

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,

Petitioner,

v.

PROXENSE, LLC,

Patent Owner.

Case No. IPR2024-01319
U.S. Patent No. 9,679,289
Filing Date: December 7, 2015
Issue Date: June 13, 2017

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

I.	Requirements For IPR	1
A.	Standing	1
B.	Challenge and Relief Requested	1
C.	Claim Construction	3
1.	Hybrid Device	3
2.	Personal Digital Key (“PDK”)	4
3.	Receiver-decoder circuit (“RDC”)	5
D.	Level of Ordinary Skill in the Art	5
II.	The ’289 Patent	6
A.	Brief Description	6
B.	Prosecution History	7
III.	The Challenged Claims Are Unpatentable	7
A.	[GROUND 1A/1B]—Claims 1-20 are rendered obvious by Giobbi-157 and Giobbi-139 [1A] and Giobbi-157, Giobbi-139, and Dua [1B]	7
1.	Overview of Giobbi-157	7
2.	Overview of Giobbi-139	11
3.	The combination of Giobbi-157 and Giobbi-139	13
4.	Overview of Dua	22
5.	Combination of Giobbi-157, Giobbi-139, and Dua	24
6.	Analysis	26

B.	[GROUND 2A] – Claims 1-8, 10-11, and 14-19 are rendered obvious by Broadcom	61
1.	Overview of Broadcom	61
2.	Analysis	64
C.	[GROUND 2B] – Claims 1-20 are rendered obvious by Broadcom and Giobbi-157	84
1.	The combination of Broadcom and Giobbi-157	84
2.	Analysis	86
IV.	Discretionary Denial Is Not Warranted	89
A.	Discretionary Denial Is Not Warranted under §325(d).	89
B.	Discretionary Denial Is Not Warranted Under <i>Fintiv</i>	90
C.	35 U.S.C. §314(a) – <i>General Plastic</i>	91
V.	Mandatory Notices	92
A.	Real Parties-in-Interest Under 37 C.F.R. §42.8(b)(1)	92
B.	Related Matters Under 37 C.F.R. §42.8(b)(2)	92
C.	Counsel and Service Information Under 37 C.F.R. §42.8(b)(3)	92
D.	Service Information Under 37 C.F.R. §42.8(b)(4)	93
VI.	Conclusion	94

TABLE OF EXHIBITS

Exhibit	Description
MS-1001	U.S. Patent No. 9,679,289 to David L. Brown (“the ’289 Patent”)
MS-1002	Excerpts from the Prosecution History of the ’289 Patent (“the Prosecution History”)
MS-1003	Declaration and Curriculum Vitae of Dr. Patrick Traynor
MS-1004	Complaint, <i>Proxense, LLC v Microsoft Corporation</i> , 6:23-cv-00319, W.D. Tex., filed May 2, 2023
MS-1005	U.S. Patent Publication No. 2007/0245157 A1 (“Giobbi-157”)
MS-1006	U.S. Patent Publication No. 2004/0255139 A1 (“Giobbi-139”)
MS-1007	U.S. Patent No. 9,042,819 (“Dua”)
MS-1008	European Patent No. EP 1 536 306 A1 (“Broadcom”)
MS-1009	Claim Construction Order, <i>Proxense, LLC v. Samsung Elecs. Co., Ltd.</i> , No. 6:21-cv-00210-ADA (W.D. Tex. Jan. 18, 2022)
MS-1010	Provisional Application No. 60/798,843
MS-1011	U.S. Patent No. 9,049,188 to David L. Brown (“the ’188 Patent”)
MS-1012	Memorandum, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (USPTO June 21, 2022) (“Director’s Guidance”)
MS-1013	Microsoft’s Opening Claim Construction Brief, <i>Proxense, LLC v Microsoft Corporation</i> , 6:23-cv-00319, W.D. Tex., filed November 6, 2023
MS-1014	Microsoft’s Opening Brief in support of its Motion to Dismiss for Failure to State a Claim, <i>Proxense, LLC v Microsoft Corporation</i> , 6:23-cv-00319, W.D. Tex., filed July 10, 2023
MS-1015	Microsoft’s Reply in support of its Motion to Dismiss for Failure

	to State a Claim, <i>Proxense, LLC v Microsoft Corporation</i> , 6:23-cv-00319, W.D. Tex., filed August 10, 2023
MS-1016	W.D. Tex. Order Cancelling Markman Hearing, <i>Proxense, LLC v Microsoft Corporation</i> , 6:23-cv-00319, W.D. Tex., issued 1/9/2024
Ex. 1017	Google's Proposed Constructions, <i>Proxense, LLC v. Google LLC</i> , No. 6:23-cv-00320 (W.D. Tex)
Ex. 1018	Complaint, <i>Proxense, LLC v Google LLC</i> , 6:23-cv-00320 (W.D. Tex. filed May 2, 2023)
Ex. 1019	Proxense's Proposed Constructions, <i>Proxense, LLC v. Google LLC</i> , No. 6:23-cv-00320 (W.D. Tex)
Ex. 1020	Claim Construction Order, <i>Proxense, LLC v. Google LLC</i> , No. 6:23-cv-00320 (W.D. Tex. January 23, 2024)
Ex. 1021	Scheduling Order, <i>Proxense, LLC v. Google LLC</i> , No. 6:23-cv-00320 (W.D. Tex. January 23, 2024)
Ex. 1022	RESERVED
Ex. 1023	Supplemental Declaration of Dr. Patrick Traynor

LISTING OF CHALLENGED CLAIMS

Claim 1	
[1.pre]	A hybrid device comprising:
[1.1]	an integrated, secure memory storing local, secured information; and
[1.2]	an integrated reader-decoder circuit (RDC) for communicating wirelessly with at least one external device within a proximity zone, the integrated RDC communicatively coupled to the integrated, secure memory for communication with the integrated, secure memory,
[1.3]	wherein one or more of (a) the integrated RDC communicating wirelessly with the at least one external device within the proximity zone and (b) the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and service.
Claim 2	
[2]	The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service is enabled, at least in part, on the hybrid device.
Claim 3	
[3]	The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service is enabled, at least in part, external to the hybrid device using an external RDC, the hybrid device communicatively coupled to wirelessly communicate with the external RDC.
Claim 4	
[4]	The hybrid device of claim 1, wherein the local, secured information includes biometric information for authenticating a user.
Claim 5	
[5]	The hybrid device of claim 1, wherein the local, secured information includes biometric information based on a biometric scan of a finger, the biometric information for authenticating a user.

Claim 6	
[6]	The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information.
Claim 7	
[7]	The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on a signal received from the at least one external device by the integrated RDC.
Claim 8	
[8]	The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on an authorization of the financial information using an external authentication database, the financial information transmitted to the external authentication database.
Claim 9	
[9]	The hybrid device of claim 8, wherein the external authentication database is separate from a merchant providing a sale in the financial transaction.
Claim 10	
[10]	The hybrid device of claim 1, wherein the one or more of the application, the function and the service enabled based on the local, secured information stored by the integrated, secure memory includes a first application, function or service based on a first subsets of local, secured information stored by the integrated, secure memory and a second application, function or service based on a second subset of local, secured information, the first and second subset of local, secured information having different accessibility.
Claim 11	
[11]	The hybrid device of claim 1, wherein the hybrid device is a cell phone.

Claim 12	
[12]	The hybrid device of claim 1, wherein the at least one external device is included in jewelry.
Claim 13	
[13]	The hybrid device of claim 1, wherein the at least one external device is a watch.
Claim 14	
[14.pre]	A method comprising:
[14.1]	creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external device, the hybrid device including an integrated, secure memory and the integrated RDC, wherein the integrated, secure memory stores local, secured information;
[14.2]	receiving a first signal, at the integrated RDC, via the first wireless link, from the external device; and
[14.3]	generating an enablement signal enabling one or more of an application, a function and a service.
Claim 15	
[15]	The method of claim 14, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on the hybrid device.
Claim 16	
[16]	The method of claim 14 further comprising: sending the enablement signal, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on a device external to the hybrid device and communicatively coupled to an external RDC.
Claim 17	
[17]	The method of claim 14, wherein the local, secured information includes biometric information for authenticating a user.
Claim 18	
[18]	The method of claim 14, wherein the local, secured information includes financial information and wherein the one or more of the application, the function and the service completes a financial transaction.

Claim 19	
[19]	The method of claim 14, wherein the hybrid device is a cell phone.
Claim 20	
[20]	The method of claim 14, wherein the external PDK is included in a watch.

Google LLC (Petitioner) requests *inter partes* review of claims 1-20 (“Challenged Claims”) of U.S. Patent No. 9,679,289 (“’289 patent”). This petition is substantively the same as instituted IPR2024-00407 and is being filed concurrently with a motion for joinder with respect to that proceeding. Petitioner respectfully requests institution of an IPR if the Board declines to institute Petitioner’s original petition (IPR2024-00783).

I. Requirements For IPR

A. Standing

Petitioner certifies that the ’289 patent is available for IPR, and Petitioner is not barred or estopped from requesting IPR on the grounds identified in this Petition.

B. Challenge and Relief Requested

Petitioner requests an IPR of the Challenged Claims on the grounds noted below. These grounds are identical to those advanced in IPR2024-00407, which are substantially similar to those advanced by Samsung in instituted and terminated IPRs (IPR2021-01438 and 01439) directed to related US Patent Nos. 9,049,188 and 9,235,700. Dr. Patrick Traynor provides a supplemental declaration (Ex. 1023) that he maintains and agrees with the facts, analysis, and conclusions set forth in his original declaration (MS-1003). Ex. 1023, ¶8. For consistency with Microsoft’s petition, citations herein to Dr. Traynor’s opinion will be citations to MS-1003 containing those opinions as originally expressed by Dr. Traynor.

Ground	Claim(s) Challenged	35 U.S.C. §	Reference(s)
1A	1-20	103	Giobbi-157, Giobbi-139
1B	1-20	103	Giobbi-157, Giobbi-139, and Dua
2A	1-8, 10-11, and 14-19	103	Broadcom
2B	1-20	103	Broadcom, Giobbi-157

The '289 Patent claims priority to a number of provisional applications, the earliest of which was filed 12/6/2007. MS-1001, Cover. While Petitioner does not concede that 12/6/2007 is the priority date that should be afforded to the '289 Patent, for the purposes of this proceeding, each of the references asserted in this Petition qualifies as prior art under 35 USC §102(a), §102(b), and/or §102(e) (as shown in the table below) even if the 12/6/2007 date of the provisional application is used as the priority date of the '289 Patent. MS-1003, ¶[29].

Reference	Filing Date	Publication Date
Giobbi-157	May 5, 2007	Oct. 18, 2007
Giobbi-139	May 17, 2004	Dec. 16, 2004
Dua	Sep. 30, 2014 ¹	May 26, 2015

¹ Dua is a continuation of an application claiming priority to May 12, 2005.

Broadcom	Sep. 30, 2004	Jun. 1, 2005
----------	---------------	--------------

C. Claim Construction²

Petitioner submits that all claim terms should be construed according to the *Phillips* standard. *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005); 37 C.F.R. §42.100. Under the *Phillips* standard, the “words of a claim are generally given their ordinary and customary meaning as understood by a person of ordinary skill in the art when read in the context of the specification and prosecution history.” *Thorner v. Sony Computer Entertainment America LLC*, 669 F.3d 1362, 1366 (Fed. Cir. 2012) (citing *Phillips*, 415 F.3d at 1313). Petitioner identifies the following terms for construction for the purposes of this proceeding.

1. Hybrid Device

For the purposes of the present proceeding, this term, which appears in claims 1-16 and 19, should be construed to mean “a device comprising an integrated, secure memory storing local, secured information and an integrated receiver-decoder circuit.” This construction is consistent with the use of the term in the specification

² Petitioner and Microsoft advanced modified constructions in their respective claim construction pleadings in co-pending litigations. MS-1013; Ex. 1017.

Petitioner adopts constructions that are consistent with those advanced by the court, as explained below, for the purposes of this proceeding.

of the '289 patent. *See, e.g.*, MS-1001, Abstract, 2:25-48. The district court in related proceeding (6:21-CV-00210-ADA) previously construed “hybrid device” to be “a device comprising an integrated personal digital key (PDK) and an integrated receiver-decoder circuit.” MS-1009. This construction reflected the recitation of the term “PDK” in the “hybrid device” independent claims. Petitioner submits that because the '289 patent does not recite “PDK” in the “hybrid device” independent claims³, but instead recites an “integrated, secure memory storing local, secured information,” that the construction proposed herein is also consistent with the district court’s construction in 6:21-CV-00210-ADA. MS-1001, Claims 1, 14. Although Petitioner does not concede to the correctness of the district court construction, the below analysis demonstrates that the claims are obvious even under the proposed construction. *See infra*, §§III.A.6.[1.pre], III.B.2.[1.pre]; MS-1003, ¶[25].

2. Personal Digital Key (“PDK”)

For the purposes of the present proceeding, this term, which appears in claim 20, should be construed to mean “an operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a

³ Notably, the term “PDK” is only recited once in the claim language of the '289 patent. MS-1001, Claim 20. Moreover, as explained below, this singular use of “PDK” appears to lack antecedent basis. *See infra*, §III.A.6.[20].

controller and memory for storing information particular to a user.” This construction is consistent with the use of the term in the specification of the ’289 patent (*see, e.g.*, MS-1001, 14:15-28) and was adopted in 6:21-CV-00210-ADA and in 6:21-CV-00320-ADA. MS-1009; Ex. 1020; MS-1003, ¶[26].

3. Receiver-decoder circuit (“RDC”)

For the purposes of the present proceeding, this term, which appears in claims 1, 3, 7, 14, and 16, should be construed to mean “a component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing.” This construction is consistent with the use of the term in the specification of the ’289 patent (*see, e.g.*, MS-1001, 7:39-57) and was adopted in 6:21-CV-00210-ADA and in 6:21-CV-00320-ADA. MS-1009; Ex. 1020; MS-1003, ¶[27].

D. Level of Ordinary Skill in the Art

A person of ordinary skill in the art (“POSITA”) relating to the subject matter of the ’289 Patent as of December 6, 2007 would have had (1) at least a bachelor’s degree in computer science, computer engineering, electrical engineering, or a related field, and (2) at least two years of industry experience in the field of encryption and security. MS-1003, ¶¶[21]-[22]. Additional graduate education could substitute for professional experience, and *vice versa. Id.*

II. The '289 Patent

A. Brief Description

The '289 Patent is directed to “a hybrid device” that includes a personal digital key (PDK) and a receiver-decoder circuit (RDC) coupled in communication with each other. MS-1001, 1:45-52. The integrated PDK communicates wirelessly with an external RDC and the integrated RDC communicates wirelessly with at least one external PDK within its proximity zone. MS-1001, 4:26-52. The specification discloses that the integrated PDK is capable of storing local, secured financial information, or secured biometric information for authenticating a user. MS-1001, 3:51-62. Similarly, the external PDK is also capable of storing information. MS-1001, 4:26-52. For example, in one embodiment, the integrated PDK carries credentials such as credit card or account information that are used to enable services associated with the external RDC. MS-1001, 5:29-37. A user can make a purchase with the hybrid device provided that they are in possession of the external PDK and in proximity to the hybrid device. If so, the external PDK wirelessly connects to the integrated RDC and authorizes the integrated PDK to enable a transaction by sharing credit card or account information with the external RDC. *Id.*; MS-1003, ¶¶[28]-[29].

B. Prosecution History

The '289 Patent was allowed after a single office action that presented only a double-patenting rejection. MS-1002, 90-110. During prosecution, the Examiner did not consider any of Giobbi-157, Giobbi-139, Dua, or Broadcom. *Id.* As discussed below, these references render obvious the Challenged Claims. MS-1003, ¶[30].

III. The Challenged Claims Are Unpatentable

A. [GROUND 1A/1B]—Claims 1-20 are rendered obvious by Giobbi-157 and Giobbi-139 [1A] and Giobbi-157, Giobbi-139, and Dua [1B]

1. Overview of Giobbi-157

Giobbi-157 is directed at a system and method to “provide efficient, secure and highly reliable authentication for transaction processing and/or access control applications.” MS-1005, Abstract, ¶¶[0011]-[0014]. The disclosure further explains that a “transaction includes enabling access to secure physical or digital assets (e.g., unlocking a door, opening a vault, providing access to a secured hard drive, etc.).” MS-1005, ¶[0063]. This process is accomplished using “secure and tamperproof memories” to store information for “identification and authentication.” MS-1005, ¶[0036], *see also* ¶¶[0026]-[0029], [0035]-[0048]. Giobbi-157 is a continuation in part of a prior application and claims priority to five provisional applications. MS-1005, Cover, ¶[0002]; MS-1003, ¶[32].

Giobbi-157 discloses a Personal Digital Key (PDK) that “stores one or more profiles (e.g., a biometric profile) in a tamperproof memory that is acquired in a secure and trusted process.” MS-1005, ¶[0063], *see also* ¶¶[0026]-[0029], [0035]-[0048]. Giobbi-157 further teaches that the PDK may be integrated into an electronic device, such as **a cellphone**. MS-1005, ¶[0035] (“a portable electronic device such as a cell phone”), *see also* ¶[0080], claims 27, 33; MS-1003, ¶[33].

Giobbi-157 teaches that its integrated PDK can communicate with a receiver-decoder circuit (RDC). MS-1005, ¶¶[0049]-[0058], [0064]. The RDC establishes a secure communication channel between the PDK and RDC, then sends “profile authentication requests to the PDK 102 requesting transmission of one or more stored profiles over the secure channel.” MS-1005, ¶[0064]. In some examples, Giobbi-157 teaches that information stored on a PDK, such as fingerprint information, is transmitted to an external RDC located on a “Reader 108.” MS-1005, ¶[0049]; MS-1003, ¶[34]. An example of Giobbi-157’s PDK and Reader configuration is shown in the annotated version of Figures 2 and 3 below.

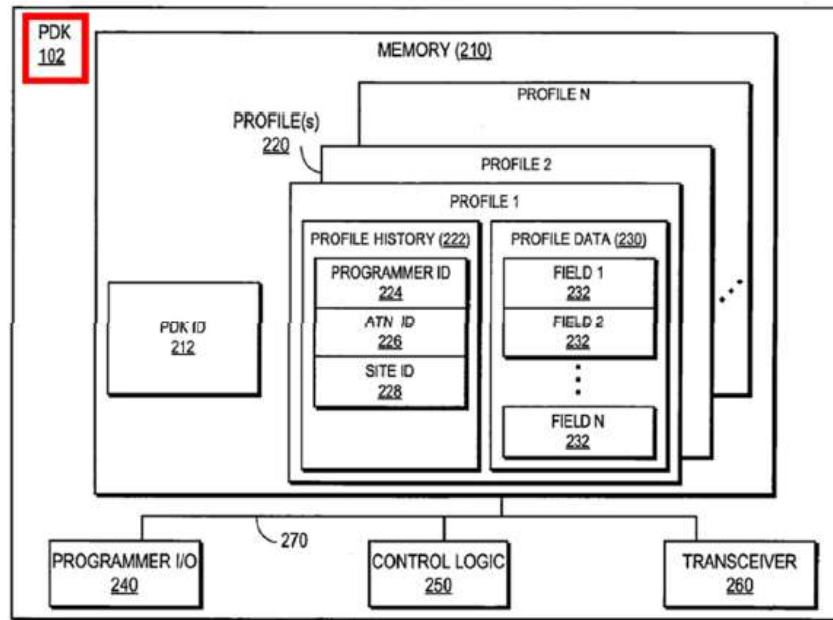


FIG. 2

MS-1005, FIG. 2⁴.

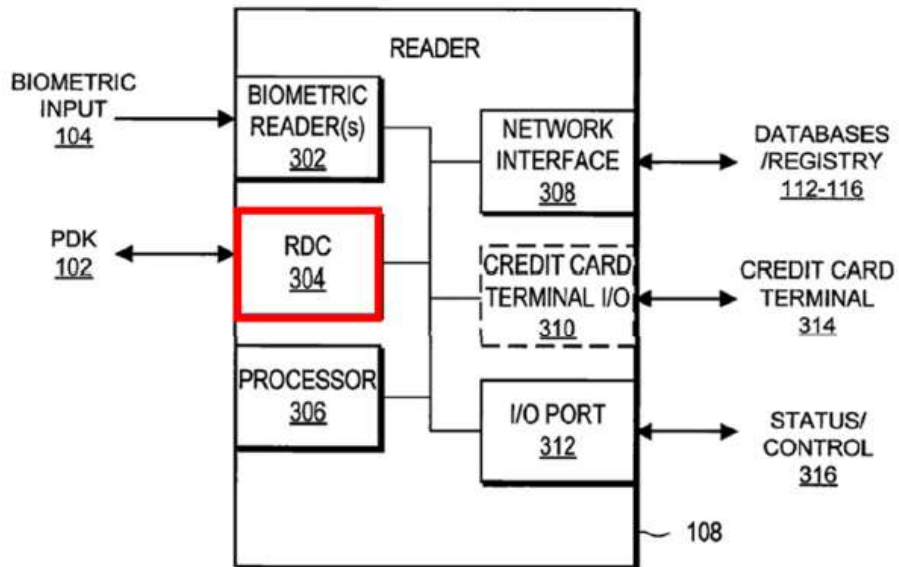


FIG. 3

MS-1005, FIG. 3.

⁴ Annotations to the figures in this petition are shown in color.

Giobbi-157 teaches that its RDC can authenticate a PDK and then enable a “transaction,” the “transaction includ[ing] enabling access to secure physical or digital assets (e.g., unlocking a door, opening a vault, providing access to a secured hard drive, etc.).” MS-1005, ¶¶[0057]-[0058], [0063], FIG. 4; MS-1003, ¶[35].

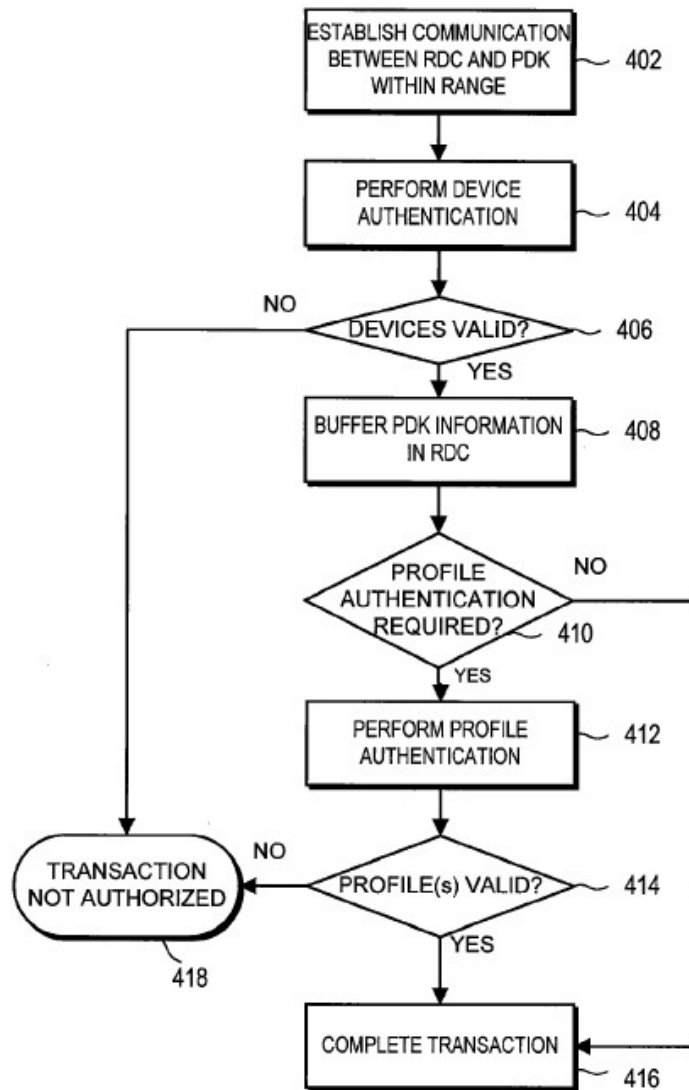


FIG. 4

MS-1005, FIG. 4.

Giobbi-157 also discloses that “the PDK can store other information such as credit/debit card information, bank information, or personal information in a memory for use in authorizing or completing a transaction.” MS-1005, ¶¶[0011], [0063], [0065]; MS-1003, ¶[36].

The Giobbi-157 provisional applications disclose several use cases of the PDK and RDC systems and detail both the process and components necessary to setup and operate a PDK and RDC system. MS-1010, pp. 2-14. The details include exemplary form factors for the PDKs and RDCs and explanations as to how a user could incorporate these devices into a user’s current devices to setup and operate a PDK and RDC system. *Id.*; MS-1003, ¶[37].

2. Overview of Giobbi-139

Giobbi-139 shares the same goal of securing physical or digital access as Giobbi-157, disclosing a “Personal Digital Key Digital Content Security System” which prevents “unauthorized use and protect[s] the digital content stored on computers from being wrongfully accessed, copied, and/or distributed.” MS-1006, Abstract, ¶[0010]. Like the Giobbi-157 publication, Giobbi-139 discusses using RDCs to communicate with PDKs to enable access and functions on devices. MS-1006, ¶¶[0010], [0071]-[0078]. The disclosure of Giobbi-139 further teaches that an RDC can be incorporated into **a cell phone** and that the RDC “is an integrated circuit able to process PDK-Key information, as well as encrypt/decrypt PDK-

compliant digital content.” MS-1006, ¶[0077], [0088] (“This embodiment involves integrating RDCs into...PDAs, cell phones [etc.]”); MS-1005, ¶[0035]; MS-1003, ¶[38].

Giobbi-139 teaches the PDK and RDC relationship as being flexible and capable of being integrated with existing equipment. MS-1006, ¶¶[0087]-[0099]. Giobbi-139 also teaches that an RDC can be acquired independently and integrated into a device. MS-1006, ¶¶[0088]-[0090]. The integrated RDC could then be used to secure the device and can even “enable/disable” the device based on communication with a PDK. MS-1006, ¶¶[0087]-[0090]. When using a PDK to secure a device with an integrated RDC, “[t]his security mechanism protects any data stored on such devices in the event they are ever stolen, left unattended, or even purposely ‘disabled’ to prevent access to sensitive content (i.e. preventing minors from accessing adult files, websites, etc.).” MS-1006, ¶[0090]. “When the associated PDK-Key(s) is not present, these devices and their storage means are locked and disabled.” *Id.*; MS-1003, ¶[39].

