

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner,

v.

PROXENSE, LLC,

Patent Owner.

Case No. IPR2024-01399
U.S. Patent No. 8,646,042
Filing Date: April 12, 2012
Issue Date: February 4, 2014

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

	Page
I. Relief Requested.....	1
II. The '042 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. Lee	13
D. Nishikawa.....	14
E. Hoffmann.....	15
IV. Grounds 1 and 2: Claim 10 Would Have Been Obvious Over Dua alone, or in the alternative, in view of Kotola.....	16
A. [10pre] “A method comprising:”	16
B. [10a] “creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external personal digital key (PDK), the hybrid device including an integrated PDK and the integrated RDC;”	16
C. [10b] “receiving a first signal at the integrated RDC via the first wireless link from the external PDK;”	25
D. [10c] “generating an enablement signal enabling one or more of an application, a function and a service on one or more of the hybrid device and a device associated with an external RDC; and”	26

E.	[10d] “sending the enablement signal to one or more of the hybrid device and the device associated with an external RDC.”	30
V.	Ground 3: Claims 1, 3-6, 8-15, and 17 Would Have Been Obvious Over Buer.....	30
A.	Buer renders obvious each of independent claims 1 and 10.....	30
1.	Claim 10.....	30
2.	Claim 1.....	49
B.	Buer renders obvious claims 3-6, 8, 9, 11-15, and 17.....	57
1.	[3] “The hybrid device claim 1, wherein the integrated PDK is capable of communicating with the at least one external RDC at the same time the integrated RDC communicates with the at least one external PDK.”	57
2.	[4] “The hybrid device of claim 1, wherein the integrated RDC communicates an enable signal to the device using the second signal line.”	58
3.	[5] “The hybrid device of claim 1, wherein the one or more of the hybrid device and the device associated with the external RDC are enabled subsequent to the external PDK entering the proximity zone of the integrated RDC and based on the information stored by one or more of the external PDK and the integrated PDK.”	60
4.	[6] “The hybrid device of claim 1, wherein the hybrid device is a cell phone and the hybrid device is enabled to provide cell phone service subsequent to the external PDK entering the proximity zone of the integrated RDC and based on the information stored by one or more of the external PDK and the integrated PDK.”	60
5.	[8] “The hybrid device of claim 1, wherein the integrated PDK communicates with the external RDC subsequent to	

	the external PDK entering the proximity zone of the integrated RDC.”.....	61
6.	[9] “The hybrid device of claim 1, comprising storage for inheritance information.”	61
7.	[11] “The method of claim 10, wherein the hybrid device is a cell phone and the enablement signal is sent to the cell phone enabling one or more of a service, a feature and a functionality of the cell phone.”.....	62
8.	[12] “The method of claim 11, wherein the external PDK is adapted to receive and couple with a subscriber identity module (SIM) card.”	62
9.	[13].....	63
10.	[14] “The method of claim 11, wherein the integrated PDK modifies the enablement signal to produce a modified enablement signal, and the modified enablement signal is sent from the integrated PDK to the external RDC.”	64
11.	[15].....	65
12.	[17] “The method of claim 10, wherein the first signal includes service inheritance information.”	68
VI.	Ground 4: Claim 2 Would Have Been Obvious Over Buer and Lee.	71
A.	[2] “The hybrid device of claim 1 further comprising one or more of another integrated PDK and another integrated RDC.”	71
VII.	Ground 5: Claim 12 Would Have Been Obvious Over Buer and Nishikawa	72
A.	[12] “The method of claim 11, wherein the external PDK is adapted to receive and couple with a subscriber identity module (SIM) card.”.....	72
VIII.	Ground 6: Claims 3 and 18-20 Would Have Been Obvious Over Buer and Hoffmann	74

A.	[3] “The hybrid device claim 1, wherein the integrated PDK is capable of communicating with the at least one external RDC at the same time the integrated RDC communicates with the at least one external PDK.”	74
B.	[18] “The method of claim 10, wherein the first signal includes feature inheritance information.”	76
C.	[19] “The method of claim 10, wherein the first signal includes personality inheritance information.”	78
D.	[20] “The method of claim 10 comprising: receiving a signal from the external PDK that a second external PDK includes inheritance information; creating a second wireless link between the integrated RDC and the second external PDK; and receiving the inheritance information from the second external PDK.”	80
IX.	Discretionary Denial Is Not Warranted	82
A.	Discretionary Denial Is Not Warranted under §325(d).....	82
B.	Discretionary Denial Is Not Warranted Under <i>Fintiv</i>	83
C.	35 U.S.C. §314(a) – <i>General Plastic</i>	85
X.	Mandatory Notices.....	86
A.	Real Parties-in-Interest Under 37 C.F.R. §42.8(b)(1).....	86
B.	Related Matters Under 37 C.F.R. §42.8(b)(2)	86
C.	Counsel and Service Information Under 37 C.F.R. §42.8(b)(3).....	88
D.	Service Information Under 37 C.F.R. §42.8(b)(4).....	88
XI.	Standing	89
XII.	Conclusion	89

TABLE OF AUTHORITIES

Cases

<i>Advanced Bionics LLC v. MED-EL Elektromedizinische Gerate GmbH</i> , IPR2019-01469, Paper 6 (PTAB Feb. 13, 2020)	82
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020)	83-85
<i>Commonwealth Sci. & Indus. Rsch. Org. v. Buffalo Tech. (USA), Inc.</i> , 542 F.3d 1363 (Fed. Cir. 2008)	22
<i>Fresenius USA, Inc. v. Baxter Int’l, Inc.</i> , 582 F.3d 1288 (Fed. Cir. 2009)	29, 5, 7
<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)	84
<i>Realtime Data, LLC v. Iancu</i> , 912 F.3d 1368, 1375 (Fed. Cir. 2019)	7

Statutes

35 U.S.C. §102(b)	7, 10, 13-15
35 U.S.C. §103	1
35 U.S.C. §314(a)	85
35 U.S.C. §315(d)	85
35 U.S.C. §325(d)	82-83

Regulations

37 C.F.R. §42.8(b)(1)	86
37 C.F.R. §42.8(b)(2)	86
37 C.F.R. §42.8(b)(3)	88
37 C.F.R. §42.8(b)(4)	88

37 C.F.R. §42.122(a).....	85
---------------------------	----

TABLE OF EXHIBITS

Exhibit	Description
Ex-1001	U.S. Patent No. 8,646,042 to David L. Brown (“the ’042 patent”)
Ex-1002	Prosecution history of U.S. Patent No. 8,646,042
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. (“Giobbi ’157”)
Ex-1007	U.S. Patent Application Publication No. 2004/0255139 to Giobbi (“Giobbi ’139”)
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 D, <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 Hoffmann (“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)
EX-1023	Reserved
EX-1024	<i>Proxense LLC v. Microsoft Corp.</i> , Case No. 23-cv-00319, Dkt. No. 66, Claim Construction Order (W.D. Tex. May 24, 2024)
EX-1025	<i>Microsoft Corp. v. Proxense, LLC</i> , IPR2024-00573, Paper 11 (PTAB Aug. 13, 2024)
EX-1026	U.S. District Court National Judicial Case Load Profile ending June 30, 2024.
EX-1027	Docket Sheet for <i>Proxense, LLC v. Apple Inc.</i> , Case No. 6-24-cv-00143 (W.D. Tex) (pulled Sep. 12, 2024)

EX-1028	Scheduling Order in <i>Proxense, LLC v. Apple Inc.</i> , Case No. 6-24-cv-00143 (W.D. Tex)
EX-1029	Patents and Applications related to the '042 Patent

LISTING OF CHALLENGED CLAIMS

Claim 1	
[1pre]	A hybrid device comprising:
[1a]	an integrated personal digital key (PDK) for storing information and capable of communicating wirelessly with at least one external receiver-decoder circuit (RDC); and
[1b]	an integrated RDC for communicating wirelessly with at least one external PDK within a proximity zone,
[1c]	the integrated RDC coupled to the integrated PDK by a first signal line for communication,
[1d]	the integrated RDC coupled to at least one other component of the hybrid device by a second signal line,
[1e]	one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service on one or more of the hybrid device and a device associated with the external RDC.
Claim 2	
[2]	The hybrid device of claim 1 further comprising one or more of another integrated PDK and another integrated RDC.
Claim 3	
[3]	The hybrid device claim 1, wherein the integrated PDK is capable of communicating with the at least one external RDC at the same time the integrated RDC communicates with the at least one external PDK.
Claim 4	
[4]	The hybrid device of claim 1, wherein the integrated RDC communicates an enable signal to the device using the second signal line.
Claim 5	
[5]	The hybrid device of claim 1, wherein the one or more of the hybrid device and the device associated with the external RDC are enabled subsequent to the external PDK entering the

	proximity zone of the integrated RDC and based on the information stored by one or more of the external PDK and the integrated PDK.
Claim 6	
[6]	The hybrid device of claim 1, wherein the hybrid device is a cell phone and the hybrid device is enabled to provide cell phone service subsequent to the external PDK entering the proximity zone of the integrated RDC and based on the information stored by one or more of the external PDK and the integrated PDK.
Claim 8	
[8]	The hybrid device of claim 1, wherein the integrated PDK communicates with the external RDC subsequent to the external PDK entering the proximity zone of the integrated RDC.
Claim 9	
[9]	The hybrid device of claim 1, comprising storage for inheritance information.
Claim 10	
[10pre]	A method comprising:
[10a]	creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external personal digital key (PDK), the hybrid device including an integrated PDK and the integrated RDC;
[10b]	receiving a first signal at the integrated RDC via the first wireless link from the external PDK;
[10c]	generating an enablement signal enabling one or more of an application, a function and a service on one or more of the hybrid device and a device associated with an external RDC; and
[10d]	sending the enablement signal to one or more of the hybrid device and the device associated with an external RDC.

Claim 11	
[11]	The method of claim 10, wherein the hybrid device is a cell phone and the enablement signal is sent to the cell phone enabling one or more of a service, a feature and a functionality of the cell phone.
Claim 12	
[12]	The method of claim 11, wherein the external PDK is adapted to receive and couple with a subscriber identity module (SIM) card.
Claim 13	
[13pre]	The method of claim 10, wherein the integrated PDK is electrically coupled to the integrated RDC, and the method comprises:
[13a]	sending the enablement signal from the integrated RDC to the integrated PDK;
[13b]	creating a second wireless link between the integrated PDK and an external RDC; and
[13c]	sending the enablement signal from the integrated PDK to the external RDC using the second wireless link.
Claim 14	
[14]	The method of claim 11, wherein the integrated PDK modifies the enablement signal to produce a modified enablement signal, and the modified enablement signal is sent from the integrated PDK to the external RDC.
Claim 15	
[15]	The method of claim 10, wherein the integrated PDK is electrically coupled to the integrated RDC, and the method comprises: creating a second wireless link between the hybrid device and an external RDC; and receiving a second signal at the hybrid device via the second wireless link from the external RDC, wherein the enablement signal is generated responsive to receiving the first and second signals.

Claim 17	
[17]	The method of claim 10, wherein the first signal includes service inheritance information.
Claim 18	
[18]	The method of claim 10, wherein the first signal includes feature inheritance information.
Claim 19	
[19]	The method of claim 10, wherein the first signal includes personality inheritance information.
Claim 20	
[20]	The method of claim 10 comprising: receiving a signal from the external PDK that a second external PDK includes inheritance information; creating a second wireless link between the integrated RDC and the second external PDK; and receiving the inheritance information from the second external PDK.

I. Relief Requested

Apple Inc. (Petitioner) requests *inter partes* review of U.S. Patent No. 8,646,042 (“’042 patent,” Ex-1001) based on the following grounds:

Ground	Claim(s) Challenged	35 U.S.C. §	Reference(s)
1	10	103	Dua
2	10	103	Dua, Kotola
3	1, 3-6, 8-15, and 17	103	Buer
4	2	103	Buer, Lee
5	12	103	Buer, Nishikawa
6	3 and 18-20	103	Buer, Hoffmann

The ’042 patent relates to using keys and readers, such as Radio Frequency Identification (RFID) tags and RFID readers, Ex-1001, 1:19-42, and refers to a key as a “personal digital key (PDK)” and a reader as a “receiver-decoder circuit (RDC).” *Id.*, 1:21-27. The challenged claims recite a “hybrid device” (e.g., cellular phone) that includes both a PDK and an RDC, which can respectively communicate with external RDCs and PDKs in the proximity of the hybrid device.

But hybrid devices having both an internal key and reader were known years before the ’042 patent was filed. Indeed, Dua discloses a cellular phone with an integrated RFID Tag-Reader Module that includes both RFID tag (PDK) and 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 that includes both an internal authentication component (PDK) and a proximity reader (RDC) to secure access to various services using external RFID tokens and readers in its proximity. Ex-1005, [0014]. Indeed, numerous prior art references 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. Accordingly, the challenged claims are unpatentable.

II. The '042 Patent

A. Overview

The earliest claimed priority of the '042 patent is December 6, 2007. The '042 patent relates to keys and readers, such as RFID tags and RFID readers, Ex-1001, 1:29-61, and is directed to a “hybrid device” (**red**) that includes both an integrated PDK (**blue**) and RDC (**yellow**) that communicate with each other via a signal line. *Id.*, 1:65-2:2. The '042 patent discloses that the hybrid device may be part of a cellphone.

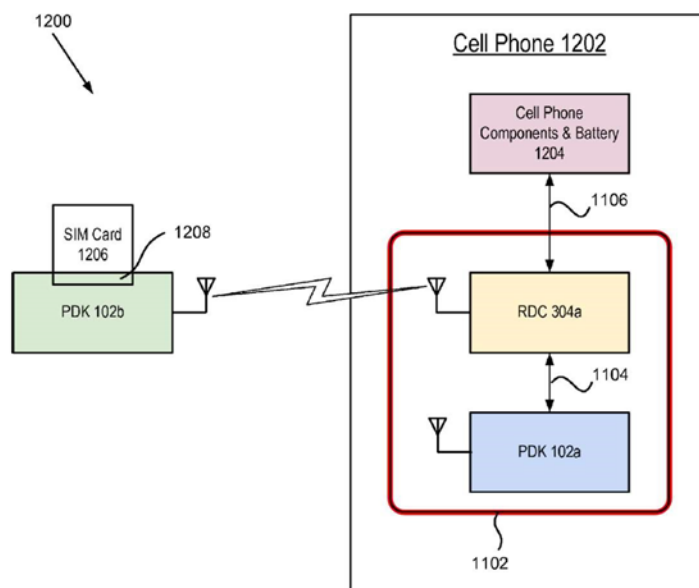


FIG. 12

Id., Fig. 12 (annotated); 14:4-6. As shown, additional cellphone components and a battery (pink) may be coupled to the integrated RDC by a signal line. *Id.*, 14:4-23. The integrated RDC may further communicate wirelessly with an external PDK. *Id.*, 14:18-20.

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

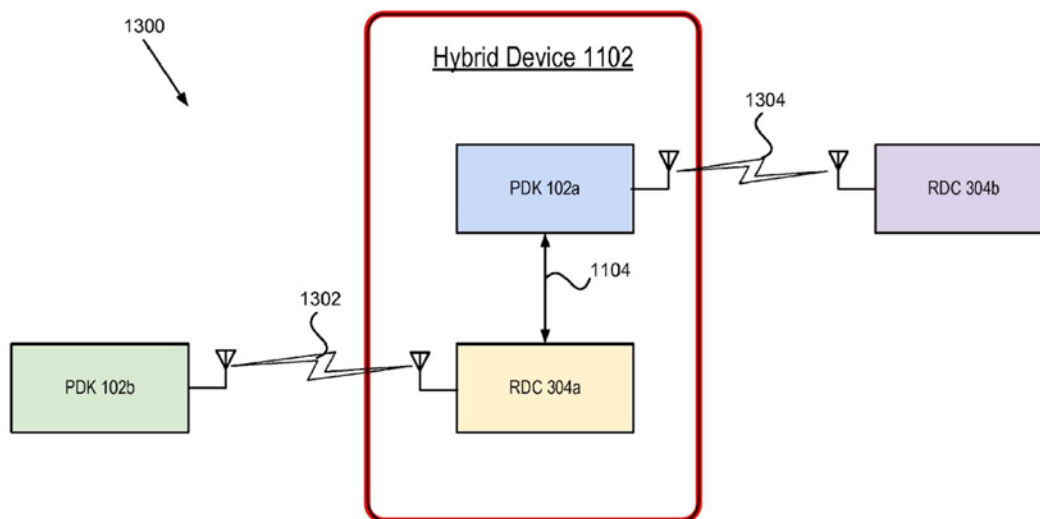


FIG. 13

Id., Fig. 13 (annotated), 16:3-19, 21:52-57.

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.*, 4:5-15, 6:40-59, 16:20-27. When used to access or enable a Wi-Fi service, an external PDK 102b “provides...information to the [integrated] RDC 304a,” so the hybrid device “communicates with the [external] RDC 304b to access the Wi-Fi service.” *Id.*, 19:23-45. Here, the hybrid device and external PDK may belong to

different users, so the hybrid device may use another user's information stored on the external PDK. *Id.*, 19:23-45.

As another example, the credit card information stored on the integrated PDK is used to provide authorization to the external RDC to make a purchase, and in this way, “to enable a service associated with the...[external] RDC.” *Id.*, 16:20-28. The purchase authorization may depend on the presence of an external PDK being in proximity to the hybrid device. *Id.*, 16:27-34, 16:39-63. Here, the external PDK first “authorizes the hybrid device,” which “in turn authorizes” the external RDC to make a purchase when the external PDK is in proximity. *Id.*, 16:27-34, 16:39-42. Thus, the external PDK may be “used to enable specific features in the hybrid device.” *Id.*, 16:32-34.

B. Claim Construction¹

In a previous district court litigation against Samsung (6:21-cv-00210-ADA), the court construed the following terms in a related 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

¹ See also EX-1024 and EX-1025.

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. In *Proxense, LLC v. Google LLC*, No. 6:23-cv-00320 (W.D. Tex.) (“the Google litigation”),² the court adopted its prior constructions for “personal digital key” and “receiver-decoder circuit.”³ Ex-1020. Because the prior

² In IPR2024-00782, Petitioner Google stated that it agreed to certain constructions, Ex-1015, 1, and that Proxense contended no other terms “beyond what the Court had previously construed in the *Samsung* case” need to be construed. Ex-1016, 1.

³ In IPR2024-00782, Petitioner Google stated that it proposed alternative constructions for “personal digital key” and “receiver-decoder circuit” in its pending litigation. Ex-1015, 1.

art in this Petition renders obvious all claims regardless of the construction, the Board need not construe terms to resolve unpatentability in this Petition⁴. *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

⁴ 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)

teaches a hybrid device—e.g., a “cellular phone[]” containing “both an RFID tag and an RFID reader”—that establishes wireless connections with other devices to enable functions and to exchange data. Ex-1004, [0004], [0015], [0070]; Ex-1003 ¶¶49-53. Dua teaches integrating an “RFID Tag-Reader Module” into the cellular phone to “rapidly exchange information with an electronic device that is in close proximity.” Ex-1004, [0070].

