194]. The extracted credential would be stored in its integrated, secure memory via the local data memory 824. *Id.*, [0185]; Ex-1003, ¶193. As Buer explains, the mobile device’s TPM may include an RFID client, which generates an enablement signal (e.g., RF signal containing credit card information) that is transmitted to another processing system, such as a computer with a point-of-sale device. Ex-1005, [0192]-[0195]. Thus, similar to the ’960 patent, “data services” may be enabled on the external security processing system. *Id.*, [0195]; Ex-1003, ¶193.

2. Claim 1

a. [1pre] “A device comprising:”

To the extent the preamble is limiting, Buer discloses the preamble because it discloses an access device that combines an authentication circuitry and a wireless proximity reader to provide a device. *See* claim 14; Ex-1003, ¶194; §V.A.1.b.

b. [1a] “a battery;”

Buer renders obvious that its access device would have a battery when implemented as a mobile device, such as a cellular phone. Ex-1005, [0163], [0195]; Ex-1003, ¶¶195-196; §V.A.1.b.

c. [1b] “an integrated, secure memory storing local, secured information; and”

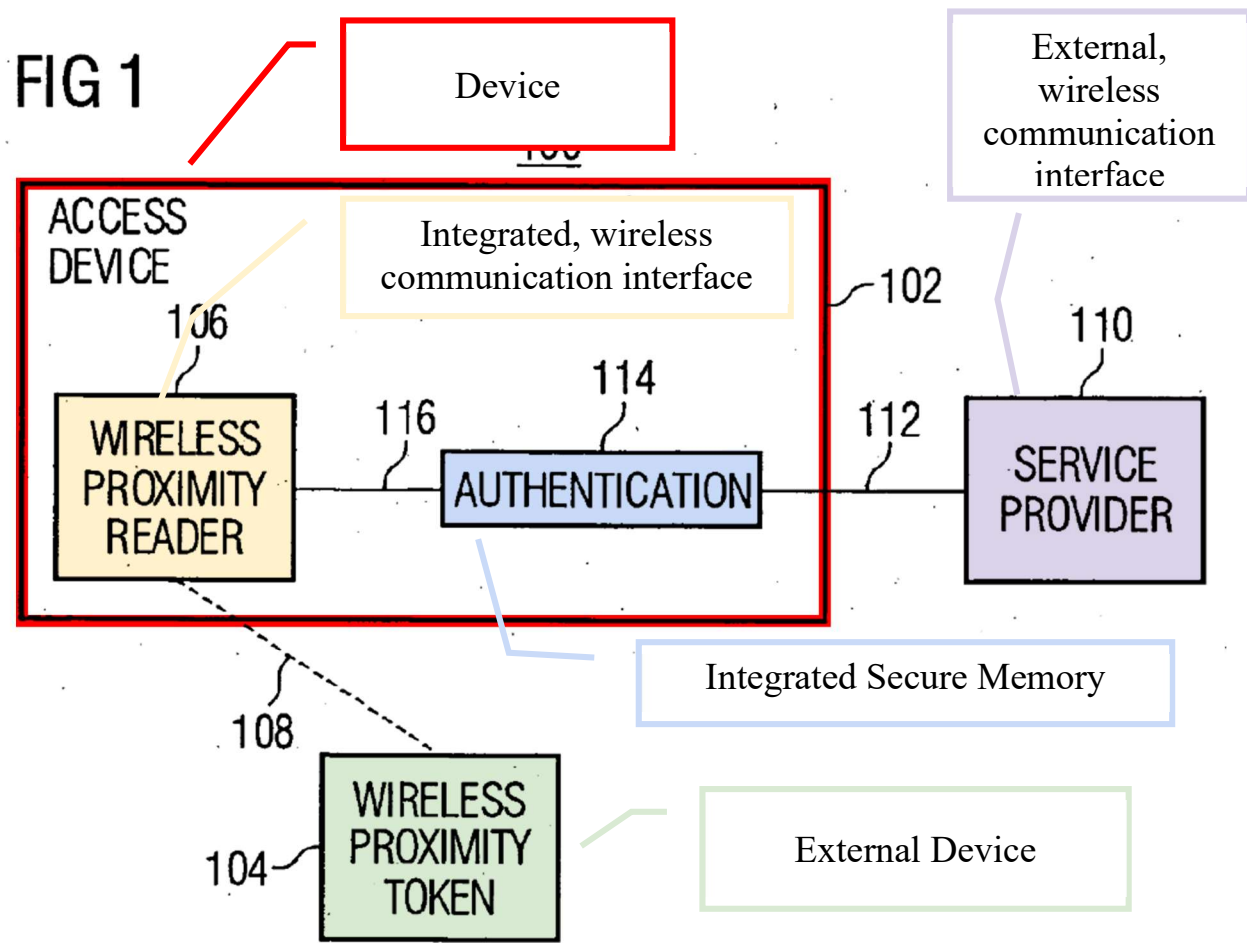
Buer’s device includes an integrated, tamper-resistant memory storing local, encrypted information. Ex-1005, [0013], [0134]-[0137]; Ex-1003, ¶¶197-198; §V.A.1.b.

d. [1c] “an integrated, wireless communication interface for communicating wirelessly with at least one external device within a proximity zone, the integrated, wireless communication interface communicatively coupled to the integrated, secure memory and coupled to draw power from the battery,”

Buer’s integrated wireless proximity reader (integrated, wireless communication interface) communicates “wirelessly with at least” an external token

“within a proximity zone.” Ex-1003, ¶¶199-203; §V.A.1.b. Buer’s wireless proximity reader (integrated, wireless communication interface) is configured to receive RF signals when the token is “proximate to the access device,” such as “when they are within a predefined distance of each other.” Ex-1005, [0111], [0146].