Giobbi-139 also discloses the scalability of RDC and PDK architecture. MS-1006, ¶¶[0091]-[0096]. For example, Giobbi-139 teaches that a user can “assign (or remove)” additional PDKs to a device with an integrated RDC. MS-1006, ¶¶[0092], [0095]; MS-1003, ¶[40].

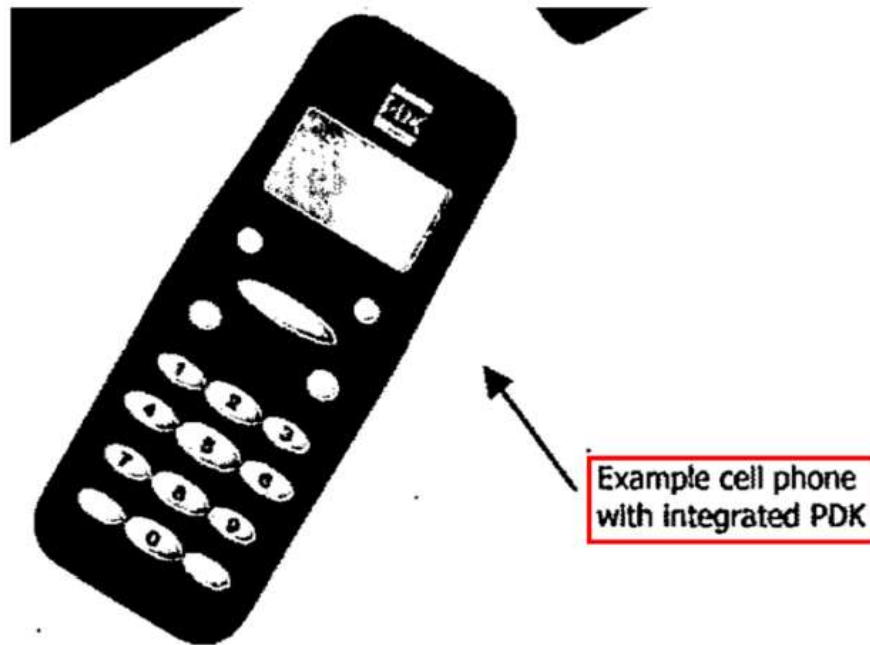
Giobbi-139 further discloses a version of communication between a PDK and RDC that is not wireless. ¶¶[0041], [0071]-[0073]. Particularly, Giobbi-139 teaches alternative embodiments where an RDC and PDK are communicatively coupled to each other by a wired signal line. MS-1006, ¶¶[0041], [0071]-[0073]; MS-1003, ¶[41].

3. The combination of Giobbi-157 and Giobbi-139

a. Giobbi-157 teaches integrating a PDK into a mobile device to enable a user to enjoy secure storage functionality via a commonly carried item

Giobbi-157 expressly and repeatedly discloses the portability of a PDK, emphasizing that a PDK can be carried by a user on their person and expressly teaches integrating the PDK into cell phones, PDAs, and other commonly carried items. MS-1005, ¶¶[0012], [0027], [0030], [0035] (“integrated into commonly carried items ... such as a cell phone, [or PDA]”); MS-1010, p. 3, 14. Based on these teachings, a POSITA would have readily recognized that integration of PDKs into mobile devices, such as cell phones, provides the benefits of simplicity and convenience by, for example, providing a secure and local storage location for the user’s biometric data. MS-1005, ¶¶[0012], [0027], [0030], [0035]. As Dr. Traynor explains, such integration enables a user who already carries a cell phone to enjoy the security benefits offered by Giobbi-157’s system without having to carry a

separate PDK. MS-1003, ¶[45]. The incorporated '157 provisional application provides an illustration of a cell phone with integrated PDK. MS-1003, ¶[45].



MS-1010, p. 28 (image cropped).

b. Giobbi-139 teaches integrating an RDC into a mobile device to provide enhanced security for the data stored on the mobile device.

Giobbi-139 teaches integrating an RDC into the same type of device disclosed in Giobbi-157 (e.g., a mobile device, such as a cell phone). MS-1006, ¶[0088]; MS-1005, ¶[0035]. Specifically, Giobbi-139 discloses the PDK and RDC architecture “to protect computers from unauthorized use and protect the digital content stored on computers from being wrongfully accessed, copied, and/or distributed.” MS-1006, Abstract. Like Giobbi-157, Giobbi-139 teaches that the PDK

stores the data that authenticates a user via an RDC. MS-1006, ¶¶[0022]-[0044]; MS-1003, ¶[46].

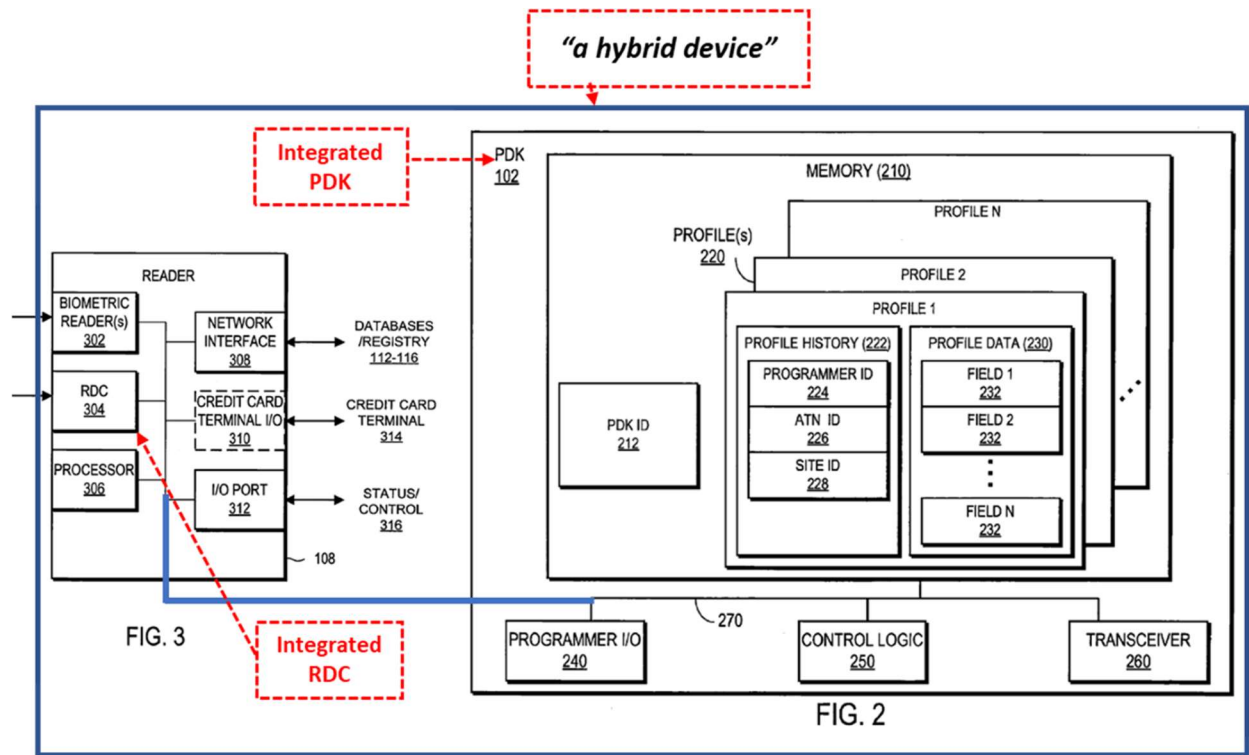
Giobbi-139 provides additional implementation details for its RDCs, noting that an RDC “is an integrated circuit able to process PDK-Key information, as well as encrypt/decrypt PDK-compliant digital content.” MS-1006, ¶[0072]. Giobbi-139 also notes that its integrated RDC may communicate with a PDK wirelessly or through a physical connection. MS-1006, ¶¶[0022]-[0044]. Thus, Giobbi-139 teaches similar components as Giobbi-157, where an RDC can communicate with at least one PDK to grant digital or physical access. MS-1006, Abstract, ¶¶[0036]-[0037], [0088]-[0090]. Giobbi-139 also discloses that it would have been desirable to include an RDC in a device holding data, such as a cell phone, to increase security by requiring a valid PDK to be used to permit access to the data. MS-1006, ¶[0088], FIG. 4. Dr. Traynor explains that, given these teachings, a POSITA would have found it obvious and advantageous to integrate an RDC into Giobbi-157’s cell phone to thereby enhance the security of the data stored on the cell phone. MS-1003, ¶[47].

Giobbi-139 additionally teaches a broader way to secure data on a cell phone and discloses that an RDC integrated into a cellphone can be used with a PDK to “effectively enable[]/disable[] the device itself.” MS-1006, ¶¶[0088]-[0090]. In this configuration, the cell phone with the integrated RDC can enable or disable the device through authentication with a PDK. *Id.*; MS-1003, ¶[48].

c. Combining Giobbi-157 and Giobbi-139

As Dr. Traynor explains, given the teachings of Giobbi-157 and Giobbi-139, a POSITA would have been motivated to integrate a PDK and RDC into the same mobile device (thus, creating a “*hybrid device*”). MS-1005, ¶¶[0012], [0027], [0030], [0035]; MS-1006, ¶¶[0022]-[0044], MS-1003, ¶[49]. As stated above, Giobbi-157 enumerates the advantages and motivations of incorporating a PDK into a mobile device. MS-1005, ¶¶[0035], [0080], claims 27, 33. For example, a user carrying the hybrid device would be able to be wirelessly authenticated with RDCs to securely complete transactions or gain access to physical or digital assets. Each RDC would be capable of communicating with the PDK’s “secure and tamperproof memories,” in which biometric authentication data is stored securely on the device in a format retrievable by an RDC. MS-1005, ¶¶[0036], [0064]. Additionally, Giobbi-139 teaches the benefits of integrating an RDC into this hybrid device. MS-1006, ¶¶[0087]-[0099]. For instance, a user can use an RDC integrated in the hybrid device to secure the data within the hybrid device (cell phone) to thereby protect it from loss or theft. MS-1006, ¶[0091]. Further the RDC would allow other external PDKs to interact with the hybrid device. Accordingly, Dr. Traynor explains that a POSITA would have recognized that a mobile device having an integrated RDC and PDK would provide increased security in accessing both assets internal to

the mobile device and assets external to the mobile device. MS-1003, ¶[49].



MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139's teachings).

- d. A POSITA would have found it obvious to integrate a PDK and RDC in a mobile device to enable secure access to assets internal to the mobile device and assets external to the mobile device

A POSITA would have found it obvious to communicatively couple the integrated PDK and RDC within the mobile device with a physical connection based on Giobbi-139's teachings that a PDK can be connected to an RDC by a "transmission line such as a serial cable." MS-1006, ¶[0041]. By coupling the integrated PDK and RDC in this manner, assets internal to the mobile device (e.g., files, applications, etc.) can thereby be protected using the PDK-RDC techniques

disclosed by Giobbi-157 and Giobbi-139. MS-1005, ¶¶[0012], [0027], [0030], [0035]; MS-1006, ¶¶[0022]-[0044], MS-1003, ¶[50].

For example, the mobile device may be equipped with or otherwise communicatively coupled to a biometric scanner that receives a biometric input from a user. MS-1005, ¶[0071]. To authenticate the user, the integrated RDC securely accesses the valid biometric information from the integrated PDK or from an external PDK as taught by Giobbi-157 to thereby enable a comparison of the inputted biometric information with the valid biometric information stored in the PDK. MS-1005, ¶¶[0050], [0053], [0061]. A match results in a successful authentication, thereby enabling the user to access assets internal to the mobile device. A mismatch results in a failed authentication, preventing such access. MS-1005, ¶¶[0056], [0062]-[0063], [0070], [0072]. Dr. Traynor explains that, consistent with the teachings of Giobbi-157 and Giobbi-139, “the internal assets of the mobile device would be protected from access by unauthorized users who would be unable to provide a biometric input that matches the valid biometric stored in the tamper proof memory of the integrated PDK of the mobile device or, in some implementations, of a PDK external to the mobile device.” MS-1003, ¶[51].

As Dr. Traynor explains, a POSITA would have further recognized and found it obvious that integrating a PDK and RDC into the same device would facilitate the Notary process disclosed by Giobbi-157 to initialize or otherwise securely edit the

information securely stored in the integrated PDK. MS-1005, ¶¶[0050], [0053], [0061]; MS-1003, ¶[52]. For example, Giobbi-157 discloses that a PDK can store information used in the verification of the PDK user. MS-1005, ¶¶[0011]-[0012], [0036]-[0039]. The information stored within the PDK is stored in profiles, which can be accessed and edited in a secure, auditable way. MS-1005, ¶¶[0012], [0036]-[0039], [0043]. Giobbi-157's "Notary" PDK is used to verify that authorized individuals are creating or editing information inside a PDK, and to maintain a history of changes to the PDK including the identity of the "Notary" PDK that was present during the change. MS-1005, ¶¶[0037], [0043]; MS-1010, p. 4. As shown in FIG. 2 of Giobbi-157, a PDK profile contains a history (Profile History 222) that includes the identification of the Authorized TruProx Notary PDK ID (ATN ID 225). MS-1005, FIG. 2. For an integrated PDK to record the ATN PDK ID into the profile history of the integrated PDK in a mobile device, an RDC can be used to (1) interface with and read the ATN PDK, and (2) record the ATN PDK ID into the PDK. MS-1006, ¶¶[0022]-[0044]. Accordingly, a POSITA would have recognized the need for both a PDK and an RDC to be integrated into the same mobile device (a "*hybrid device*") and communicatively coupled together. MS-1005, ¶¶[0012], [0027], [0030], [0035]; MS-1006, ¶¶[0022]-[0044], MS-1003, ¶[52].

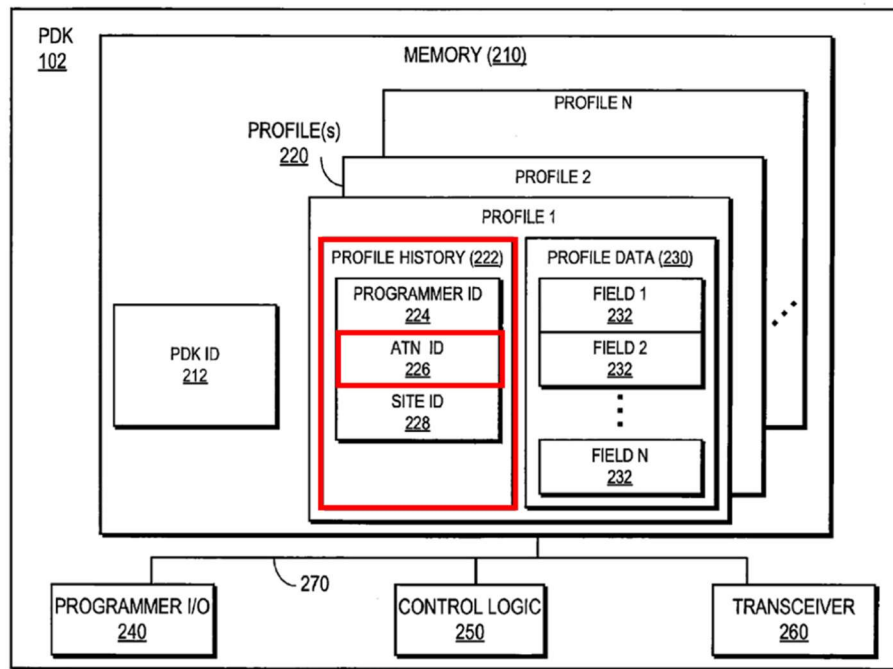


FIG. 2

MS-1005, FIG. 2.

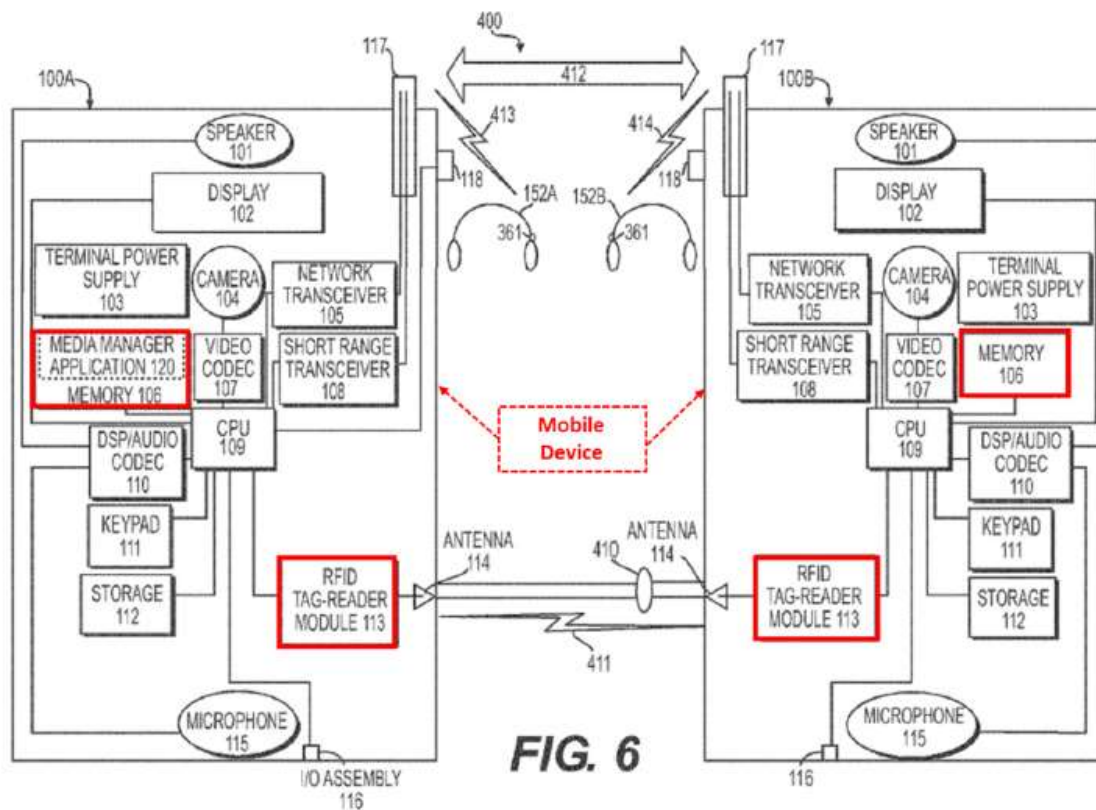
In addition to using the integrated RDC to enable secure access to assets internal to the mobile device, as Dr. Traynor explains, a POSITA would have further recognized the benefit of using the integrated PDK to enable secure access to assets external to the mobile device. MS-1003, ¶[53]. For example, as taught by Giobbi-139, the owner of the mobile device could separately use the integrated PDK of the mobile device to securely authenticate themselves for the purpose of accessing all or portions of an external hard drive equipped with an RDC. MS-1006, ¶¶[0087]-[0090]. Moreover, as taught by Giobbi-157, the owner of the mobile device could separately use the integrated PDK of the mobile device to securely access physical items, such as a room or safe. MS-1005, ¶¶[0011]-[0012], [0063].

Dr. Traynor explains that, for at least the aforementioned reasons, a POSITA would have found it obvious to modify Giobbi-157's portable electronic device to include an RDC as taught by Giobbi-139 (thus creating a "*hybrid device*"). MS-1003, ¶[54]. Combining Giobbi-157 and Giobbi-139 would have involved (1) combining prior art elements according to known methods to yield predictable results; (2) use of a known technique to improve similar devices (methods, or products) in the same way; and (3) applying a known technique to a known device ready for improvement to yield predictable results. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421, 82 USPQ2d 1385, 1395-97 (2007); MPEP 2143. Further, Giobbi-157 expressly teaches the integration of a PDK into a mobile device. MS-1005, ¶[0035], claim 27. Giobbi-139 expressly teaches the integration of a RDC into a mobile device. MS-1006, ¶[0088], claim 9, FIG. 4. Specifically, a POSITA would have been motivated to integrate a PDK and RDC into a *hybrid device* by recognizing that (i) Giobbi-157 and Giobbi-139 are directed to similar operations having similar purposes (e.g., "provide efficient, secure, and highly reliable authentication for ... access control applications" and "protect[ing] any data stored on such devices"; (ii) Giobbi-157 and Giobbi-139 describe similar structures for performing those operations (e.g., PDKs and RDCs); (iii) the techniques of Giobbi-157 and Giobbi-139 are compatible with each other, given that both were filed by the same applicant and describe similar techniques; and (iv) combining the

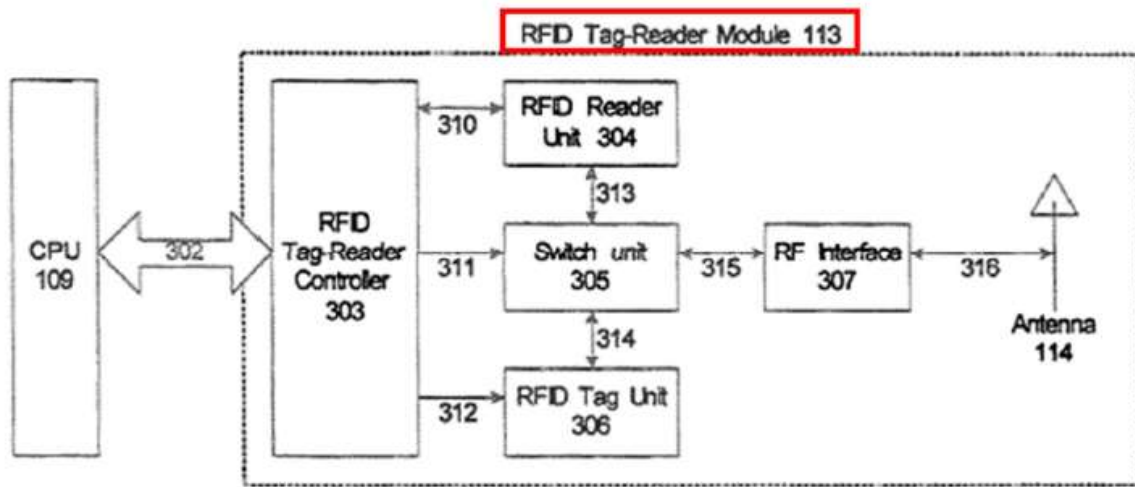
techniques of Giobbi-157 and Giobbi-139 would have worked in the same manner already described in the references. MS-1005, $\{0011\}$; MS-1006, $\{0090\}$; MS-1003, $\{55\}$.

4. Overview of Dua

Dua discloses a wireless media player or related system (e.g., a cell phone) which establishes wireless connections with other devices to enable functions and exchange data. MS-1007, 6:46-65, FIG. 6; MS-1003, ¶[42]. Dua's device is shown, for example, in annotated Fig. 6:



MS-1007, FIG. 6.



MS-1007, FIG. 4A.

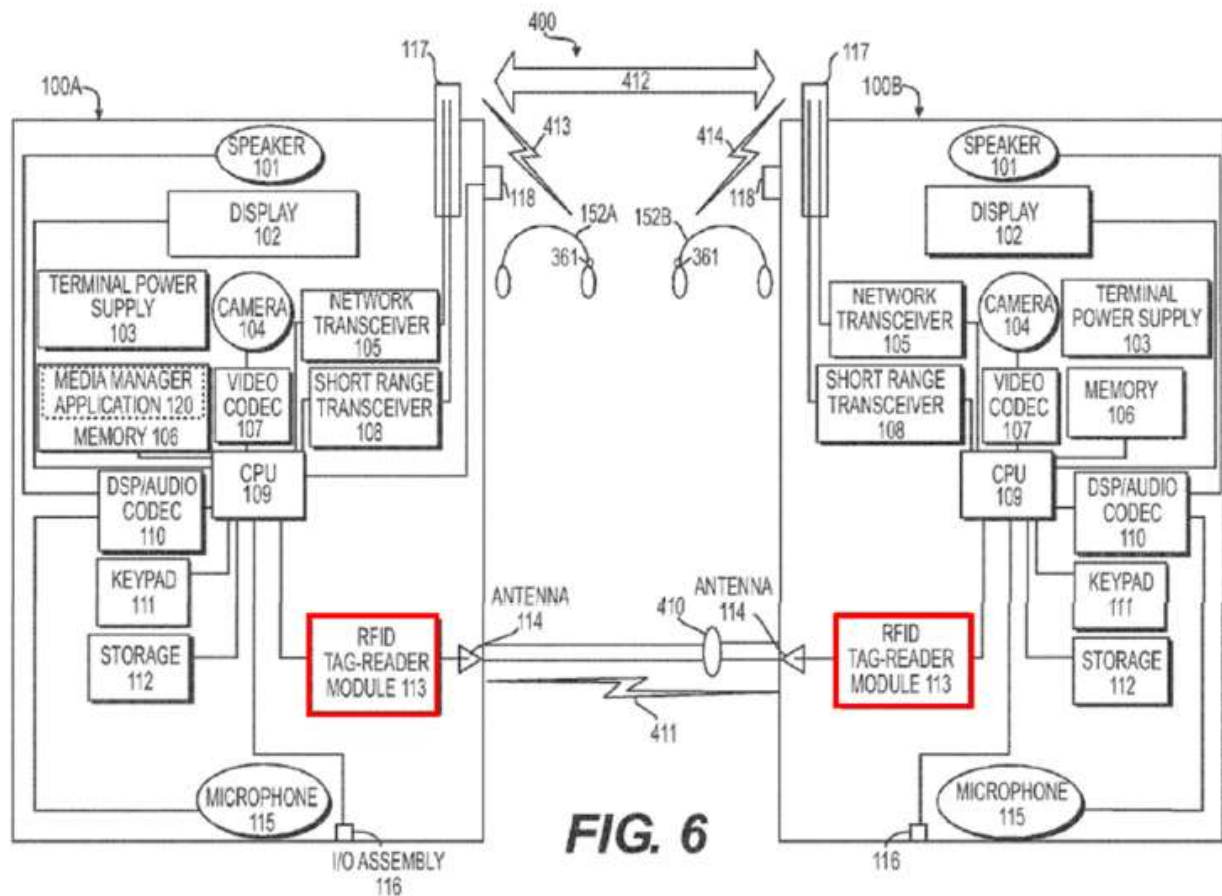
Dua employs an RFID system to secure data and applications on its device using an RFID “electronic key” (e.g., for point-of-sale transactions). MS-1007, 12:51-64. Dua uses an RFID Tag as an electronic “key” and an RFID Reader as the electronic “lock.” *Id.* Specifically, Dua discloses that its device uses RFID Tag-Reader Module (shown above in FIG. 4A), that includes both an RFID Reader Unit 304 and RFID Tag Unit 306. MS-1007, 13:22-48, FIGS. 4A, 6; MS-1003, ¶[43].