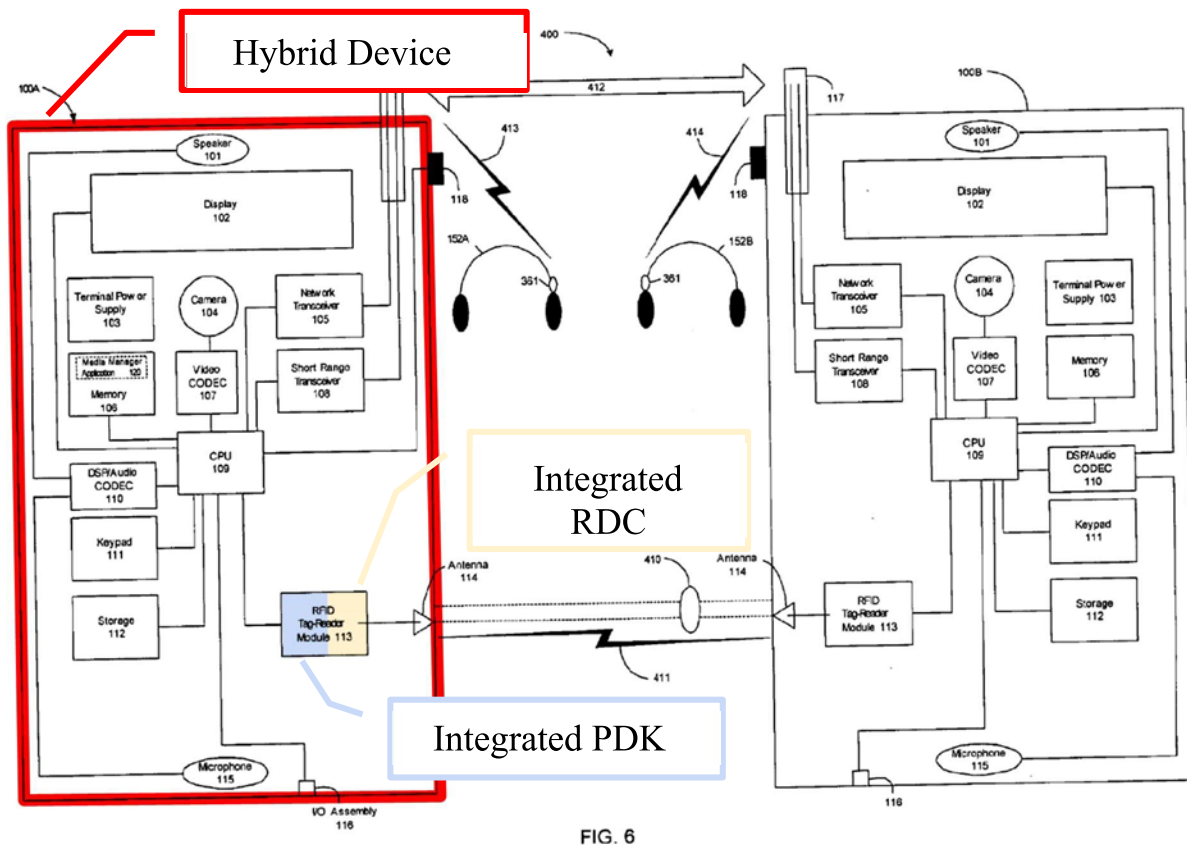


FIG. 6

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].

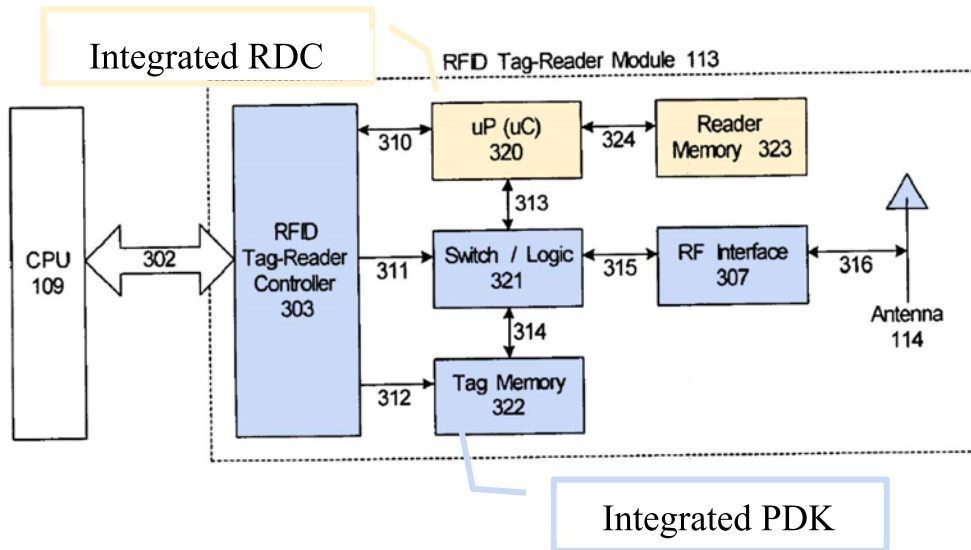


FIG. 4B

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, which reads the information to establish a secure connection. *Id.*, [0092], [0100]-[0101], [0139]; Ex-1003 ¶¶54-55.

The components for “RFID reader functionality” (yellow) are designed to communicate with external RFID tags. Ex-1004, [0071]. When operating with enhanced security, the RFID reader may receive encrypted data and decode the

encrypted data using an encryption key. *Id.*, [0152]; Ex-1003 ¶¶56-58. 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].

Dua further incorporates by reference Kotola, U.S. Patent Application Publication No. 2004/0176032, for details concerning such “other RFID Tag-Reader Module designs.” Ex 1004, [0114] (citing Ex 1017). Kotola published on September 9, 2004, and qualifies as prior art under pre-AIA 35 U.S.C. §102(b).

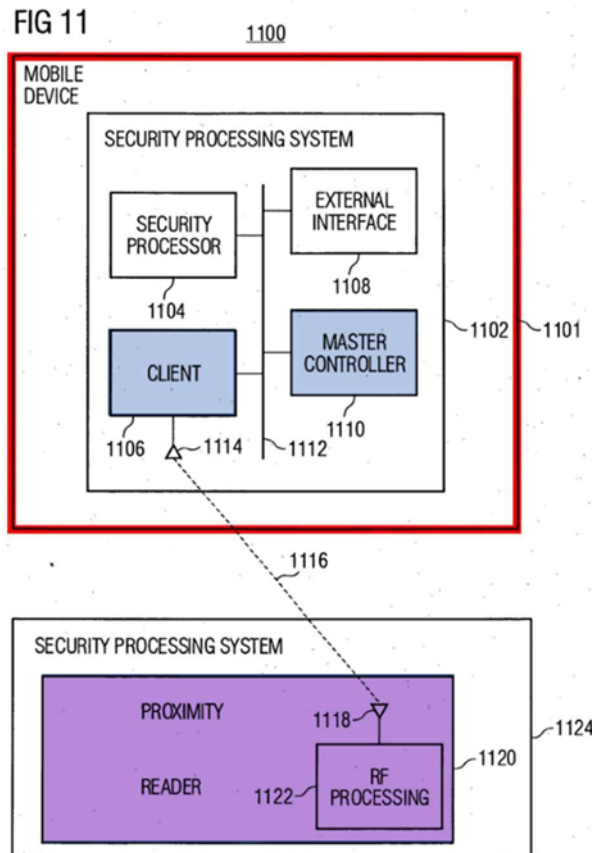
B. Buer

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 through which access to the secured services is obtained.” Ex-1005, Abstract; Ex-1003 ¶¶60-66. “An authorized user may be provided access to a service only when a wireless token assigned to the user is in the proximity of the computing device.” Ex-1005, Abstract. The computing device (e.g., access device) may be implemented as a mobile device, such as a 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.),” as shown below.

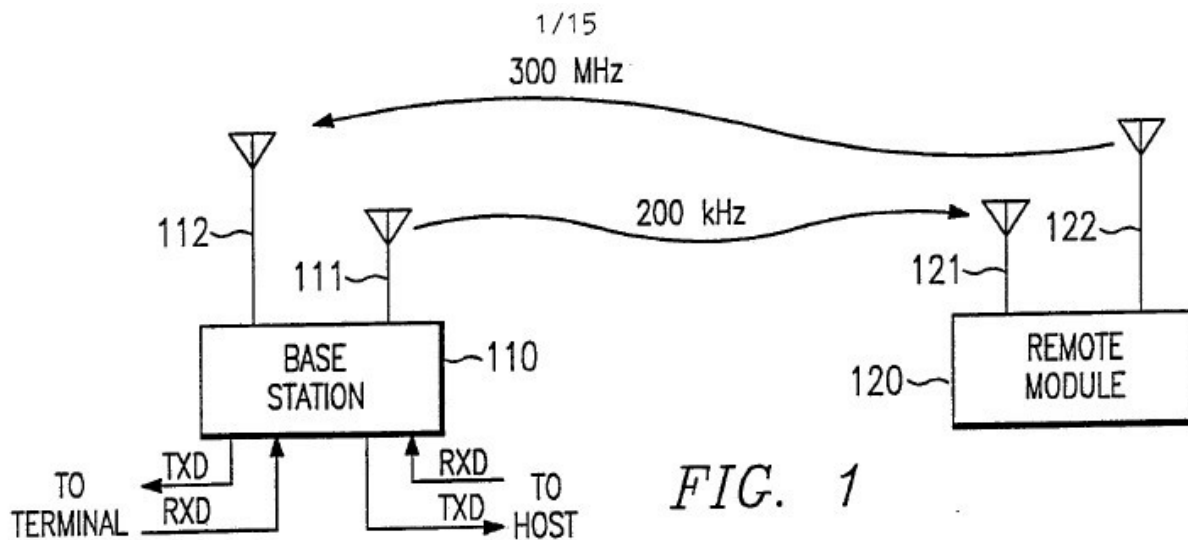
reader 1120 or a computer that includes “point-of-sale components” (not shown) to “perform a sales transaction” (e.g., “credit card transactions”) as shown below.



Id., Fig. 11 (annotated), [0193]-[0196].

C. Lee

Lee, PCT Application Publication No. WO 90/06633, published on June 14, 1990, qualifies as prior art under pre-AIA 35 U.S.C. §102(b). Lee discloses a data communication system, in which base stations can interface with battery-powered portable data modules as they are brought within range. Ex-1008, Abstract; Ex-1003 ¶¶67-72.



Ex-1008, Fig. 1. Lee teaches that its portable data module is extremely compact and powered by a small battery. *Id.*, 26:26-31. Lee's portable module can store extensive identification parameters, including biometric information (e.g., "fingerprints, faces, or retinas"), for "access" control of applications. *Id.*, 31:30-32:2. The portable module includes an access control chip that "act[s], in effect, as an electronic key." *Id.*, 78:16-24. Lee teaches that "multiple access control chips" can reside on "a common bus." *Id.*, 80:20-26.

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" and "to provide the reader/writer with a short-distance communication

function and a fingerprint sensing function.” Ex-1014, [0001], [0017]; Ex-1003 ¶¶73-79. 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’s key holder type ID module could be used “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].

E. Hoffmann

Hoffmann, U.S. Patent Application Publication No. 2005/0151623, published on July 14, 2005, qualifies as prior art under pre-AIA 35 U.S.C. §102(b). Ex-1003 ¶¶80-83. Hoffmann discloses “a personalized security system” using “a password from an electronic key.” Ex-1019, Abstract. In Hoffmann, “selected functions or all functions of the electronic device” are enabled if the device is within proximity of the key. *Id.*, Abstract, [0002], [0021]. Hoffmann discloses a personal preference monitoring system that transfers personal preferences based on proximity. Lastly, Hoffmann discloses enabling “access or functions remotely in a secure, on demand fashion” to provide access to a “person [who] does not routinely need access or is otherwise restricted from routine use.” *Id.*, [0041].

IV. Grounds 1 and 2: Claim 10 Would Have Been Obvious Over Dua alone, or in the alternative, in view of Kotola

Independent claim 10 is the broadest independent claim and is asserted in the Google litigation. Dua, alone or in view of Kotola, renders obvious claim 10. *Id.*, ¶¶97-99.

A. [10pre] “A method comprising:”

To the extent the preamble for claim 10 is limiting, Dua discloses the preamble because its method automatically set up and establish a wireless connection between two devices based on their proximity. Ex-1004, [0013]; Ex-1003, ¶104.

B. [10a] “creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external personal digital key (PDK), the hybrid device including an integrated PDK and the integrated RDC;”

Dua discloses [10a].

(1) A hybrid device including an integrated PDK and an integrated RDC:

Dua discloses a hybrid device because its media player (“hybrid device,” **red**) includes an RFID Tag-Reader Module 113 (e.g., “integrated PDK,” **blue**; “integrated RDC,” **yellow**), as shown below. Ex-1004, [0057], [0070]; Ex-1003 ¶¶105-107.

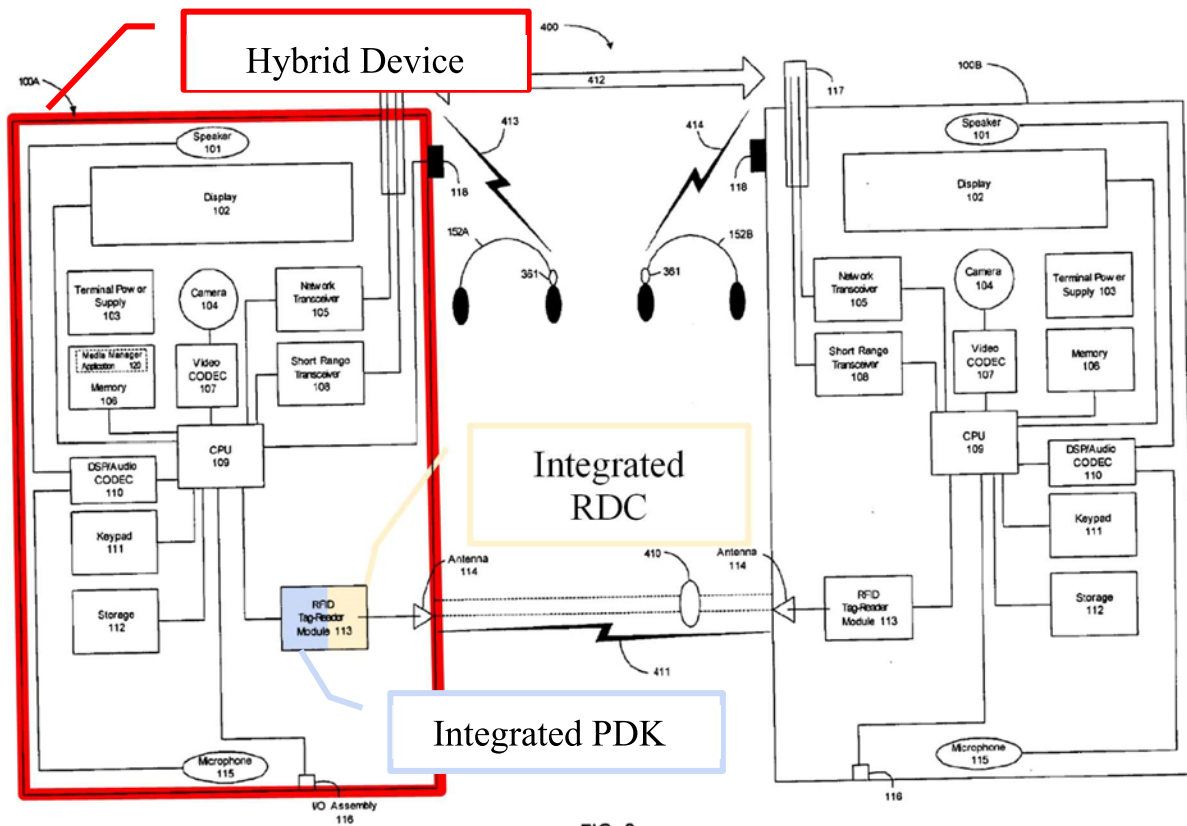


FIG. 6

Ex-1004, Fig. 6 (annotated). Dua’s media player (hybrid device) can “exchange information with an electronic device that is in close proximity.” *Id.*, [0057], [0070], Figs. 1, 6.

Dua’s RFID Tag-Reader Module includes “both an RFID tag [(“integrated PDK,” blue)] and an RFID reader [(“integrated RDC,” yellow)],” as shown below. *Id.*, [0089].

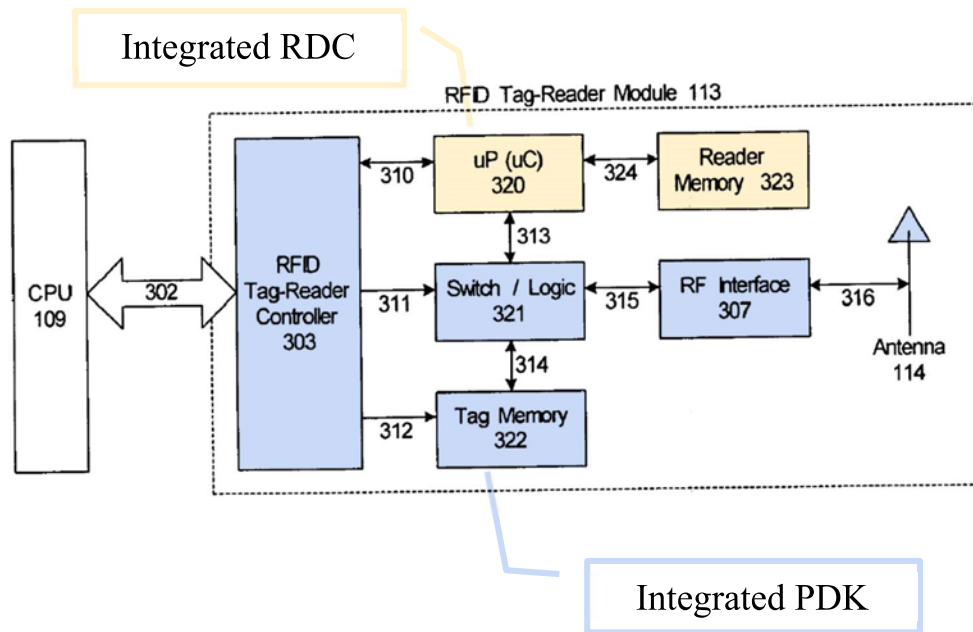


FIG. 4B

Id., Fig. 4B (annotated).

Dua's Tag-Reader Module, as shown, includes a collection of circuit components (**blue**) that makes up a "personal digital key" under either the court's construction or Google's proposed construction. Ex-1003 ¶¶110-113. This operably connected collection of components includes an antenna 114 and an RF Interface 307 (a transceiver) capable of modulating and demodulating RF signals for communications with an external tag reader (an RDC). Ex-1004, [0101], [0104], [0106], Fig. 4B; Fig. 6; Ex-1003 ¶111. Dua's RFID Tag-Reader Module (**blue**) 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). Ex-1004, [0106], [0108]. "Correspondingly, the tag memory 322 is connected to the

switch/logic component 321” and “to the RFID Tag-Reader Controller 303 in order to receive configuration data.” *Id.*, [0108]. The Tag Memory 322 may be a “nonvolatile configurable memory” and “tamper resistant...to prevent hackers from retrieving confidential information and encryption keys” stored therein. *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 services with an external device, including “electronic payments at the point-of-sale and secure key access to buildings, cars, etc.” *Id.*, [0070], [0089]. Tag-Reader Controller 303 and Tag Memory 322 thus store information particular to a user.

Dua’s Tag-Reader Module, as shown, includes a collection of circuit components (yellow) that makes up a “receiver-decoder circuit” under either the court’s construction or Google’s proposed construction. Ex-1003 ¶¶114-117. These operably connected components include a reader logic 320 that is implemented as a microcontroller (μ C) and a microprocessor (μ P). Ex-1004, [0106]. “The reader logic operates the interface and protocol framework for communicating with RFID tags (passive communication mode) and in particular, when supporting active communication mode, for communicating with RFID tag reader devices.” *Id.*, [0106]. 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, and receiving a response signal from the external device's RFID tag." *Id.*, [0071], [0100]. The response signal includes "RFID transmission data." *Id.*, [0130]-[0143]. 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].

Dua explains that exchange of configuration information between two devices is "generally insecure," and "a solution that allows for the automatic establishment of a secure wireless connection" is needed. *Id.*, [0009]-[0010]. When "enhanced security is desired," such as when sharing "sensitive" information, "encryption keys" are used and shared between the devices. *Id.*, [0152], [0139]. A POSITA would have understood that the encryption keys provide enhanced security by encrypting "sensitive" information using those keys. *Id.*, [0152]; Ex-1003 ¶¶118-119. It would have been obvious to encrypt the "confidential information" stored in the tag memory to enhance security. Ex-1004, [0109]; Ex-1003 ¶119. A POSITA would have been motivated to use an encryption key to improve RFID security so that the data transfer between a tag and a reader could be encrypted so that "hackers" could not access the confidential information, as Dua suggests. Ex-1004, [0109], [0152]; Ex-1003 ¶120; *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”). Doing so would ensure that any response signal that includes “sensitive” information would have been received by the reader via a secure wireless connection. Ex-1003 ¶120. A POSITA would have had a reasonable expectation of success in using encryption to enhance security because Dua explains that the 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, [0108]-[0109], [0152]; Ex-1003 ¶121. The reader thus would receive any confidential data in an encrypted format and decode the encrypted data using the encryption key. Ex-1003 ¶121.