Buer discloses that the integrated “[wireless proximity] reader 106” is communicatively coupled to the integrated, secure memory in the “authentication component 114” “via a connection 116 within a common integrated circuit” as in [1c], as shown below. Ex-1005, [0116]; Ex-1003, ¶201.



Ex-1005, Fig. 1 (annotated).

As discussed above for [1a], when Buer's authentication component is implemented as a cryptographic processing system, it is coupled to the reader via a first data bus 320 in Figure 3 or via a first internal lead 622 in Figure 6. *Id.*, [0137], [0167].

Buer renders obvious that its integrated, wireless communication interface is coupled to draw power from the battery. Ex-1003, ¶¶202-203; §V.A.1.b.

- e. **[1d] “wherein one or more of (a) the integrated, wireless communication interface communicating wirelessly with the at least one external device within the proximity zone enables one or more of an application, a function, and a service and (b) the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and a service.”**

Buer discloses the authentication component enabling a wide variety of applications, functions, or services, as in [1d]. *See* [14c]; Ex-1003, ¶¶204-205; §V.A.1.d. [1d] is recited as allowing “mixed operations” involving several alternatives: (1) what component is used to enable the application, function, or service (e.g., “either or both RDC and PDK functionality”), (2) what is being enabled (e.g., application, function, or service), and (3) which device is being enabled (e.g., device or device with external, wireless communication interface). Ex-1001, Abstract, 16:47-54. Because [1d] recites alternative events, “the entire

element is disclosed by the prior art if one alternative...is in the prior art.” *Fresenius*, 582 F.3d at 1298.

(a) The Integrated, Wireless Communication Interface Communicating Wirelessly with the External Device Within the Proximity Zone Enables an Application, Function, or Service:

Buer discloses that its integrated proximity reader (integrated, wireless communication interface), communicating wirelessly with an external token within a proximity zone, enables network access on a device, as in [1d](a). Ex-1005, [0120], [0122], [0165], [0174]-[0175], Figs. 6-7; Ex-1003, ¶¶206-208; §V.A.1.d.

(b) The Local, Secured Information Stored by the Integrated, Secure Memory Enables an Application, Function, or Service:

Buer also discloses that the local, encrypted information stored by the integrated, tamper-resistant memory enables network access by sending encrypted or signed information to the “network access provider (e.g., access point 608),” as in [1d](b). Ex-1005, [0165], [0174], [0013], [0134]; Ex-1003, ¶209; §V.A.1.d. Alternatively, Buer discloses that credit card information stored in its trusted platform module (TPM) is used to enable another processing system, such as a computer with a point-of-sale device. Ex-1005, [0192]-[0195]. Thus, similar to the ’960 patent, “data services” may be enabled on the external security processing system. *Id.*, [0195]; Ex-1003, ¶210.

B. Dependent Claims

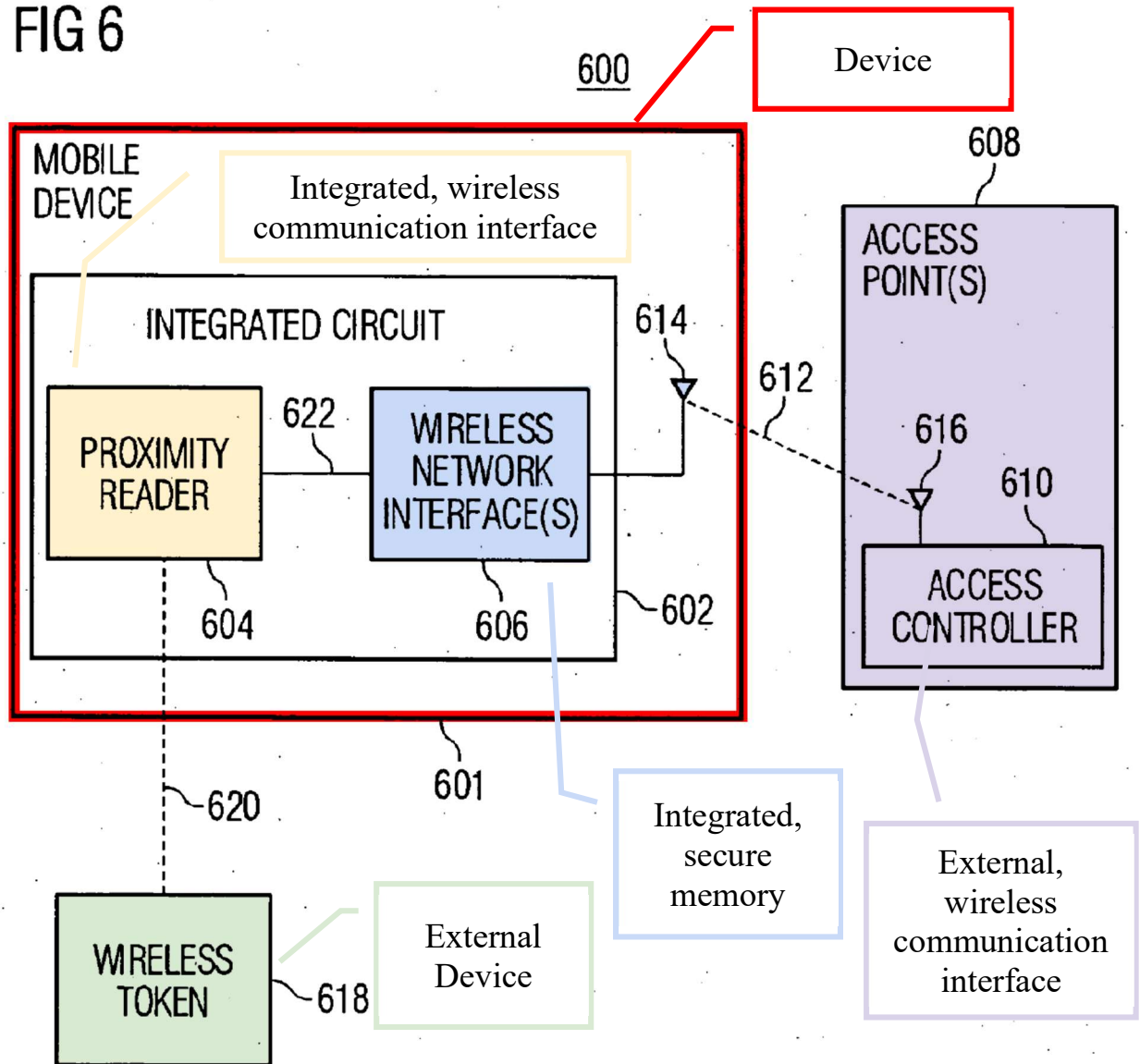
- 1. [2] “The device of claim 1, wherein at least one of the one or more of the application, the function, and the service is enabled, at least in part, on the device.”**