Dua’s RFID Tag Unit 306 stores information necessary to gain access to an external device in an encrypted internal tag memory and transmits this information to an external Reader when establishing a connection. MS-1007, 13:9-18, 14:53-64, 15:42-56, 16:31-34. As shown in FIG. 4A above, Dua also discloses an integrated Reader Unit 304 for reading information transmitted by external Tag Units. MS-1007, 14:53-64, FIG. 4A; MS-1003, ¶[44].

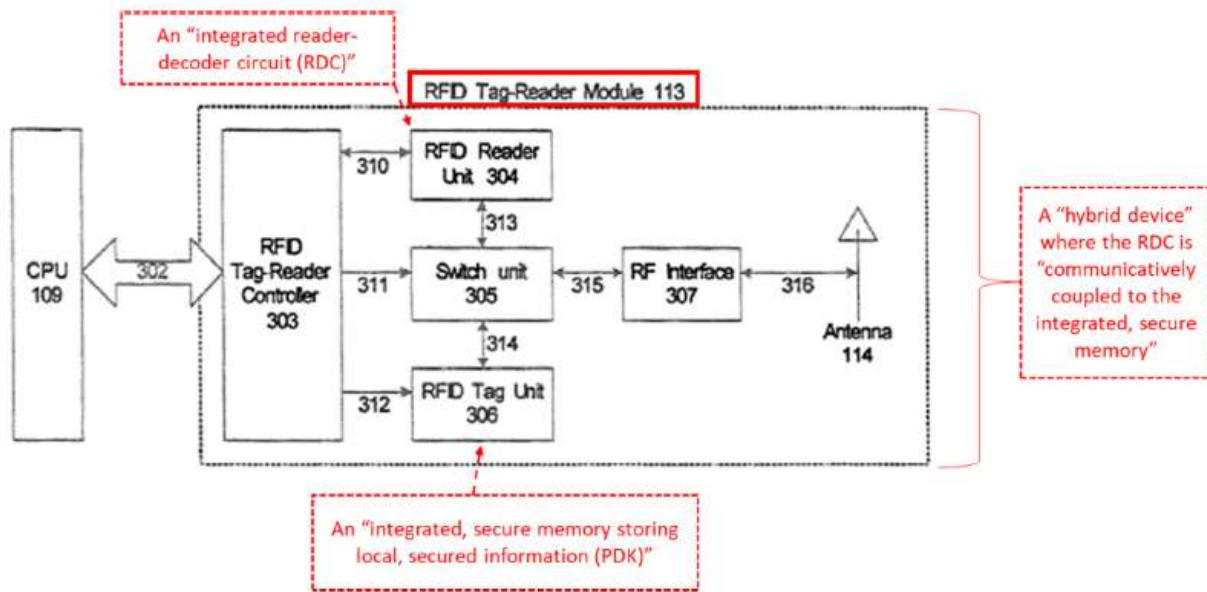
5. Combination of Giobbi-157, Giobbi-139, and Dua

Dua further corroborates the teachings of the Giobbi references and provides implementation details for integrating an RDC and PDK into the same device. MS-1003, ¶[56]. As Dr. Traynor explains, a POSITA would have recognized the similarity between 1) the RFID Tag in Dua and the PDK in Giobbi-157; and 2) the RFID Reader in Dua and the RDC in Giobbi-139. This is because, like RFID technology, Giobbi's PDK and RDC architecture require both components within proximity of each other. For example, two RFID tags without a reader would not be usable. Likewise, two PDKs without an RDC would not be usable. An RFID tag becomes usable when in range of an RFID reader, comparable to how a PDK is usable when in range of an RDC. Dr. Traynor goes on to explain, a POSITA would have been motivated to combine the teachings of the Giobbi references and Dua because, at least, these references are all in the same field of endeavor (e.g., incorporating proximity based enabling technology into mobile devices to allow secure data sharing and services). MS-1005, Abstract, ¶¶[0011]-[0014]; MS-1006, Abstract, ¶[0010]; MS-1007, Abstract, 6:46-65, FIGS. 4A, 6.; MS-1001, Abstract, claim 1; MS-1003, ¶[57]. Accordingly, with proximity enabling technology (RFID) like Dua integrating both transmitters (PDKs/RFID Tags) and receivers (RDCs/RFID Readers) into the same mobile device, a POSITA would have had a reasonable expectation of success integrating an RDC from Giobbi-139 into the

Giobbi-157 device to create a hybrid device. *Id.* This reasonable expectation of success is further bolstered by the teachings of Dua, which, as discussed above, also teaches integrating an “RDC” and “PDK” into the same type of device. MS-1007, 13:19-14:64, Fig. 4A; MS-1003, ¶¶[56]-[57].



MS-1007, FIG. 6.



MS-1007, FIG. 4A.

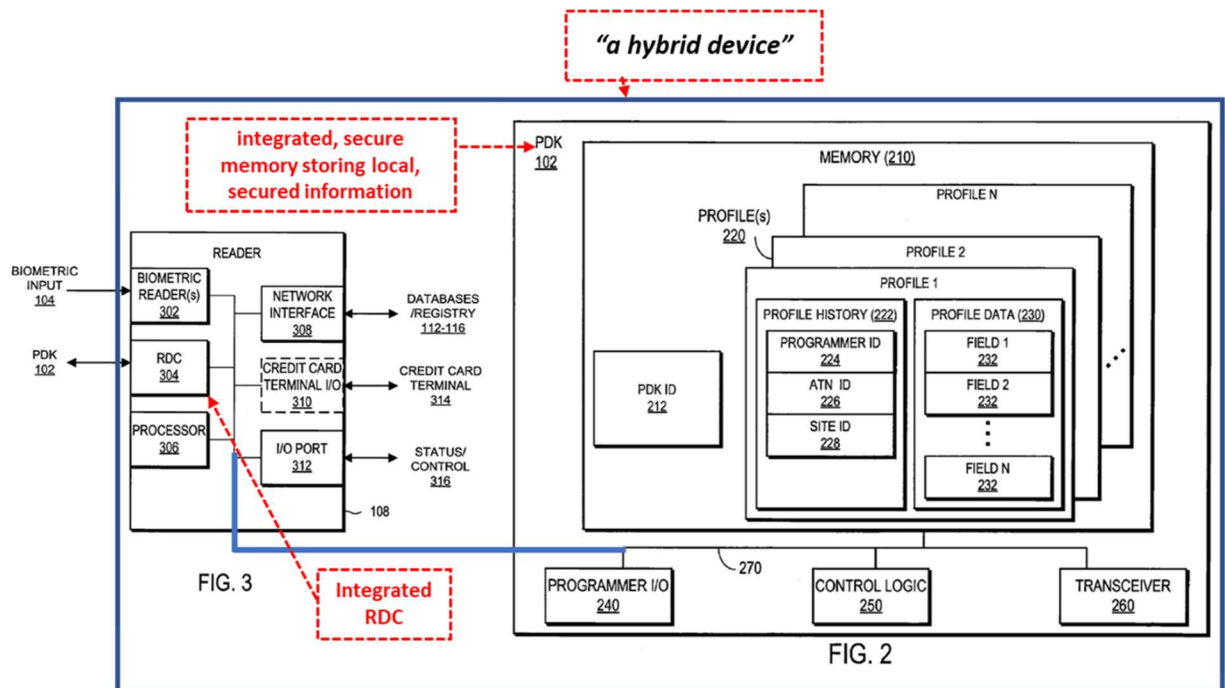
6. Analysis

[1.pre]

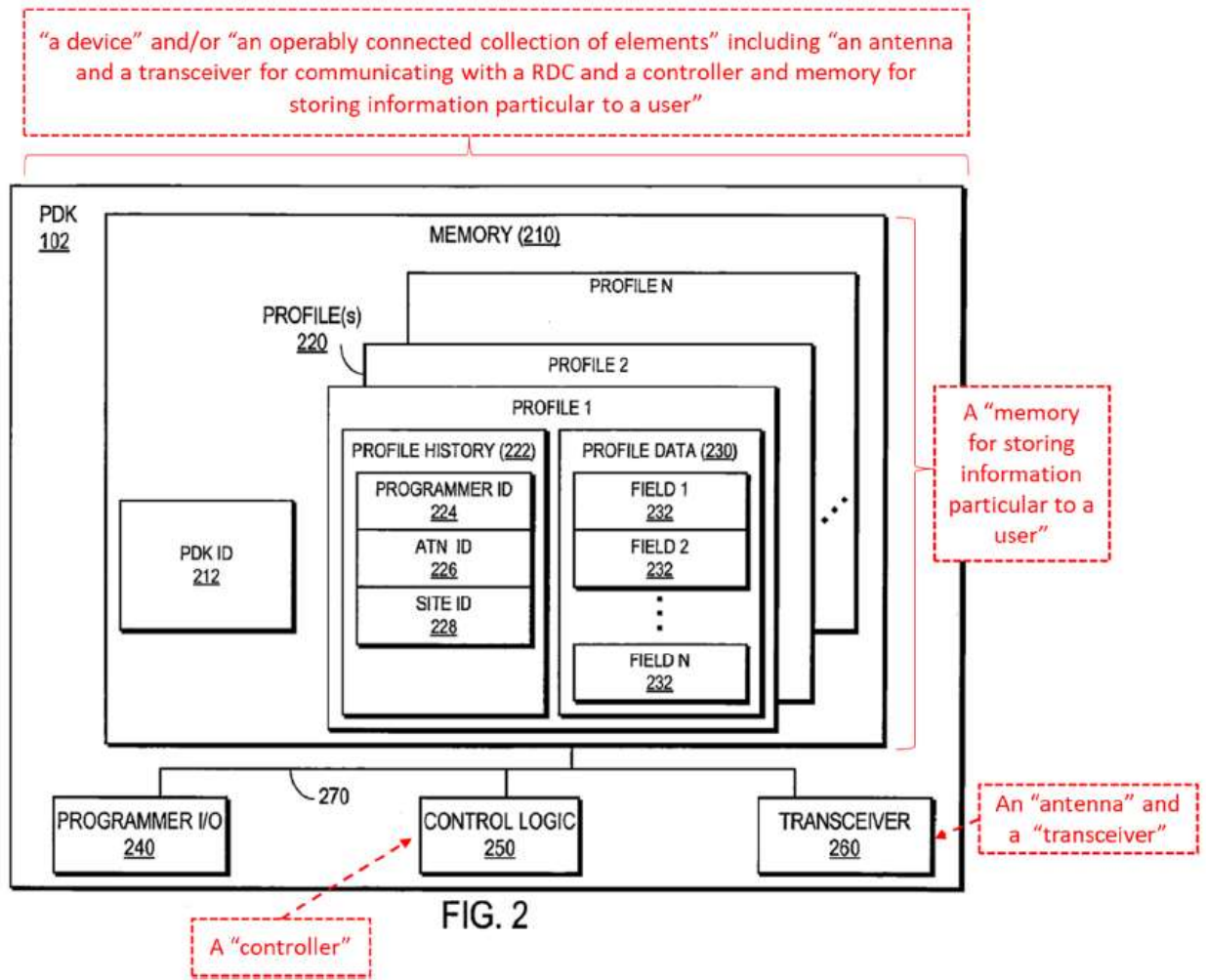
Grounds 1A/1B

To the extent the preamble is limiting, the combination of Giobbi-157 and -139 discloses a “*hybrid device*.” MS-1005, ¶¶[0012], [0027], [0030], [0035]; MS-1006, ¶¶[0022]-[0044], MS-1003, ¶[58]. For example, Giobbi-157 discloses incorporating PDKs (“integrated, secure memory storing local, secured information”) into different electronic devices, while Giobbi-139 discloses incorporating RDCs into different electronic devices. MS-1005, ¶¶[0012], [0027], [0030], [0035]; MS-1006, ¶¶[0022]-[0044]; *see supra*, §§III.A.1-3; *see infra*, [1.1]. Accordingly for the reasons described in detail in Sections III.A.1-3 and 5 above,

the combination of these two references renders obvious “a device comprising an integrated, secure memory storing local, secured information and an integrated [RDC],” and “a device comprising an integrated personal digital key (PDK) and an integrated [RDC].” *See supra*, §§I.C.1-3, III.A.3. As shown below in FIGS. 2-3, Giobbi-157’s cell phone includes an integrated PDK. MS-1005, FIGS. 2-3. In the combination of Giobbi-157 and Giobbi-139, this integrated PDK communicates with an integrated RDC (a “*hybrid device*”). *Id.*; MS-1003, ¶¶[58]-[59].



MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139’s teachings).



MS-1005, FIG. 2.

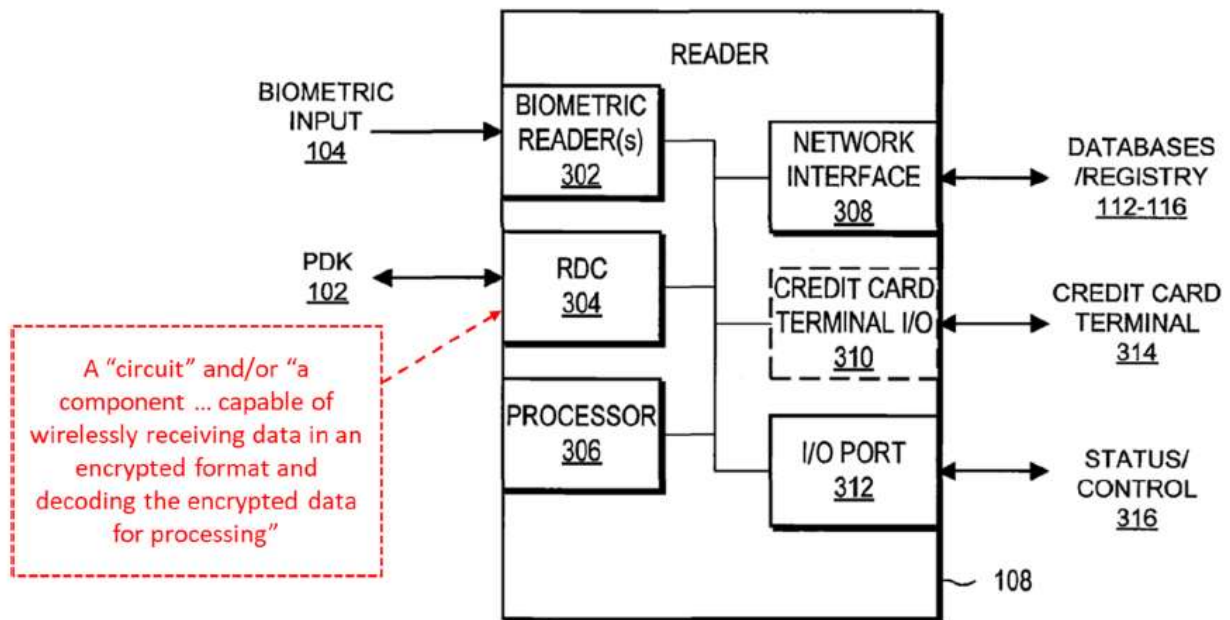


FIG. 3

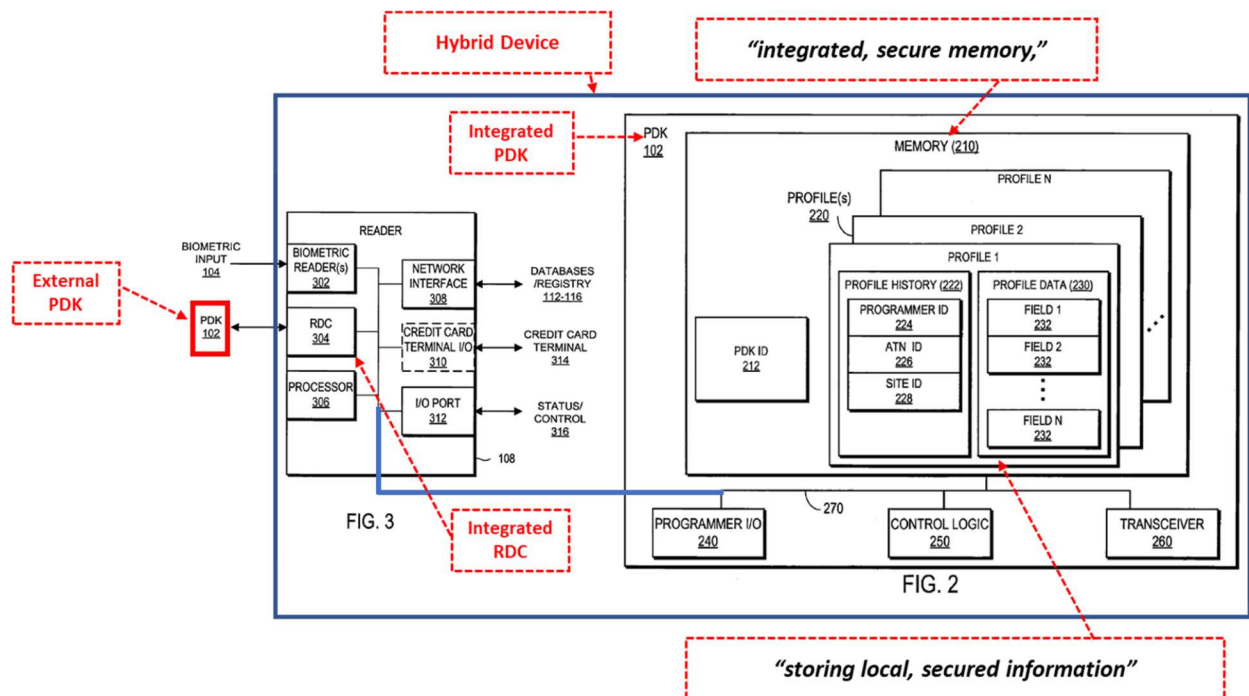
MS-1003, FIG. 3.

[1.1]

Ground 1A

Giobbi-157 discloses a “Personal Digital Key (PDK),” which is an example of an *integrated secure memory*. MS-1005, ¶[0011] (“A portable physical device, referred to herein as a Personal Digital Key or ‘PDK,’ stores one or more profiles (e.g., a biometric profile) [“*secured information*”] in a tamper-proof [“*secure*”] memory”). As discussed above, Giobbi-157 also discloses that its PDK is *integrated* into a hybrid device, such as a cell phone. MS-1005, ¶[0035] (“The PDK 102 can be standalone as a portable, physical device or can be integrated into commonly carried

items ... such as a cell phone”); *see supra*, §III.A.1, [1.pre]. Accordingly, the hybrid device of the Giobbi-157-Giobbi-139 combination includes an “*integrated, secure memory*.” Additionally, Giobbi-157’s PDK stores information in *local* storage as the PDK is integrated into the hybrid device. MS-1005, ¶¶[0011], [0027]-[0028]; MS-1003, ¶[60].



MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139’s teachings).

Ground 1B

Like Giobbi-157 and Giobbi-139, Dua uses an RFID system to secure data and applications on its hybrid device. MS-1007, 6:46-65, 12:51-64, 13:9-18, 14:53-64, 15:42-56, 16:31-34, FIGS. 4A, 6; *see supra* §III.A.4. Dua teaches that its RFID setup may act as an “electronic key” for point-of-sale transactions and uses an RFID

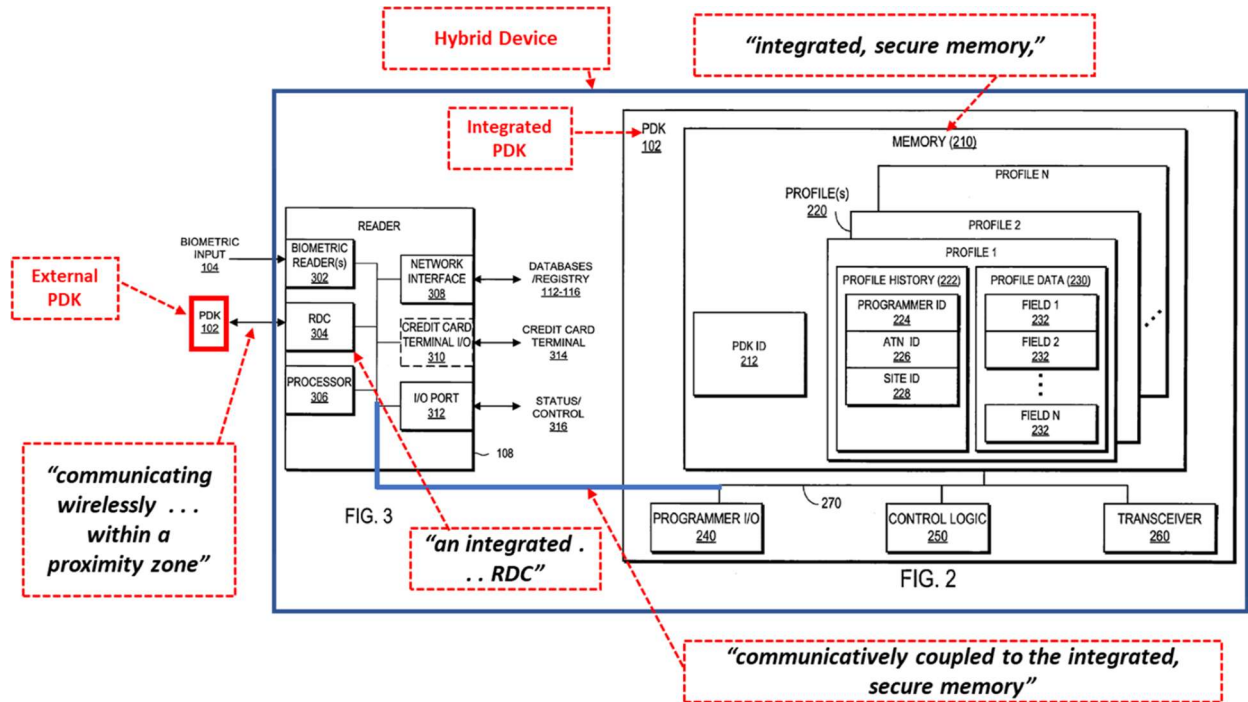
Tag as an electronic “key” and an RFID Reader as the electronic “lock.” *Id.* Accordingly, as Dr. Traynor explains, Dua’s RFID Tag Unit 306 is another example of an “*an integrated, secure memory storing local, secured information.*” MS-1003, ¶[61].

[1.2]

Ground 1A

The combination of Giobbi-157 and Giobbi-139 discloses “a component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing” as required by the district court’s construction for an “*integrated reader-decoder circuit (RDC).*” *See supra*, §§I.C.3, III.A.1-3. In particular, Giobbi-157 teaches that “the RDC 304 wirelessly receives data from the PDK 102 in an encrypted format and decodes the encrypted data for processing.” MS-1005, ¶[0050]. Giobbi-157 also discloses an integrated RDC “*communicating wirelessly*” with “*at least one external device within a proximity zone.*” MS-1005, ¶¶[0026]-[0044] (“The Reader 108 wirelessly communicates with the PDK 102 when the PDK 102 is within a proximity zone of the Reader 108”); *see supra* §III.A.1. As described above, the hybrid device includes an RDC that is “*communicatively coupled*” to the PDK (“*integrated, secure memory*”) for “*communication with the [PDK].*” MS-1005, ¶¶[0012], [0027],

[0030], [0035]; MS-1006, ¶¶[0022]-[0044], MS-1003, ¶[62]; *see supra*, §III.A.3. An RDC is illustrated in FIG. 3 of Giobbi-157 below. MS-1005, FIG. 3.



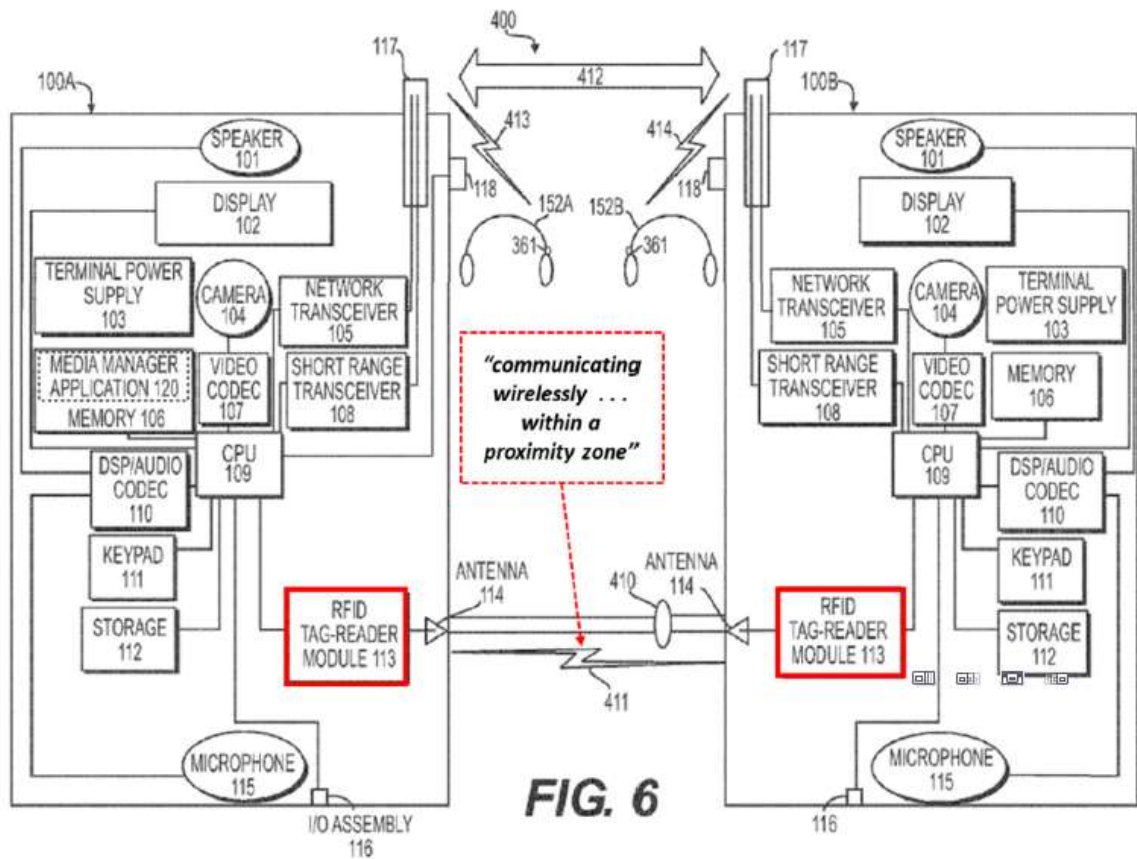
MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139's teachings).