To the extent that Proxense contends the claimed RDC requires separate wireless communication components (e.g., RF interface and antenna) different from the claimed PDK, it would have been obvious to include a separate RF interface and antenna, instead of a common RF interface and antenna, in Dua’s RFID Tag-Reader Module. *Id.*, ¶122. A POSITA would have been motivated to use multiple antennas because doing so provides antenna diversity for mitigating fading and improving signal reception and enables simultaneous transmission and reception of signals. Ex-1003 ¶123. Adding an additional RF interface and antenna to Dua’s RFID Tag-Reader Module would have been no more than duplicating known elements using known methods to yield predictable results because Dua already uses multiple

antennas and transceivers for sending and receiving different signals. Ex-1004, [0062], [0084]; Ex-1003 ¶123. Moreover, Dua itself fully incorporated by reference details concerning such “other RFID Tag-Reader Module designs.” Ex-1004, [0114] (citing Ex-1017); Ex-1017, Fig. 4, [0056]-[0058]. A POSITA would have had a reasonable expectation of success in duplicating the RF interface and antenna to include separate wireless communication components for the RFID tag and RFID reader. Ex-1003, ¶123.

Alternatively, Dua in view of Kotola (ground 2) renders obvious having separate wireless communication components (e.g., RF interface and antenna) for the claimed PDK and RDC. *Id.*, ¶¶124-127. Kotola discloses an integrated RFID tag and an integrated RFID reader, Ex-1017, Fig. 4, [0056]-[0058], where the RFID tag is connected to “[a]n antenna film or coil 220” and “analog circuit 223 for converting the RF signals...into digital signals,” *id.*, [0057], and the separate RFID reader is connected to “antenna 219,” *id.*, [0058]. It would have been obvious to implement Kotola’s separate antennas in Dua’s hybrid device, because Dua’s citation to Kotola “provide[s] a justification for combining the references for obviousness purposes.” *Commonwealth Sci. & Indus. Rsch. Org. v. Buffalo Tech. (USA), Inc.*, 542 F.3d 1363, 1372 (Fed. Cir. 2008); Ex-1004, [0114] (citing Ex-1017). Additionally, a POSITA would have been motivated to use multiple antennas because doing so enables simultaneous transmission and reception of signals. Ex-1003 ¶126. Using separate

RF interface and antenna in Dua's RFID Tag-Reader Module would have been no more than adding prior art elements using known methods to yield predictable results.

Id.

Accordingly, Dua discloses a hybrid device including both an integrated PDK and an integrated RDC. *Id.*, ¶¶127-128.

(2) Creating a First Wireless Link between an Integrated RDC and an External PDK:

Dua discloses creating a first wireless link during an RFID-discovery process as in [10a] because the RFID-reader component generates and transmits interrogation signals to create an RFID link between the integrated RFID reader in the hybrid device and an external RFID tag, as shown below. Ex-1004, [0122]; Ex-1003 ¶¶129-133.

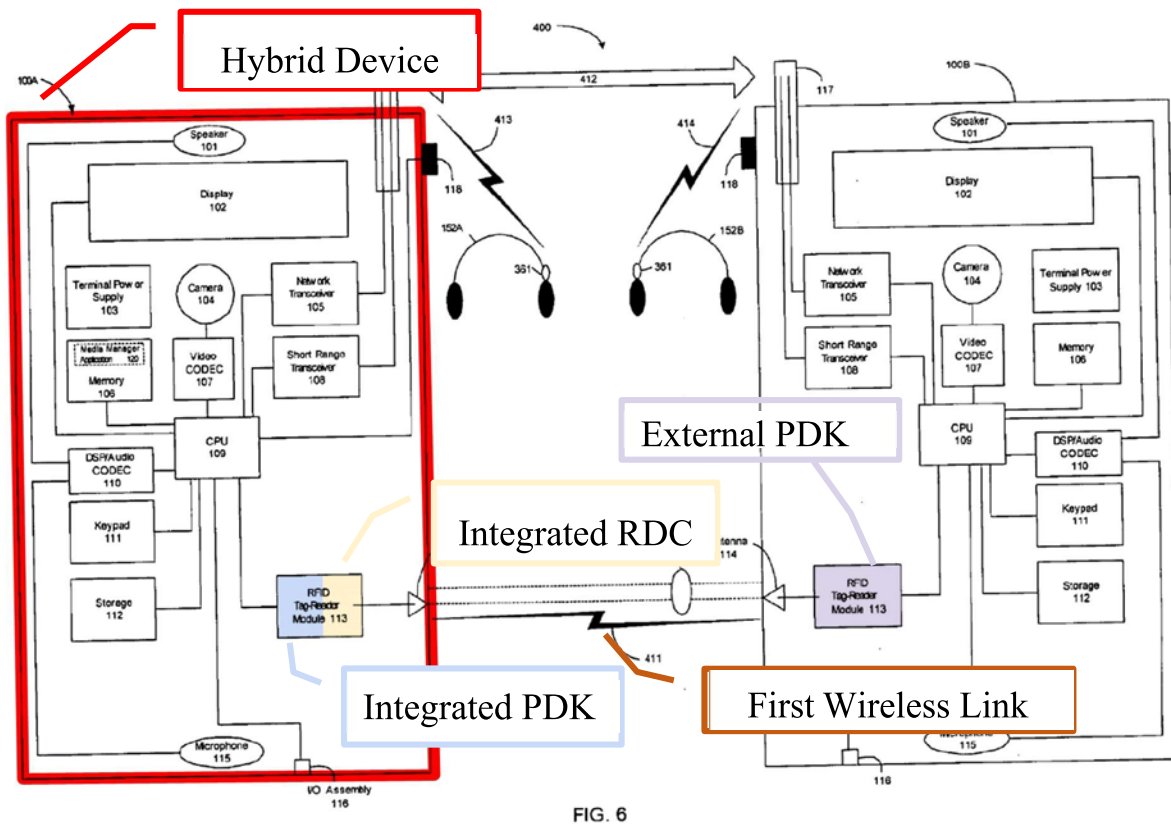


FIG. 6

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 “PDK” and “RDC,” as addressed above. The “reader component” of the “RFID Tag-Reader Module 113” in device 100A (integrated RDC) communicates with the “tag component” of the “RFID Tag-Reader Module 113” in device 100B

(external PDK).⁵ Ex-1004, [0071]-[0072], [0127]-[0128], Fig. 4B. As Dua explains, the “reader component” is used for transmitting interrogation signals to an external electronic device’s RFID tag when in proximity. Ex-1004, [0071]-[0072], [0127].

C. [10b] “receiving a first signal at the integrated RDC via the first wireless link from the external PDK;”

Dua discloses [10b] because it discloses receiving “RFID transmission data” (a first signal) at the hybrid device’s reader component (the integrated RDC) via the first wireless link from the external RFID tag (the external PDK). Ex-1004, [0127], [0130]; Ex-1003 ¶¶134-137. As Dua explains, during the RFID discovery process, after the external device’s RFID tag receives the interrogation signals, the external device’s RFID tag transmits RFID transmission data to the hybrid device. Ex-1004, [0127]-[0144]; Ex-1003 ¶136. The transmitted RFID 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].

⁵ The “tag components” of the “RFID Tag-Reader Module 113” in device 100A (integrated PDK) also communicate with the “reader components” of the “RFID Tag-Reader Module 113” in device 100B (external RDC).

D. [10c] “generating an enablement signal enabling one or more of an application, a function and a service on one or more of the hybrid device and a device associated with an external RDC; and”

Dua discloses [10c] because after an RFID tag-reader module receives the external device’s RFID transmission data, Dua’s hybrid device automatically generates “a Bluetooth paging message” (an enablement signal) to enable an application, function, or service. Ex-1004, [0123], [0128]; Ex-1003 ¶¶138-150.

To the extent that an enablement signal must be generated by the integrated RFID reader (integrated RDC), Dua discloses this. Ex-1003 ¶¶143-144. As Dua explains, a user of the hybrid device may decide to transmit the digital media playing on a hybrid device to an external device. Ex-1004, [0126]. By bringing the external device into proximity with the hybrid device, the hybrid device’s integrated RFID reader (RDC) wirelessly communicates interrogation signals to the external device’s RFID tag, which in turn wirelessly communicates RFID transmission data to the integrated RFID reader (RDC). *Id.*, [0127]-[0142]. This RFID discovery/paging process causes the integrated RFID reader to transfer the data to the CPU to generate a Bluetooth paging message (enablement signal) to enable a service (e.g., wireless connection and transmission of media) on the external device. *Id.*, [0123]. The Bluetooth paging message causes the external device to perform a wireless connection setup, and upon completion, the hybrid device “automatically transmits” media content to the external device. *Id.*, [0128]. The Bluetooth paging message may

be used to enable wireless transmission of media to the external device, even if the media is not supported by the external device. *Id.*, [0161], [0172]; *see also id.*, [0123], [0127].

Alternatively, the Bluetooth paging message is generated to enable a function (e.g., wireless connection) between the hybrid device and external device. *Id.*, [0144], [0123], [0127]. The hybrid device and external device may “conserve power by not always having their wireless interface turned on.” *Id.*, [0144], [0137]. In Dua, the 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 ¶145. Thus, the function (e.g., wireless connection) is enabled on both the hybrid device and external device based on the Bluetooth paging message (enablement signal).

To the extent that an enablement signal must be generated by the integrated RFID tag (integrated PDK), 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 hybrid device. *Id.*, [0224]. During electronic payments using RFID technology, the

integrated RFID tag (integrated PDK) would generate an RFID signal (enablement signal) to exchange financial information with the external point-of-sale device that is in close proximity to enable electronic payments. *Id.*, [0070]; Ex-1003 ¶¶146-147. Thus, the function (e.g., point-of-sale transaction) is enabled on the external device. *Id.*, ¶147.

While Dua does not expressly disclose where the credit card profile or other payment information is stored, a POSITA would have understood that the device's digital wallet application (for point-of-sale transactions) would store its confidential information and data in the tag memory, *see* Ex-1004, [0105], [0121], so it could utilize the RFID capability to transact e-commerce transactions "over-the-air," *id.*, [0058]; Ex-1003 ¶148. 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." Ex-1004, [0105], [0109]; *see also* Ex-1006, [0036], [0042], [0063]. A POSITA would have been capable of storing the "credit card profile or other payment information" in Dua's tag memory because doing so would require minimal modification without undue experimentation. Ex-1003 ¶149. Dua also teaches that its RFID Tag-Reader Module "can also be used in connection with other applications...such as electronic payments at the point-of-sale," and explains how an application can update its information and data in the tag memory. Ex-1004, [0070], [0105], [0121]. Such an implementation would have been no more

than using prior art elements using known methods to yield predictable results. *Id.*, ¶149. *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 the “credit card profile or other payment information” in Dua’s tamper-resistant tag memory. Ex-1003 ¶149.

[10c] is recited as allowing “mixed operations” involving several alternatives: (1) what is being enabled (e.g., application, function, or service) and which device is being enabled (e.g., hybrid device or device associated with external RDC). Ex-1001, Abstract, 15:62-16:2. Because [10c] recites alternative events,⁶ “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). Dua discloses enabling an application, function, or service on either device with an RFID tag-reader module. Ex-1003 ¶150.

⁶ This is consistent with Proxense’s purported interpretation in its infringement contentions that the “one or more of the hybrid device and a device associated with an external RDC” requires only “a device associated with an external RDC.” Ex-1018, 11 (Ex. D, Preliminary Infringement Contentions). Proxense served Final Infringement Contentions, and its position remains the same.

E. [10d] “sending the enablement signal to one or more of the hybrid device and the device associated with an external RDC.”

Dua discloses [10d] because it discloses sending the Bluetooth paging message (the enablement signal) to the external device to enable an application, function, or service. Ex-1004, [0123], [0128], [0159]; Ex-1003 ¶¶151-156; §IV.D. Dua discloses sending a Bluetooth paging message to the external device to enable a service (e.g., wireless connection and transmission of media) on the external device. Ex-1004, [0128]. Alternatively, the Bluetooth paging message is sent to the external device to perform a connection set up, which then enables a function (e.g., wireless connection) on the hybrid device and the external device. *Id.*, [0144].

Lastly, Dua’s integrated RFID tag (integrated PDK) generates and sends an RFID signal to the external point-of-sale device for electronic payment. *Id.*, [0052], [0070].

V. Ground 3: Claims 1, 3-6, 8-15, and 17 Would Have Been Obvious Over Buer.

A. Buer renders obvious each of independent claims 1 and 10.

Independent claim 10 is representative. Ex-1003 ¶157.

1. Claim 10

a. [10pre] “A method comprising:”

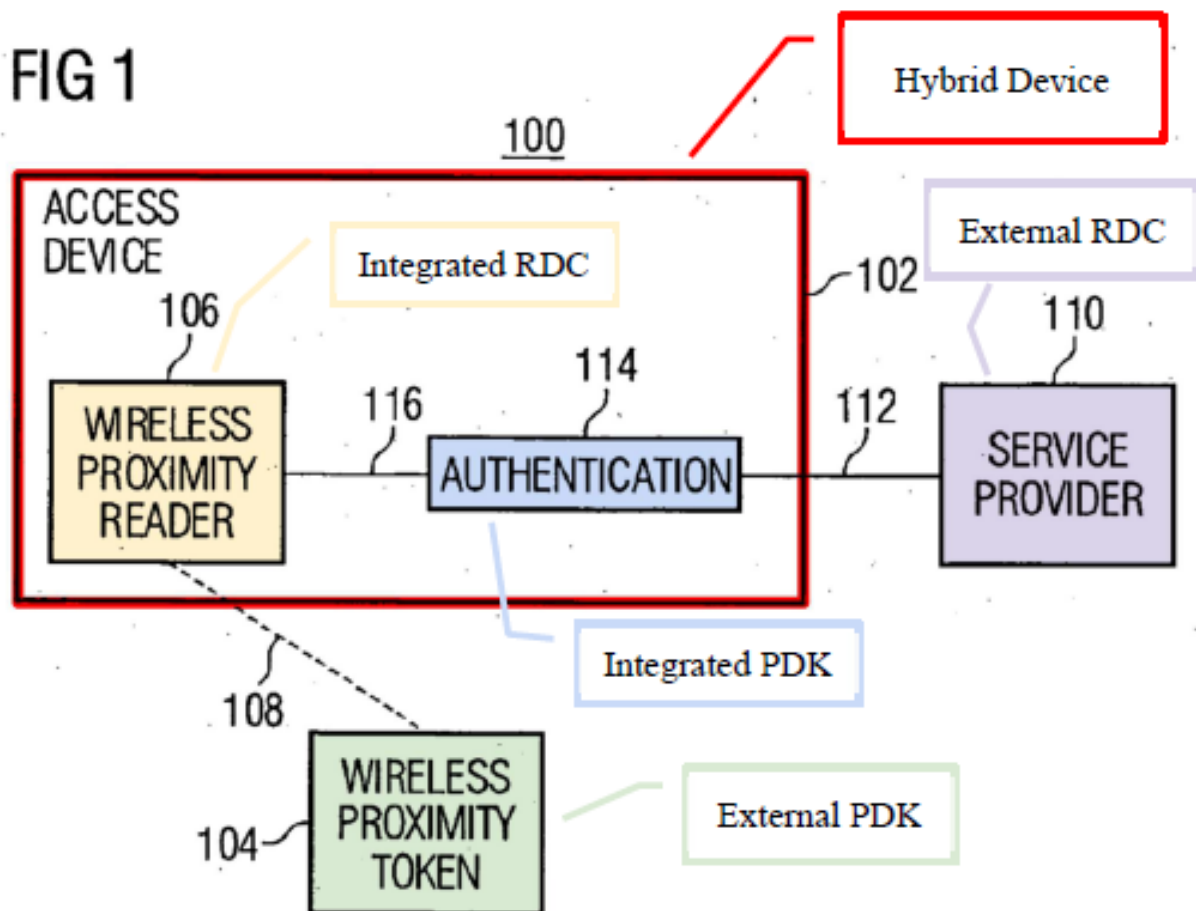
To the extent [10pre] is limiting, Buer discloses the preamble because it discloses a method for an access device to access a secured service. *Id.*, ¶¶158.

- b. [10a] “creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external personal digital key (PDK), the hybrid device including an integrated PDK and the integrated RDC;”

Buer discloses [10a].

(1) A hybrid device including an integrated PDK and an integrated RDC:

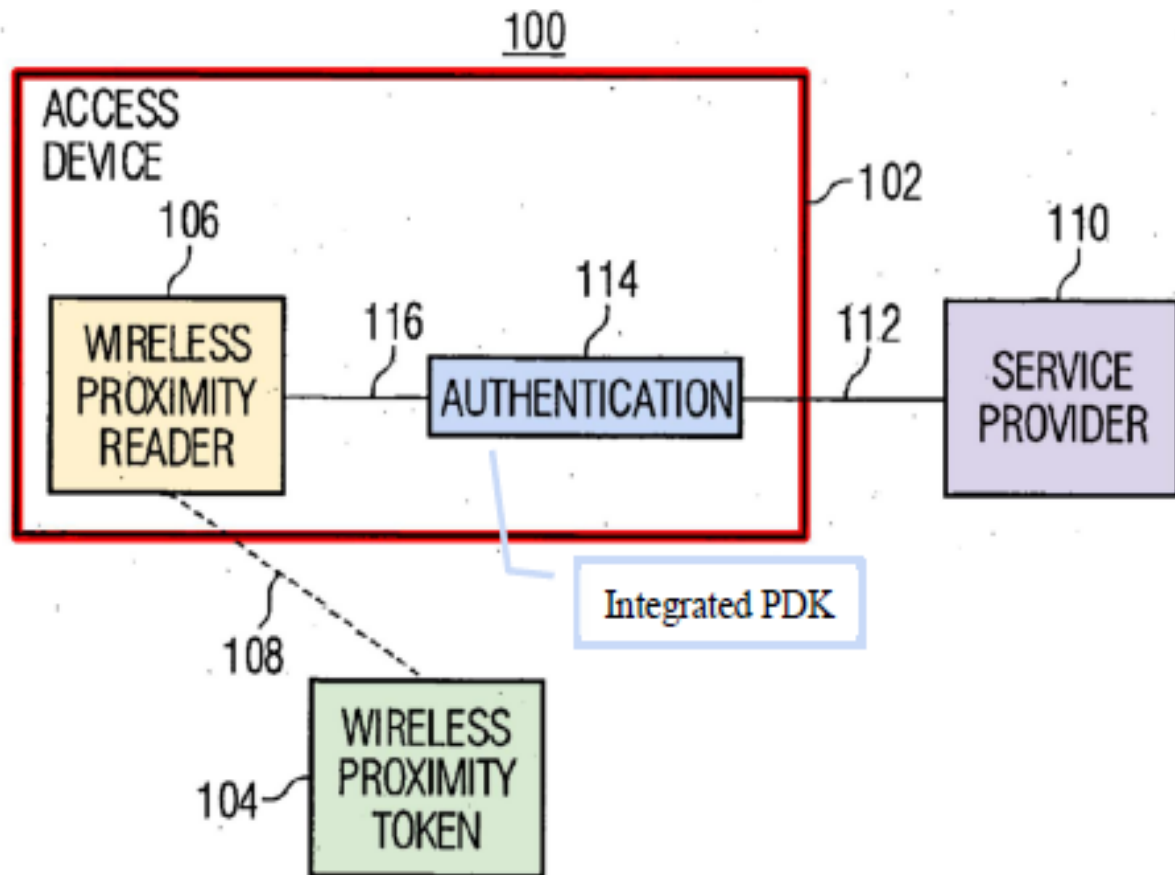
Buer discloses the hybrid device in [10a] because it discloses an access device that combines an authentication circuitry (an integrated PDK) and a proximity reader (an integrated RDC) to provide a hybrid device, as shown below. *Id.*, ¶¶159-164.