Buer discloses that its integrated proximity reader (integrated, wireless communication interface), communicating wirelessly with an external token within a proximity zone, enables network access on a device. Ex-1005, [0120], [0122], [0165], [0174]-[0175], Figs. 6-7; *see* [1d](a); Ex-1003, ¶¶211-212; §V.A.1.d.

- 2. [3] “The device of claim 1, wherein at least one of the one or more of the application, the function, and the service is enabled, at least in part, external to the device using an external, wireless communication interface, the device communicatively coupled to wirelessly communicate with the external, wireless communication interface.”**

Buer discloses that encrypted information stored on the integrated, secure memory is wirelessly communicated to an external, wireless communication interface to enable an application, function, or service, as shown below. *See* [1d](b); Ex-1003, ¶¶213-214.

FIG 6

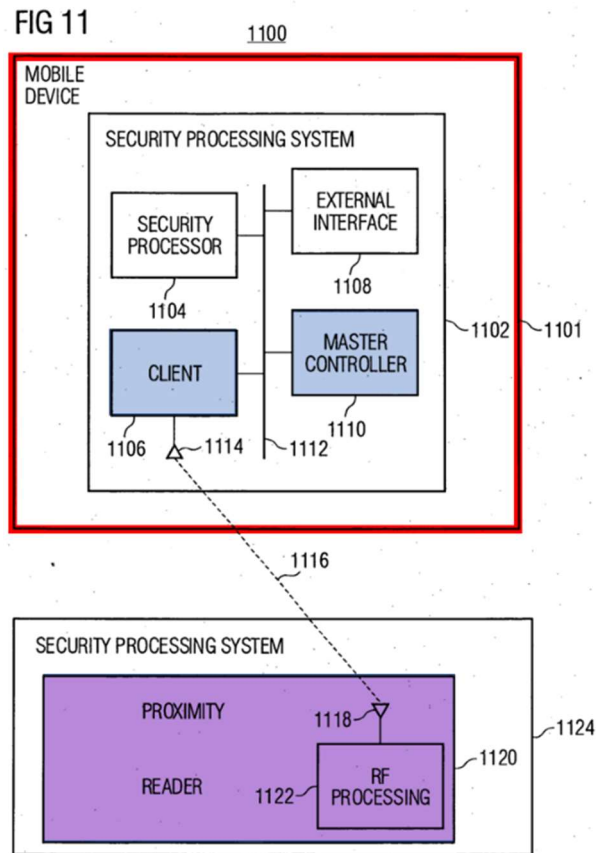


Ex-1005, Fig. 6 (annotated).

Buer's service provider, *id.*, Figs. 1, 3, 6, as a whole, or the internal cryptographic processor 322, 327, or access controller 610 individually, is an external, wireless communication interface because they are "capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing," as the court has construed, or under Google's proposed construction.

Id., [0153], [0165]. In Figure 3, Buer's external cryptographic processor 322, 327 (purple) is capable of receiving encrypted information and "decrypti[ng] and/or authenticati[ng] operations necessary to...receive the encrypted information and provide the information in the clear for internal processing." *Id.*, [0138]. In Figure 6, the access controller 610 is capable of wirelessly receiving data over a given wireless network. *Id.*, [0165]. Buer's access controller 610 receives encrypted or "signed information." *Id.*, [0174]-[0175]. A POSITA would have understood that the access controller 610, or the service provider (e.g., access point 608), would decode the encrypted or signed information for further verification of the credentials, similar to the cryptographic processing disclosed in Figure 3. Ex-1003, ¶¶215-217. Like the '960 patent, Buer discloses enabling network access by sending encrypted or signed information to the "network access provider (e.g., access point 608)." Ex-1005, [0165], [0174].

Alternatively, Buer discloses that credit card information stored by the integrated, secure memory may "be used to authenticate a user to another processing system" (external device) associated with an external proximity reader 1120 (external, wireless communication interface) with "point-of-sale components" to "perform a sales transaction," such as "credit card transactions," as shown below. *Id.*, [0193]-[0196].



Id., Fig. 11 (annotated). Ex-1003, ¶218.

3. [4] “The device of claim 1, wherein the local, secured information includes biometric information for authenticating a user.”

Buer discloses claim 4 because the various authorization data for authenticating a user includes “password” and biometric information. Ex-1005, [0181], [0130], [0114]. A POSITA would have understood that when a token transfers its stored information (such as stored biometric information), *id.*, [0149], that information is sent to the device, the biometric information is encrypted using

Buer's cryptographic processing and stored in the local, secured memory in the device. Ex-1005, [0135]. Ex-1003, ¶¶219-221.