Giobbi-139 also discloses an integrated RDC “communicating wirelessly with the at least one external device within a proximity zone.” MS-1006, ¶¶[0026]-[0044] (“The Reader 108 wirelessly communicates with the PDK 102 when the PDK 102 is within a proximity zone of the Reader 108”); MS-1003, ¶[63].

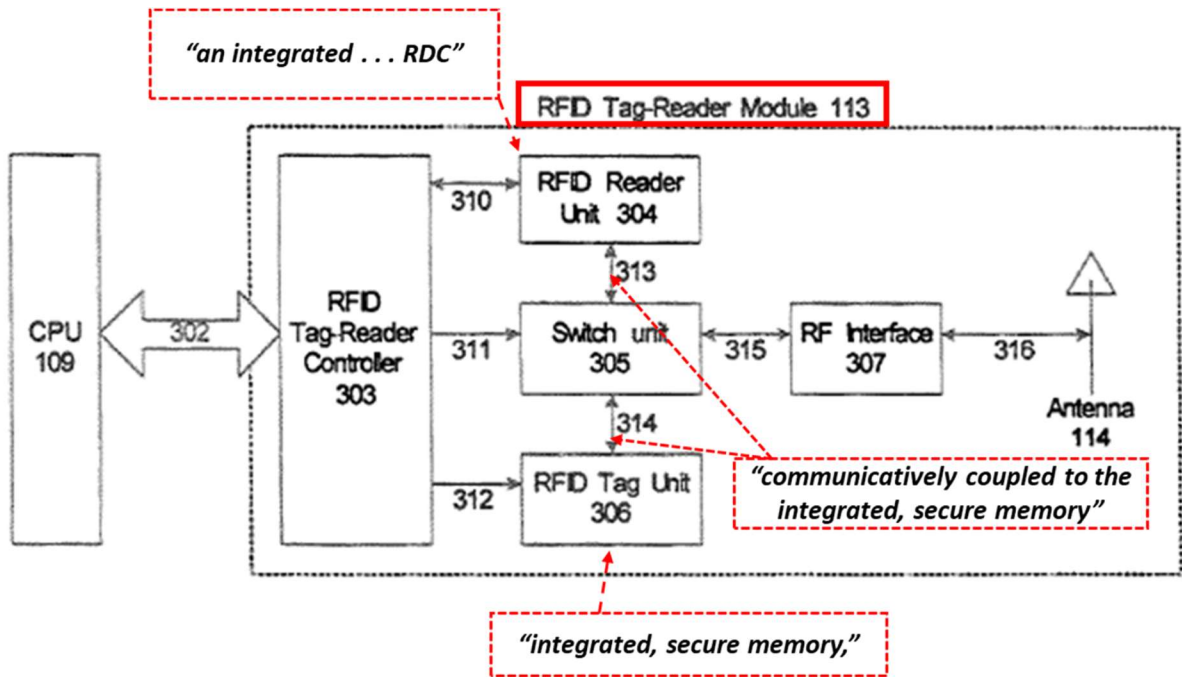
Ground 1B

Like Giobbi-157 and Giobbi-139, Dua uses a proximity (RFID) system to secure data and applications on its “hybrid device.” MS-1007, 6:46-65, 12:51-64, 13:9-18, 14:53-64, 15:42-56, 16:31-34, FIGS. 4A, 6; *see supra* §III.A.4. Dua teaches

that its RFID setup may act as an “electronic key” for point-of-sale transactions and uses an RFID Tag (PDK) as an electronic “key” and an RFID Reader (RDC) as the electronic “lock.” MS-1007, 12:60-61. FIG. 6 of Dua illustrates a hybrid device that includes an RFID Tag-Reader Module (an “*integrated reader-decoder circuit (RDC)*” and an RFID Tag Unit 306 (the “*integrated, secure memory enables one or more of an ...*” of [1.2]). MS-1007, FIG. 6. As explained, the patent’s disclosure of integrating PDKs and RDCs in a hybrid device is merely a recitation of technology commonly used in RFID applications, such as Dua’s application, function, and service. *Id.* Accordingly, as Dr. Traynor explains, Dua’s Reader Unit 304 is another example of an “*integrated reader-decoder circuit (RDC)*” as the Reader Unit 304 also “*communicat[es] wirelessly with at least one external device within a proximity zone*” and is “*communicatively coupled to [an] integrated, secure memory*” (the RFID Tag Unit 306). MS-1007, 6:46-65, 12:51-64, 13:9-18, 14:53-64, 15:42-56, 16:31-34, FIGS. 4A, 6; MS-1003, ¶[64].



MS-1007, FIG. 6.



MS-1007, FIG. 4A.

[1.3]

Ground 1A/1B

Giobbi-157 discloses that, “[w]hen a PDK 102 comes within range of a Reader 108, communication is automatically established 402 between the RDC 304 ... and the PDK 102 ... when it enters a proximity zone of the [RDC]” (“*the integrated RDC communicating wirelessly with the at least one external device within the proximity zone*”). MS-1005, ¶¶[0059-0063]. The RDC then requests profile data stored within the external PDK for authentication. MS-1005, ¶[0061]. If the profile data received from the “secure memory” of the external PDK is valid, the RDC “completes the transaction.” MS-1005, ¶[0063]. A “transaction includes enabling access to secure physical or digital assets (e.g., unlocking a door, opening a vault, providing access to a secured hard drive, etc.)” (“*enables one or more of an application, a function, and service*”). MS-1006, ¶[0063]; MS-1003, ¶[65].

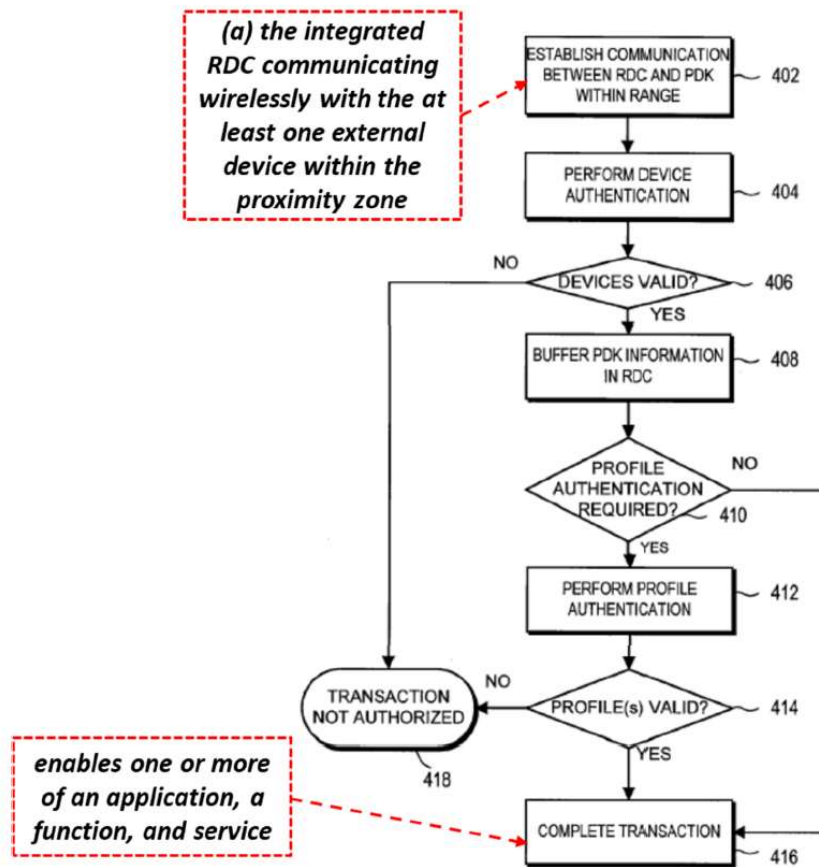


FIG. 4

MS-1005, FIG. 4.

Alternatively, the integrated secure memory of the hybrid device “*enables one or more of an application, a function, and service*” using “*the local, secured information stored by the integrated, secure memory.*” MS-1005, Abstract, ¶[0011]. Transactions in Giobbi-157 are performed by transmitting authenticating information from the integrated PDK (“*integrated, secure memory*”) to a reader (an external RDC in the Giobbi-157-Giobbi-139 combination), for example, when completing a withdrawal from an ATM. MS-1005, ¶[0065]; MS-1003, ¶[66]. An example authentication process and function enablement is shown below in FIG. 4.

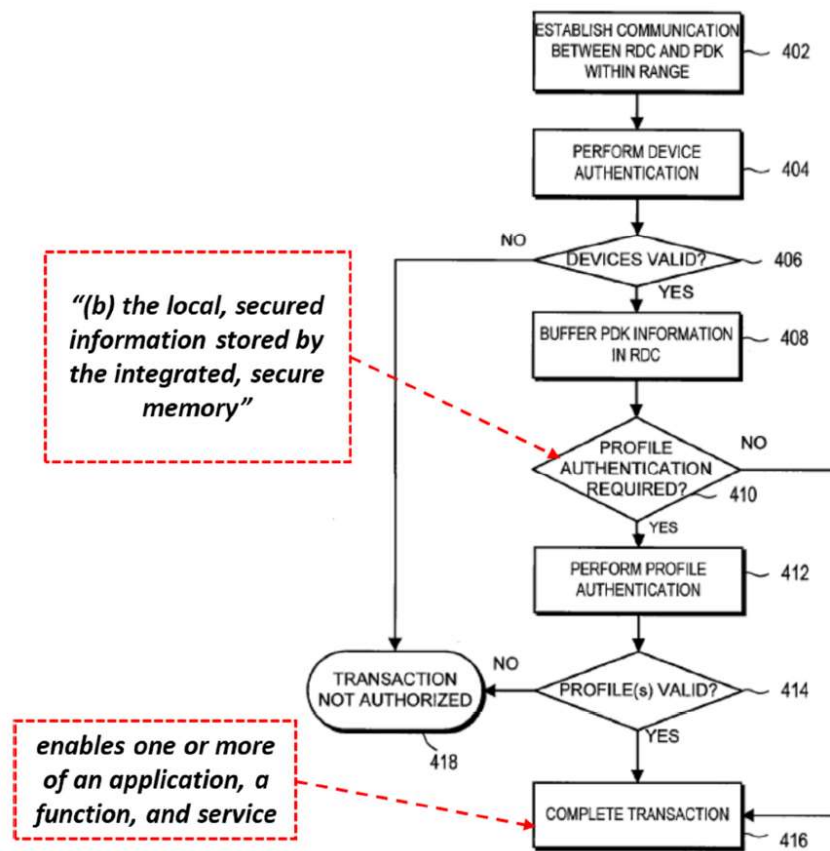


FIG. 4

MS-1005, FIG. 4.

Giobbi-157 explicitly teaches that the “transaction” in FIG. 4 *“enables one or more of an application, a function, and service”* when stating that “the transaction includes enabling access to secure physical or digital assets (e.g., unlocking a door, opening a vault, providing access to a secured hard drive, etc.).” MS-1005, ¶[0063]; MS-1003, ¶[67]. Additionally, Giobbi-139 discloses a use case where an integrated RDC can be incorporated into cell phones, PDAs, and MP3 players. MS-1006, ¶[0088]; *see supra* §§III.A.2-3. If an authorized PDK (“*integrated, secure memory*”) is used in conjunction with the integrated RDC the

application/function/service runs on the hybrid device, e.g., the hybrid device “plays the digital content,” such as music (“*enables one or more of an application, a function, and service*”). MS-1006, ¶[0037]; MS-1003, ¶[68].

[2]

Grounds 1A/1B

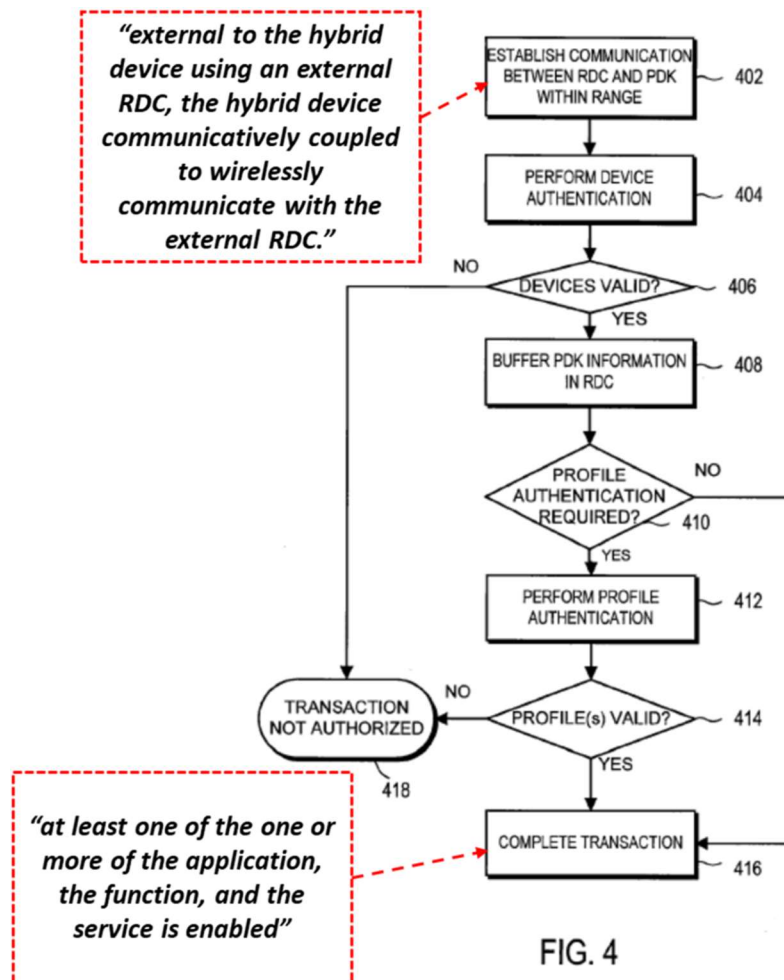
Giobbi-139 teaches that signals between PDKs (either integrated or external) and RDCs can “enable/disable” functions on the device with the integrated RDC (“*at least one of the one or more of the application, the function, and the service is enabled at least in part on the hybrid device*”). MS-1006, ¶[0089]-[0091]; *see supra* §III.A.2. Accordingly, the Giobbi-157-Giobbi-139 combination would have used the integrated RDC to control “*applications, ... function[s], and ... service[s]*” within the hybrid device as taught by Giobbi-139. MS-1006, ¶[0067]-[0069], [0089]-[0091]; MS-1003, ¶[69].

[3]

Grounds 1A/1B

As described above, the Giobbi-157-Giobbi-139 combination can use the integrated PDK to “*wirelessly communicate*” with “*external RDC[s]*.” MS-1006, ¶¶[0087]-[0090]; *see supra* §III.A.3. Additionally, Giobbi-157 discloses that RDCs (both internal and external) are communicatively coupled to “remote databases” over “network 110” which are used for “remote authentication” that can “enable[e] access

to secure physical or digital assets” (“*the application, the function, and the service is enabled, at least in part, external to the hybrid device*”). MS-1005, ¶[0031], FIG. 3, *see also* ¶[0009], [0026]-[0027], [0063]. Accordingly, in the Giobbi-157-Giobbi-139 combination, “*one of the one or more of the function, and the service is enabled, at least in part, external to the hybrid device using an external RDC.*” MS-1005, ¶[0009], [0026]-[0027], [0031], FIG. 3; MS-1006, ¶[0087]-[0090]; *see supra* §III.A.3; MS-1003, ¶[70].



MS-1005, FIG. 4.

Alternatively, Giobbi-139 teaches that a device with an RDC can be “enabled/disabled” by the presence of a PDK. MS-1006, ¶¶[0087]-[0090]. Thus a device external to the hybrid device that has an RDC installed can then have the “*the application, the function, and the service is enabled*” by the “*external RDC*” when the hybrid device’s PDK comes within range of the external RDC (“*the hybrid device communicatively coupled to wirelessly communicate with the external RDC*”). MS-1006, ¶¶[0087]-[0090]; MS-1003, ¶[71].

[4]

Grounds 1A/1B

As discussed above, Giobbi-157 discloses that PDKs contain “biometric profile” that include “profile data 230 representing physical and/or behavioral information that can uniquely identify the PDK owner” (“*the local, secured information includes biometric information*”) and that this information is used “for authentication” (“*authenticating a user*”). MS-1005, ¶¶[0037]-[0038], *see also* ¶¶[0011]-[0013], [0026]-[0030], [0043], [0048]-[0052], [0065]; MS-1003, ¶[72].

[5]

Grounds 1A/1B

Giobbi-157 discloses that biometric information for authenticating a user can be based on “the touch of a finger to a fingerprint scanner” (“*biometric information based on a biometric scan of a finger*”). MS-1005, ¶[0065]. As discussed above in

[4], this biometric information is stored as “***local, secured information***” and is used “***for authenticating a user.***” See *supra*, [4]; MS-1003, ¶[73].

Further, as previously discussed, biometric information can be stored in the secure memory of the hybrid device combination during the initialization process where “some types of profile information (e.g., a biometric profile) can only be acquired during a trusted initialization process that is administered by a trusted Notary.” MS-1005, ¶[0043]. This “biometric information” can then be used to authenticate the user. MS-1005, ¶[0048]; MS-1003, ¶[74].

[6]

Grounds 1A/1B

Giobbi-157 discloses that PDKs store “bank information, debit/check/ATM card information, coupon codes, or any other purchasing means information” (“***the local, secure information includes financial information***”). MS-1005, ¶[0063], see also ¶¶[0027], [0033], [0041]-[0043], [0048]-[0049], [0055]. Additionally, Giobbi-157 discloses that this financial information “can be transmitted by the PDK 102 in place of credit card information” for “different types of transactions” (“***at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information***”). *Id.*; MS-1003, ¶[75].

[7]

Grounds 1A/1B

As discussed above in [6], PDKs store “bank information, debit/check/ATM card information, coupon codes, or any other purchasing means information” (“*the local, secure information includes financial information*”). MS-1005, ¶[0063], *see also* ¶¶[0027], [0033], [0041]-[0043], [0048]-[0049], [0055]; *see supra* [6]; MS-1003, ¶[76].

Additionally, Giobbi-157 discloses that RDCs (including *integrated RDCs*) are communicatively coupled to “remote databases” (“*at least one external device*”) used for “remote authentication.” MS-1005, ¶[0031], FIG. 3, *see also* ¶¶[0009], [0026]-[0027]; *see supra* [3]. Indeed, Giobbi-157’s databases (e.g., “validation database 112”) are used for “authorizing a transaction to be processed at the Reader 108” (“*the service enabled completes a financial transaction based on a signal received from the at least one external device by the integrated RDC*”). MS-1005, ¶[0033], FIG. 3; MS-1003, ¶[77].

Moreover, Giobbi-157 teaches that the RDCs and PDKs can communicate back and forth in order to complete transactions (including financial transactions). MS-1005, ¶¶[0059]-[0063], FIG. 4. Therefore, the hybrid device, which includes an *integrated RDC* is capable of receiving a signal from an external device (such as an external PDK) and completing a financial transaction (“*completes a financial*

transaction based on a signal received from the at least one external device”).

MS-1003, ¶[78].

[8]

Grounds 1A/1B

As described above, Giobbi-157 discloses “one or more external databases including a validation database 112” that performs “remote authentication” (“*authorization ... using an external authentication database, the ... information transmitted to the external authentication database*”). MS-1005, ¶¶[0009], [0026]-[0027], [0031], FIG. 1, *see supra* [3], [6]-[7] (“*the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction*”); MS-1003, ¶[79].

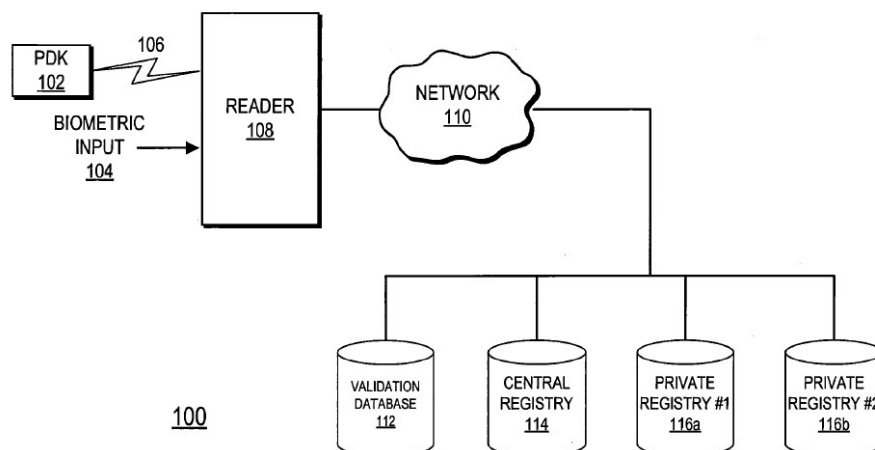


FIG. 1

MS-1005, FIG. 1.

For example, Giobbi-157 discloses that an RDC receives “a credit card number” transmitted from the secure memory of a PDK. MS-1005, ¶[0074]. The RDC then transmits through the network to the registries 114-116 and determines “if the status is valid 772 or invalid 770” (*“authorization of the financial information using an external authentication database, the financial information transmitted to the external authentication database”*). MS-1005, ¶[0074]; MS-1003, ¶[80].

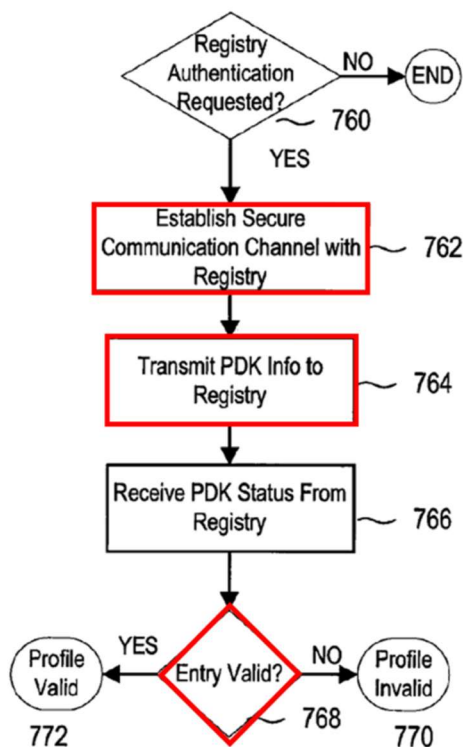


FIG. 7D

MS-1005, FIG. 7D.

[9]

Grounds 1A/1B

Giobbi-157 discloses that when “authentication is requested, a secure communication channel is established 762 over the network 110 between the Reader 108 and one or more registries (e.g., the Central Registry 114, any private registry 116, or other validation database 112)” (each “*external authentication database[s]*”). MS-1005, ¶[0074], FIG. 1; MS-1003, ¶[81].

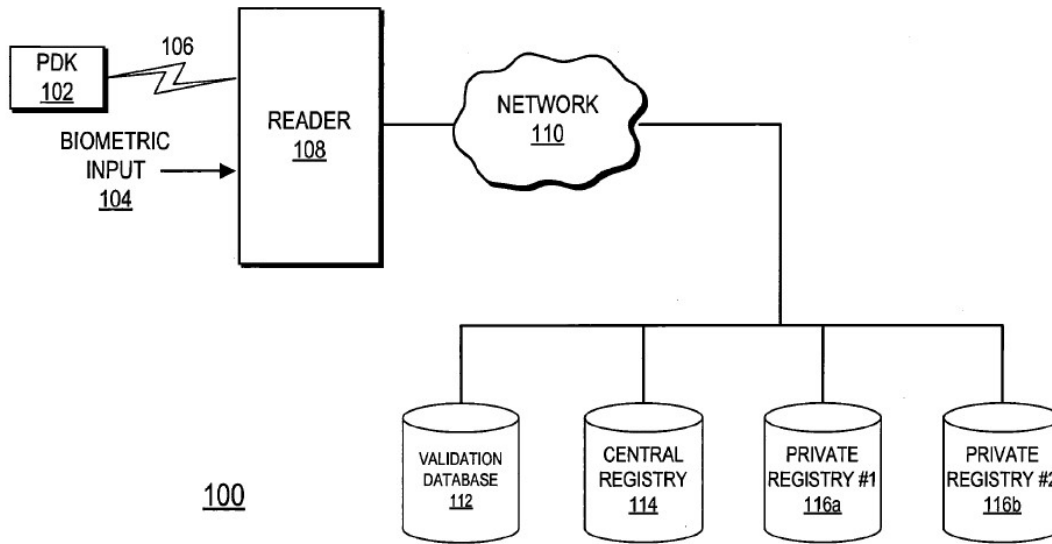


FIG. 1

MS-1005, FIG. 1.

Additionally, Giobbi-157’s “Central Registry” is “administered by a trusted third-party organization” (“*separate from a merchant providing a sale in the*

financial transaction”). MS-1005, ¶¶[0032]-[0034], [0053], [0074], Claim 8; *see supra* [3], [6]-[8]; MS-1003, ¶[82]. Alternatively, or in addition, Giobbi-157’s “private registries 116” can also be registered to a PDK 102. *Id.* Giobbi-157’s FIG. 7D illustrates the process of using a Central Registry 114 or private registry 116 to authenticate PDK information in a transaction. MS-1005, FIG. 7D; MS-1003, ¶[82].

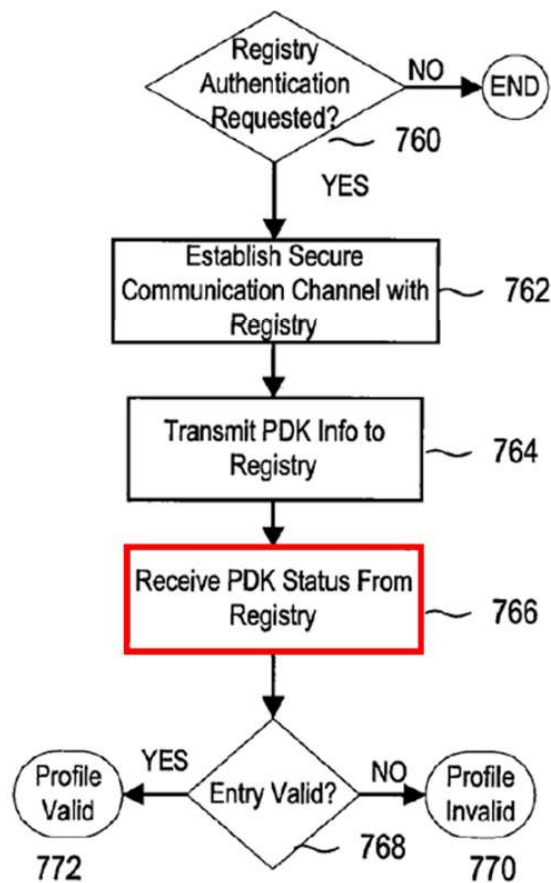


FIG. 7D

MS-1005, FIG. 7D.