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 ¶162. In Figure 1, Buer's access device 102 ("hybrid device," red) includes two components: an authentication component 114 ("integrated PDK," blue) and a proximity reader 106 ("integrated RDC," yellow). The authentication component 114 is configured to process (e.g., encrypt or sign) the information before sending it to the service provider 110 (purple). The proximity reader 106 is configured to receive information from a token 104 ("external PDK," 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 PDK. Ex-1003 ¶¶164-174.

FIG 1

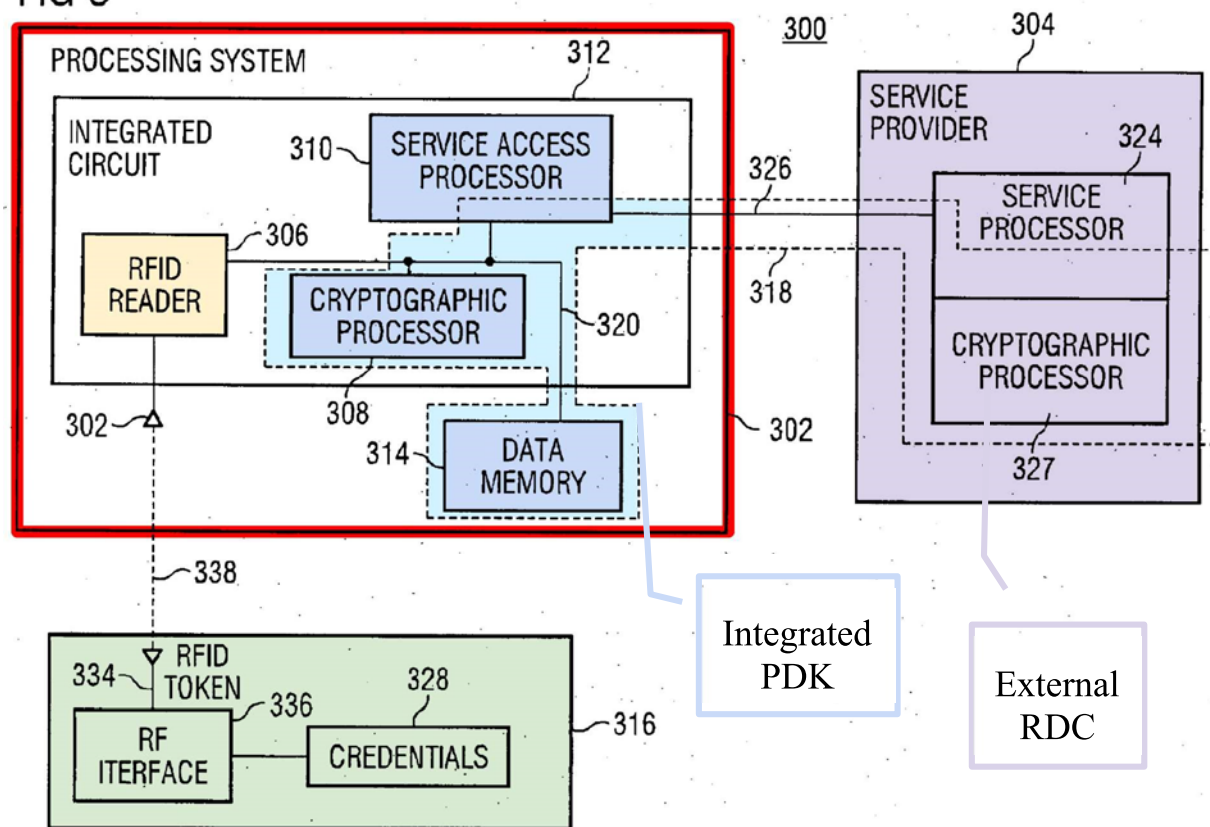


Ex-1005, Fig. 1 (annotated). In Buer, the authentication component is implemented as a cryptographic processing system (*id.*, Figs. 3, 6) and is a “personal digital key” under either the court’s construction or Google’s proposed construction.

The authentication component (e.g., cryptographic processing system), as shown below, is an operably connected collection of circuit components (blue) that includes a service access processor for communicating with an external service provider (“an antenna and a transceiver for communicating with a[n] RDC”) and a

cryptographic processor and data memory (“controller and memory for storing information particular to a user”). *Id.*, [0137].

FIG 3



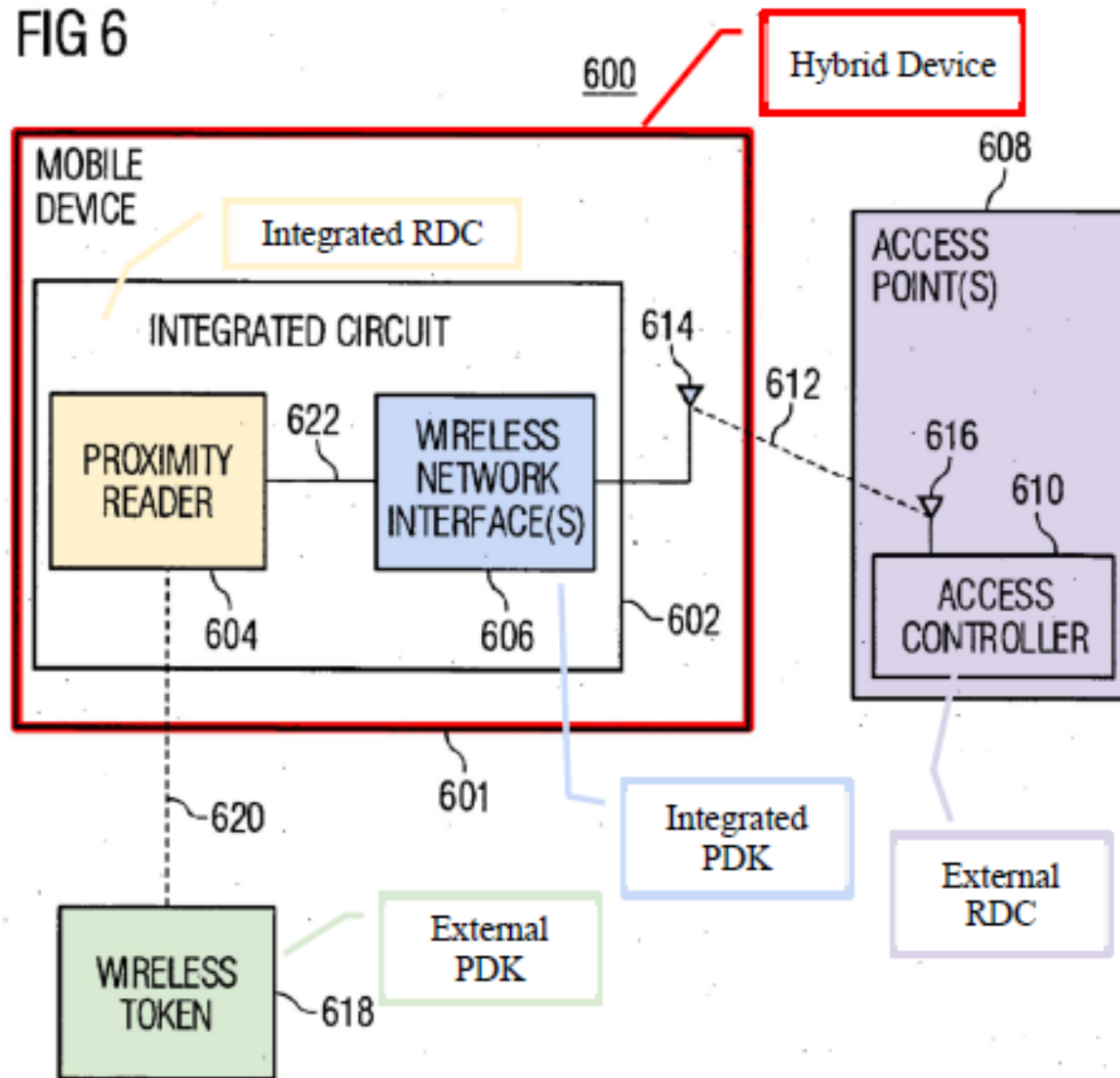
Id., Fig. 3 (annotated). Buer's cryptographic processor 308 acts as a controller for encrypting any important information, such as a user's credentials ("information particular to a user"), received from the external token. *Id.*, [0119], [0135]-[0137], [0141], [0150]. The encrypted information (and credentials) is stored in data memory 314 within the cryptographic boundary 318 (**light blue**). *Id.*, [0135], [0137].

The service access processor 310 then sends encrypted information via a communication link 326 to an external cryptographic processor 322, 327⁷ (purple) for decryption and/or authentication processing as necessary. *Id.*, [0138], [0152]-[0153]. It would have been obvious that Buer's communication link 326 would have included a wireless link to wirelessly transmit the encrypted information over "air" via an antenna/transceiver from the processing system 302 to the service provider 304. *Id.*, [0113], [0199]-[0201]; Ex-1003 ¶170. A POSITA would have been motivated to apply the cryptographic process (Figure 3) over a wireless communication link because Buer expressly teaches so. Ex-1004, [0163], [0165], Fig. 6; Ex-1003 ¶171. Buer teaches that a wireless communication link, as expressly disclosed in Figures 5-7, would have been used for a mobile device to access a wireless service provider (e.g., cellular network provider, 802.11 network provider, Bluetooth network provider, etc.). Ex-1005, [0162]-[0163]; *see also id.*, [0200] (a signal includes "electromagnetic (e.g., RF or infrared) radiation transmitt[e] through the air"). Doing so would provide the processing system access to wireless service provider and ensure any information that is sent over the air via communication link 326 is encrypted within a security boundary. *Id.*, [0139]-[0142], [0151]; Ex-1003 ¶171.

⁷ Figure 3 appears to include a typographical error.

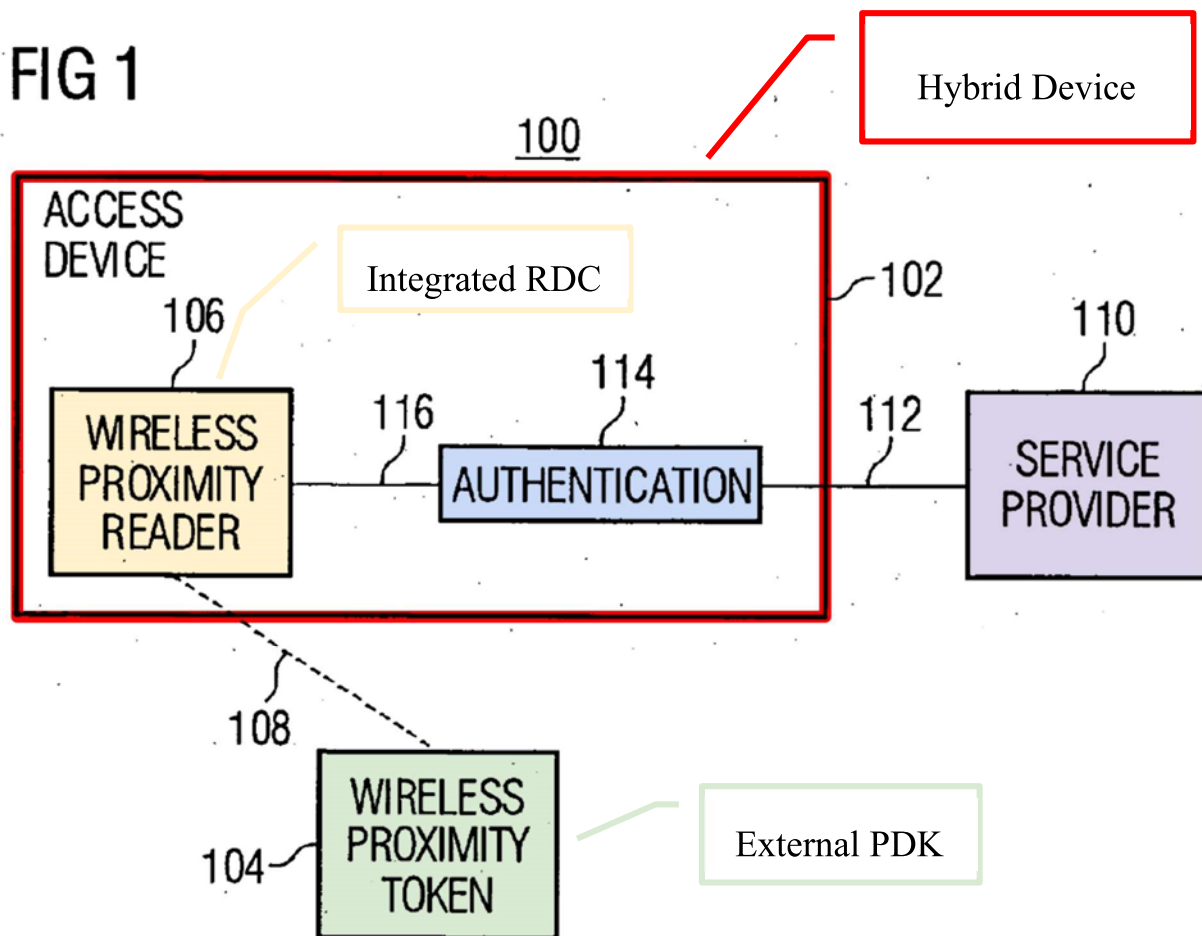
Buer expressly explains how a wireless token would be used with a mobile device to access a wireless network provider using “cryptographic techniques as discussed [in Buer].” Ex-1005, [0170]. As Buer explains, when the access device is implemented in Buer’s mobile device (**red**), the cryptographic processing system is used to “cryptographically encrypt/sign the information” before the mobile device “sends the signed information” via a wireless network interface (**blue**) “to the network access provider (e.g., access point 608)” (**purple**). *Id.*, [0165], [0170], [0174]. As shown in Figure 6, the mobile device (**red**) includes an antenna 614 and wireless network interface(s) 606 (**blue**) that are used to send the encrypted (or signed) information over a wireless network (e.g., a cellular network, an 802.11 network, a Bluetooth network, etc.) via RF signals 612 to the network access provider. *Id.*, [0163], [0165], [0174].

FIG 6



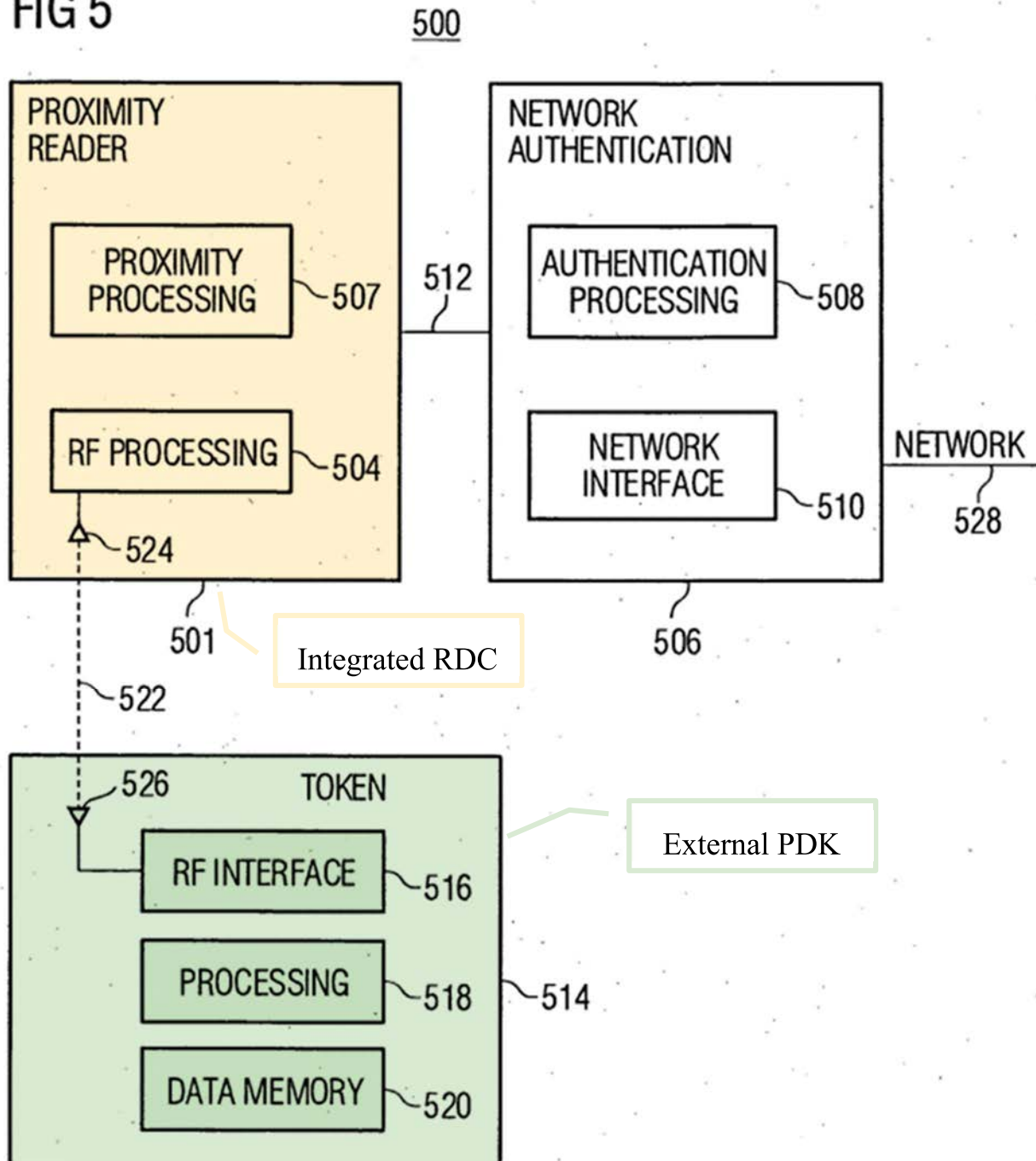
Id., Fig. 6 (annotated). While the cryptographic processing is not shown in Figure 6 to “reduce the complexity” of the figure, *id.*, [0170], a POSITA would have understood that the cryptographic processing system (in Figure 3) would have been implemented in the mobile device. Ex-1003 ¶173. Accordingly, Buer’s cryptographic processing system, including its cryptographic processor, service access processor, and data memory, is an integrated PDK. *Id.*, ¶174.

Buer's proximity reader discloses the integrated RDC in [10a] and is a "receiver-decoder circuit" under either the court's construction or Google's proposed construction. Buer's proximity reader 106 ("integrated RDC," **yellow**), as shown below, is a component that is "configured to receive signals 108 (e.g., RF signals)" from at least one proximity token 104 ("external PDK," **green**) when the token 104 is "proximate to the access device 102." *Id.*, [0111]; Ex-1003 ¶¶175-179.



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

FIG 5



Id., Fig. 5 (annotated).