Alternatively, Buer and Giobbi157 render obvious that the local, encrypted information is biometric information for authenticating a user. Buer discloses that its device may include "a biometric reader to further verify the authenticity of the user" using a "biometric characteristic," such as "a fingerprint." Ex-1005, [0114], [0181]. Giobbi157 teaches storing a "biometric profile" in a local, secured memory, so that a user would use "a matching biometric input" obtained from the device to "unlock" the tag memory. Ex-1006, [0043]. Giobbi157 teaches that the biometric input would be used to compare "stored biometric information" to authenticate the user (e.g., fingerprint authentication). *Id.*, [0028], [0037]-[0038], [0048]. A POSITA would have been motivated to include biometric information for authenticating a user in Buer's local, tamper-resistant memory, because doing so would promote Buer's purpose of restricting access to service until the user satisfies additional verification queries. Ex-1005, [0114]; [0013], [0134]; Ex-1003, ¶¶239-242. A POSITA would have been capable of storing "biometric information for authenticating a user" in Buer's memory, as Giobbi157 teaches, because storing "biometric information for authenticating a user" in memory would require minimal modification without undue experimentation. Ex-1003, ¶243. Such a combination would have been no more than combining prior art elements using known methods

to yield predictable results. Ex-1003, ¶243; *see, e.g., Friskit*, 306 F. App'x at 616. A POSITA would have had a reasonable expectation of success in storing “biometric information for authenticating a user” in Buer’s tamper-resistant memory. Ex-1003, ¶243.

4. **[5] “The device of claim 1, wherein the local, secured information includes biometric information based on a biometric scan of a finger, the biometric information for authenticating a user.”**

Buer discloses that the biometric information may be “a fingerprint” used to verify the authenticity of the user. Ex-1005, [0114], [0196], [0130]. Ex-1003, ¶¶222-223.

5. **[6] “The device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information.”**

Buer discloses that the local, secure information may be “credit card information,” and the information is used to “perform a sales transaction.” Ex-1005, [0195]. Ex-1003, ¶¶224-225.

6. [7] **“The device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on a signal received from the at least one external device by the integrated, wireless communication interface.”**

Buer discloses sending financial information from the integrated, secure memory to the external RF processing component for use by the RF processing component. Ex-1005, [0194]-[0195]. Ex-1003, ¶¶226-229; §V.B.2. Buer explains that its external token may also be equipped “with smart card functionality” (e.g., “credit cards”) so that a user’s “credit card information” may be provided to an integrated proximity reader in an access device. Ex-1004, [0129]-[0130], [0193], Fig. 8. It would have been obvious to implement Buer’s “key management functions” to “back[up]” or store the external token’s credit card information on the user’s cellular phone for point-of-sale transactions. *Id.*, [0177], [0195]. A POSITA would have been motivated to use the token to transfer the credit card information in a secure manner to the cellular phone without the user having to directly enter the information into the device. Ex-1005, [0007]; Ex-1003, ¶228. Moreover, a POSITA would have been motivated to provide financial transactions “only when a wireless token assigned to the user is in the proximity of” the cellular phone to further protect against unauthorized use of the credit card information, Ex-1005, [0011], or to utilize

the cellular phone's "biometric reader to further verify the authenticity of the user," *id.*, [0114]. Ex-1003, ¶229.

7. [8] **"The device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on an authorization of the financial information using an external authentication database, the financial information transmitted to the external authentication database."**

Buer and Giobbi¹⁵⁷ render obvious that a financial transaction is completed based on an authorization of the financial information using an external authentication database. Ex-1003, ¶¶244-245. In Giobbi¹⁵⁷, its external reader is communicatively coupled "to receive and/or transmit information to remote databases for remote authentication." Ex-1006, [0031], [0053]. The remote databases include a "validation database...for authorizing a transaction to be processed." *Id.*, [0033]. In Giobbi¹⁵⁷, "the process involves transmitting credit card (or other purchasing information) to a validation database 112 to authorize the purchase and receive the status of the card." *Id.*, [0074]. A POSITA would have been motivated to implement Giobbi¹⁵⁷'s validation database in Buer's security processing system 1124 with the point-of-sale components because doing so would enhance Buer's "credit card transactions," Ex-1005, [0193]-[0196], to provide status information concerning whether "the card is active and not reported lost or stolen and that sufficient funds are present to execute the purchase," Ex-1006, [0074],

which can only be verified using an external database.]; Ex-1003, ¶246. Accordingly, a POSITA would have been motivated to implement Buer's external processing system with access to a validation database to authorize the purchase and to "display[] status to a user." Ex-1006, [0026], [0074]. A POSITA would have been motivated to implement Buer's external processing system with Giobbi157's validation database, at least, because Buer and Giobbi157 are in the same field of endeavor—the field of incorporating RDC/PDK (wireless communication interface and secure memory) technology into devices to allow secure data sharing and services. Ex-1005, Abstract; Ex-1006, [0026]. Likewise, a POSITA would recognize that Buer and Giobbi157 use similar techniques to solve the same problem. Ex-1003, ¶247. A POSITA would have been capable of coupling one or more external databases to Buer's external processing system because Buer and Giobbi157 use similar hardware, and the combination would require minimal modification without undue experimentation. Ex-1005, [0114], [0125], [0163]; Ex-1006, [0030], [0035]; Ex-1003, ¶248. Such a combination would have been no more than combining prior art elements using known methods to yield predictable results. Ex-1003, ¶248; *see, e.g., Friskit*, 306 F. App'x at 616. A POSITA would have had a reasonable expectation of success in integrating those components into Buer because Giobbi157 explains how to do so via a network. Ex-1003, ¶248.

8. [9] **“The device of claim 8, wherein the external authentication database is separate from a merchant providing a sale in the financial transaction.”**

Buer and Giobbi¹⁵⁷ render obvious claim 9 because Giobbi¹⁵⁷ discloses that “in purchase transactions, the validation database 112 is a credit card validation database that is separate from the merchant providing the sale.” Ex-1006, [0033]. Ex-1003, ¶¶249-250.