[10]

Grounds 1A/1B

Giobbi-157 discloses that a PDK memory, reproduced below in FIG. 2, contains “one or more profiles 220” that each contain one or more of “a different type of biometric information,” “one or more pictures of the PDK owner,” and “include personal identification information such as name, address, phone number, etc., bank information, credit/debit card information, or membership information” (at least a “*first*” and a “*second subset of local, secured information*” that enable at least a “*first*” and “*second application, function or service*”). MS-1005, ¶¶[0036]-[0043], FIG. 2; MS-1003, ¶[83].

For example, Giobbi-157 discloses multiple use cases where information from a PDK is used to enable an application, function, or service. MS-1005, ¶¶[0065]-[0067](at least a “*first*” and a “*second application, function or service*”). Additionally, the above use cases also contain at least a “*first*” and a “*second subset of local, secured information*” each having “*different accessibility*.” *Id.* For example, “boarding a transportation vehicle” would have required different credentials than “entering a hotel room” or “confirm[ing] that the user is a ticket holder [for a venue].” *Id.*; MS-1003, ¶[84].

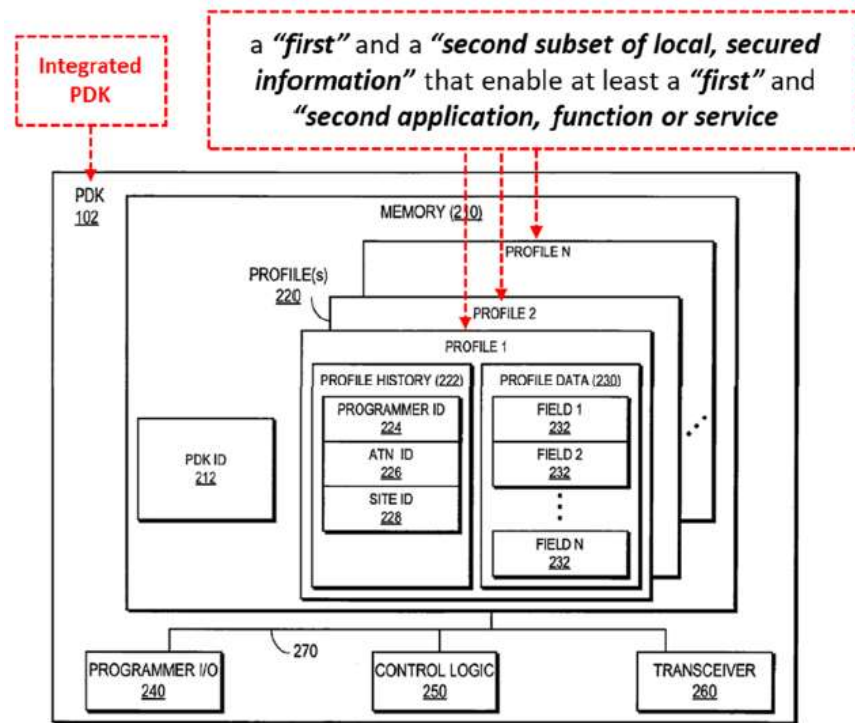


FIG. 2

MS-1005, FIG. 2.

Additionally, *In re Harza* has held that “mere duplication of parts has no patentable significance unless a new and unexpected result is produced.” 274 F.2d 669, 124 USPQ 378 (CCPA 1960).

[11]

Grounds 1A/1B

See supra, §§III.A.1-3, [1.pre]-[1.3]; MS-1003, ¶[85].

[12]

Grounds 1A/1B

Giobbi-157 discloses that its external PDK can be included in jewelry, including “watches, rings, necklaces or bracelets” (“*the at least one external device is included in jewelry*”). MS-1005, ¶[0035]; MS-1003, ¶[86].

[13]

Grounds 1A/1B

See supra, [12]; MS-1003, ¶[87].

[14.pre]

Grounds 1A/1B

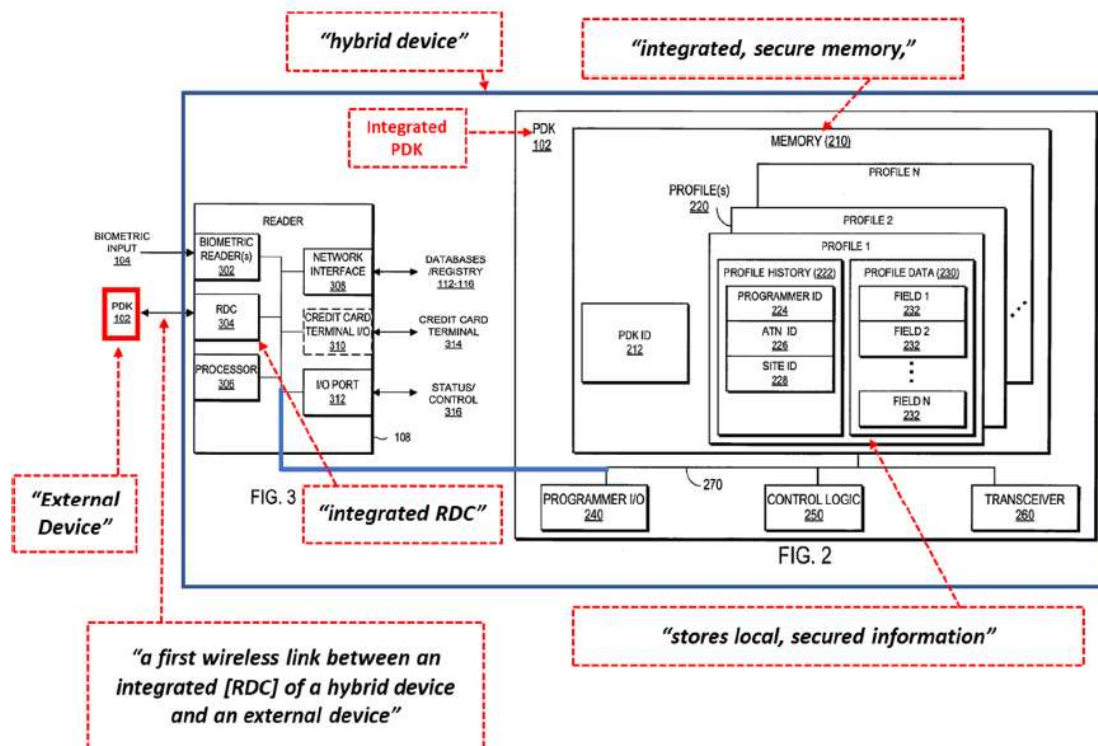
See supra [1.pre]. Giobbi-157 discloses that its techniques can be implemented as a “method.” MS-1005, Abstract, ¶[0011]; MS-1003, ¶[88].

[14.1]

Grounds 1A/1B

As described above in [1.1] and [1.2], the Giobbi-157-Giobbi-139 combination includes both an RDC 304 (“*integrated receiver-decoder circuit (RDC)*”) and a PDK (“*an integrated, secure memory*”). MS-1005, ¶¶[0011], [0027]-[0028], [0050]; *see supra* §III.A.3, [1.1]-[1.2]; MS-1003, ¶[89]. Additionally, Giobbi-157 discloses that, “[w]hen a PDK 102 [(an external PDK – the “*external device*”)] comes within range ... communication is automatically established 402

between the RDC 304 ... and the PDK 102 ... when it enters a proximity zone of the [RDC]” (“*creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external device*”). MS-1005, ¶[0059]. As described above, “*the hybrid device*” of the Giobbi-157-Giobbi-139 combination “*include[s] an integrated, secure memory and the integrated RDC, wherein the integrated, secure memory stores local, secured information.*” See *supra* [1.1]-[1.2]; MS-1005, FIG. 2-4 (presented below). Additionally, FIG. 1 of Giobbi-157 (which includes the Reader 103 and integrated RDC of FIG. 3) shows a contextual use of the Giobbi-157-Giobbi-139 combination hybrid device and the “external device[s].” MS-1005, FIG. 1; MS-1003, ¶[89].



MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139’s teachings).

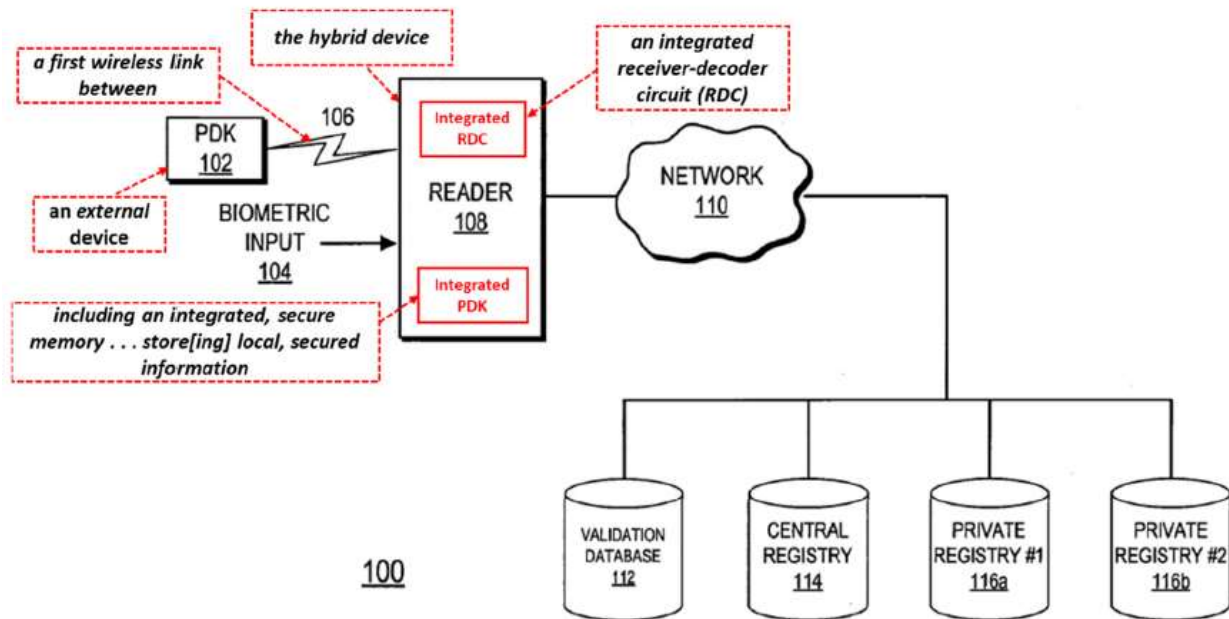


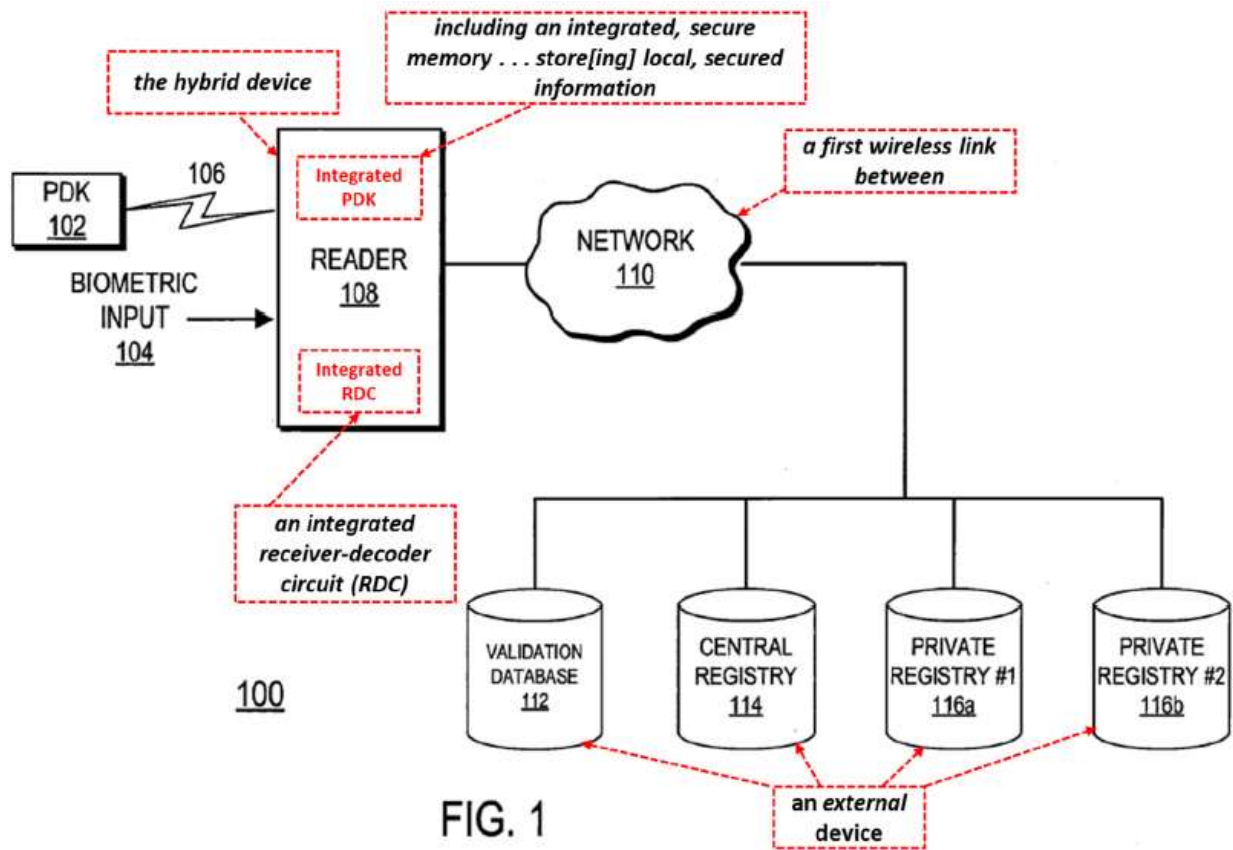
FIG. 1

MS-1005, FIG. 1 (modified to incorporate Giobbi-139’s teachings).

Alternatively, Giobbi-157 discloses that RDCs (including *integrated [RDCs]*) are communicatively coupled to “remote databases” (“*external device[s]*”) used for “remote authentication.” MS-1005, ¶[0031], FIG. 3, *see also* ¶¶[0009], [0026]-[0027]; *see supra* [3]; MS-1003, ¶[90].

The wireless connection can originate from the integrated RDC to remote systems (authentication registries). MS-1003, ¶[91]. For example, Giobbi-157 discloses “a process for authentication with a private registry 114 or [a] Central Registry 116” (“*an external device*”) via a “secure communication channel ... over the network 110 between the Reader 108 and one or more registries” (“*a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid*

device and an external device”). MS-1005, ¶[0074], FIG. 7D. From the teaching of Giobbi-157, the device can be “coupled to a network 110 by either a wired or *wireless link*.” MS-1005, ¶[0026]. “These registries receive the PDK credentials from Reader 108’s RDC and “determine [] if the [PDK] status is valid 772 or invalid 770” and “returns a validation decision to the Reader 108.” *Id.*; MS-1003, ¶[91]. This process is illustrated in FIG. 1 and FIG. 7D below.



MS-1005, FIG. 1 (annotated).

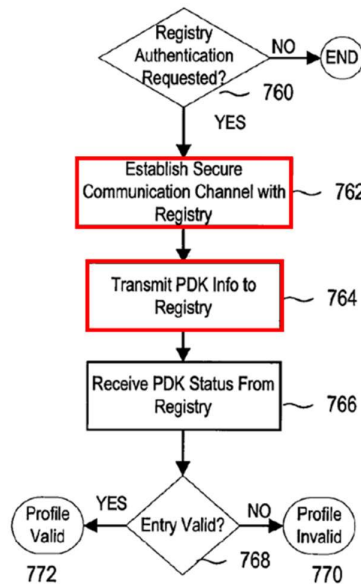


FIG. 7D

MS-1005, FIG. 7D

[14.2]

Grounds 1A/1B

Giobbi-157 discloses that, when an external “PDK 102 [(“*the external device*”)] comes within range of a Reader 108, communication [(“*receiving a first signal*”)] is automatically established 402 between the RDC 304 ... and the PDK 102 ... when it enters a proximity zone of the [RDC].” MS-1005, ¶[0059], FIGS. 4-5; *see supra* [14.1]; MS-1003, ¶[92]. When in the proximity zone, the PDK and RDC are coupled by “a *wireless link*.” MS-1005, ¶[0059]. “The RDC 304 receives and analyzes 502 information from the PDK 102 [(“*external device*”)]” (“*receiving a first signal, at the integrated RDC, via the first wireless link, from the external*

device”). MS-1005, ¶[0061]. Additionally, Giobbi-157 provides one example of establishing communication between a PDK and an RDC where “the communication is ... initiated by the PDK 102 and acknowledged by the Reader 108” (“*receiving a first signal, at the integrated RDC, via the first wireless link, from the external device*”). MS-1005, ¶[0059]; MS-1003, ¶[92].

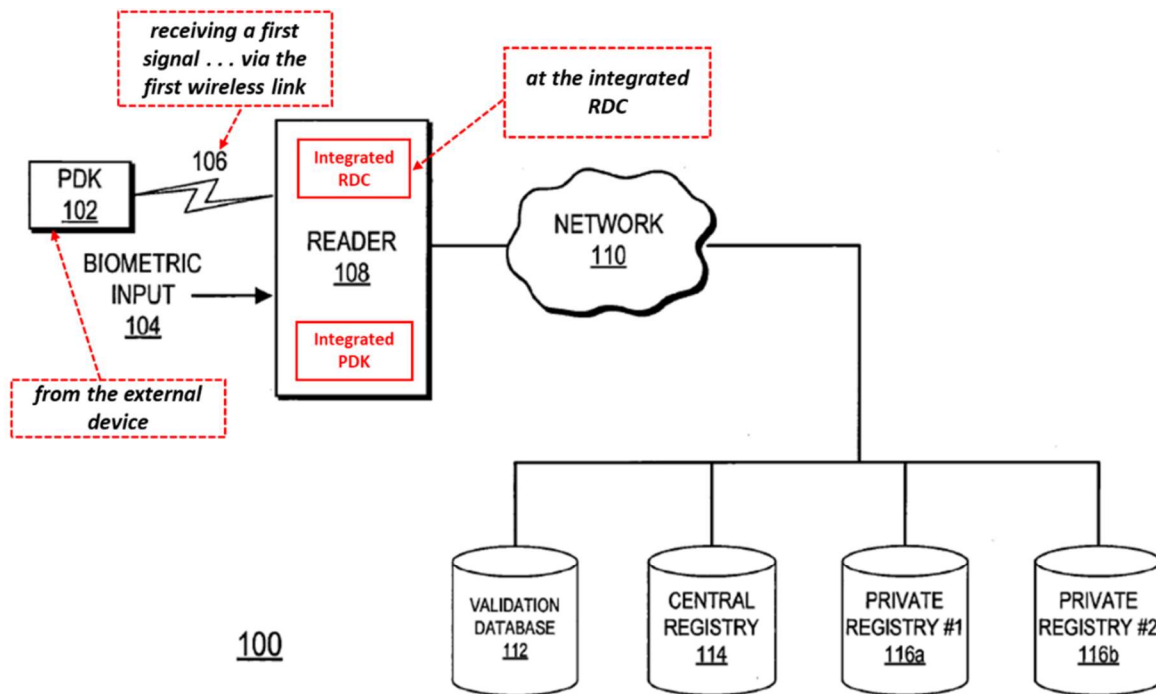
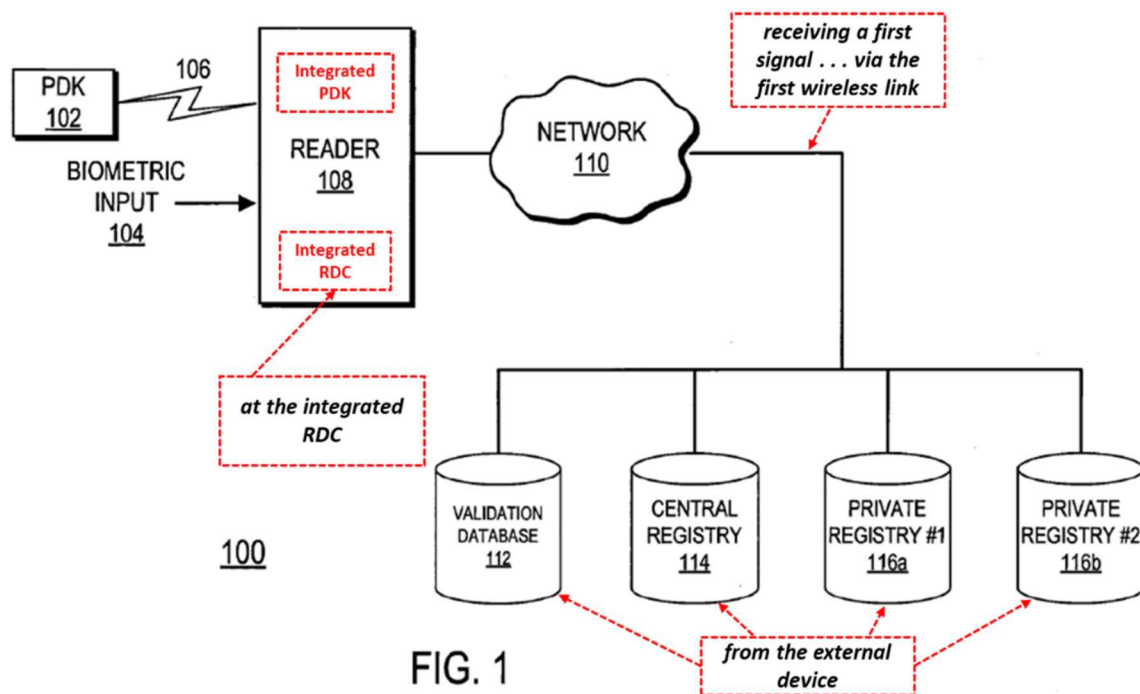


FIG. 1

MS-1005, FIG. 1.

Alternatively the RDC is further capable of being coupled to “external databases[(“*external device*”)]” by “a network 110 by either a wired or *wireless link*.” MS-1005, ¶[0026]. As discussed above, the registries of Giobbi-157 also receive PDK credentials from Reader 108’s RDC and “determine 768 if the [PDK]

status is valid 772 or invalid 770” and “returns a validation decision to the Reader 108” (“*receiving a first signal, at the integrated RDC, via the first wireless link, from the external device*”). MS-1005, ¶[0074], FIG. 7D; *see supra* [14.1]; MS-1003, ¶[93].



MS-1005, FIG. 1.

[14.3]

Grounds 1A/1B

As shown in Giobbi-157’s FIG. 4, the wireless authentication process between the PDK and RDC “completes a transaction.” MS-1005, FIG. 4. These transactions include “*enabling* access to secure physical or digital assets (e.g., unlocking a door,

opening a vault, providing access to a secured hard drive, etc.)” (“***enable[ing] one or more of an application, a function, and service***”). MS-1005, ¶[0063]. Moreover, Giobbi-139 states “access to the storage is ***enabled***/disabled by interrupting the communications path, signaling to the hosting device that the storage is either ‘ready’ or ‘busy,’ effectively ***enabling***/disabling the device itself.” MS-1006, ¶[0089]. Accordingly, a POSITA would have found it obvious that “enabling access to secure physical or digital assets” (e.g., “unlocking a door” or “opening a vault” (“***one or more of an application, a function, and service***”)) would include a generated electronic signal (“***an enablement signal***”). MS-1003, ¶[94].

Additionally, Giobbi-157 discloses a “trigger” that can be required to allow a transaction to complete or continue. MS-1005, ¶[0065]. Giobbi-157 provides an example where a “biometric contact” (“***an enablement signal***”) is provided for “biometric authentication” of a service (“***enable[ing] one or more of an application, a function, and service***”) and provides examples of triggers, to include: “the touch of a finger to a fingerprint scanner, the positioning of a face in front of a facial or retinal scanner, the receipt of a signature, the detection of a voice, the receipt of a DNA sample, RNA sample, or derivatives or any other action that permits the Reader 108 to begin acquiring the biometric input 104.” *Id.*; MS-1003, ¶[95].

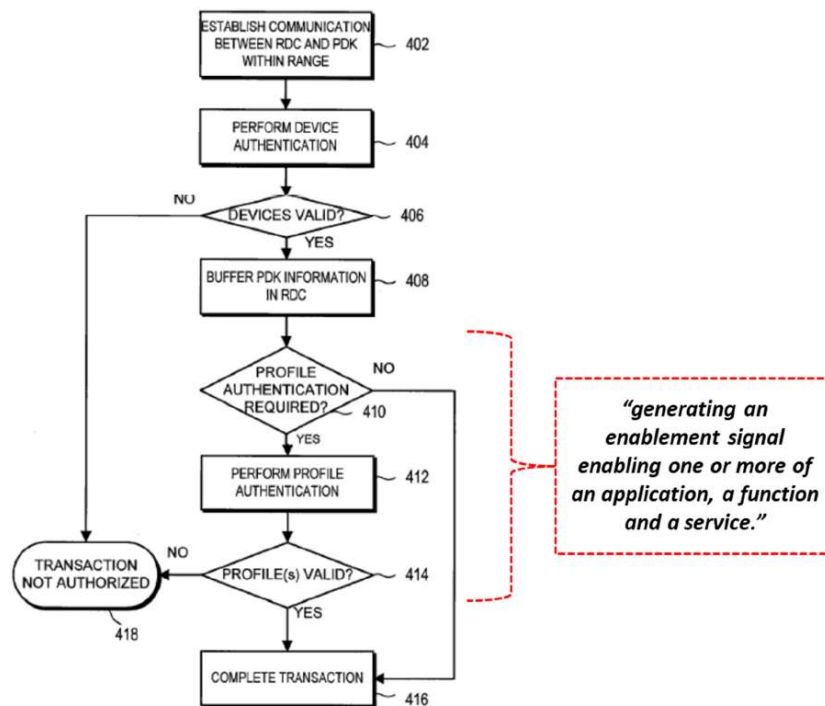


FIG. 4

MS-1005, FIGS. 4.