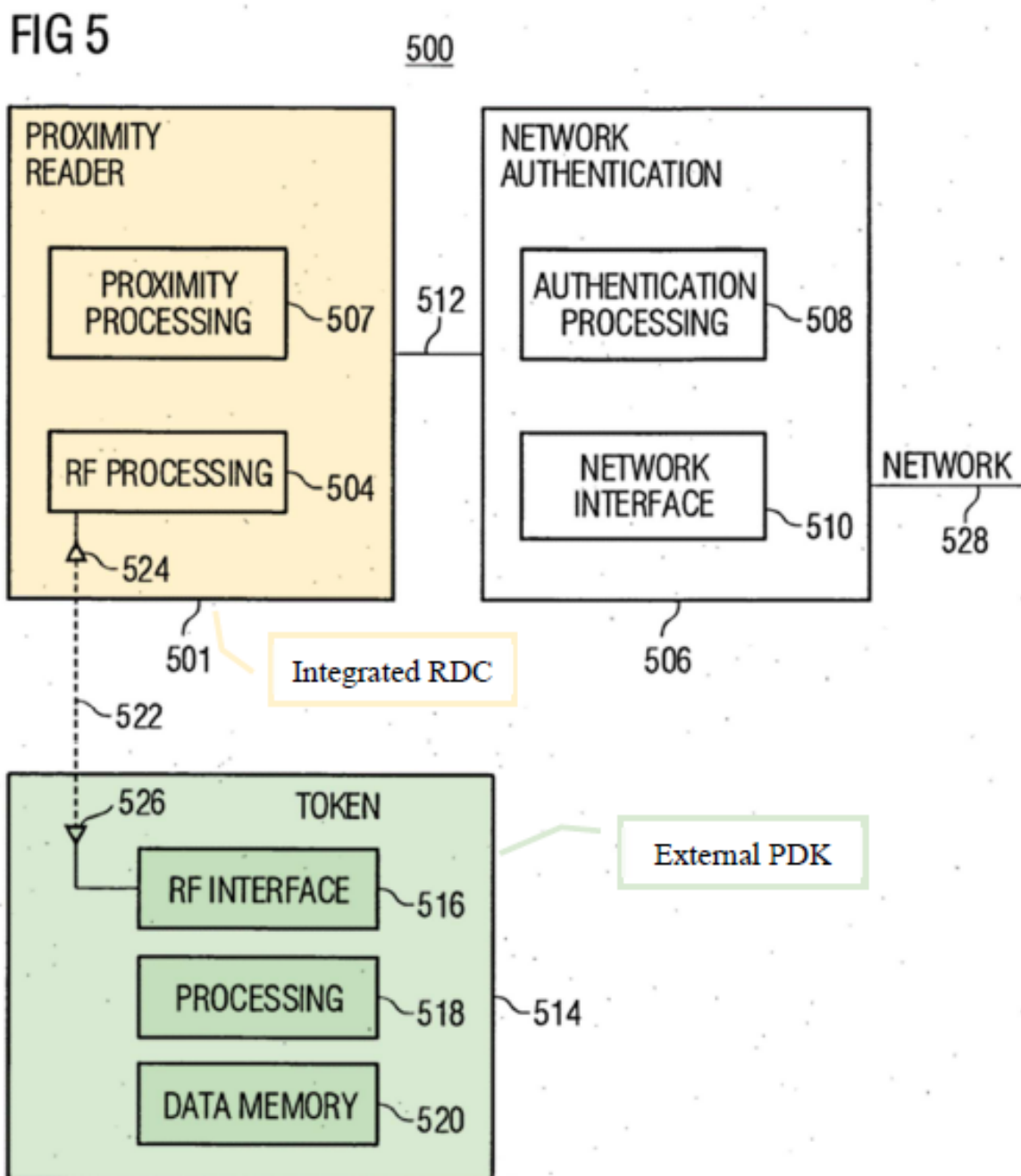
In Buer, the “proximity reader and token may be implemented using one or more of a wide variety of wireless proximity techniques.” *Id.*, [0128]. As Buer explains, the proximity reader and the external token communicate via RF signals when they are within proximity to one another. *Id.*, [0112], [0146], [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 decodes the encrypted information for later processing (including for extracting the embedded information, as disclosed). Ex-1003 ¶178.

Because Buer’s access device includes an integrated authentication component and a wireless reader, Buer discloses a hybrid device that includes both an integrated PDK and an integrated RDC as recited in [10a]. *Id.*, ¶179.

(2) Creating a First Wireless Link between an Integrated RDC and an External PDK:

Buer discloses creating a first wireless link between the proximity reader (integrated RDC) and a token (external PDK) as in [10a]. *Id.*, ¶¶180-184. As Buer explains, “an RFID 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].

Buer's wireless token is an "external PDK" 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]. But "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.*, Ex-1005, [0120]-[0122], [0155]. Buer's external token discloses the 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 shown in Figure 5. *Id.*, [0157]-[0159].



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 is a controller for "control[ling]

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[ling] 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 ¶¶183-184.

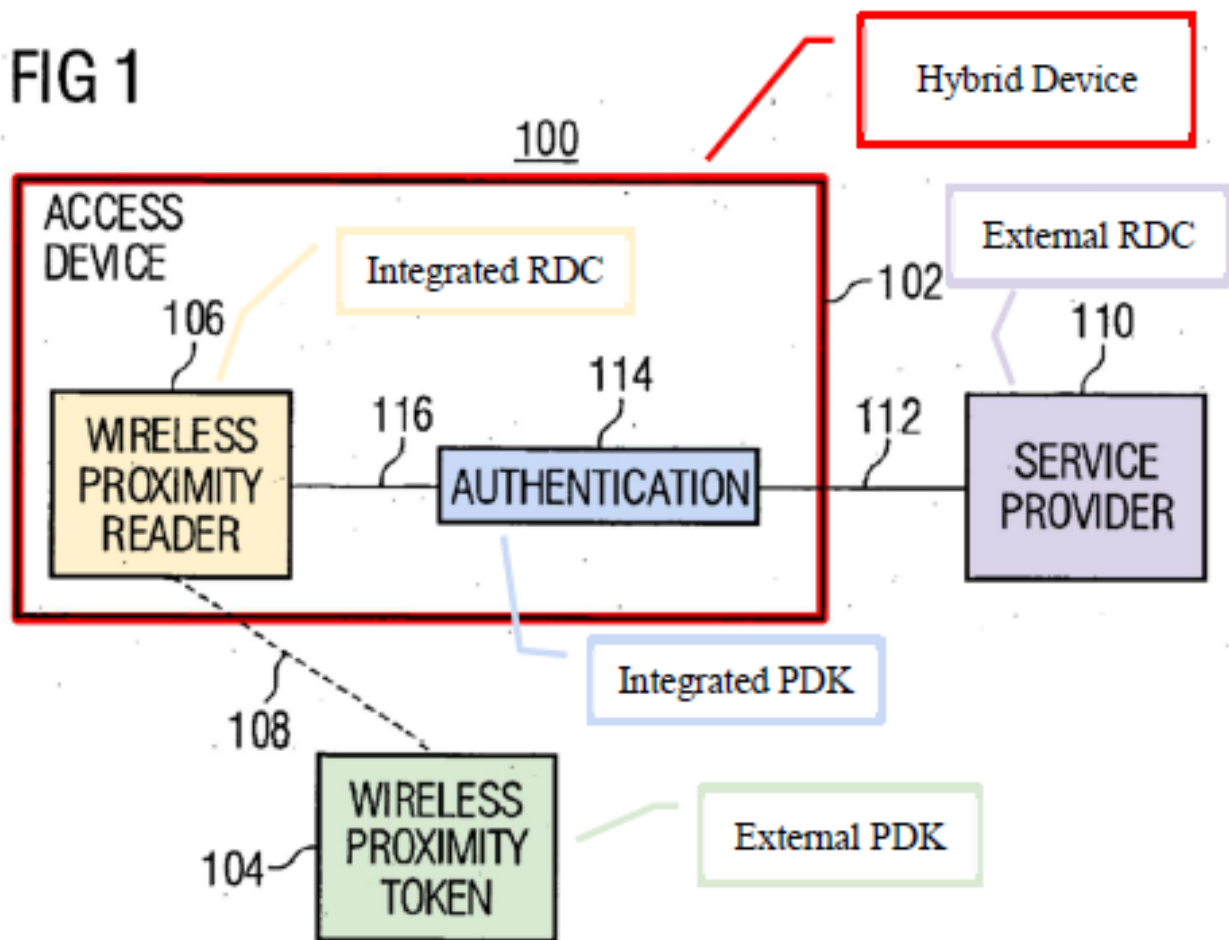
c. [10b] “receiving a first signal at the integrated RDC via the first wireless link from the external PDK;”

Buer discloses receiving RF signals at the integrated RDC from the external PDK as in [10b] because the integrated reader receives RFID signals, including proximity signaling and authentication information, during the RFID signaling from the external token. *See* [10a]; §V.A.1.b; Ex-1003 ¶¶185-186. 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.*, Fig. 7, Fig. 9. Ex-1003 ¶¶187-188.

- d. **[10c] “generating an enablement signal enabling one or more of an application, a function and a service on one or more of the hybrid device and a device associated with an external RDC; and”**

Buer discloses the authentication component generating an enablement signal enabling a wide variety of applications, functions, or services as in [10c] because it provides encrypted or signed credentials to a service provider to enable access to secured services, as shown below. Ex-1003 ¶¶189-203.



Ex-1005, Fig. 1 (annotated); *see also id.*, [0113] (“[T]he communication media 112 may comprise...electric wires, optical cables or air.”). Because [10c] is recited as allowing “mixed operations,” Ex-1001, Abstract, 15:62-16:2, “the entire element is disclosed by the prior art if one alternative...is in the prior art.” *Fresenius*, 582 F.3d at 1298.

To the extent that [10c] requires that the application, service, or function runs on the hybrid device itself, Buer discloses this. Ex-1003 ¶¶192-199. 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 to enable a wide variety of applications, functions, or services on the hybrid device. Ex-1005, [0152], [0174]. The service provider may enable access to the following requested service:

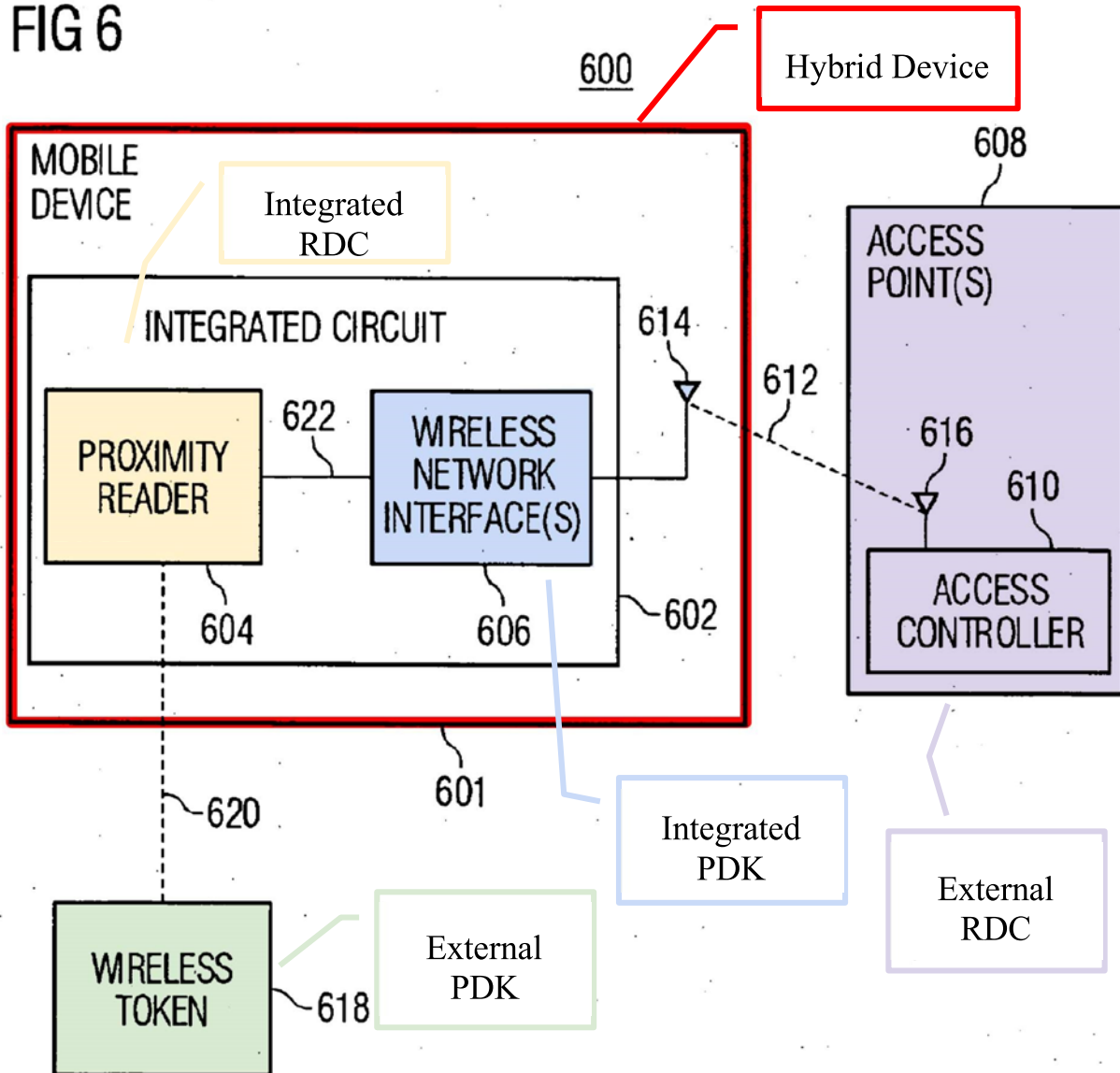
[S]ervice may include, for example, access to data and/or a data processing service. Thus, a service may enable an access device to, for example, read or write data in a data memory, access encrypted data, use cryptographic keys, gain access to cryptographic material such as security associations and keys, access a web page, access a data network or access a processing application.

Id., [0120]; *see also, e.g., id.* [0122], [0155], [0162], [0195]-[0196]. In Buer, 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.*, [0122].

Like the '042 patent, Buer discloses enabling network access on a hybrid 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.

To the extent that [10c] requires that an application, function, or service runs on an external device, Buer discloses this. Ex-1003 ¶¶200-203. In particular, Buer discloses that its mobile device may also “be used to authenticate a user to another processing system” (external device) associated with an external proximity reader 1120 (external RDC), which includes “point-of-sale components,” to “perform a sales transaction,” such as “credit card transactions.” Ex-1005, [0194]-[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], [194]. The extracted credential would be stored in its integrated PDK via the local data memory 824. *Id.*, [0185]; Ex-1003 ¶201. 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, like the ’042 patent, “data services” may be enabled on the external security processing system. *Id.*, [0195]; Ex-1003 ¶¶202-203.

e. [10d] “sending the enablement signal to one or more of the hybrid device and the device associated with an external RDC.”

As discussed in §V.A.1.d, Buer discloses sending the enablement signal (e.g., RF signal containing the encrypted or signed information) to the external service provider to enable an application, function, or service on the access device, including enabling access to a data network. Ex-1005, [0120], [0122], Fig. 7; Ex-1003 ¶¶204-205.

Alternatively, as discussed in §V.A.1.d, Buer discloses sending the enablement signal (e.g., RF signal containing credit card information) to the external security processing system to enable an application, function, or service on the external security processing system, including enabling performance of a sales transaction,” such as a “credit card transaction[.]” Ex-1005, [0195]-[0196]; Ex-1003 ¶206.

2. Claim 1

a. [1pre] “A hybrid device comprising:”

As discussed in §V.A.1.b, Buer discloses [1pre] because it discloses an access device that combines an authentication circuitry and a proximity reader to provide a hybrid device. *See* claim 10; Ex-1003 ¶207.

- b. [1a] “an integrated personal digital key (PDK) for storing information and capable of communicating wirelessly with at least one external receiver-decoder circuit (RDC); and”**

As discussed in §V.A.1.b, Buer’s authentication component (e.g., cryptographic processing system) discloses an integrated PDK, in accordance with the court’s and Google’s construction, for storing information, and is capable of communicating wirelessly with an external RDC. *See* [10a]; Ex-1003 ¶¶208-213.

Buer discloses that the service provider, Ex-1005, Figs. 1, 3, 6, as a whole, or the internal cryptographic processor 322, 327, or access controller 610 individually, *id.*, [0153], [0165], is an external RDC in [1a] because they are either a component or collection of circuit components, “capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing,” as the court has construed and Google has proposed. Ex-1003 ¶209. Buer’s external cryptographic processor 322, 327 in Figure 3 is capable of receiving encrypted information and “decrypti[ng] and/or authenticati[ng]...the encrypted information and provid[ing] the information in the clear for internal processing.” Ex-1005, [0138]. The external access controller 610 is also capable of wirelessly receiving encrypted data or “signed information” over a given wireless network. *Id.*, [0165], [0174]-[0175]. Buer explains that the “information contained within the broadcast RF signal may be extracted only within a security boundary.” *Id.*, [0174]. A POSITA would have

understood that the access controller 610, or the service provider (e.g., access point 608), would need to decode the encrypted or signed information to extract the credentials for verification, using the cryptographic processing “techniques discussed herein [in Buer]” with respect to Figure 3. *Id.*, [165], [0174]; Ex-1003 ¶212.

Thus, Buer discloses an integrated PDK for storing encrypted user information and capable of communicating wirelessly with an external RDC. Ex-1003 ¶213.

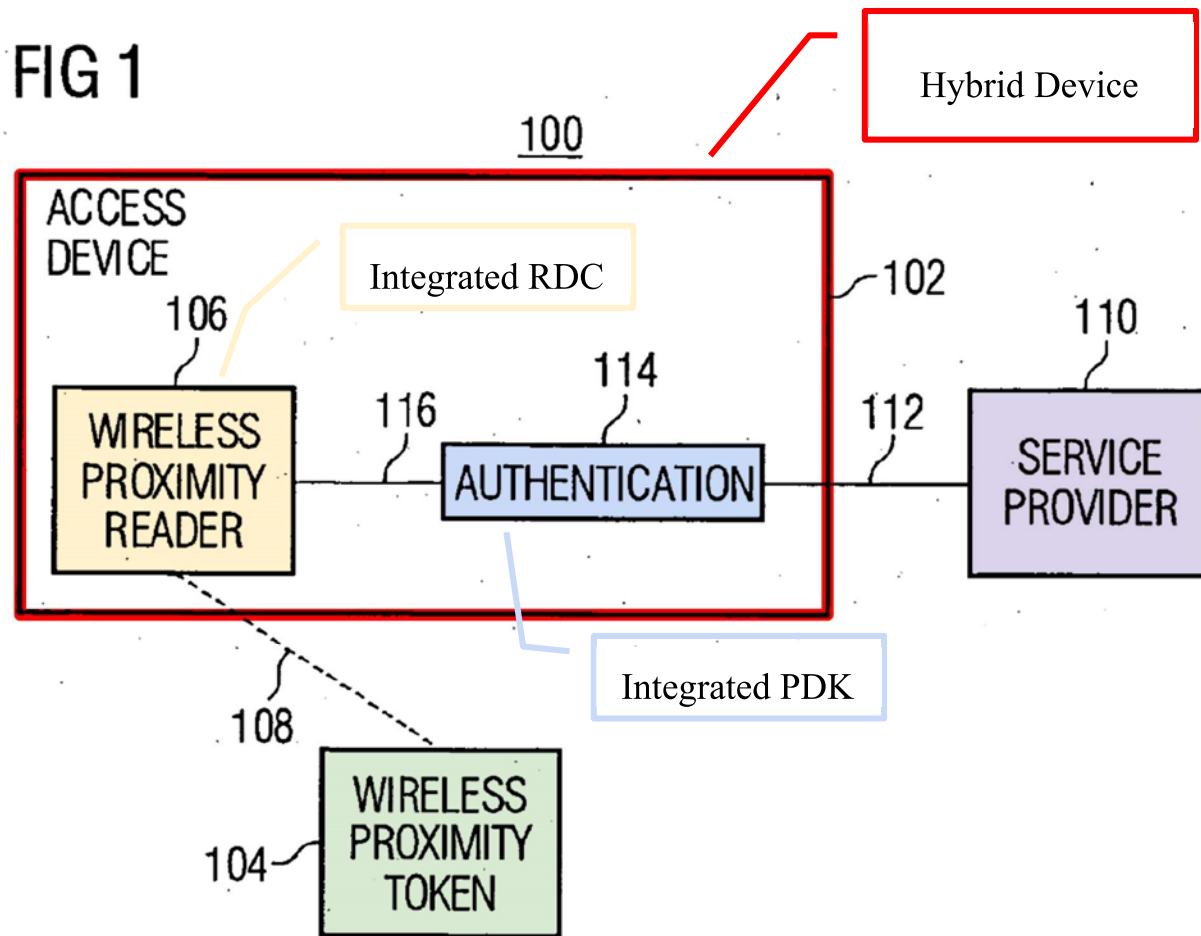
c. [1b] “an integrated RDC for communicating wirelessly with at least one external PDK within a proximity zone,”

As discussed in §§V.A.1.b-V.A.1.c, Buer discloses that the integrated proximity reader (RDC) communicates “wirelessly with at least” an external token “within a proximity zone.” *See* [10a]-[10b]; Ex-1003 ¶¶214-216. Buer’s proximity reader 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]; Ex-1003 ¶216.

d. [1c] “the integrated RDC coupled to the integrated PDK by a first signal line for communication,”

Buer discloses that the integrated “[proximity] reader 106” is coupled to the integrated “authentication component 114” “via a connection 116 within a common integrated circuit” as in [1c], as shown below. Ex-1005, [0116]; Ex-1003 ¶¶217-219.