9. [10] **“The device of claim 1, wherein the one or more of the application, the function and the service enabled based on the local, secured information stored by the integrated, secure memory includes a first application, function or service based on a first subsets of local, secured information stored by the integrated, secure memory and a second application, function or service based on a second subset of local, secured information, the first and second subset of local, secured information having different accessibility.”**

Buer discloses that its access device can secure access to multiples applications, functions, or services. Ex-1005, [0120]-[122], [0193]-[0195]. Buer provides different examples of services the access device may have access, including “data and/or a data processing service,” “a web page,” “processing application,” and “sales transactions.” *Id.* Buer explains that “multiple sets of information (e.g., credentials) may be included on a single token to enable a user to access different services.” *Id.*, [0127], [0177]. Ex-1003, ¶230.

A POSITA would have found obvious that the different services would have had “different accessibility” based on the “key” or “credential” that may be “linked

to a particular” service. Ex-1003, ¶231. A POSITA would have understood that each of the keys or credentials stored in the access device would enable different applications, functions, or services, such that a first “key” or “credential” would be used to access data services, while a second “key” or “credential” would be used to access sales transactions. Ex-1003, ¶231.

Alternatively, Buer and Giobbi¹⁵⁷ render obvious enabling a different application, function, or service based on different subsets of local, secured information. Ex-1003, ¶¶251-252. Buer teaches that the access device “may include a database (not shown) that matches a given token (or information from the token) with one or more default services,” and the access device may “automatically request the services” based on which token is within its proximity zone. Ex-1005, [0115], [0143]. Buer’s stored key on the access device “may be linked to a particular user, application, etc.” *Id.*, [0177]. Giobbi¹⁵⁷ teaches storing multiple user profiles, such as biometric profile, PIN profile, picture profile, registry profile, credit cards, and personal information, in its secured and tamperproof memories. Ex-1006, [0037]-[0042], [0058]. Each of the profiles provides a different accessibility to certain application, function, or service. One profile may be used to enable “access to secure physical or digital assets,” and another may be used for completing a purchase transaction. *Id.*, [0063]. A POSITA would have been motivated to implement Buer’s database to store multiple profiles, as Giobbi¹⁵⁷ teaches, because doing so would

allow Buer to securely store information from multiple tokens to enable different accessibility of applications based on the linked tokens. Ex-1005, [0115], [0143]; Ex-1006, [0037]-[0042], [0058]; Ex-1003, ¶¶253-254. A POSITA would have been motivated to implement Buer's database to store multiple profiles, at least, because Buer and Giobbi157 are in the same field of endeavor—the field of incorporating RDC/PDK (wireless communication interface and secure memory) technology into devices to allow secure data sharing and services. Ex-1005, Abstract; Ex-1006, [0026]. Likewise, a POSITA would recognize that Buer and Giobbi157 use similar techniques to solve the same problem. Ex-1003, ¶254. A POSITA would have been capable of storing multiple profiles in Buer's database because Buer and Giobbi157 use similar hardware, and the combination would require minimal modification without undue experimentation. Ex-1003, ¶255. Such a combination would have been no more than combining prior art elements using known methods to yield predictable results. *Id.*; *see, e.g., Friskit*, 306 F. App'x at 616. A POSITA would have had a reasonable expectation of success in integrating those components into Buer because Giobbi157 explains how to do so. Ex-1003, ¶255.

10. [11] “The device of claim 1, wherein the device is a cell phone.”

Buer discloses its access device may be a mobile device, such as “a cellular phone.” Ex-1005, [0163]. Ex-1003, ¶¶232.

11. [12] “The device of claim 1, wherein the at least one external device is included in jewelry.”

Buer teaches that its external token may be included in “smart cards, credit cards, dongles, badges, biometric devices such as fingerprint readers, mobile devices such as cellular telephones, PDAs, etc.” Ex-1005, [0130]. Giobbi157 teaches that a token “can be integrated into commonly carried items,” such as “jewelry items such as watches.” Ex-1006, [0035]. It would have been obvious in view of Buer’s disclosure of including an external token in a wearable, such as a badge, to include the external token in other wearables, like jewelry such as watches, as Giobbi157 teaches. Ex-1003, ¶¶256-257. A POSITA would have been motivated to integrate Buer’s token into a watch because a watch is a commonly carried item that would be typically worn by an individual, as Giobbi157 teaches. Ex-1006, [0028], [0035], claim 26. Integrating a token into a watch would also further Buer’s purpose of providing further verification by “what the user possesses.” Ex-1005, [0114]. A POSITA would also be motivated to combine these references because Giobbi157 and Buer are in the same field of endeavor as the ’960 patent—the field of incorporating RDC/PDK (wireless communication interface and secure memory) technology into devices. Ex-1003, ¶258. A POSITA would recognize that Giobbi157 and Buer use similar techniques to solve the same problem as the ’960 patent—as discussed throughout this Petition, and the Giobbi157 and Buer references integrate

secure memory and wireless communication interface in the same manner claimed by the '960 patent. *Id.*, ¶259. A POSITA would have had a reasonable expectation of success in the proposed combination—Giobbi¹⁵⁷ already teaches that a token can be incorporated into a jewelry such as watches, and Buer already contemplates including its token in a wearable. *Id.*

12. [13] “The device of claim 1, wherein the at least one external device is a watch.”

See [12]; Ex-1003, ¶260.

13. [15] “The method of claim 14, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on the device.”

See [2]; Ex-1003, ¶233.

14. [16] “The method of claim 14 further comprising: sending the enablement signal, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on a device external to the device and communicatively coupled to an external, wireless communication interface.”