[16]

Grounds 1A/1B

As discussed above, Giobbi-157 discloses that authentication is first performed after a PDK has connected to an external RDC (e.g., “RDC 304” in “Reader 108”) and the “registry 114-116 [(“*external device*”)] returns a validation decision to the Reader 108” (“*sending the enablement signal ... enabled at least in part on a device external to the hybrid device and communicatively coupled to an external RDC*”). MS-1005, ¶[0074], FIGS. 3, 7D; *see supra* [14.1]-[14.3]; MS-1003, ¶[97].

Additionally, Giobbi-139 discloses and shows in FIG. 14 devices that include RDC's can “effectively enabl[e]/disabl[e] the device itself.” MS-1006, ¶[0088-0090]. Thus the PDK of the hybrid device, when brought within range of an external RDC, can “*enable[] at least in part on a device external to the hybrid device and communicatively coupled to an external RDC*” a “*application,*” “*function,*” or “*service*” on that device with “an external RDC.” MS-1003, ¶[98].

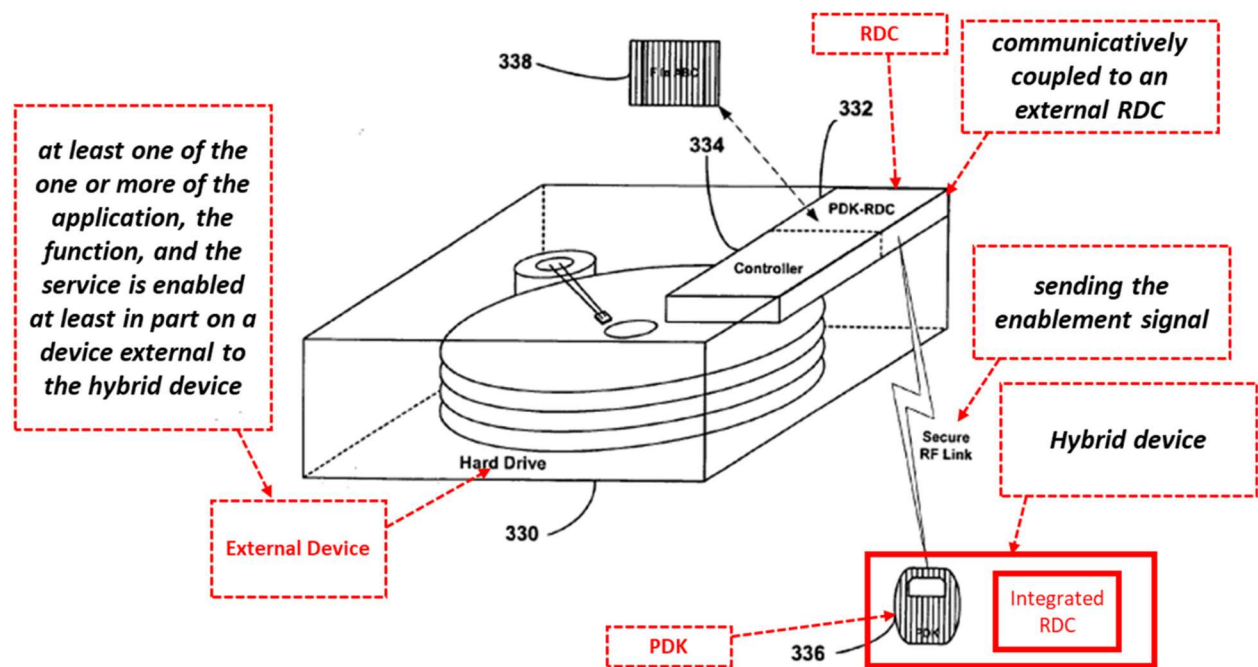


FIG. 14

MS-1006, FIG. 14.

[20]⁵

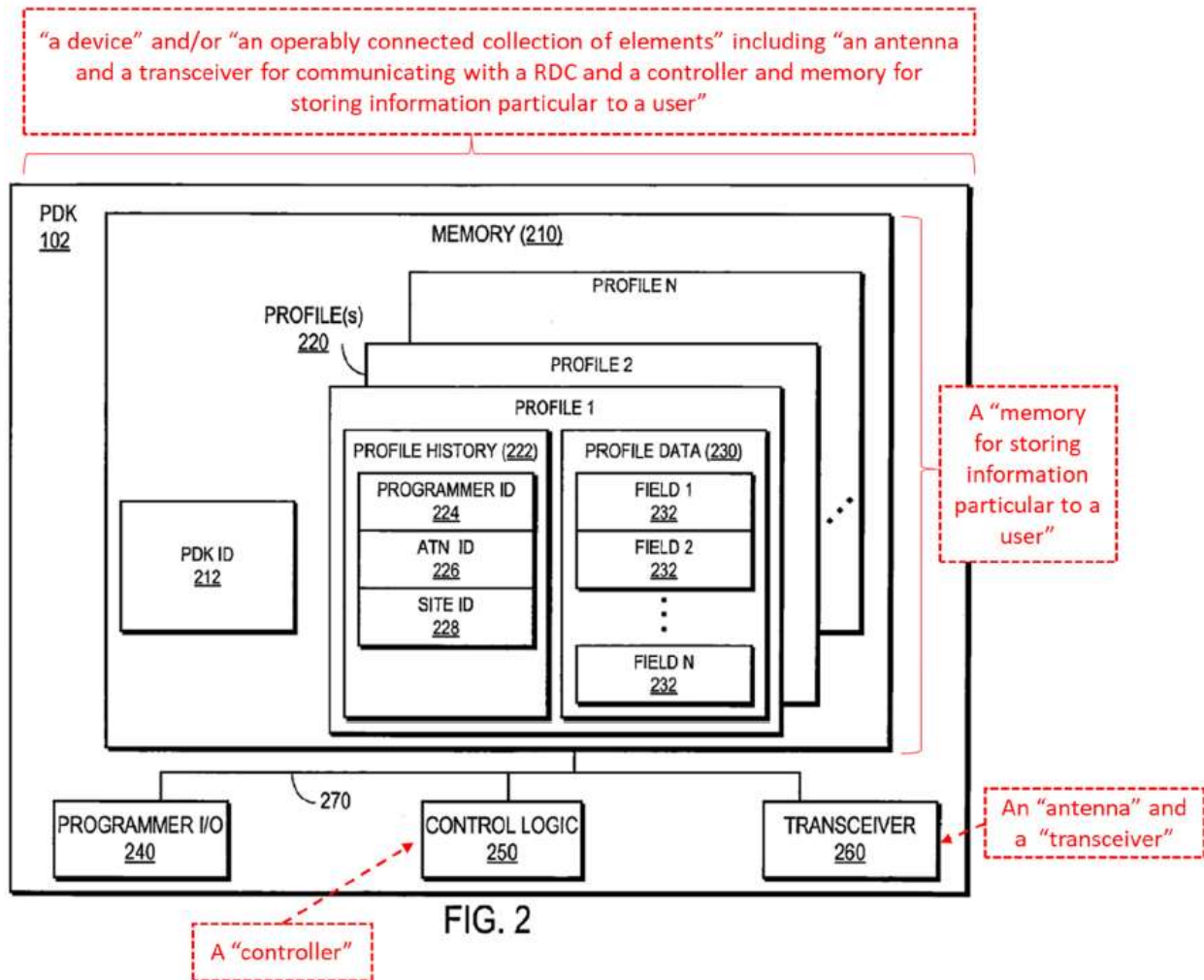
Ground 1A

Giobbi-157 discloses that PDKs can be integrated in watches and thus, a PDK external to the hybrid device (“*the external PDK*”) would have been “*included in a watch*.” MS-1005, ¶[0035]; *see supra* [12] (“*the [integrated, secure memory] is included in a watch*”); MS-1003, ¶[102].

Giobbi-157 also teaches “an operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for storing information particular to a user” as required by the above construction of a “*PDK*.” MS-1005, ¶[0035] (“an embodiment of the PDK 102 ... comprises a memory 210, a programmer I/O 240, control logic 250, and a transceiver 260, coupled by a bus 270”), FIG. 2; *see supra* I.C.2. Further, Giobbi-157 describes its transceiver in open-ended terms as a “wireless transmitter and receiver” that may utilize “electromagnetic signals.” *Id.* ¶[0047]. As Dr. Traynor explains, a

⁵ Petitioner notes that “the external PDK” in claim 20 lacks antecedent basis. For the purposes of IPR, Petitioner has analyzed this claim treating “the external PDK” as the “integrated, secure memory” of claim 14, while also showing how Grounds 1A/1B render a “PDK” obvious. Petitioner reserves the right to advance §112 arguments against this claim in litigation.

POSITA would have readily understood that antennas were commonly used with a transceiver to transmit and receive electromagnetic signals, and accordingly, that Giobbi-157 teaches using an antenna. MS-1003, ¶[103].



MS-1005, FIG. 2.

Ground 1B

It also would have been obvious to use an antenna as illustrated in the teachings of Dua, which discloses a "transceiver 108 and antenna 117 [to] provide

wireless connectivity.” MS-1008, 8:20-29; *see supra* [12] (“*the [integrated, secure memory] is included in a watch*”); MS-1003, ¶[104].

[15], [17]-[19]

Grounds [1A] and [1B] render these claims obvious in the same manner as explained above for the corresponding claims listed in the following table. MS-1003, ¶¶[96], [99]-[101].

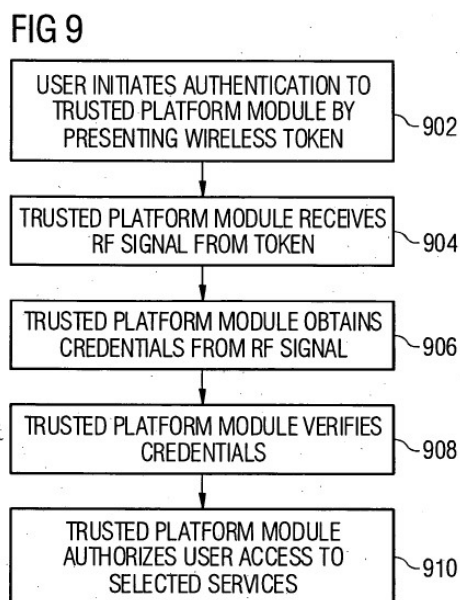
Claim	Corresponding Claim
[15]	[2]
[17]	[4]
[18]	[6]
[19]	[11]

B. [GROUND 2A] – Claims 1-8, 10-11, and 14-19 are rendered obvious by Broadcom

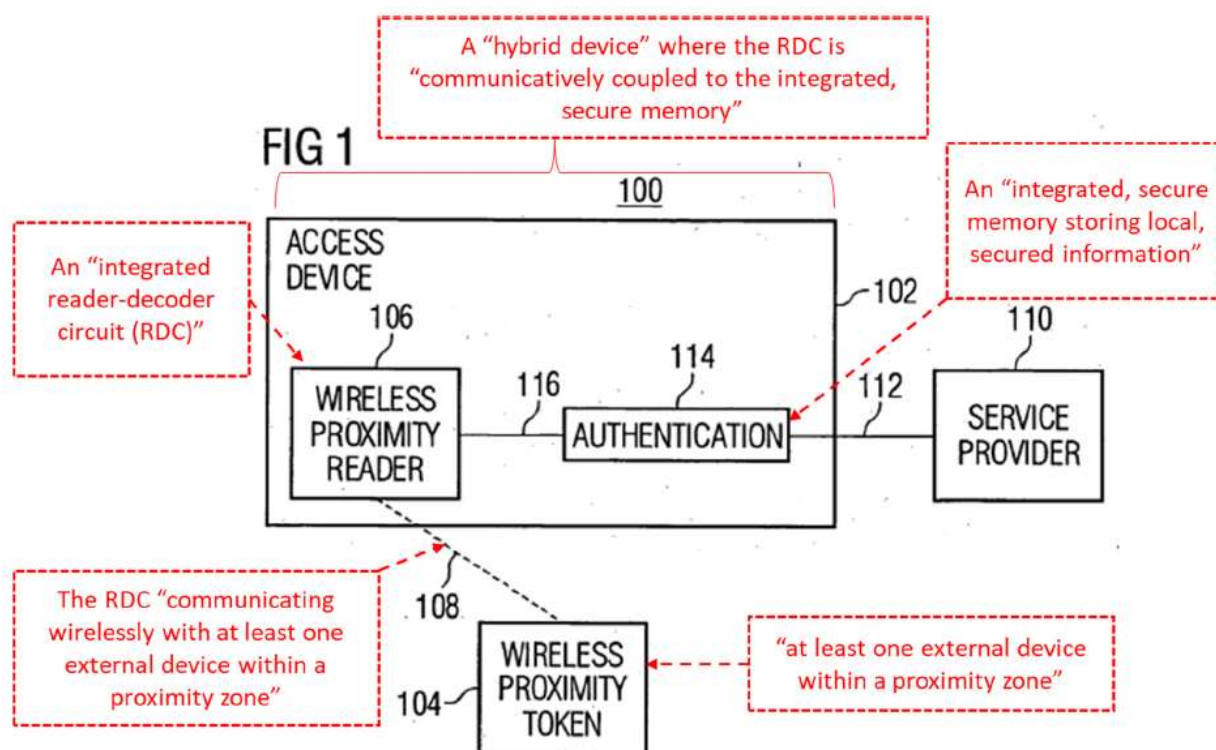
1. Overview of Broadcom

Broadcom discloses a system for secured access to a service based on a wireless device coming within the proximity of a reader. MS-1008, Abstract; ¶¶[0009]-[0016]. Broadcom teaches that a user’s credentials can be stored on an RFID token, and this token and the associated authentication credentials may be read by an RFID reader located in an Access Device. *Id.* The Access Device (including

the RFID reader) can authenticate the RFID token and permit access to the secured service after authentication. *Id.*; MS-1003, ¶¶105].



MS-1008, FIG. 9.



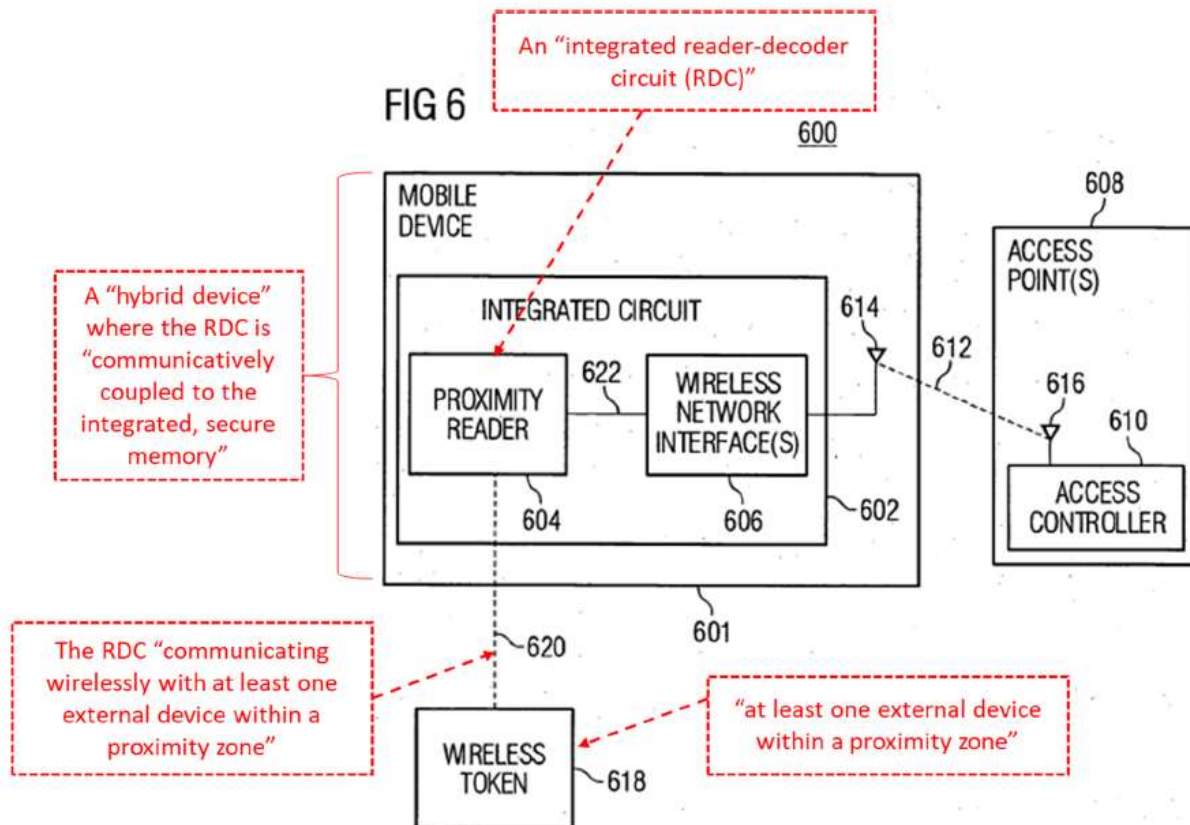
MS-1008, FIG. 1 (annotated).

The authentication information is stored securely within memory that is “tamper resistant,” and “is not exposed in the mobile device.” MS-1008, ¶¶[0013], [0134], [0167], [0187]. The “authentication information” and “credentials” are secured in this memory. MS-1008, ¶¶[0013], [0134], [0167], [0187], [0192]; MS-1003, ¶[106].

As shown in the figure, Access Device 102 requests access to a service provider 110 and “verif[ies] that the information sent from the token 104 includes a credential associated with an authorized user and or access device.” MS-1008, ¶¶[0113]-[0119]. In some instances, “the user may be asked to input a password and/or provide a biometric (e.g., a fingerprint) to a biometric reader to further verify the authenticity of the user.” MS-1008, ¶¶[0114]-[0115], [0181]. This input can be the presentation of a token to the reader. MS-1008, ¶¶[0130], [0181]. Example tokens include: “smart cards, credit cards, dongles, badges, biometric devices such as fingerprint readers, mobile devices such as cellular telephones, PDAs, etc.” MS-1008, ¶¶[0130], [0181]; MS-1003, ¶[107].

Additionally, Broadcom discloses enabling “computer functions to be securely executed” via this method. MS-1008, ¶¶[0177]-[0180], [0184]-[0186]. The authentication of the device and the “user may then be allowed to access the secured service.” MS-1008, ¶[0010]; MS-1003, ¶[108].

Broadcom discloses that the Access Device 102 can be a mobile phone which facilitates access to an access point for mobile communications, as illustrated below in FIG 6. MS-1008, ¶¶[0123]-[0124], [0191]; MS-1003, ¶[109].



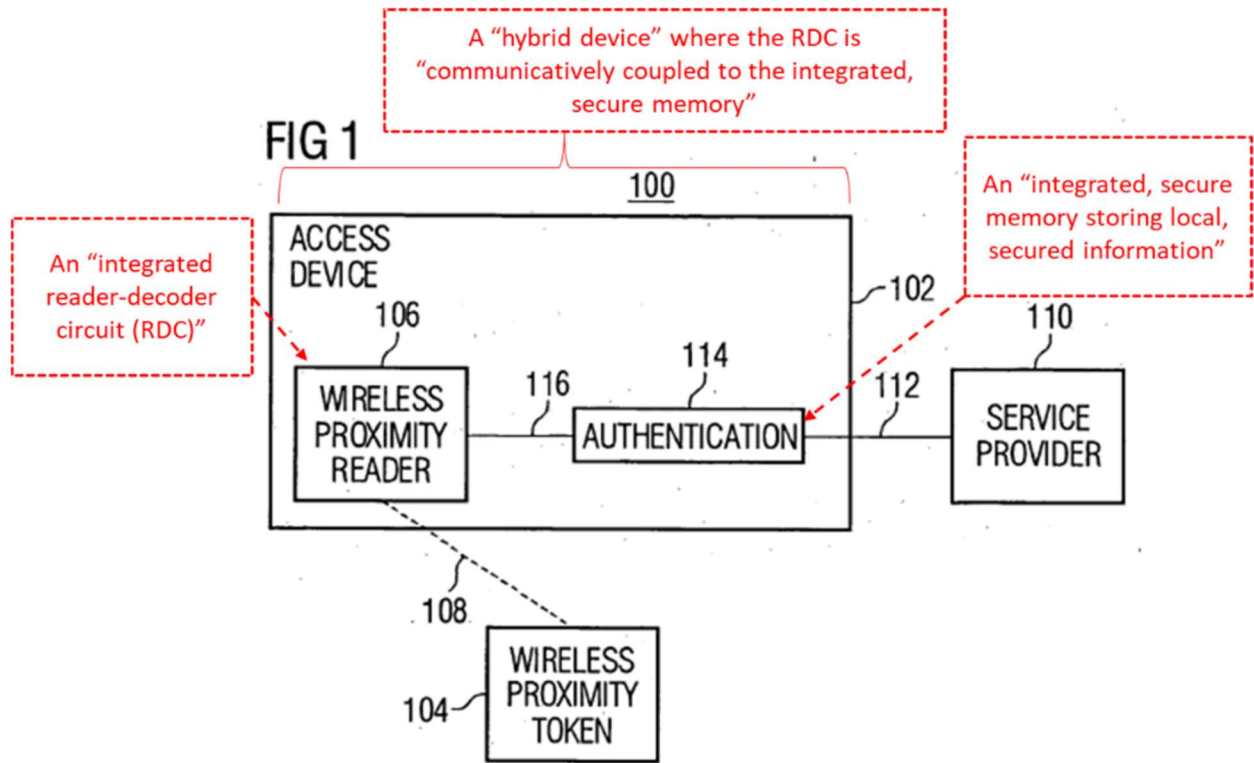
MS-1008, FIG. 6 (annotated).

2. Analysis

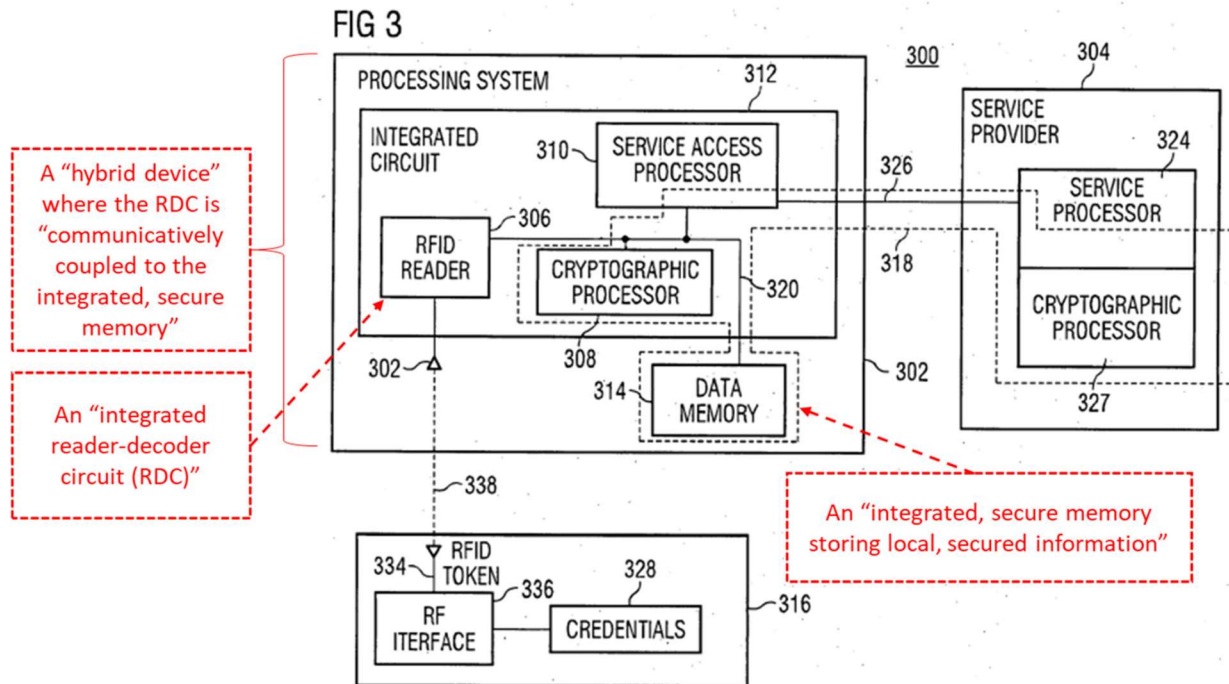
[1.pre]

To the extent the preamble is limiting, Broadcom discloses a “*hybrid device*,” (“a device comprising an integrated, secure memory storing local, secured information and an integrated receiver-decoder circuit” or “a device comprising an

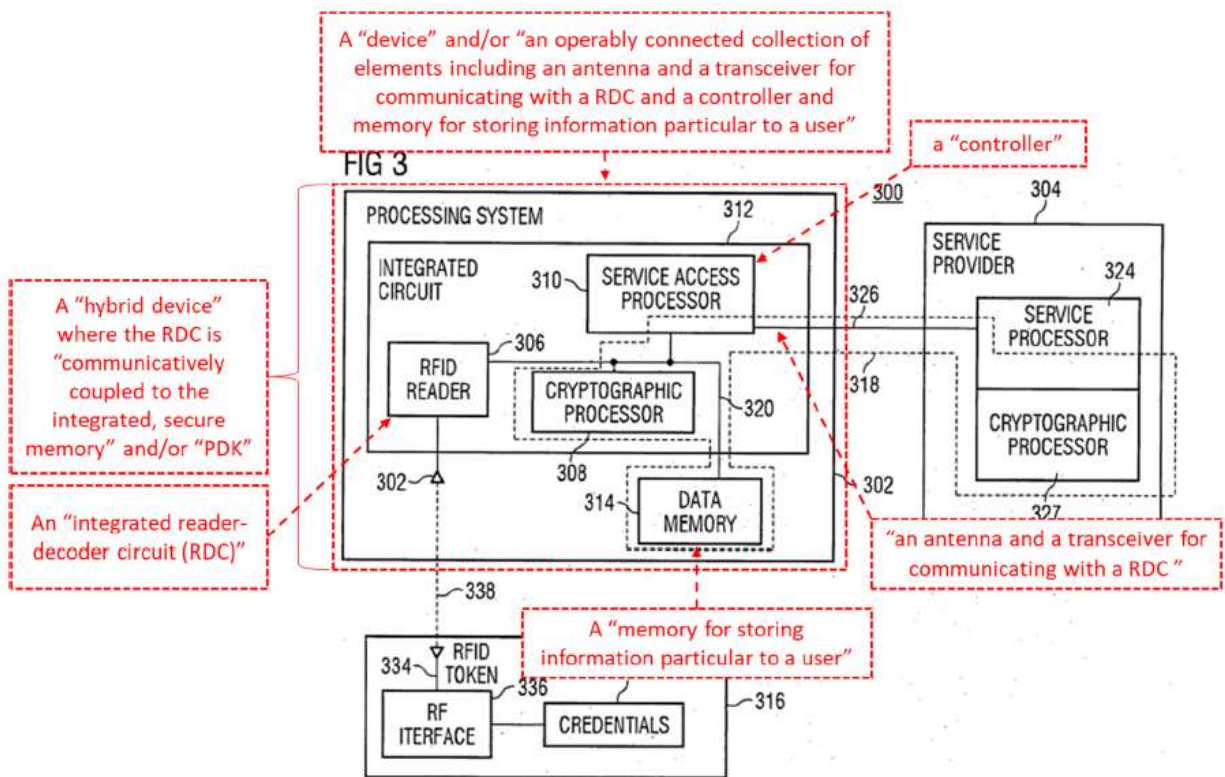
integrated personal digital key (PDK) and an integrated receiver-decoder circuit”). MS-1008, ¶¶[0110]-[0119], FIGS. 1, 6, MS-1003, ¶[110]; *see supra* §I.C.1-3. Broadcom’s “access device 102” reads credentials stored on a “wireless proximity token 104,” using a “wireless proximity reader 106” (“an integrated reader-decoder circuit (RDC)”). MS-1008, ¶¶[0110]-[0119], FIGS. 1, 6. Broadcom also discloses that “the information provided by the token may be maintained within the access device 102 in a secure manner” using an “authentication component 114” (and an “integrated circuit 312” and “data memory 314” disclosed in FIG. 3) (an “integrated, secure memory storing local, secured information” and an “integrated personal digital key (PDK)”). MS-1008, ¶¶[0116]-[0118], [0135]-[0137], FIGS. 1, 3. Additionally, Broadcom’s access device 102 can be a “mobile device,” such as a “cellular phone.” MS-1008, ¶¶[0125], [0130], [0162]-[0163], [0195], FIGS. 1, 3, 6. Accordingly, Broadcom renders obvious “a device comprising an integrated, secure memory storing local, secured information and an integrated [RDC]” and “a device comprising an integrated personal digital key (PDK) and an integrated [RDC]” for the reasons discussed above. *See supra*, §§I.C.1-3, III.B.1; MS-1003, ¶[110]. As shown below in FIGS. 1 and 3, Broadcom’s cell phone includes an integrated, secure memory storing local, secured information and an integrated RDC (a “*hybrid device*”). *Id.*



MS-1008, FIG. 1.