FIG 1

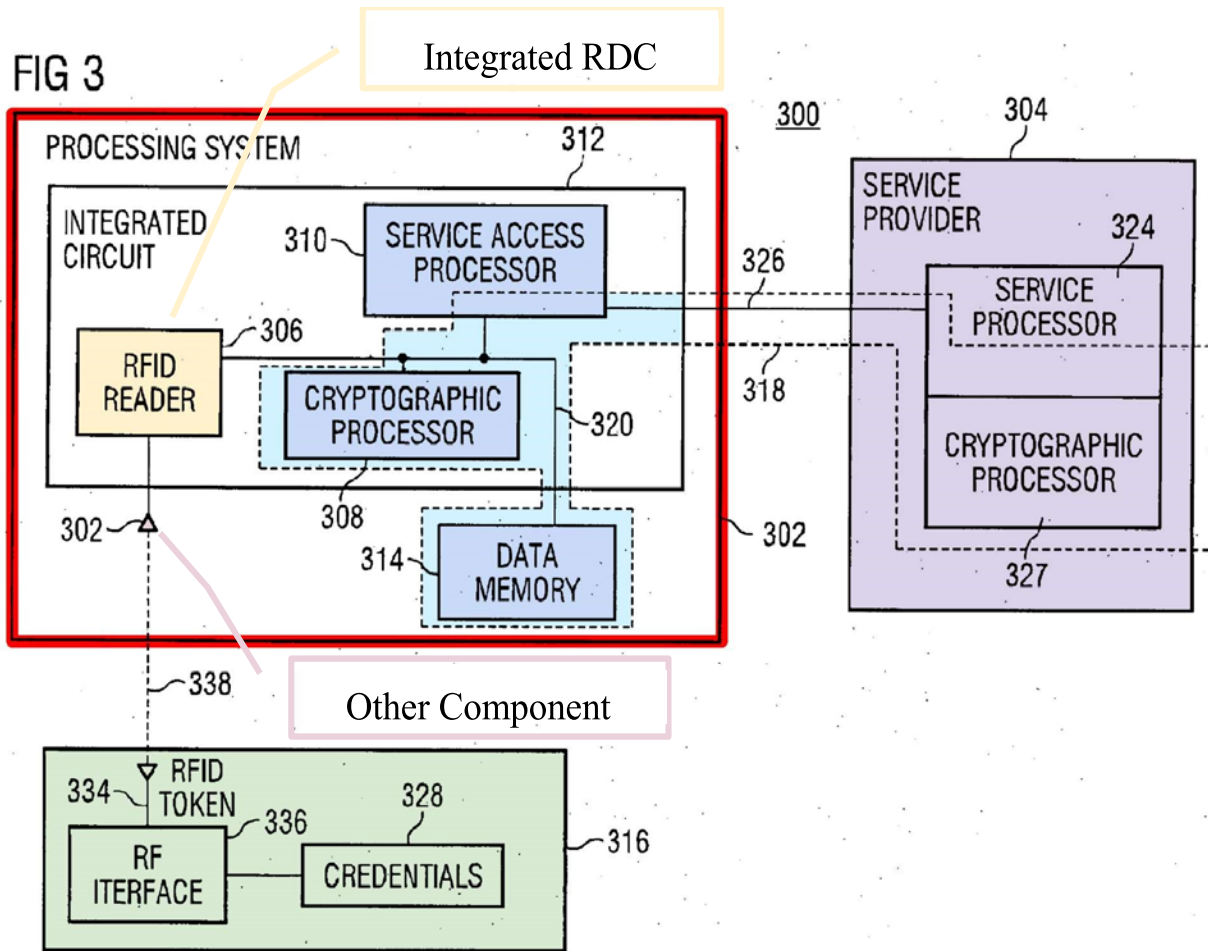


Ex-1005, Fig. 1 (annotated). As discussed above for [1a], when Buer's authentication component is implemented as a cryptographic processing system, it is coupled to the reader via a first data bus 320 in Figure 3 or via a first internal leads 622 in Figure 6.

Ex-1005, [0137], [0167].

- e. [1d] "the integrated RDC coupled to at least one other component of the hybrid device by a second signal line,"

Buer discloses that the integrated reader is coupled to at least one other component of Buer's hybrid device by a second signal line as in [1d] because the integrated reader is coupled to RF components, as shown below. Ex-1003 ¶¶220-221.

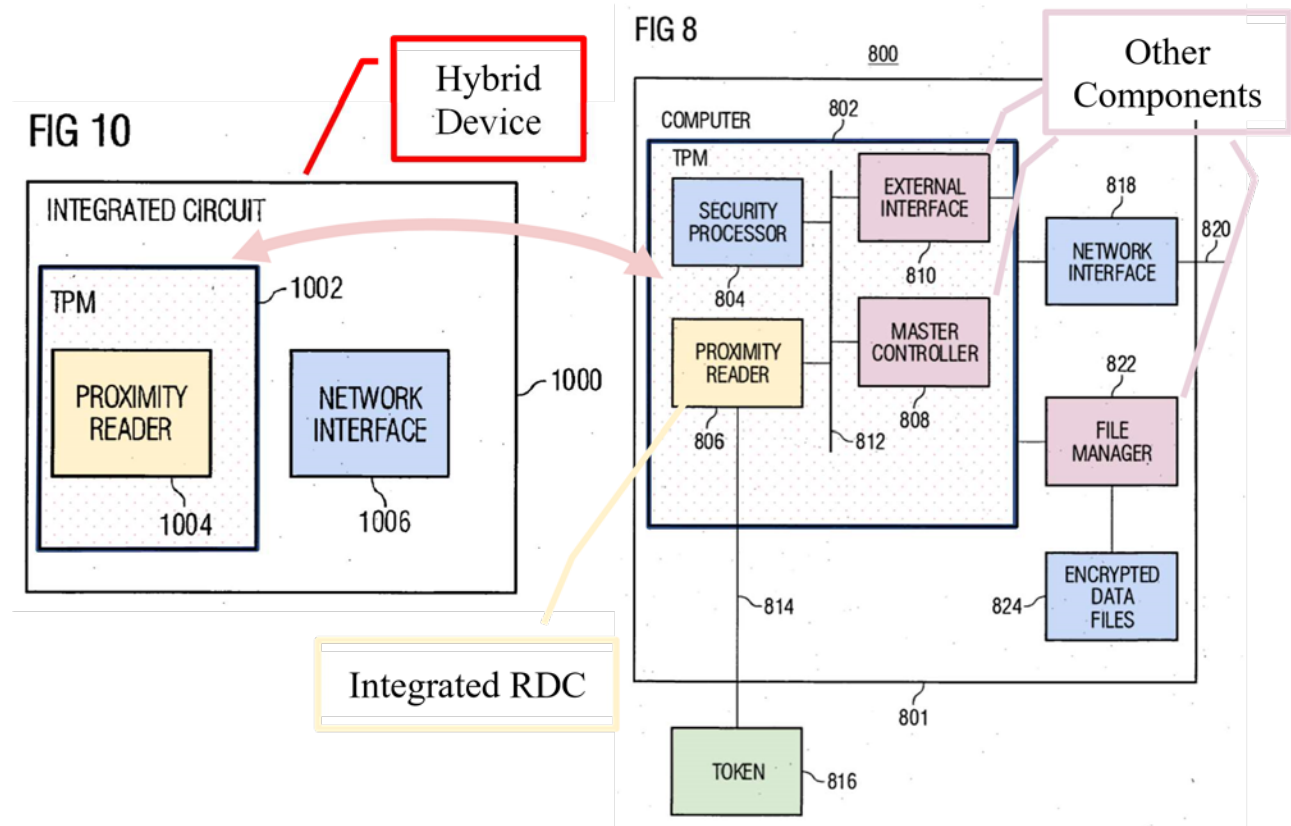


Ex-1005, Fig. 3 (annotated). In Figure 3, Buer’s RFID reader is coupled to an antenna⁸ for broadcasting RFID signaling and receiving RFID data. *Id.*, [0146].

A POSITA would have understood that other additional components are included in Buer’s mobile device, as shown in Figure 10, where a trusted platform

⁸ Figure 3 of Buer labels the antenna as 302, but the specification refers to it as “antenna 332.” Ex-1005, [0146].

module (“TPM”) and network interfaces are combined on a single integrated circuit to reduce the cost of the system. Ex-1003 ¶222; Ex-1005, [0190]-[0191].



Ex-1005, Figs. 10 & 8 (annotated). Although the TPM in Figure 10 does not show additional components, it would have been obvious to a POSITA that the TPM in Buer’s mobile device would have had other components such as a master controller “for controlling the overall operation of the TPM” and an external interface “for interfacing with other components.” *Id.*, [0180]; Ex-1003 ¶223. To facilitate the cryptographic processing and boundary, Buer’s mobile device would have also included a file manager for accessing encrypted data files stored in data memory. Ex-

1005, [0178], [0185]; Ex-1003 ¶224. The integrated reader within the TPM would communicate with these various components via a bus 812. Ex-1005, [0180].

A POSITA would have understood that the mobile device may include, although not shown, other components for providing verification responses, such as a display screen and/or a haptic motor. Ex-1003 ¶225. The integrated RDC would necessarily be connected to these components, including, at a minimum, to the phone's display screen to provide confirmation of authorization. As Buer explains, the access device may also include components that enable the access device "to further verify the authenticity of the user." Ex-1005, [0114]. These components may include a "keyboard" or touch sensor for inputting a password or a "biometric reader" (e.g., a fingerprint reader) for inputting biometric information. *Id.*, [0114] ("In this way, access to a service may be restricted until the user satisfies one or more verification queries including, for example, what the user knows (e.g., a password), ... and who the user is (e.g., a physical or biometric characteristic)."). An RDC in a mobile phone would be connected to those various input devices (e.g., keyboard, touch sensor, biometric reader) and ordinarily to an application processor as well. This allows processing of the credentials as well as interactions with a user in response to the presentation of credentials. Ex-1003 ¶226.

Buer teaches that these components can be "connected/coupled in many different ways" and are not limited by the drawings. Ex-1005, [0199]. As Buer notes,

“one or more integrated circuits” can be used to house the internal components within a mobile phone. *Id.*, [0198]. Buer teaches that its components may be “connected/coupled directly or indirectly” through intervening devices such as buffers. *Id.*, [0204]. Thus, Buer teaches that its internal components, including its integrated RDC, may be connected with a plurality of other components, including other circuits, either directly or indirectly. A POSITA would readily understand that multiple signal lines would be necessary to connect the integrated RDC directly to a plurality of integrated circuits. Ex-1003 ¶227. Accordingly, Buer teaches using a second signal line to connect the integrated RDC to another component in the hybrid device. *Id.*, ¶228. In a typical mobile phone in use at the time, a variety of such components would be connected by one or more system buses, I/O buses, and peripheral ports, including common hardware interfaces such as a universal asynchronous receiver / transmitter (UART), serial peripheral interface (SPI), and Inter-IC (I²C). Any one or more of these would be the claimed second signal line. *Id.*

- f. **[1e] “one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service on one or more of the hybrid device and a device associated with the external RDC.”**

As discussed in §V.A.1.d, Buer discloses the authentication component enabling a wide variety of applications, functions, or services as in [1e]. *See* [10c]; Ex-1003 ¶229. [1e] 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., hybrid device or external RDC). Ex-1001, Abstract, 15:62-16:2. Because [1e] 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. To the extent that [1e] requires that the application, service, or function runs on the hybrid device itself, as discussed in §V.A.1.d, Buer discloses enabling an application, function, or service on the access device, including enabling application access, data access, or network access on the access device. Ex-1003 ¶232. To the extent that [1e] requires that the application, function, or service runs on an external device, as discussed in §V.A.1.d, Buer discloses enabling one or more of an application, function, or service on the external device associated with an external RDC, including enabling data services such as performing sales transactions. Ex-1003 ¶233.

B. Buer renders obvious claims 3-6, 8, 9, 11-15, and 17.

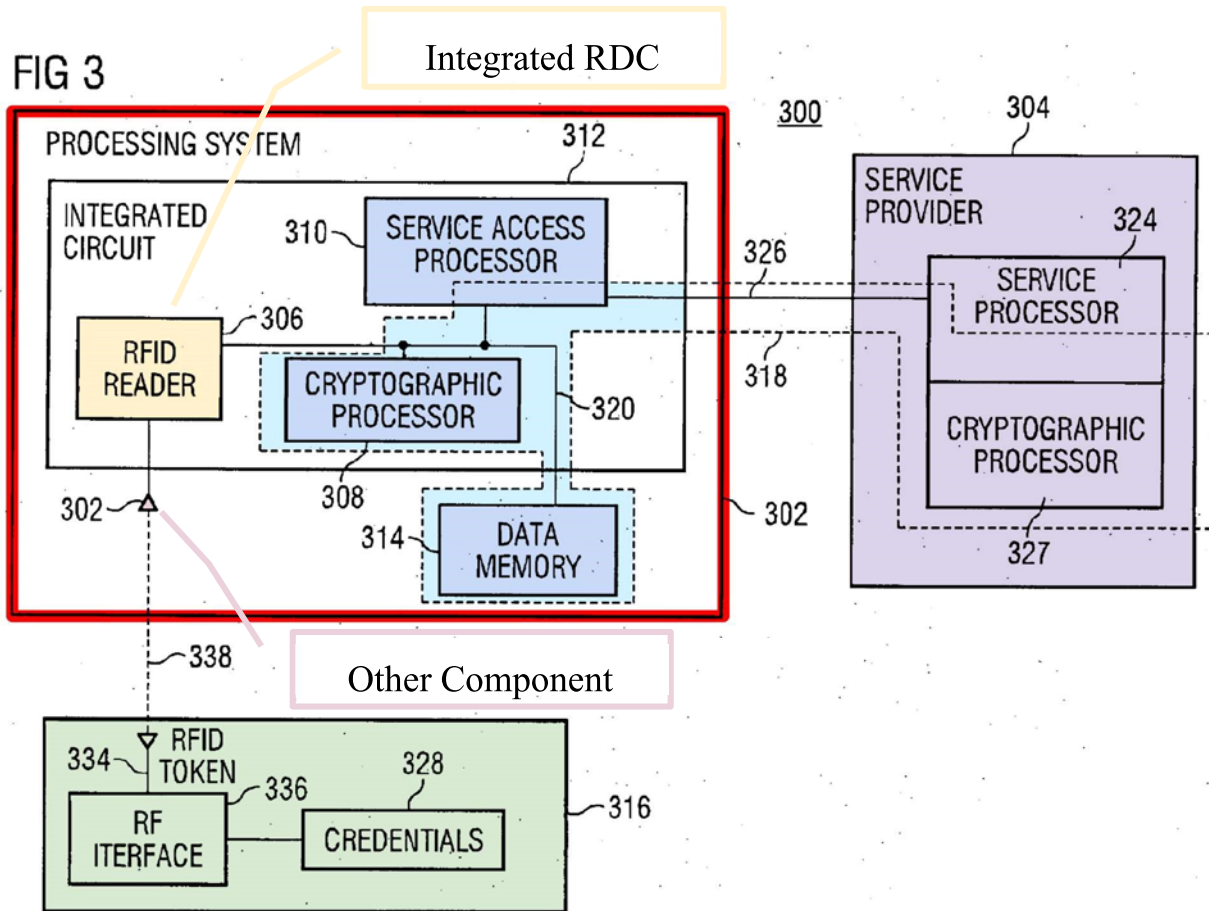
1. **[3] “The hybrid device claim 1, wherein the integrated PDK is capable of communicating with the at least one external RDC at the same time the integrated RDC communicates with the at least one external PDK.”**

Buer renders obvious [3]. Ex-1003 ¶235. Buer discloses that the integrated PDK is capable of communicating wirelessly with at least one RDC, as in [1a], and that the integrated RDC communicates wirelessly with at least one external PDK, as

in [1b]. §§V.A.2.b-V.A.2.c. It would have been obvious that they communicate *at the same time* because Buer uses a token's physical presence to authenticate a user. Ex-1005, [0114], [0011]; Ex-1003 ¶237. It would have been obvious that while an authentication system (integrated PDK) communicates with an external service provider (external RDC), the integrated proximity reader (integrated RDC) also communicates with an external proximity token (external PDK) *at the same time* to ensure that the request was made while the token is “in the proximity” of the device. Ex-1005, Buer, [0011]; Ex-1003 ¶237.

2. [4] “The hybrid device of claim 1, wherein the integrated RDC communicates an enable signal to the device using the second signal line.”

Buer's integrated proximity reader (integrated RDC) is coupled by a second signal line to various internal components, including an antenna 332. Ex-1003 ¶¶238-239; §V.A.2.e.



Ex-1005, Fig. 3 (annotated). The integrated proximity reader (integrated RDC) may communicate an RFID signal (enable signal) to the antenna 332 (302) using the second signal line to generate RF signals that are then broadcasted via the antenna to the nearby token to “power and activate the token.” Ex-1005, [0146]-[0147]; Ex-1003 ¶240.

3. **[5] “The hybrid device of claim 1, wherein the one or more of the hybrid device and the device associated with the external RDC are enabled subsequent to the external PDK entering the proximity zone of the integrated RDC and based on the information stored by one or more of the external PDK and the integrated PDK.”**

Buer discloses that an application, function, or service is enabled on the hybrid device subsequent to the external token entering the proximity zone of the integrated proximity reader and based on the information stored by one or more of the external PDK and the integrated PDK as in claim 5. Ex-1003 ¶¶241-242; §V.A.2.f. In the '042 patent, a hybrid device may be enabled to access a Wi-Fi service when an external PDK enters the integrated RDC's proximity zone. Ex-1001, 19:15-45. In Buer, a cell phone may similarly be enabled to access a wireless network only after an external token “is proximate to the access device.” Ex-1005, [0111], [0155], [0163]-[0165], [0176], [0184]. Buer's process is also based on the credential information stored in the token. *Id.*, [0119].

4. **[6] “The hybrid device of claim 1, wherein the hybrid device is a cell phone and the hybrid device is enabled to provide cell phone service subsequent to the external PDK entering the proximity zone of the integrated RDC and based on the information stored by one or more of the external PDK and the integrated PDK.”**

Buer discloses that its access device may be “a cellular phone,” *id.*, [0163], and that cellphone service is enabled subsequent to the external token (external PDK) entering its proximity zone, as in claim 6, because “access to the wireless network

may be provided when a user moves the token...within relatively close proximity...to the reader” “to enable communication with a given wireless network,” such as cellular telephone networks. *Id.*, [0162], [0164]-[0165]; *see also* §V.A.1.d. Buer discloses that the cell phone service is enabled based on the authentication information stored in the external token. Ex-1005, [0163]-[0165]; Ex-1003 ¶¶245-247.

5. [8] “The hybrid device of claim 1, wherein the integrated PDK communicates with the external RDC subsequent to the external PDK entering the proximity zone of the integrated RDC.”

Buer discloses that the authentication component (integrated PDK) communicates with the external service provider subsequent to the external token entering the proximity zone of the integrated reader, as in claim 8, because authorization to access a service is dependent on the external token being proximate to the access device. Ex-1005, [0111], [0155], [0164]-[0165], [0176], [0184]; Ex-1003 ¶¶248-249; *see also* §V.B.1.

6. [9] “The hybrid device of claim 1, comprising storage for inheritance information.”