See [3]; Ex-1003, ¶234.

15. [17] “The method of claim 14, wherein the local, secured information includes biometric information for authenticating a user.”

See [4]; Ex-1003, ¶235.

- 16. [18] “The method of claim 14, wherein the local, secured information includes financial information and wherein the one or more of the application, the function and the service completes a financial transaction.”**

See [6]; Ex-1003, ¶236.

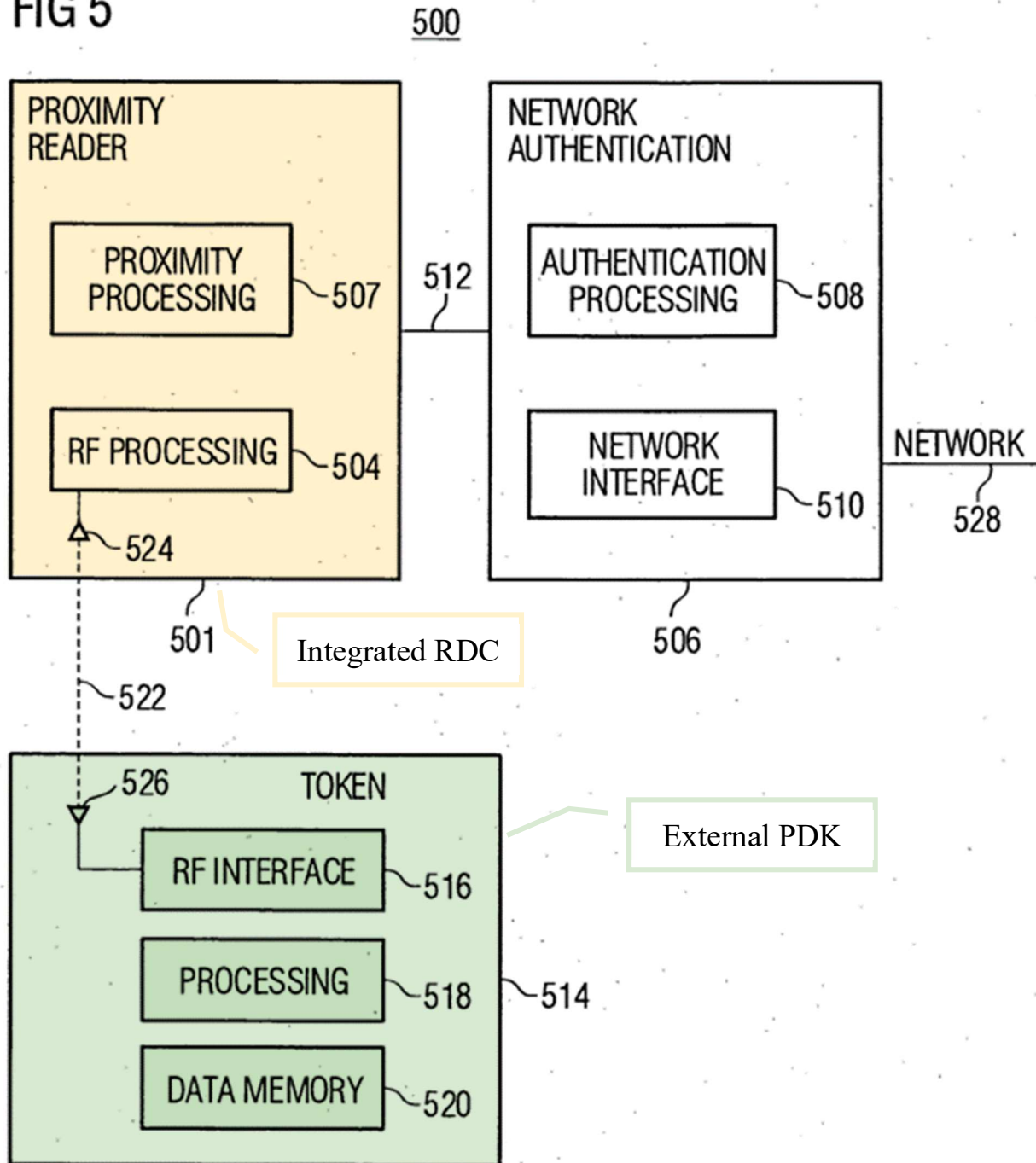
- 17. [19] “The method of claim 14, wherein the device is a cell phone.”**

See [11]; Ex-1003, ¶237.

- 18. [20] “The method of claim 14, wherein the external PDK is included in a watch.”**

Buer’s wireless token (integrated into a watch) is an “external PDK” that acts as a physical authentication/verification mechanism (for “what the user possesses”). Ex-1005, [0114]. Without the token, access may be denied. *Id.*, [0011]. But when token “is relatively close to the device,” access to data networks, applications, or financial transactions may be enabled. *Id.*, [0120]-[0122], [0155]. Buer’s external token is an external PDK because, similar to Buer’s integrated PDK, it is also an operably connected collection of circuit elements including antenna 526, an RF interface 516 (transceiver), processing component 518, and data memory 520 for storing user information, as in Figure 5. *Id.*, [0157]-[0159].

FIG 5



Id., Fig. 5 (annotated). In Figure 5, Buer's RF interface 516 with antenna 526 is used to transmit/receive RF signals via line 522 to/from the proximity reader (integrated RDC). *Id.*, [0157]. Buer's processing component 518 acts as a controller for

“control[ing] communication with the proximity reader 501,” “enabl[ing] the token 514 to be programmed with the authentication information,” “process[ing] RF signals received from the proximity reader 501,” and “control[ing] the generation of appropriate signals to send the authentication information.” *Id.*, [0159]. And Buer’s processing component 518 and data memory 520 are used to store the “authentication information such as network authentication credentials, passwords and/or certificates” (e.g., “information particular to a user”). *Id.*, [0158]-[0159]. Thus, Buer’s external token discloses an external PDK, consistent with the court’s and Google’s constructions. Ex-1003, ¶¶261-265.