MS-1008, FIG. 3⁶.



MS-1008, FIG. 3.

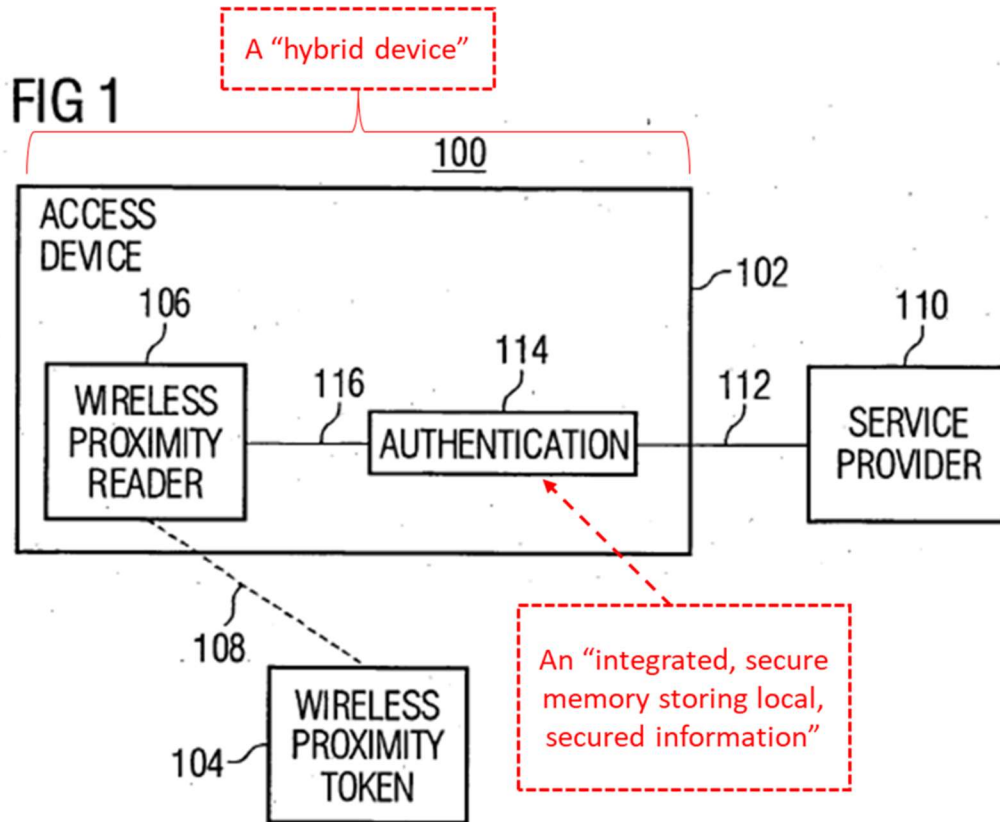
Additionally, it would have been obvious to a POSITA to include the PDK components (“an antenna ... a transceiver for communicating with a RDC and a

⁶ Broadcom discloses that FIG 3 illustrates “additional details of proximity-based authentication” (e.g., the embodiment illustrated in FIG. 1). MS-1008, ¶[0131]. It would have also been obvious to a POSITA to turn to Broadcom’s more detailed figures (e.g., FIGS. 3 and 6) for implementation details for creating the hybrid devices generally described by Broadcom in FIG. 1. MS-1003, ¶[110].

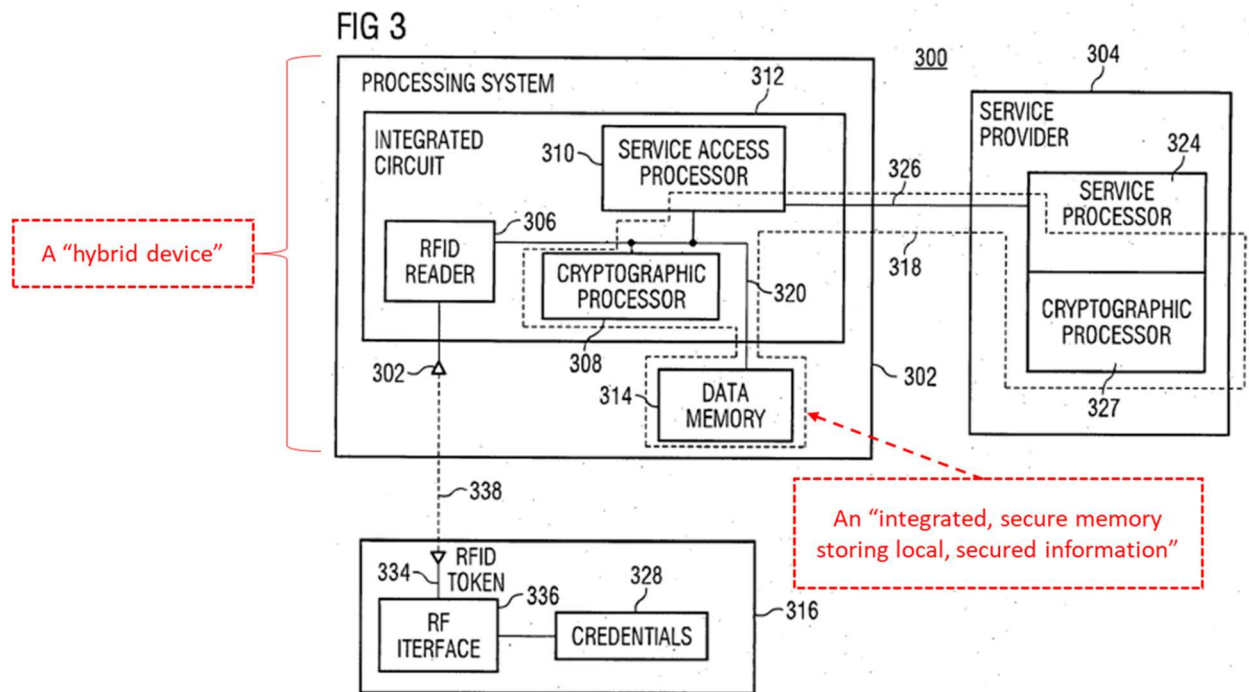
controller and memory ...) in the same device, and to have these components be “operably connected.” MS-1003, ¶[110]. For example, as discussed above in Ground 1A/1B, the integration of a PDK into a single device (e.g., a cellphone) is convenient for a user and negates the need to carry multiple devices. *See supra*, §III.A.3; MS-1003, ¶[110].

[1.1]

Broadcom’s “authentication component 114” stores information locally on the access device 102 and is “cryptographically secured” (“*an integrated, secure memory*”). MS-1008, ¶¶[0116]-[0118], FIG. 1. Additionally, Broadcom discloses an “integrated circuit 312” and a “data memory 314” (“*an integrated, secure memory*”) to store encrypted keys used for authentication (“*local, secured information*”). MS-1008, ¶¶[0135]-[0137], FIG. 3. FIGS. 1 and 3 below illustrate these components within Broadcom’s access device (“*an integrated, secure memory*”), which can be a “a personal computer, a server, a cellular phone, a personal data assistant (“PDA”). MS-1008, ¶[0125], FIGS. 1, 3; MS-1003, ¶[111].



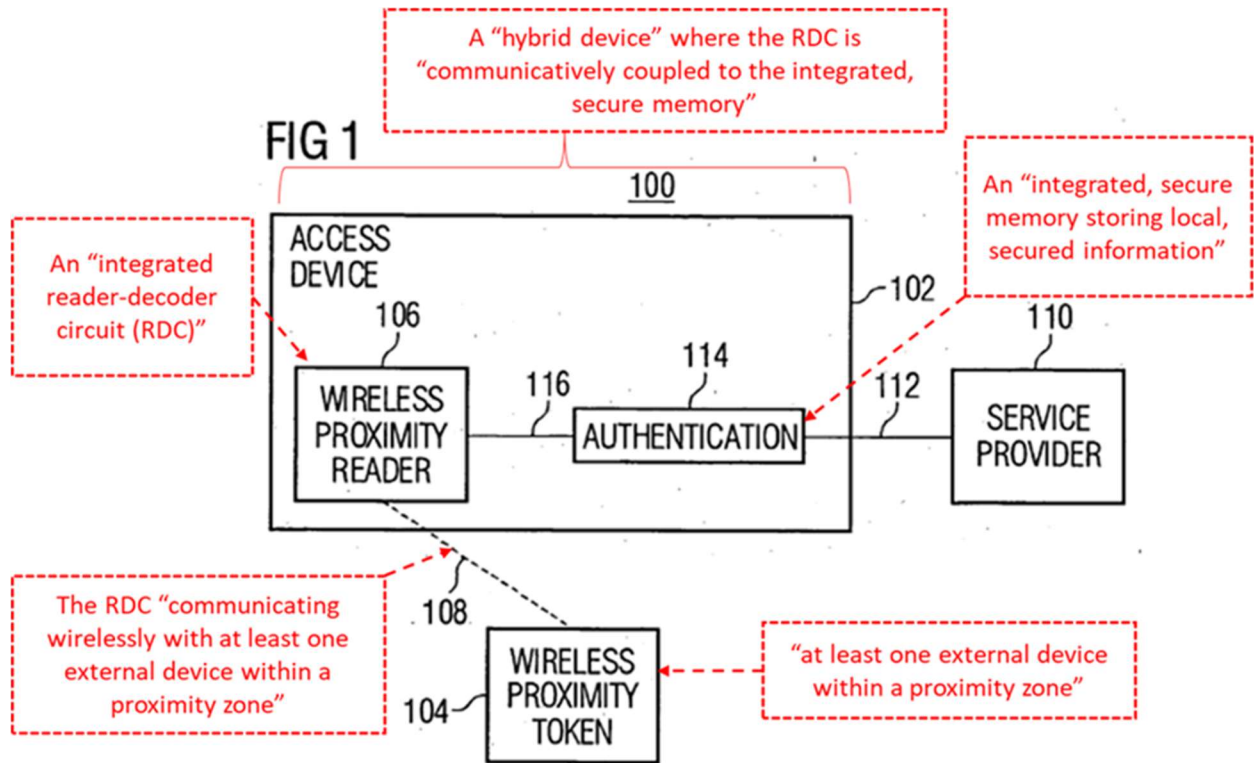
MS-1008, FIG. 1.



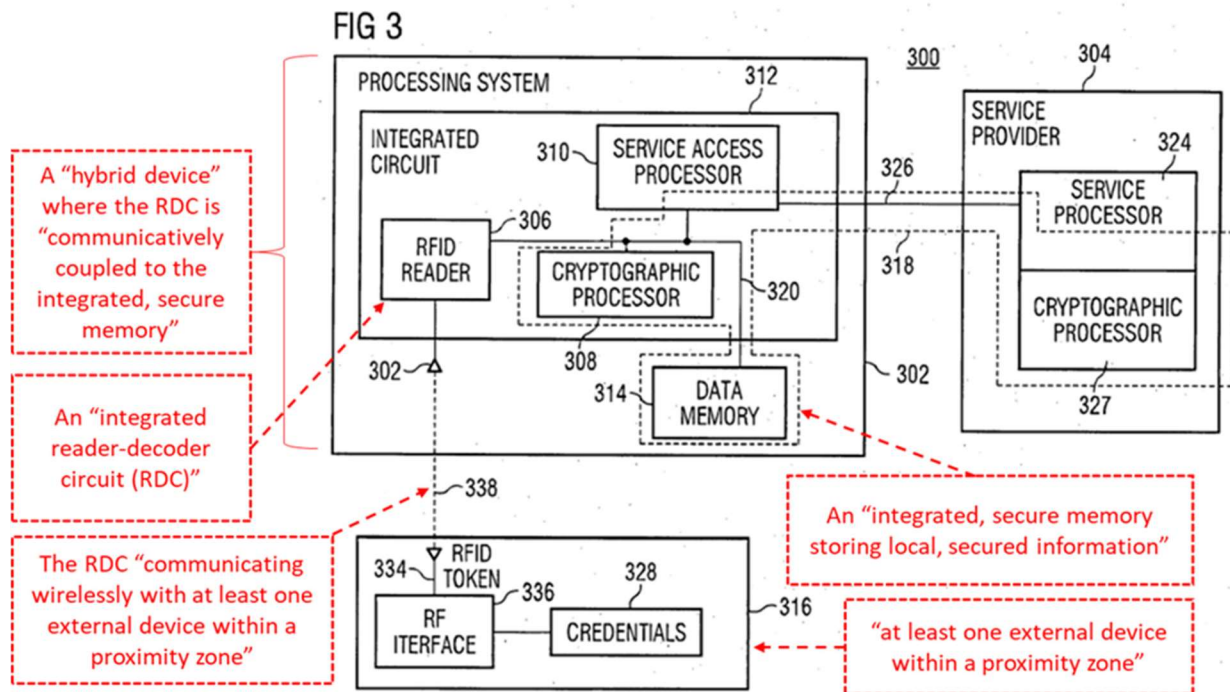
MS-1008, FIG. 3.

[1.2]

Broadcom discloses that its access device 102 includes a “wireless proximity reader 106” (“*an integrated reader-decoder circuit (RDC)*”) to “receive signals 108” (“*for communicating wirelessly*”) from a “wireless proximity token 104” (“*at least one external device*”) that is “proximate to the access device 102” (“*within a proximity zone*”). MS-1008, ¶¶[0110]-[0119], FIGS. 1, 6; MS-1003, ¶[112]. Additionally, Broadcom discloses that “information may only pass between the reader 106 and the authentication component 114 via a connection 116” (“*the integrated RDC communicatively coupled to the integrated, secure memory for communication with the integrated, secure memory*”). MS-1005, ¶[0116]. Additionally, Broadcom discloses, as part of its detailed FIG. 3 view, an “RFID reader 306” (“*integrated RDC*”) that is connected to a “data memory 314” via a “data bus 320” (“*the integrated RDC communicatively coupled to the integrated, secure memory for communication with the integrated, secure memory*”). MS-1008, ¶¶[0133]-[0137], FIG. 3. Accordingly, Broadcom discloses “a component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing” as required by the district court’s construction for an “*integrated reader-decoder circuit (RDC)*.” *See supra*, §§I.C.3, III.B.1; MS-1003, ¶[112].



MS-1008, FIG. 1.



MS-1008, FIG. 3.

[1.3]

Broadcom discloses that “the access device 102 may automatically request a predefined service once the user places the token 104 (*“at least one external device”*) proximate the access device 102” using “a wireless proximity reader 106 [*“integrated RDC”*]... configured to receive signals 108 (e.g., RF signals) from the wireless proximity token 104” (*“the integrated RDC communicating wirelessly with the at least one external device within the proximity zone”*). MS-1008, ¶¶[0111]-[0117]. After the token 104 has been brought within the proximity zone of the reader 106, “the service provider 110⁷ may then enable access to the requested service” (*“enables one or more of an application, a function, and a service”*). MS-1008, ¶[0119]. Broadcom also discloses that “the authentication component 114 may be in secure communication with the service provider 110” (*“the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and a service”*). MS-1008, ¶[0117]. More generally, Broadcom discloses a “method for providing access to a secured service based on a user's proximity to a proximity reader. Once the proximity is authenticated the user

⁷ Broadcom discloses that the “service provider” can be located “local or remote with respect to the entity requesting service (e.g., access device 102).” MS-1008, ¶¶[0123]-[0125].

may then be allowed to access the secured service” (“*one or more of an application, a function, and a service*”). MS-1008, ¶[0010]. Broadcom notes that “the term service 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.” MS-1008, ¶[0120]; MS-1003, ¶[113].

[2]

Broadcom discloses various functions, applications, and services that can be enabled on the access device 102. MS-1008, ¶[0120]; MS-1003, ¶[114]. For example, Broadcom teaches that “network access may only be provided to [a] mobile device [(an access device (“*hybrid device*”)))] when a token is proximate to the mobile device and when that token has been assigned to an authorized user of that mobile device and the network(s).” MS-1008, ¶[0016]; MS-1003, ¶[115].

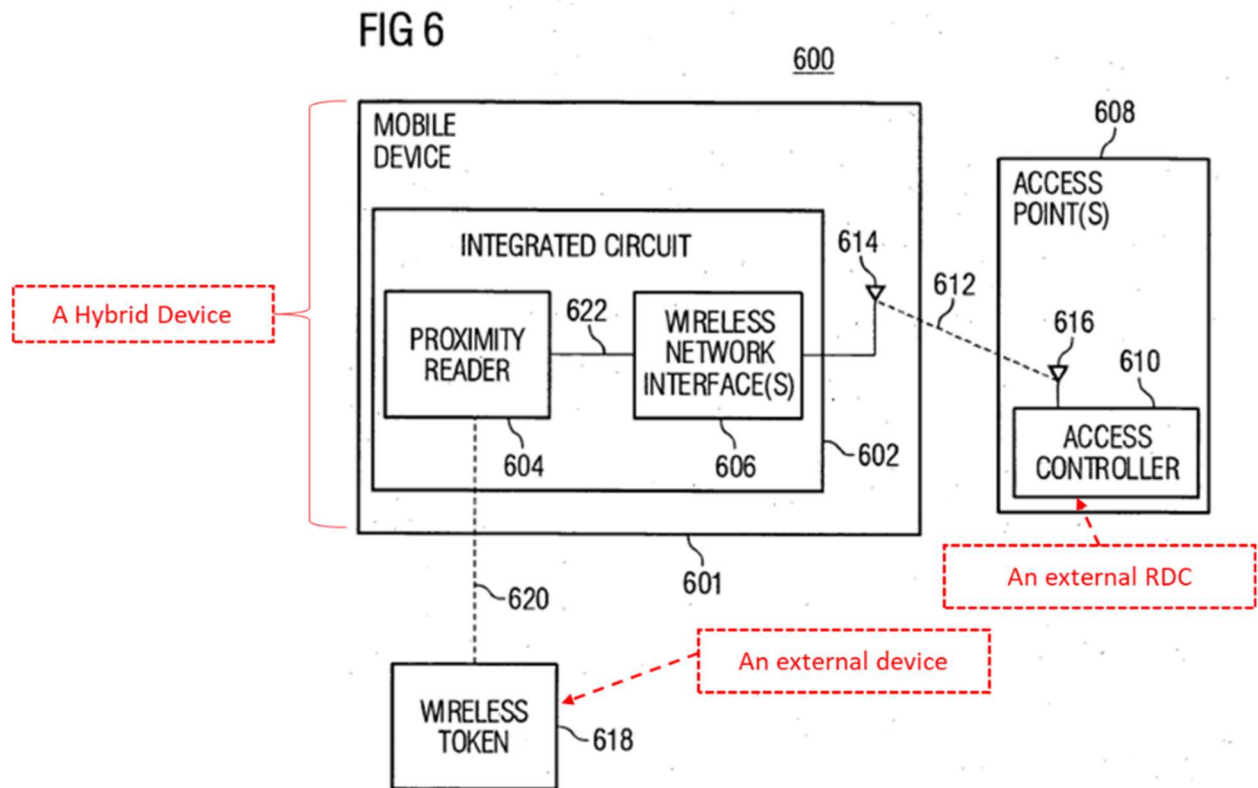
Moreover, Broadcom discloses that the “authentication component 114 and the service provider 110 on the same integrated circuit” (e.g., on the same access device (“*hybrid device*”), such that “*one or more of the application, the function, and the service is enabled, at least in part, on the hybrid device*”). MS-1008,

¶[0117], [0119] (“the service provider 110 may then enable access to the requested service”); *see supra* [1.3]; MS-1003, ¶[116].

[3]

Broadcom discloses that the access device 102 (in the form of a “mobile device 601”) can access a network via an “access controller 610” (“*external RDC*”) in an external “access point(s) 608” (“*the hybrid device communicatively coupled to wirelessly communicate with the external RDC*”) by “perform[ing] network authentication and connection processing to enable communication with a given wireless network” (“*the one or more of the application, the function, and the service is enabled, at least in part, external to the hybrid device using an external RDC*”). MS-1008, ¶¶[0163]-[0165], FIG. 6; *see supra* [1.3]; MS-1003, ¶[117].

A POSITA would have found it obvious that the Access Controller 610 performs a similar function to the proximity reader 604 because Broadcom discloses that these components receive and transmit similar Radio Frequency (RF) signals, have similar security measures, and perform similar enabling functions. MS-1003, ¶[118]; MS-1008, ¶¶[0163]-[0168].



MS-1008, FIG. 6.

[4]

Broadcom discloses that a biometric characteristic can be used to authenticate a user:

Typically, access to the service will be initiated by the user's interaction with the access device 102 ... the user may be asked to input a password and/or provide a biometric (e.g., a fingerprint) to a biometric reader to further verify the authenticity of the user (*“biometric information for authenticating a user”*).

MS-1008, ¶[0114], *see also* ¶¶[0130], [0181]. Biometric information can be embodied in a “token” (*“local, secured information”*) and this token information

can be stored on the “authentication component 114” and/or “data memory 314.” MS-1008, ¶¶[0118], [0130], [0148], [135]; MS-1003, ¶[119].

Further, Broadcom’s explicitly teaches “a user’s credentials [] stored on an RFID token,” and “authorization information is stored on the token 816.” MS-1008, ¶¶ [0012], [0118]. MS-1008, ¶[0158]. From this disclosure, a POSITA would have found it obvious that a storage device (e.g., the authentication component 114 or token 104) includes memory to securely store “credentials” and “authorization information.” MS-1003, ¶[120].

[5]

See supra, [4]; MS-1003, ¶[121].

[6]

Broadcom discloses that token information stored on the “authentication component 114” and/or “data memory 314” includes “credit cards” (“***the local, secure information includes financial information***”). MS-1008, ¶[0130], *see also* ¶¶[0008], [0129], [0193], [0195]. The tokens in Broadcom can “provide the user’s credit card information” to a computer system to “perform a sales transaction” (“***at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information***”). MS-1008, ¶¶[0193]-[0196]; MS-1003, ¶[122].

[7]

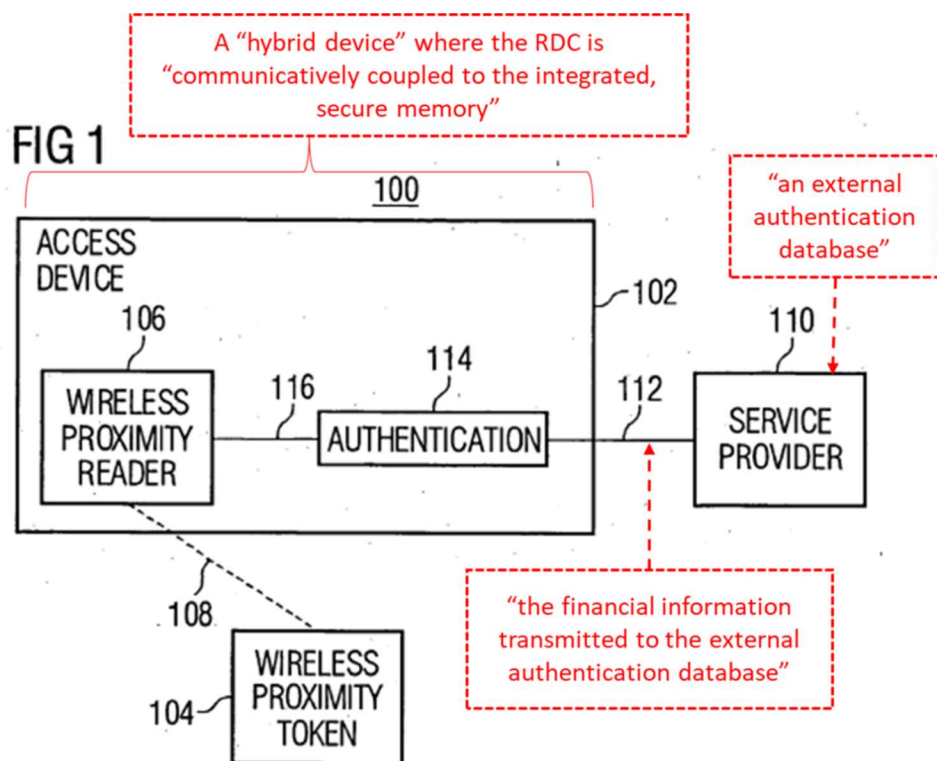
As discussed above in [6], token information stored on the “authentication component 114” and/or “data memory 314” includes “credit cards” (“*the local, secure information includes financial information*”) and tokens in Broadcom can “provide the user's credit card information” to a computer system to “perform a sales transaction” (“*at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information*”). MS-1008, ¶¶[0130], [0193]-[0196]; *see supra* [6]; MS-1003, ¶[123].