Proxense previously construed, and the court adopted, the term “inheritance information” as “[i]nformation passed from a first device to a second device for use by the second device.” Ex-1009, 4; Ex-1010, 38. Buer discloses that the integrated PDK stores inheritance information, as in claim 9, because Buer’s integrated PDK

stores network authentication information that is passed from the integrated PDK (“first device”) to the cryptographic processing component (“second device”) for use by the second device to obtain wireless network access. Ex-1005, [0148], [0151], [0155], Figs. 3, 6. Alternatively, Buer’s integrated PDK stores credit card information that is passed from the integrated PDK (“first device”) to the RF processing component (“second device”) for use by the point-of-sale components associated with the security processing system, consistent with the court’s construction. Ex-1005, [0195], Fig. 11; Ex-1003 ¶¶250-253.

7. **[11] “The method of claim 10, wherein the hybrid device is a cell phone and the enablement signal is sent to the cell phone enabling one or more of a service, a feature and a functionality of the cell phone.”**

As explained in §V.B.4, Buer discloses that the access device is a cell phone and the enablement signal is sent to the cell phone to enable a service, feature or functionality of the cell phone, such as enabling access to a cellular network. Ex-1003 ¶¶254-255.

8. **[12] “The method of claim 11, wherein the external PDK is adapted to receive and couple with a subscriber identity module (SIM) card.”**

Buer discloses that the external token may be adapted to receive and couple with a subscriber identity module (SIM) card as in claim 12 because examples of Buer’s tokens “may include, without limitation...mobile devices such as cellular telephones.” Ex-1005, [0130]. A POSITA would have understood that when Buer’s

token is implemented as a cellular phone, the cellular phone would have included a socket that is adapted to receive and couple with a subscriber identity module (SIM) card. Ex-1003 ¶¶256-258.

9. [13]

- a. [13pre] **“The method of claim 10, wherein the integrated PDK is electrically coupled to the integrated RDC, and the method comprises:”**

Buer discloses that the integrated PDK is electrically coupled to the integrated RDC as in claim 13. §V.A.2.d. Buer’s integrated reader transmits an electrical signal over connection 116 to the integrated authentication component. Ex-1005, [0116]; Ex-1003 ¶¶259-261.

- b. [13a] **“sending the enablement signal from the integrated RDC to the integrated PDK;”**

Buer discloses sending a credential from the integrated reader to its integrated PDK for storage in the local data memory. Ex-1005, [0135], [0185]; Ex-1003 ¶¶262-263; §V.A.2.f.

The ’042 patent’s enablement signal (or enable signal) is a signal used to enable functionality. Ex-1001, 17:3-11; Ex-1010, 40. Patent Owner has alleged that the “enablement signal” can be satisfied by an authentication response that includes a credential ID, Ex-1018 (infringement contentions), 12, and Buer discloses that too, Ex-1005, [0164]-[0165], [0173]-[0175]; Ex-1003 ¶265. Buer discloses that when a token is within “close proximity” to the proximity reader (integrated RDC), the token

“sends authentication information to the proximity reader,” Ex-1005, [0164], including “a credential such as a password.” *Id.*, [0172]. The proximity reader (integrated RDC) then sends the authentication information (e.g., credential) through Buer’s “cryptographic processing” (integrated PDK), which “cryptographically encrypt[s]/sign[s] the information.” *Id.*, [0173]-[0174]; Ex-1003 ¶266.

c. [13b] “creating a second wireless link between the integrated PDK and an external RDC; and”

Buer discloses creating a second RF signal between the integrated PDK via the transceiver or RFID client and the external RDC. Ex-1005, [0165], [0174], [0190], [0194]; Ex-1003 ¶¶267-268; §V.A.2.b, §V.A.2.f.

d. [13c] “sending the enablement signal from the integrated PDK to the external RDC using the second wireless link.”

Buer discloses sending the encrypted credential from the integrated PDK to the external RDC using the RF signals. Ex-1005, [0165], [0174], [0190], [0194]; Ex-1003 ¶¶269-270; §V.A.2.f.

10. [14] “The method of claim 11, wherein the integrated PDK modifies the enablement signal to produce a modified enablement signal, and the modified enablement signal is sent from the integrated PDK to the external RDC.”

Buer’s integrated PDK modifies the enablement signal to produce a modified enablement signal, as in claim 14, because the authentication component “cryptographically encrypt[s]/sign[s] the [credential] information” to produce an

encrypted or “signed information” before it is sent “to the network access provider.”

Ex-1005, [0174]; *see also id.*, Fig. 4, [0170]; Ex-1003 ¶¶271-272.

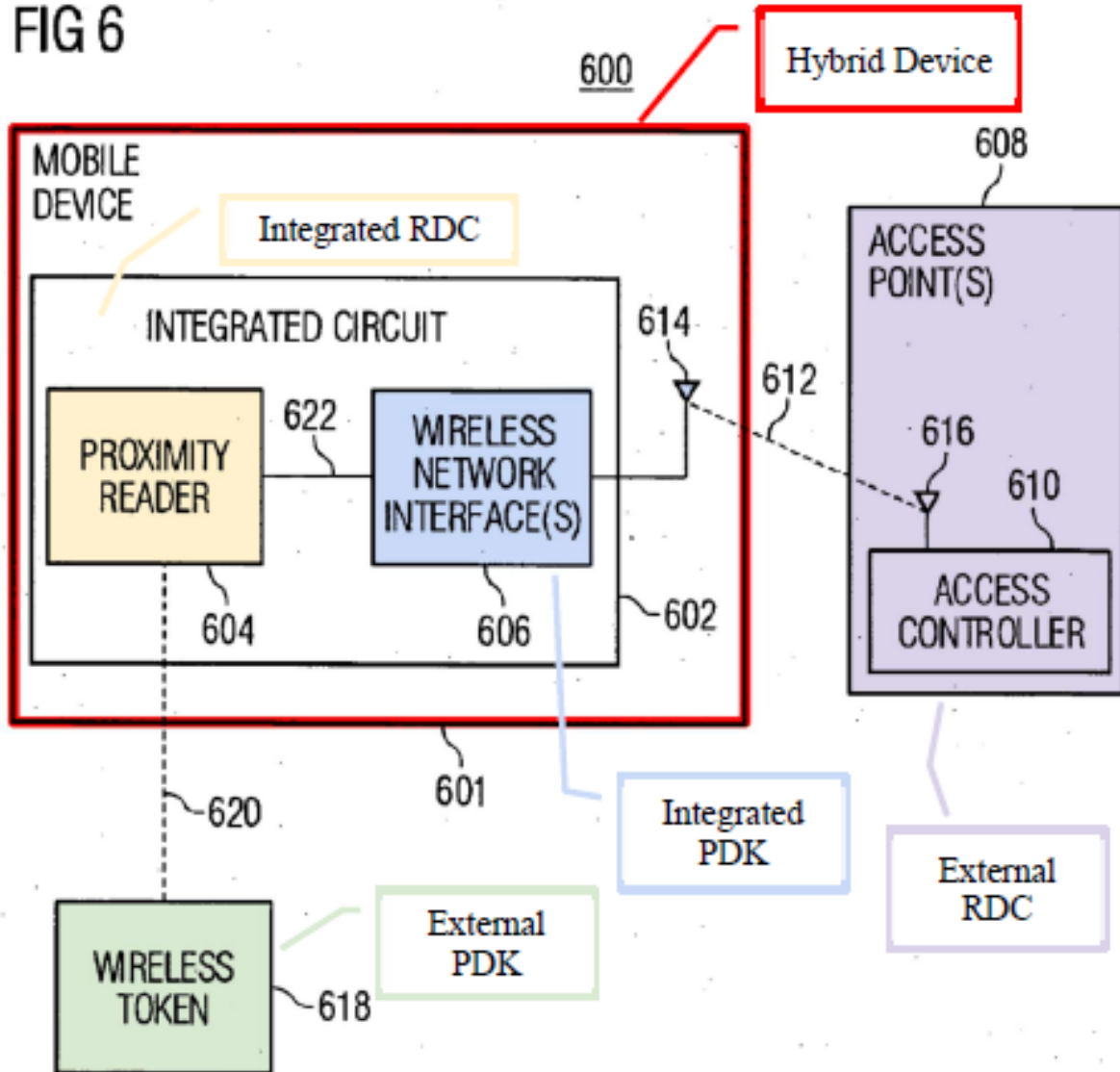
11. [15]

Buer discloses that the integrated PDK is electrically coupled to the integrated RDC. Ex-1003 ¶¶273-274; §V.A.2.d.

- a. [15a] “The method of claim 10, wherein the integrated PDK is electrically coupled to the integrated RDC, and the method comprises: creating a second wireless link between the hybrid device and an external RDC; and”**

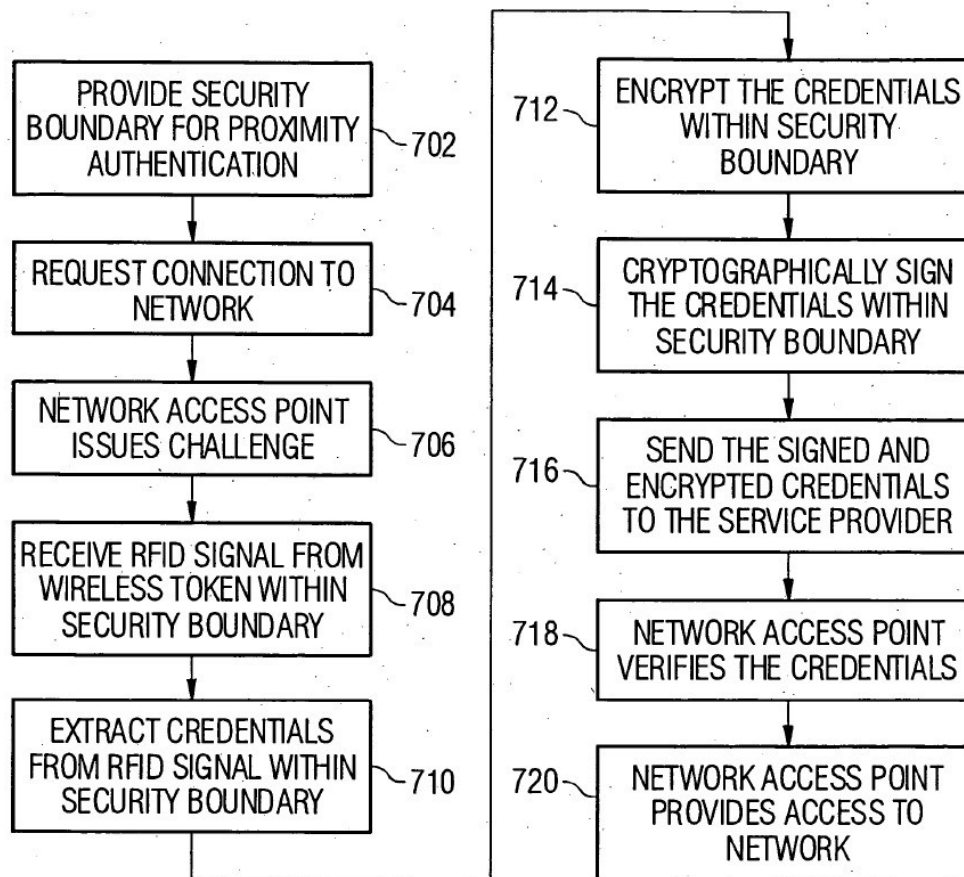
Buer discloses creating a first wireless link (wireless link 620 in Fig. 6) between the integrated RDC and an external PDK. Ex-1005, [0164]; §IV.B. Buer discloses creating a second wireless link (wireless link 612 in Fig. 6) between the access device and the external RDC. *Id.*, [0165], [0168]; Ex-1003 ¶¶275-277.

FIG 6



Ex-1005, Fig. 6 (annotated). The second wireless link is created after establishing a security boundary with the access point (*id.*, [0170], Fig. 7 (Step 702)) or when the access device requests a network connection with the access point (*id.*, [0171], Fig. 7 (Step 704)), as shown below. *See also id.*, [0132], [0141]-[0143], Fig. 4.

FIG 7



Id., Fig. 7.

- b. [15b] “receiving a second signal at the hybrid device via the second wireless link from the external RDC, wherein the enablement signal is generated responsive to receiving the first and second signals.”

Buer discloses receiving a first signal (proximity signaling or authentication information) at the integrated reader from the external token. §IV.B. Buer discloses receiving a second signal (a challenge requesting a credential) at the hybrid device from the external network access point. *Id.*, [0172], Fig. 7 (step 706); *see also id.*,

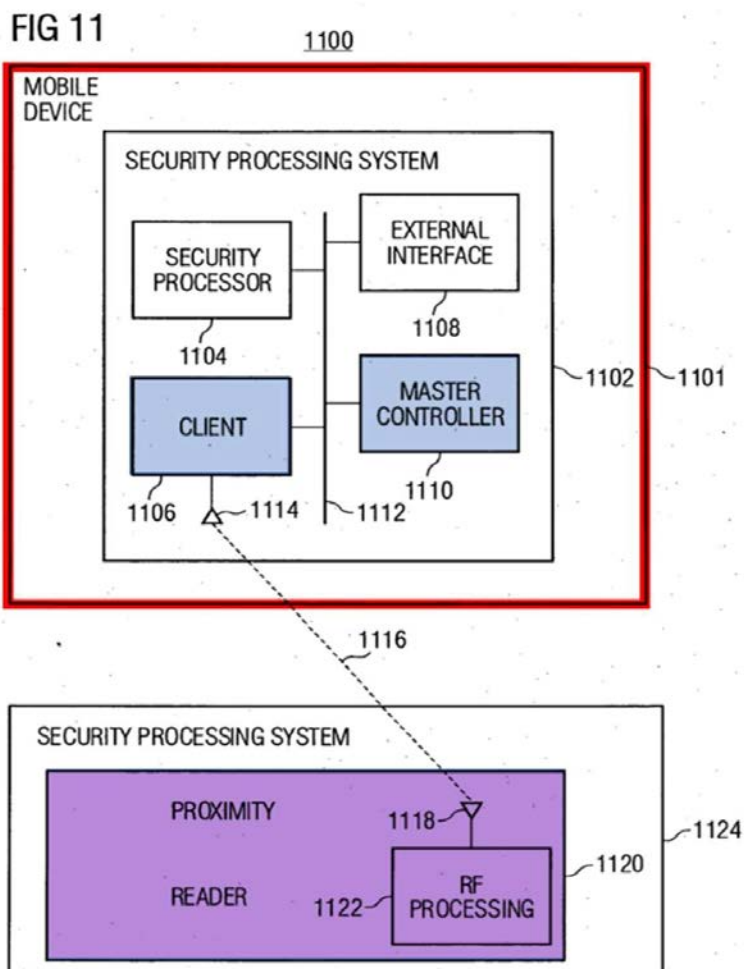
[0145], [0156], Fig. 4 (step 406). Ex-1003 ¶¶279-282. Buer's authentication component generates the cryptographically signed credential (enablement signal) (e.g., Ex-1005, Fig. 7 (step 716), Fig. 4 (step 416)) that is sent to the network access provider after receiving the first signal (credential extracted from the authentication information from the wireless token at Fig. 7 (steps 708, 710) or Fig. 4 (steps 408, 410)) and second signal (challenge from the access device at Fig. 7 (step 706) or Fig. 4 (step 406)). *Id.*, [0172]-[0174]; Ex-1003 ¶282.

12. [17] “The method of claim 10, wherein the first signal includes service inheritance information.”

Buer discloses that “the first signal includes service inheritance information.” §V.B.6. Buer's network authentication information such as “credentials, passwords and/or certificates may be stored in a data memory (e.g., a non-volatile memory) on the token.” Ex-1004, [0148]. The network authentication information is sent from the token via RF signal (the first signal) to be encrypted and stored in the access device before being routed to the service provider. Ex-1004, [0141]-[0142]. This is similar to the '042 patent's example of “the service inheritance information” includes “Wi-Fi access information.” Ex-1001, '042 patent, 18:22-25; Ex-1003 ¶¶284-285.

Alternatively, Buer discloses sending financial information from the integrated PDK to the external RF processing component for use by the RF processing component, as shown below, for performing a service (sales transaction). Ex-1005,

[0194]-[0195]. Ex-1003 ¶286. This is similar to the '042 Patent's example of "the service inheritance information...includes a first credit card account." Ex-1001, 18:22-25. Ex-1003 ¶287.



Ex-1005, Fig. 11 (annotated). It would have been obvious that the credit card information stored within the integrated PDK is received from the first signal via the first wireless link from the external token (external PDK). Ex-1003 ¶288. Buer's external token may 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-1005, [0129]-[0130], [0193], Fig. 8. Accordingly, the transferring of the “credit card information” from the external token to the access device is the claimed first signal. Ex-1003 ¶289.

A POSITA would have been motivated to use the external token to transfer credit card information (a first signal) to a mobile device, as Buer teaches, so that the mobile device would “inherit” the information from the external token for at least three reasons:

1. Using Buer’s “key management functions” to “back[]up” the external token’s credit card information for secure storage on the user’s cellular phone would allow the user to maintain an encrypted backup for point-of-sale transactions. Ex-1005, [0177], [0195]; Ex-1003 ¶¶290-291.
2. Using the token to transfer the credit card information in a secure and encrypted manner, instead of having the user directly entering the sensitive information into the device would address Buer’s concern that sensitive information may be compromised when directly inputted by a user. Ex-1005, [0007]-[0008]; Ex-1003 ¶292.
3. Using an external token would improve security during financial transactions, so that “only when a wireless token assigned to the user is in the proximity of” the cellular phone would the sales transaction be performed. Ex-1005, [0011], [0114]; Ex-1003 ¶293.

Using the external token to transfer credit card information (a first signal) to a mobile device for storage would have been no more than combining prior art elements using known methods to yield predictable results. Ex-1003 ¶294. *See, e.g., Friskit*, 306 F. App'x at 616. A POSITA would have had a reasonable expectation of success in doing so because Buer itself explains how to do so. Ex-1003 ¶294.

VI. Ground 4: Claim 2 Would Have Been Obvious Over Buer and Lee.

A. [2] “The hybrid device of claim 1 further comprising one or more of another integrated PDK and another integrated RDC.”

Buer and Lee render obvious that the hybrid device includes another integrated PDK. *Id.* ¶¶295-301. Lee teaches using multiple access control chips (electronic keys) on a common bus for separately storing identification parameters. Ex-1008, 31:30-32:2, 78:16-24, 80:20-26. Each access control chip can be wiped during programming to enhance “data security.” *Id.*, 78:16-24, 79:21-25. A POSITA would have been motivated to duplicate Buer’s PDK to include another integrated PDK, as Lee teaches, because doing so would enhance Buer’s key management functions to separately provide secured storage of electronic keys. Ex-1005, [0154], [0177]; Ex-1003 ¶297. A POSITA would have been motivated to improve data security by implementing multiple PDKs, Ex-1003 ¶298; Ex-1005, [0115], and to securely store information from the multiple external tokens in separate integrated PDKs, as Lee teaches, to enable separate storage of data and to enhance the ability to securely wipe each integrated PDK for data security. Ex-1003 ¶299. Buer and Lee are in the same

field of endeavor—the field of incorporating RDC/PDK technology into devices to allow secure data sharing and services. Ex-1005, Abstract; Ex-1008, 31:30-32:2, 78:16-24. A POSITA would have recognized that Buer and Lee use similar techniques to solve the same problem, and would have been capable of implementing another PDK in Buer’s cell phone with minimal modification without undue experimentation. *Id.*, ¶¶300-301. Such a modification 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 Lee explains how to do so using a common bus. Ex-1003 ¶301.

VII. Ground 5: Claim 12 Would Have Been Obvious Over Buer and Nishikawa

A. [12] “The method of claim 11, wherein the external PDK is adapted to receive and couple with a subscriber identity module (SIM) card.”

Buer and Nishikawa render obvious that the external PDK is adapted to receive and couple with a subscriber identity module (SIM) card. *Id.*, ¶¶302-303. Nishikawa discloses “ways to improve the convenience of” a small “e-token” by using a SIM card. Ex-1014, [0017] (“the key holder type ID module”), [0006], [0001], [0021]-[0026], [0065]. The SIM is 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.” *Id.*, [0111]. The key holder type ID module

(e.g., SIM reader/writer) “is provided with the fingerprint sensor, [so] the user can be authenticated on the basis of biometric data.” *Id.*, [0017], [0114]. A POSITA would have been motivated to adapt Buer’s wireless token to receive a conventional SIM card, as Nishikawa teaches, to improve the convenience of Buer’s token and to add additional capability (storing electronic money and electronic ticket). *Id.*, [0111]; Ex-1013, 3:34-4:4, 11:15-27; Ex-1003 ¶¶306. A POSITA would have also been motivated to improve Buer’s authentication process by using 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 ¶308. A POSITA would have been capable of adapting Buer’s wireless token to receive a SIM card, because Buer and Nishikawa use similar hardware, and the combination would require minimal modification without undue experimentation and would have been no more than combining prior art elements using known methods to yield predictable results. *Id.*, ¶308; *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 ¶308.

VIII. Ground 6: Claims 3 and 18-20 Would Have Been Obvious Over Buer and Hoffmann

- A. [3] “The hybrid device claim 1, wherein the integrated PDK is capable of communicating with the at least one external RDC at the same time the integrated RDC communicates with the at least one external PDK.”**

Buer and Hoffmann render obvious claim 3. Ex-1003 ¶309.

As discussed in §§V.A.2.b-V.A.2.c, Buer’s hybrid device’s integrated PDK is capable of communicating wirelessly with at least one external RDC, as in [1a], and that the hybrid device’s integrated RDC communicates wirelessly with at least one external PDK, as in [1b]. Ex-1003 ¶310. It would have been obvious that the communications occur at the same time because Hoffmann teaches using multiple antennas to transmit/receive data packets simultaneously, as shown below. Ex-1003 ¶311.

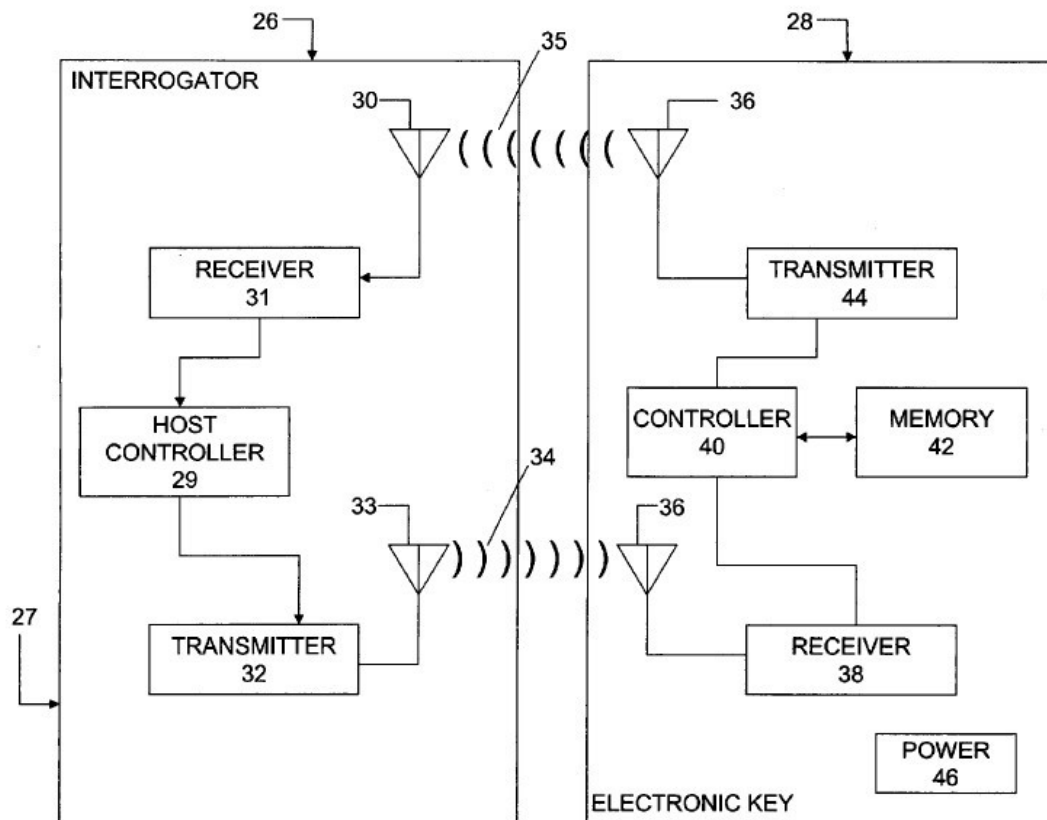


FIGURE 2

Ex-1019, Fig. 2, [0043]. Hoffmann uses different frequencies to reduce interference during simultaneous communication. *Id.*, [0081].

A POSITA would have been motivated to use multiple antennas for the transmitter and receiver to provide parallel data streams, as Hoffmann teaches, so that Buer's authentication system (integrated PDK) would communicate with the external service provider (external RDC) to obtain a service, while Buer's proximity reader (integrated RDC) is communicating with the external proximity token (external PDK) *at the same time* to ensure that the request was not being made while

the “token may not be in the proximity of the computing device.” Ex-1005, [0011]; Ex-1003 ¶312.

A POSITA would have recognized that Buer and Hoffmann are in the same field of endeavor and use similar techniques to solve the same problem. Ex-1005, [0111]; Ex-1019, [0025]-[0026], [0041]; Ex-1003 ¶313. A POSITA would have been capable of implement multiple antennas for transmitting and receiving in Buer’s access device, because Buer and Hoffmann use similar hardware, and the combination would require minimal modification without undue experimentation. *Id.* 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 Hoffmann explains how to do so. Ex-1003 ¶313.

B. [18] “The method of claim 10, wherein the first signal includes feature inheritance information.”

Buer and Hoffmann render obvious claim 18. Ex-1003 ¶314.

Buer discloses that “the first signal includes service inheritance information,” as recited in claim 17. Ex-1003 ¶315; §V.B.12. It would have been obvious to store additional information in the token, including password for unlocking all or a subset of features because Hoffmann discloses that a password stored in a remote key may be used to unlock an electronic device either “wholly or partially.” Ex-1019,

Abstract, [0002], [0028]. Hoffmann's sending of a password to unlock a subset of features is similar to the '042 Patent's example of "the feature inheritance information," which provides authorization for "a limited set of features offered by a given service." Ex-1001, 17:56-57, 19:66-67 Ex-1003 ¶316. Hoffmann's electronic key, which is remote from the device, transmits a password that enables "at least a portion of the functionality of the device." Ex-1019, Abstract, [0010].

A POSITA would have been motivated to send a password that would be used to "enable...all or only some of the functions," as Hoffmann teaches, to enable Buer's access device to selectively secure services, "either wholly or partially." Ex-1019, [0028], [0031]; Ex-1003 ¶317. A POSITA would also have also been motivated to improve Buer's access device in accordance with Buer's express teaching on storing "multiple sets of information (e.g., credentials)" on a single token to enable access to "different services." Ex-1005, [0127]; Ex-1003 ¶317. Additionally, a POSITA would have been motivated to use a token to transmit the password, as Hoffmann teaches, to "remotely program the Key in the cell phone" because doing so would "enable access or functions remotely in a secure, on demand fashion." Ex-1019, [0041]; Ex-1003 ¶318. A person who "does not routinely need access or is otherwise restricted from routine use" would then be "provide[d] access without revealing the password." Ex-1019, [0041].

A POSITA would have recognized that Buer and Hoffmann are in the same field of endeavor and use similar techniques to solve the same problem and would have been capable of adapting Buer's authentication information to include a password, because Buer and Hoffmann use similar hardware, and the combination would require minimal modification without undue experimentation. Ex-1005, [0111]; Ex-1019, [0025]-[0026], [0041]; Ex-1003 ¶319.

C. [19] “The method of claim 10, wherein the first signal includes personality inheritance information.”

Buer and Hoffmann render obvious claim 19. Ex-1003 ¶320. It would have been obvious to store additional information in the token, including preferences for providing customized access to services and/or functions because Hoffmann discloses that preferences may be stored in an RF-Key that would be used to enable specific services and/or functions. Ex-1019, [0036]-[0037]; Ex-1003 ¶321. These preferences stored in the RF-Key enables the device to act as “remote control for setting personal preferences on any of a wide variety of preference enabled devices.” Ex-1019, [0040]. Hoffmann's sharing of user preferences is similar to the '042 Patent's example of “the personality inheritance information,” where “the preferences of a user or holder of a first device are shared with a user or holder of a second device.” Ex-1001, 20:27-31; Ex-1003 ¶321. Hoffmann discloses “communicating preset personal preferences from a memory device associated with

a user, to external electronic devices in the user's surrounding environment. Ex-1019, Abstract, [0021].

A POSITA would have been motivated to send preferences that would be used to control the external devices, as Hoffmann teaches. Ex-1019, [0028], [0031]; Ex-1003 ¶322. A POSITA would have also been motivated to improve Buer's access device in accordance with Buer's express teaching on storing "multiple sets of information (e.g., credentials)" on a single token to enable access to "different services." Ex-1005, Buer, [0127]; Ex-1003 ¶322. A POSITA would also have been motivated to use a token to transmit the preferences, as Hoffmann teaches, to "remotely program the Key in the cell phone" because doing so would "enable access or functions remotely in a secure, on demand fashion." Ex-1019, [0041]; Ex-1003 ¶323. Thus, a person who "does not routinely need access or is otherwise restricted from routine use" would then be "provide[d] access without revealing the [use preferences]." Ex-1019, [0041].

A POSITA would have recognized that Buer and Hoffmann are in the same field of endeavor and use similar techniques to solve the same problem and would have been capable of adapting Buer's authentication information to include a password, because Buer and Hoffmann use similar hardware, and the combination would require minimal modification without undue experimentation. Ex-1005, [0111]; Ex-1019, [0025]-[0026], [0041]; Ex-1003 ¶324.

- D. [20] “The method of claim 10 comprising: receiving a signal from the external PDK that a second external PDK includes inheritance information; creating a second wireless link between the integrated RDC and the second external PDK; and receiving the inheritance information from the second external PDK.”**

Buer and Hoffmann render obvious claim 20. Ex-1003 ¶325. Buer discloses assigning different tokens to a user for different purposes, where “a user may be assigned one token to access certain services through certain access devices” and “another token to access other services through the same or other devices.” Ex-1005, [0127]. The “multiple sets of information (e.g., credentials) may be included on a single token to enable a user to access different services or to enable multiple users to share a token.” *Id.* A POSITA would have understood that an access device would have been capable of using one of the tokens (external PDK) to authenticate the user to access a security processing system for key management, *id.*, [0176], [0114], [0089]; Fig. 11, and a second token (second external PDK) to store multiple sets of information such that the key manager would authorize key usage based on the keys stored within the second token, *id.*, [0127], [0177]; Ex-1003 ¶326.

Hoffmann teaches a personalized security system that “can be used to enable access or functions remotely in a secure, on demand fashion.” Ex-1019, [0041]. A person that “does not routinely need access or is otherwise restricted from routine use” can obtain temporary access by a controller that “remotely program[s] the Key

in the cell phone with the access code” to provide access and tracking “without revealing the password.” *Id.*, [0041].

It would have been obvious to authenticate a user using a first token (external PDK) to provide information for securing additional key(s) (inheritance information) from the second token (second external PDK). Ex-1003 ¶328. The access device’s security processing system would then establish a secure connection (a second wireless link) using its proximity reader (integrated RDC) with the second token (second external PDK) to receive the key(s) (inheritance information) from the second token (second external PDK). A POSITA would have been motivated to implement such a two-tier process, as Buer teaches, so that a first token (external PDK) would have been used to ensure the request to obtain keys is provided only to authenticated users, Ex-1005, [0114], and not “a hacker” who does not have a token “in the proximity” of the access device, *id.*, [0011]. Ex-1003 ¶328.

A POSITA would have been motivated to implement Hoffmann’s “secure, on demand” remote programming in Buer’s security processing system to enhance Buer’s key management system. Ex-1019, [0041]; Ex-1005, [0176]; Ex-1003 ¶329. A POSITA would have been motivated to store multiple sets of information on a single token (second external PDK) to act as a central repository of keys to enable users, who do not normally have access, to obtain temporary access, as Hoffmann teaches, because doing so would have “enable[d] multiple users to share a token,” on

a secure, on demand basis. Ex-1005, [0127]; Ex-1019, [0041]; Ex-1003 ¶329. A POSITA would have recognized that Buer and Hoffmann are in the same field of endeavor and use similar techniques to solve the same problem, and would have been capable of adapting Buer's authentication information to include a password, because they use similar hardware, and the combination would require minimal modification without undue experimentation. Ex-1005, [0111]; Ex-1019, [0025]-[0026], [0041] Ex-1003 ¶330.

IX. Discretionary Denial Is Not Warranted

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

Advanced Bionics strongly favors institution. IPR2019-01469, Paper 6 (PTAB Feb. 13, 2020) (precedential).

None of the references presented herein were evaluated by the examiner or applied in any rejection. *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 otherwise, Petitioner submits that the Grounds presented herein demonstrate that the examiner erred in determining the claims are allowable over the prior art. Thus, Petitioner submits that the evidence and facts presented in the Petition warrant consideration 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 neutral. Petitioner is a defendant in a parallel proceeding. Neither party has requested a stay.

Factor 2 weighs heavily against discretionary denial. While trial is scheduled for December 8, 2025 (Ex-1028, 5), the median time to trial in WDTX is 32.7 months, projecting an actual trial around December 2026. Ex-1027, 4; Ex-1026, 37. A FWD in the IPR that Apple seeks to join, IPR2024-00782 (the “Google IPR”) should issue in November 2025. Factor 2 heavily favors institution.

Factor 3 favors institution. Petitioner acted diligently to file this IPR before its bar date. The parties have not significantly invested in the parallel proceeding. Indeed, litigation is in its early stages, with fact discovery not yet open. EX-1028, p. 3. If an IPR is instituted, subsequent investments in the District Court litigation can further be minimized.

Factor 4 favors institution. 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 here. Further, Petitioner stipulates

that if the PTAB institutes IPR2024-01399 and joins it with the Google IPR,⁹ Petitioner will not pursue the grounds raised in this Petition in the parallel district court litigation with respect to the claims for which trial is instituted. *See Sand Revolution II, LLC v. Continental Intermodal Group–Trucking LLC*, IPR2019-01393, Paper 24 at 7 (PTAB Jun. 16, 2020).

Thus, 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 where petitioner was defendant, no stay was requested, trial was projected to occur *before* the FWD, a “significant portion of work remain[ed] to be done in the district court,” e.g., “the completion of fact and expert discovery and dispositive motions,” and the overlap between claims was “complete”).

To the extent the Board considers Factor 6, 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

⁹ See Petitioner’s concurrently filed Supplemental Paper and Notice of Ranking Petitions (Paper 4).

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*

Application of the *General Plastic* analysis is inapplicable here. The present petition is not a “follow-on petition” under *General Plastic*. Moreover, the *General Plastic* factors do not favor denial. The parties challenging the ’042 Patent (Microsoft, Google, and Apple) have no significant relationship and are direct market competitors. While there is some overlap between the petitions filed by Google and Microsoft, this Petition is substantively identical to the Google IPR Petition and addresses different prior art references and different examples of arguments than the Microsoft IPR Petition. There are no concerns of road-mapping based on patent owner’s preliminary response because Google could not have taken advantage of such later-filed preliminary response in preparing its petition that Apple now seeks to join. The filing of multiple petitions against the ’042 Patent is merely the result of Proxense filing serial district court actions. Lastly, there is no risk that the Petition or Apple’s Motion for Joinder 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).

X. Mandatory Notices

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

Apple Inc. is the real party-in-interest for this Petition.

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

The '042 patent is assigned to Proxense, LLC, who is currently asserting the '042 patent against Apple Inc. in the Western District of Texas in *Proxense, LLC v. Apple Inc.*, No. 6:24-cv-00143 (W.D. Tex.). To the best of Petitioner's knowledge, the '042 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
<i>Proxense, LLC v. Google LLC</i>	6:23-cv-00320	WDTX	May 2, 2023
<i>Proxense, LLD v. Apple Inc.</i>	6:24-cv-00143	WDTX	March 18, 2024
<i>Microsoft Corp. v. Proxense, LLC</i>	IPR2024-00573	PTAB	February 15, 2024
<i>Google v. Proxense, LLC</i>	IPR2024-00782	PTAB	April 19, 2024
<i>Google v. Proxense, LLC</i>	IPR2024-01318 ¹⁰	PTAB	August 22, 2024
<i>Apple Inc. V. Proxense, LLC</i>	IPR2024-01398 ¹¹	PTAB	Concurrently

Petitioner is not aware of any disclaimers, reexamination certificates, addressing the '042 Patent. Samsung previously filed IPRs (IPR2021-01438 and 01439) against family members of the '042 Patent (U.S. Patent Nos. 9,049,188 and 9,235,700). Patent and Applications related to the '042 Patent are found in EX-1029.

¹⁰ In IPR2024-01318, Google seeks joinder with Microsoft's challenge in IPR2024-00573.

¹¹ In IPR2024-01398, Petitioner seeks joinder with Microsoft's challenge in IPR2024-00573.

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

Lead Counsel	Back-Up Counsel
PHILIP W. WOO USPTO Reg. No. 39,880 DUANE MORRIS LLP, 260 Homer Avenue #202 Palo Alto, CA 94301 P: (650) 847-4145 F: (650) 644-0150 PWWoo@duanemorris.com	MONTÉ T. SQUIRE USPTO Reg. No. 80,123 DUANE MORRIS LLP 1201 North Market Street, Suite 501, Wilmington, DE 19801 P: (302) 657-4918 F: (302) 397-2543 MTSquire@duanemorris.com
	D. STUART BARTOW USPTO Reg. No. 56,505 DUANE MORRIS LLP 1201 North Market Street, Suite 501, Wilmington, DE 19801 P: (650) 847-4158 F: (650) 618-8505 DSBartow@duanemorris.com
	PAUL BELNAP USPTO Reg. No. 73,106 DUANE MORRIS LLP 901 New York Ave. NW, Suite 700 East, Washington, D.C. 20001 P: (202) 776-7879 F: (202) 776-7801 PHBelnap@duanemorris.com

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

Please address all correspondence to lead and back-up counsel at the addresses above. Petitioner consents to electronic service by e-mail at the addresses above.

XI. Standing

Petitioner certifies that the '042 patent is available for IPR; Petitioner is not barred or estopped from requesting IPR on the grounds identified herein.

XII. Conclusion

Petitioner has established that the challenged claims are unpatentable and requests the Board institute and cancel each challenged claim as unpatentable.

Date: September 12, 2024

Respectfully submitted,

DUANE MORRIS LLP

BY: /Philip W. Woo/
Philip W. Woo
USPTO Reg. No. 39,880
Duane Morris LLP
260 Homer Avenue #202
Palo Alto, CA 94301

ATTORNEY FOR PETITIONER

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that the foregoing **PETITION FOR *INTER PARTES* REVIEW** contains 13,984 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.

Date: September 12, 2024

BY: /Philip W. Woo/

Philip W. Woo
USPTO Reg. No. 39,880
Duane Morris LLP
260 Homer Avenue #202
Palo Alto, CA 94301

ATTORNEY FOR PETITIONER

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on September 12, 2024, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided by Federal Express, to the Patent Owner, by serving the correspondence address of record as follows:

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

Additionally, a courtesy copy of the IPR and all supporting exhibits were emailed to counsel of record for the Patent Owner in the litigation before the United States District Court for the Western District of Texas:

Brian D. Melton
Susman Godfrey, LLP
1000 Louisiana St.
Suite 5100
Houston, TX 77002
Email: bmelton@susmangodfrey.com

Date: September 12, 2024

BY: /Philip W. Woo/

Philip W. Woo
USPTO Reg. No. 39,880
Duane Morris LLP
260 Homer Avenue #202
Palo Alto, CA 94301

ATTORNEY FOR PETITIONER