It would have been obvious that Buer’s external PDK may be included in jewelry, such as a watch. Ex-1005, [0130]; Ex-1006, [0035]. It would have been obvious in view of Buer’s disclosure of including an external token in a wearable to include the external token in other wearables, like jewelries such as watches, as Giobbi¹⁵⁷ teaches. Ex-1003, ¶266; §V.B.11.

VI. Ground 4: Claim 4 Would Have Been Obvious Over Buer and Nishikawa

Buer and Nishikawa render obvious that the local, secured information includes biometric information for authenticating a user. Ex-1003, ¶¶267-268. Nishikawa discloses improving a SIM card capable of “be[ing] loaded with multiple applications, such as electronic money, an electronic ticket, a fingerprint template, a

fingerprint collating engine and a personnel ID card.” Ex-1014, [0111], [0001], [0036]. Nishikawa explains that “[f]ingerprint data (biometric data) on the finger print of a special user...is stored in the SIM [card]” to authenticate the user “on the basis of biometric data.” Ex-1014, [0073], [0114]. A POSITA would have been motivated to adapt Buer’s cellular phone to load multiple applications on a SIM card, as Nishikawa teaches, to improve the convenience of Buer’s cellular phone and to add additional capability, including the ability to store biometric information in addition to credit card information, and, as prior art teaches, to use the “standard size and shape” of a conventional SIM card to introduce additional features. *Id.*; Ex-1013, 3:34-4:4, 11:15-27; Ex-1003, ¶¶269-270. A POSITA would have also been motivated to improve authentication of the user of the cellular phone, which furthers Buer’s express teaching on using a biometric to add an additional layer of authentication. Ex-1014, [0111], [0073]; Ex-1005, [0114]. A POSITA would have recognized that Buer and Nishikawa are in the same field of endeavor and use similar techniques to solve the same problem. Ex-1003, ¶271. A POSITA would have been capable of adapting Buer’s cellular phone to store biometric information on its SIM card, because Buer and Nishikawa use similar hardware, and the combination would require minimal modification without undue experimentation. Ex-1005, [0114], [0125], [0163]; Ex-1014, [0004]-[0013]; Ex-1003, ¶272. Such a combination would have been no more than combining prior art elements using known methods to yield

predictable results. Ex-1003, ¶272; *see, e.g., Friskit*, 306 F. App'x at 616. A POSITA would have had a reasonable expectation of success in integrating those components into Buer because Nishikawa explains how to do so. Ex-1003, ¶272.

VII. Discretionary Denial Is Not Warranted

A. Discretionary Denial Is Not Warranted Under § 325(d)

The Advanced Bionics framework strongly favors institution. *Advanced Bionics LLC v. MED-EL Elektromedizinische Gerate GmbH*, IPR2019-01469, Paper 6 (PTAB Feb. 13, 2020) (precedential).

Neither Dua, Buer, Nishikawa, nor Giobbi¹⁵⁷ presented herein were considered by the Examiner during prosecution or previously considered. *See generally* Ex-1002. Accordingly, Petitioner submits that the first part of the *Advanced Bionics* framework is not satisfied because this Petition includes grounds based on combinations of prior art not previously considered by the Office. Because the first part is not satisfied, the Board need not consider the second part. To the extent the Board determines an analysis under the second part of *Advanced Bionics* is warranted, Petitioner submits that the asserted Grounds demonstrate that the Examiner erred in his evaluation of the prior art. Thus, Petitioner submits that the evidence and facts presented in the Petition warrant reconsideration of the prior art, and respectfully requests the Board decline exercising its discretion to deny institution under 35 U.S.C. § 325(d).

B. Discretionary Denial Is Not Warranted Under *Fintiv*

Factors 1 and 5 are at least neutral. Petitioner is the defendant in the parallel WDTX proceeding and intends to request a stay of that proceeding if the Board institutes an IPR.

Factor 2 is at least neutral. A trial date is set for February 27, 2025 (Ex-1011, 3), but the median time to trial in WDTX is 28.3 months (projected trial date around September 2025). Ex-1022, 5. Because a FWD in this IPR would likely issue in October 2025, within one month of the median projected trial date of the parallel proceeding, Factor 2 is at least neutral.

Factor 3 favors institution because the Petitioner acted diligently to file this IPR before its bar date and the parties have not significantly invested in the parallel proceeding. Indeed, fact discovery only recently opened, and expert discovery will not close until October Ex. 1011, 1-2.

Factor 4 favors institution because this Petition challenges significantly more claims than are at issue in the parallel proceeding. Any concerns of inefficiency are outweighed by the scope of claims to be addressed in this IPR.

Thus, the totality of Factors 1-5 weigh against discretionary denial. Indeed, the Board has instituted under similar circumstances. IPR2021-01483, Paper 11 at 13-14 (PTAB March 4, 2022) (instituting IPR where petitioner was defendant, no stay was requested, trial was projected to occur *two months before* the FWD, a

“significant portion of work remains to be done in the district court proceeding—e.g., the completion of fact and expert discovery and dispositive motions,” and the overlap between claims was “complete”).

To the extent the Board determines consideration of Factor 6 is warranted, the compelling merits of this petition outweigh any concerns that might arise under *Fintiv* factors 1-5. The merits of the petition are especially strong. Petitioner relies on prior art that was never considered by the office, presents significantly different invalidity grounds, and relies on the supporting declaration of Dr. Wolfe to thoroughly explain why each of challenged claim elements are obvious over the prior art.