Also recall that “the access device 102 may automatically request a predefined service once the user places the token 104 (“*at least one external device*”) proximate the access device 102” using “a wireless proximity reader 106 [(“*integrated RDC*”)]... configured to receive signals 108 (e.g., RF signals) from the wireless proximity token 104” (“*a signal received from the at least one external device by the integrated RDC*”). MS-1008, ¶¶[0111]-[0117]; *see supra* [1.3]. Accordingly, Broadcom’s access device “*completes a financial transaction based on a signal received from the at least one external device by the integrated RDC.*” MS-1008, ¶¶[0111]-[0117], [0130], [0193]-[0196]; *see supra* [1.3], [6]; MS-1003, ¶[124].

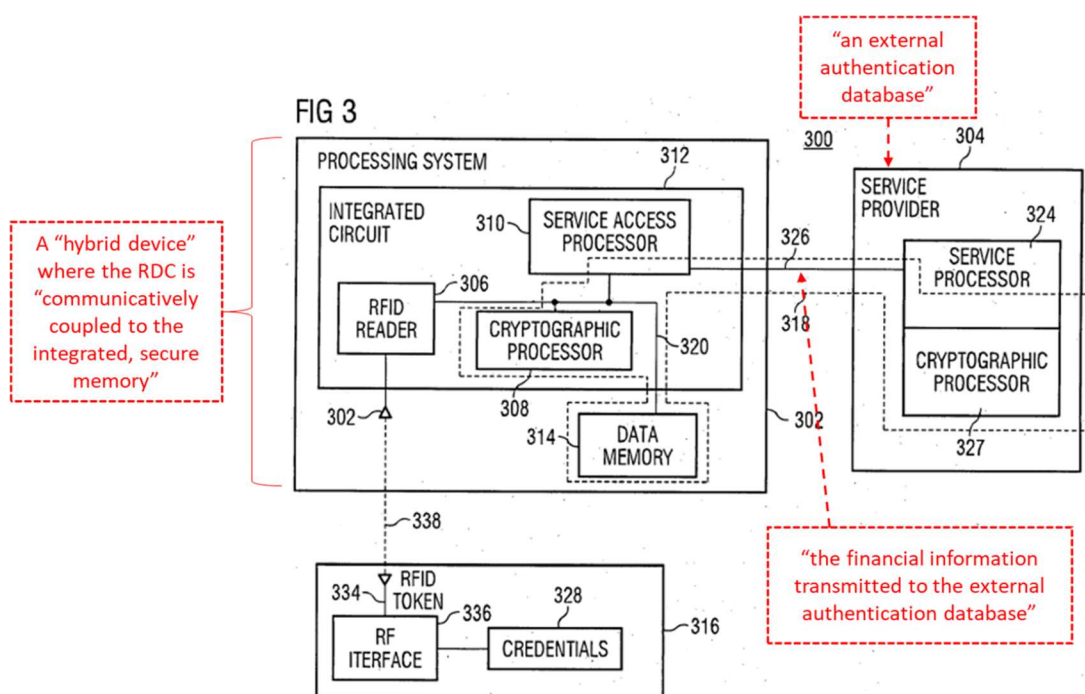
[8]

Broadcom discloses that examples of service providers 110 include a “processing system that processes requests for service, verifies whether the requester

is authorized to access the service and provides or facilitates the requested access” (a “*database*”). MS-1008, ¶[0123]. Broadcom discloses that when “a token associated with default services approaches the access device 102, the access device 102 may automatically request the services from the service provider 110” (“*an external authentication database*”), which then “enable[s] access to the requested service” (“*the service enabled completes a financial transaction based on an authorization of the financial information using an external authentication database*”). MS-1008, ¶¶[0115]-[0116], [0119]. *See also supra* [7] *and infra* [10]. Broadcom discloses that authentication information is sent to the service provider (“*the financial information transmitted to the external authentication database*”). MS-1008, ¶[0118]. Broadcom also discloses a “service provider 304” in its detailed FIG. 3 illustration that performs similar functions. MS-1008, ¶¶[0136], [0138], [0141]; MS-1003, ¶[125].



MS-1008, FIG. 1.



MS-1008, FIG. 3.

[10]

Broadcom discloses that its techniques include multiple “services” (“*a first*” and “*a second application, function or service*”) and “tokens,” which each can have “multiple sets of information ... to enable a user to access different services” (“*first*” and “*second subsets of local, secured information stored by the integrated, secure memory ... having different accessibility*”). MS-1008, ¶[0127]; MS-1003, ¶[126].

For example, Broadcom discloses different examples of services enabled by tokens, to include “access[ing] a webpage” (“*a first application, function or service based on a first subsets of local, secured information*”) and “perform[ing] a sales transaction” (“*a second application, function or service based on a second subset of local, secured information*”). MS-1008, ¶¶[0120], [0193]. A POSITA would have recognized or found it obvious that these two services (and many of the different services disclosed in Broadcom) would have had “*different accessibility*.” MS-1003, ¶[127]. Accordingly, as Dr. Traynor describes, “a POSITA would have recognized the need for compartmentalization in information storage, particularly because Broadcom advertises to a POSITA that its techniques can be applied to such a large variety of usage scenarios.” MS-1008, ¶¶[0120], [0193]; MS-1003, ¶[127].

[11]

See supra [1.pre]; MS-1003, ¶[128].

[14.pre]

See supra [1.pre]. Broadcom discloses that its techniques can be embodied in a “method.” MS-1008, ¶¶[0009]-[0010]; MS-1003, ¶[129].

[14.1]

Broadcom discloses that “the access device 102 may automatically request a predefined service once the user places the token 104 [(“*external device*”)] proximate the access device 102” using “a wireless proximity reader 106 ... configured to receive signals 108 (e.g., RF signals) from the wireless proximity token 104” (“*creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external device*”). MS-1008, ¶¶[0111]-[0117]; *see supra* [1.3]. As discussed above, the Broadcom’s hybrid device includes both an “*an integrated, secure memory*” that “*stores local, secured information*” and an “*integrated RDC.*” MS-1008, ¶¶[0116]-[0119], [0135]-[0137], FIGS. 1, 3; *see supra* [1.1]-[1.2]; MS-1003, ¶[130].

[14.2]

As discussed above in [14.1], Broadcom’s wireless proximity reader 106 is “configured to receive signals 108 (e.g., RF signals) (“*receiving a first signal, at the integrated RDC, via the first wireless link*”) from the wireless proximity token 104” (“*from the external device*”). MS-1008, ¶[0111]; *see supra* [14.1]; MS-1003, ¶[131].

[14.3]

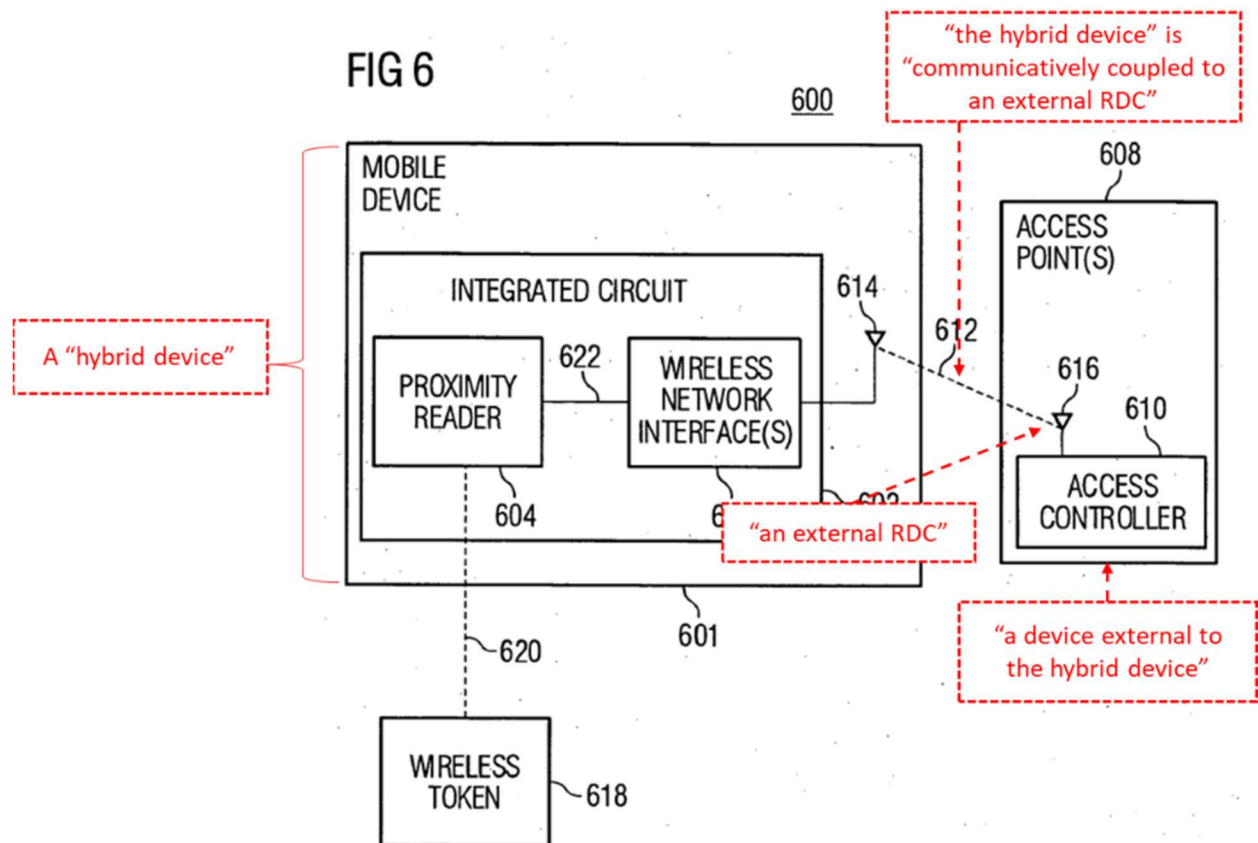
Broadcom discloses that the access device 102 sends “authentication-related information to the service provider 110 to indicate that the token 104 is proximate to the access device 102,” which then “enable[s] access to the requested service (block 208)” (“**generating an enablement signal enabling one or more of an application, a function and a service**”). MS-1008, ¶[0116]-[0119]; *see supra* [1.3]; MS-1003, ¶[132].

[16]

As discussed above, Broadcom discloses that authentication is performed after a token 104 is proximate to the proximity reader 106 of the access device 102 and the service provider 110 (“**a device external to the hybrid device**”) returns an authentication decision to the access device 102 (“**sending the enablement signal ... enabled at least in part on a device external to the hybrid device**”). MS-1008, ¶[0116]-[0119]; *see supra* [1.3], [14.1]-[14.3]. Recall that the service provider 110 “enable[s] access to the requested service” (“**the application, the function, and the service is enabled at least in part on a device external to the hybrid device**”). MS-1008, ¶[0119]; *see supra* [1.3]; MS-1003, ¶[134].

Additionally, Broadcom discloses an embodiment where the service provider 110 is replaced by a wireless “access point 608” which includes an “access controller 610.” MS-1008, ¶¶[0163]-[0168], FIG. 6. In this embodiment, access to the network

(“the one or more of the application, the function, and the service”) is enabled by “communicating with a respective access controller 610 [(“a device external to the hybrid device”)] in [the] access point(s) 608 via RF signals 612 transmitted and received via one or more antennas 614 and 616” (“the hybrid device and communicatively coupled to an external RDC”). MS-1008, ¶[0165]; MS-1003, ¶[135].



MS-1008, FIG. 6.

[15], [17]-[19]

Grounds [2A] renders these claims obvious in the same manner as explained above for the corresponding claims listed in the following table. MS-1003, ¶¶[133], [136]-[138].

Claim	Corresponding Claim
[15]	[2]
[17]	[4]
[18]	[6]
[19]	[11]

C. [GROUND 2B] – Claims 1-20 are rendered obvious by Broadcom and Giobbi-157

1. The combination of Broadcom and Giobbi-157

Giobbi-157 provides additional implementation examples for Broadcom’s system

Broadcom discloses that “tokens” (e.g., external devices that can interface with an RDC) can be implemented in a large variety of personal devices and objects. MS-1008, ¶[0139]. To the extent that it would not have been obvious in view of Broadcom’s disclosure alone to include tokens in “jewelry” and “watches,” Giobbi-157 discloses such implementations. MS-1005, ¶[0035]. Indeed, Giobbi-157’s PDKs can be implemented into many of the same devices that can

include tokens, as taught by Broadcom (e.g., a “Personal Digital Assistant (PDA)”). MS-1005, ¶[0035]; MS-1008, ¶[0139]. Accordingly, a POSITA would have recognized or found it obvious that the additional devices taught by Giobbi-157 would have also been capable of containing the tokens of Broadcom’s system. MS-1003, ¶[139].

Additionally, Giobbi-157 provides additional implementation details for Broadcom’s service providers. MS-1005, ¶¶[0032]-[0034], [0053], [0074], Claim 8; MS-1008, ¶¶[0115]-[0116], [0119]. For example, to extent it would not have been obvious in view of Broadcom’s disclosure alone, Giobbi-157 informs a POSITA that external databases can be separate from the PDKs and RDCs in a transaction. MS-1005, ¶¶[0032]-[0034], [0053], [0074], Claim 8; *see supra* [3], [6]-[8]. As Dr. Traynor explains, a POSITA would have recognized or found it obvious that certain transactions would benefit from a separate authentication service (e.g., obtaining authorization from a bank or creditor, an impartial verification service or notary, a government institution, etc.). MS-1003, ¶[140].

Combining Broadcom and Giobbi-157 would have involved (1) combining prior art elements according to known methods to yield predictable results; (2) use of a known technique to improve similar devices (methods, or products) in the same way; and (3) applying a known technique to a known device ready for improvement

to yield predictable results. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421, 82 USPQ2d 1385, 1395-97 (2007); MPEP 2143; MS-1003, ¶[141].

Specifically, a POSITA would have been motivated to integrate Giobbi-157's teachings into Broadcom's access device by recognizing that (i) Broadcom and Giobbi-157 are directed to similar operations having similar purposes (e.g., "provide efficient, secure, and highly reliable authentication for ... access control applications" and "protect[ing] any data stored on such devices"; (ii) Broadcom and Giobbi-157 describe similar structures for performing those operations (e.g., PDK and RDCs); (iii) combining the techniques of Broadcom and Giobbi-157 would have worked in the same manner already described in the references. MS-1005, ¶[0011]; MS-1008, ¶¶[0113]-[0119]; MS-1003, ¶[142].

2. Analysis

[9]

Giobbi-157 discloses multiple registries that can be used to authenticate a user (e.g., the Central Registry 114, any private registry 116, or other validation database 112) (each "***external authentication database[s]***"). MS-1005, ¶[0074]; FIG. 1. Additionally, Giobbi-157's "Central Registry" is "administered by a trusted third-party organization" ("***separate from a merchant providing a sale in the financial transaction***"). MS-1005, ¶¶[0032]-[0034], [0053], [0074], Claim 8; *see supra* [3], [6]-[8]; MS-1003, ¶[143]. Accordingly, when incorporating Giobbi-157's teachings

into Broadcom's system, Broadcom's service providers (e.g., service providers 110 or 304) would have been "*separate from a merchant providing a sale in the financial transaction*" as a POSITA would have recognized or found it obvious that some financial information would need to be authenticated separately from a merchant (e.g., credit card information authenticated remotely by a bank or creditor). MS-1005, ¶¶[0032]-[0034], [0053], [0074], Claim 8; MS-1008, ¶¶[0113]-[0116], [0136]-[0138]; *see supra* [8]; MS-1003, ¶[143].

[12]

Giobbi-157 discloses that its external PDK can be included in jewelry, including "watches, rings, necklaces or bracelets" ("*the at least one external device is included in jewelry*"). MS-1005, ¶[0035]. Accordingly, when modifying Broadcom's system based on the teachings of Giobbi-157, a POSITA would have recognized and found it obvious that, given the similarity of Broadcom and Giobbi-157, Broadcom's "*at least one external device*" (e.g., the token) would have also been capable of being "*included in jewelry*" as Broadcom discloses incorporating tokens into various transportable objects. MS-1005, ¶[0035]; MS-1008, ¶[0130]; MS-1003, ¶[144].

[13]

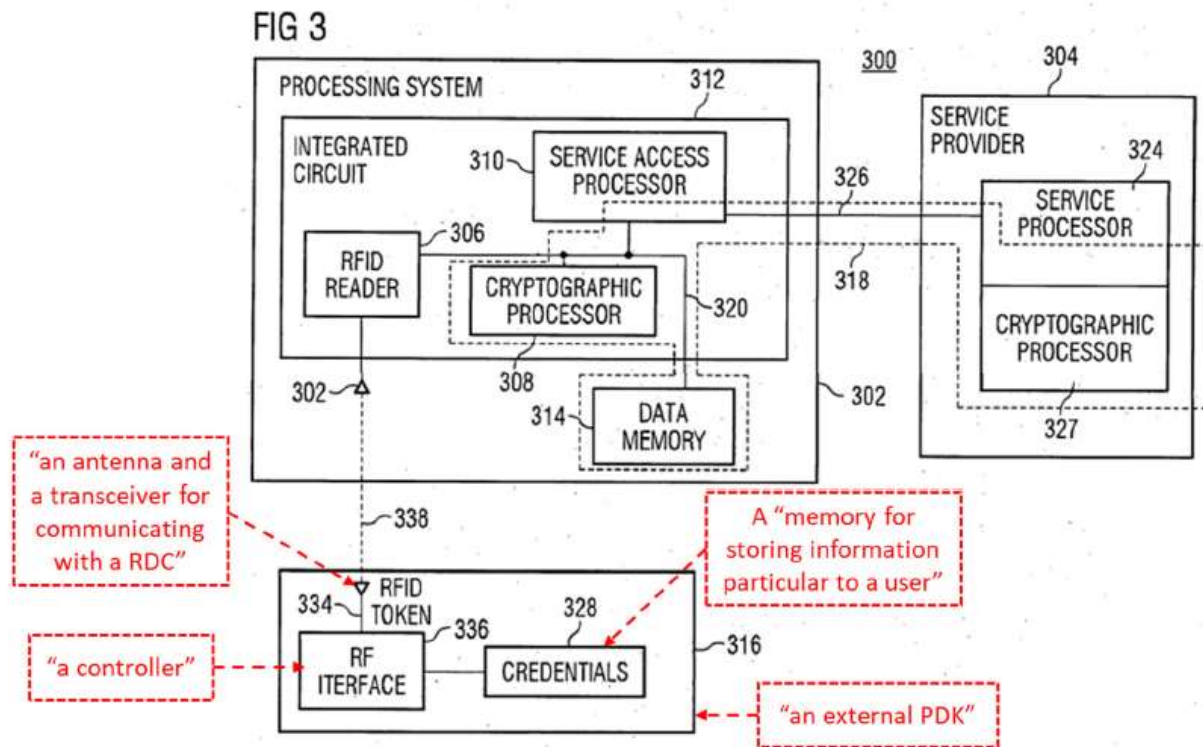
See supra, [12]; MS-1003, ¶[145].

*[20]*⁸

As described above in [12] and [13], the Broadcom-Giobbi external device can be “*a watch*.” *See supra*, [12]-[13]; MS-1003, ¶[146].

Broadcom, in its detailed FIG. 3 illustration of a token 316, also teaches “an operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for storing information particular to a user” as required by the above construction of a “*PDK*.” MS-1008, ¶¶[0146] (“an RF signal ... may be received by an antenna 334 [(“a transceiver for communicating with a RDC”)] and processed by an RF interface 336 [(a “controller”)] in the token 316”), [0148] (“The token 316 may include circuitry that stores information such as the credentials 328”), [0149] (“the RF interface 336 may generate an RFID signal that is broadcast by the antenna 334”); *see supra* I.C.2-3; MS-1003, ¶[147].

⁸ Petitioner notes that “the external PDK” in claim 20 lacks antecedent basis. For the purposes of IPR, Petitioner has analyzed this claim treating “the external PDK” as the “integrated, secure memory” of claim 14, while also showing how Grounds 1A/1B render a “PDK” obvious. Petitioner reserves the right to advance §112 arguments against this claim in litigation.



MS-1008, FIG. 3.

[1]-[7], [10]-[11], and [14]-[19]

Ground [2B] renders these claims obvious in the same manner as explained above in Ground [2A]. *See supra*, §III.B; MS-1003, ¶[148].

IV. Discretionary Denial Is Not Warranted

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

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

None of the references presented herein were evaluated by the examiner or applied in any rejection. *See generally* MS-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*

Consistent with Congressional intent, the goals of *Fintiv*, and the Interim Guidance issued by Director Vidal on June 21, 2022, Petitioner respectfully asks the Board to reach the merits of the challenges raised in this Petition, which mirror the challenges raised in Microsoft’s prior petition. *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11, 6 (PTAB Mar. 20, 2020) (precedential) (“*Fintiv*”); MS-1012, 6-7, 9. Microsoft’s petition has already been instituted, so a *Fintiv* denial would be inappropriate because (1) a reasonable likelihood of success has already been found for the presented grounds and (2) joinder petitioners that assume an understudy role consume only minimal resources of the Board and Patent Owner. Thus, the merits

of this petition are compelling and outweigh any concerns that might arise under *Fintiv* factors 1-5.

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

Petitioner respectfully submits application of the *General Plastic* analysis is inapplicable here. In *General Plastic*, the Board set forth a series of factors that may be analyzed for follow-on petitions to help conserve the finite resources of the Board. Here, both Petitioner and Microsoft submitted separate, independent petitions. In the current motion, Petitioner merely seeks to join Microsoft’s petition and does not present any new grounds. Petitioner would be taking an understudy role and the Board’s finite resources would not be impacted. Moreover, there is no strategic advantage to be gained by filing this additional petition, and there are no concerns of “road mapping” the Patent Owner’s strategy because Petitioner has submitted a petition that is substantively identical to Microsoft’s petition.

Additionally, concerning Petitioner’s earlier petition in IPR2024-00783, Petitioner has concurrently filed a **Supplemental Paper and Notice Ranking Petitions** pursuant to the Board’s Consolidated Trial Practice Guide addressing why the Board should exercise its discretion to institute both petitions.

V. Mandatory Notices

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

Google LLC is the real party-in-interest for this Petition⁹

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

The '289 patent is assigned to Proxense, LLC, who is currently asserting the '289 patent against Google LLC in the Western District of Texas in *Proxense, LLC v. Google LLC*, No. 6:23-cv-00320 (W.D. Tex.). To the best of Petitioner's knowledge, the '289 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>Microsoft Corp. v. Proxense, LLC</i>	IPR2024-00407	PTAB	January 16, 2024
<i>Google LLC v. Proxense, LLC</i>	IPR2024-00783	PTAB	April 19, 2024

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

Lead Counsel	Back-Up Counsel
Erika H. Arner (Reg. No. 57,540) erika.arner@finnegan.com Finnegan, Henderson, Farabow,	Kara A. Specht (Reg. No. 69,560) kara.specht@finnegan.com Finnegan, Henderson, Farabow,

⁹ Google LLC is a subsidiary of XXVI Holdings Inc., a subsidiary of Alphabet Inc.

XXVI Holdings Inc. and Alphabet Inc. are not real parties-in-interest here.

Garrett & Dunner LLP 1875 Explorer Street 8 th Floor Reston, VA 20190-6023 Tel: 571-203-2754 Fax: 202-408-4400	Garrett & Dunner LLP 271 17th Street, NW, Suite 1400 Atlanta, GA 30363-6209 Tel: 404-653-6400 Fax: 404-653-6444
	Cory C. Bell (Reg. No. 75,096) cory.bell@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner LLP 2 Seaport Lane, 6th Floor Boston, MA 02210-2001 Tel.: 617-646-1641 Fax: 202-408-4400
	Shawn S. Chang (Reg. No. 81,437) shawn.chang@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner LLP 271 17th Street, NW, Suite 1400 Atlanta, GA 30363-6209 Tel. 404-653-6400 Fax: 404-653-6444
	Safiya Aguilar (Reg. No. 77,212) safiya.aguilar@finnegan.com Finnegan, Henderson, Farabow, Garrett, & Dunner LLP 901 New York Avenue NW Washington, DC 20001-4413 Tel.: 202-408-4160 Fax: 202-408-4400

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

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

VI. Conclusion

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

The USPTO may charge any required fees to Deposit Account No. 06-0916.

Dated: August 22, 2024

Respectfully submitted,

/Erika H. Arner/

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

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that the foregoing **PETITION FOR *INTER PARTES* REVIEW** contains 12,200 words, excluding those portions exempted under 37 C.F.R. §42.24(a), as measured by the word-processing system used to prepare this paper.

Respectfully submitted,

/Erika H. Arner/

Erika H. Arner

Lead Counsel

Reg. No. 57,540

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a copy of the foregoing **PETITION FOR *INTER PARTES* REVIEW**, the associated Power of Attorney, and Exhibits 1001-1021 and 1023 are served on August 22, 2024, via FedEx Priority Overnight on the correspondence address of record indicated in the Patent Office's Patent Center system for U.S. Patent No. 9,679,289.

PATENT LAW WORKS/PROXENSE

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

A courtesy copy is also being sent via email to Patent Owner's counsel in *Proxense, LLC v. Google LLC*, No. 6:23-cv-00320 (W.D. Tex.), where Patent Owner has asserted the subject patent:

David L. Hecht
dhecht@hechtpartners.com

Maxim Price
mprice@hechtpartners.com

Conor B. McDonough
cmcdonough@hechtpartners.com

Yi Wen Wu
wwu@hechtpartners.com

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

Brian D. Melton
bmelton@susmangodfrey.com

Geoffrey L. Harrison
gharrison@susmangodfrey.com

Meng Xi
mxi@susmangodfrey.com

Bryce T. Barcelo
bbarcelo@susmangodfrey.com

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

Lear Jiang
ljiang@susmangodfrey.com

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

Dated: August 22, 2024

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