C. 35 U.S.C. §314(a) – *General Plastic*

Petitioner respectfully submits application of the *General Plastic* analysis is inapplicable here. The present petition is not a “follow-on petition,” as that term is used in *General Plastic*. Moreover, even if the analysis were applicable, the *General Plastic* factors do not favor denial. The parties (Microsoft and Google) have no significant relationship but rather are direct market competitors. While there are some overlapping references between the present Petition and Microsoft’s petition, this Petition addresses different prior art references and different examples of arguments. There are also no concerns of road-mapping based on patent owner’s preliminary response because Petitioner could not have taken advantage of such

later-filed preliminary response in preparing the Petition here. Further, the filing of multiple petitions here is merely the result of Proxense filing multiple actions in the district court. Lastly, there is no risk that the Petition would undermine the Office’s ability to complete the proceedings in a timely manner. Moreover, the Board has authority under the statute and regulations to consolidate proceedings to achieve efficiency. *See* 35 U.S.C. §315(d); 37 C.F.R. §42.122(a).

VIII. Mandatory Notices

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

Google LLC is the real party-in-interest for this Petition.⁸

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

The ’960 patent is assigned to Proxense, LLC, who is currently asserting the ’960 patent against Google LLC in the Western District of Texas in *Proxense, LLC v. Google LLC*, No. 6:23-cv-00320 (W.D. Tex.). To the best of Petitioner’s knowledge, the ’960 patent is/was involved in the following district court litigations/proceedings:

Name	Number	Court	Filed
<i>Proxense, LLC v. Microsoft Corp.</i>	6:23-cv-00319	WDTX	May 2, 2023

⁸ Google LLC is a subsidiary of XXVI Holdings Inc., a subsidiary of Alphabet Inc. XXVI Holdings Inc. and Alphabet Inc. are not real parties-in-interest here.

<i>Proxense, LLC v. Google LLC</i>	6:23-cv-00320	WDTX	May 2, 2023
<i>Microsoft Corp. v. Proxense, LLC</i>	IPR2024-00405	PTAB	Jan. 16, 2024

C. Counsel and Service Information Under 37 C.F.R. §42.8(b)(3)

Lead Counsel	Back-Up Counsel
Erika H. Arner (Reg. No. 57,540) erika.arners@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner LLP 1875 Explorer Street 8 th Floor Reston, VA 20190-6023 Tel: 571-203-2754 Fax: 202-408-4400	Kara A. Specht (Reg. No. 69,560) kara.specht@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner LLP 271 17th Street, NW, Suite 1400 Atlanta, GA 30363-6209 Tel: 404-653-6400 Fax: 404-653-6444
	Cory C. Bell (Reg. No. 75,096) cory.bell@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner LLP 2 Seaport Lane, 6th Floor Boston, MA 02210-2001 Tel.: 617-646-1641 Fax: 202-408-4400
	Shawn S. Chang (Reg. No. 81,437) shawn.chang@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner LLP 271 17th Street, NW, Suite 1400 Atlanta, GA 30363-6209 Tel. 404-653-6400 Fax: 404-653-6444
	Safiya Aguilar (Reg. No. 77,212) safiya.aguilar@finnegan.com Finnegan, Henderson, Farabow, Garrett, & Dunner LLP 901 New York Avenue NW Washington, DC 20001-4413

	Tel.: 202-408-4160 Fax: 202-408-4400
--	---

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

Please address correspondence to lead and back-up counsel at the addresses above and Google-Proxense-IPRs@finnegan.com. Petitioner consents to electronic service by e-mail.

IX. Standing

Petitioner certifies that the '960 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 that the challenged claims are unpatentable and requests the Board institute and cancel each challenged claim as unpatentable.

Dated: April 19, 2024

Respectfully submitted,

/Erika H. Arner/

Erika H. Arner
Lead Counsel
Reg. No. 57,540

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that the foregoing **PETITION FOR *INTER PARTES* REVIEW** contains 13,740 words, excluding those portions exempted under 37 C.F.R. § 42.24(a), as measured by the word-processing system used to prepare this paper.

Respectfully submitted,

/Erika H. Arner/

Erika H. Arner

Lead Counsel

Reg. No. 57,540

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a copy of the foregoing **PETITION FOR *INTER PARTES* REVIEW**, the associated Power of Attorney, and Exhibits 1001 through 1022 are served on April 19, 2024, via FedEx Priority Overnight on the correspondence address of record indicated in the Patent Office's Patent Center system for U.S. Patent No 10,073,960.

PATENT LAW WORKS/PROXENSE

Greg Sueoka
4516 South 700 East, Suite 290
Salt Lake City, UT 84107

A courtesy copy is also being sent via email to Patent Owner's counsel in *Proxense, LLC v. Google LLC*, No. 6:23-cv-320 (W.D. Tex.), where Patent Owner has asserted the subject patent:

David L. Hecht
dhecht@hechtpartners.com

Maxim Price
mprice@hechtpartners.com

Conor B. McDonough
cmcdonough@hechtpartners.com

Yi Wen Wu
wwu@hechtpartners.com

HECHT PARTNERS LLP
125 Park Avenue, 25th Floor
New York, New York 10017

Brian D. Melton
bmelton@susmangodfrey.com

Geoffrey L. Harrison
gharrison@susmangodfrey.com

Meng Xi
mxi@susmangodfrey.com

Bryce T. Barcelo
bbarcelo@susmangodfrey.com

SUSMAN GODFREY L.L.P.
1000 Louisiana Street, Suite 5100
Houston, Texas 77002-5096

Lear Jiang
ljiang@susmangodfrey.com

SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars, Suite 1400
Los Angeles, California 90067-6029

Dated: April 19, 2024

By: /Daniel E. Doku/
Daniel E. Doku
Litigation Legal Assistant
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP