

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner,

v.

PROXENSE, LLC,

Patent Owner.

Case No. IPR2024-01398

U.S. Patent No. 8,646,042

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

I.	REQUIREMENTS FOR IPR	1
A.	Grounds for 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 ’042 PATENT.....	5
A.	Brief Description	5
B.	Prosecution History	6
III.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	7
A.	[GROUND 1A/1B] – Claims 1, 5-6, 8-11, and 13-14 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 2] – Claims 10-11 and 13-14 are rendered obvious by Broadcom	67
1.	Overview of Broadcom.....	67
2.	Analysis.....	70
IV.	PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION.....	84
A.	35 U.S.C. §325(d) – <i>Advanced Bionics</i>	84
B.	35 U.S.C. §314(a) - <i>Fintiv</i>	85
V.	CONCLUSION.....	88
VI.	MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1).....	88
A.	Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)	88
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2)	89
C.	Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)	89
D.	Service Information.....	90

EXHIBITS

MS-1001	U.S. Patent No. 8,646,042 to David L. Brown (“the ‘042 Patent”)
MS-1002	Excerpts from the Prosecution History of the ‘042 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 Electronics Co., Ltd</i> , 6:21-CV-00210-ADA, W.D. Tex., filed January 18, 2022
MS-1010	Provisional Application No. 60/798,843
MS-1011	RESERVED
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, 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, 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, 6:23-cv-00319, W.D. Tex., filed August 10, 2023
MS-1016	W.D. Tex. Order Cancelling <i>Markman</i> Hearing, issued 1/9/2024

EX-1017-1022	Reserved
EX-1023	<i>Proxense, LLC v. Google LLC</i> , Case No. 6-23-cv-00320, Dkt. No. 59, Claim Construction Order (W.D. Tex. Jan. 23, 2024)
EX-1024	<i>Proxense LLC v. Microsoft Corp.</i> , Case No. 23-cv-00319, Dkt. No. 66, Claim Construction Order (W.D. Tex. May 24, 2024)
EX-1025	<i>Microsoft Corp. v. Proxense, LLC</i> , IPR2024-00573, Paper 11 (PTAB Aug. 13, 2024)
EX-1026	U.S. District Court National Judicial Case Load Profile ending June 30, 2024.
EX-1027	Docket Sheet for <i>Proxense, LLC v. Apple Inc.</i> , Case No. 6-24-cv-00143 (W.D. Tex) (pulled Sep. 12, 2024)
EX-1028	Scheduling Order in <i>Proxense, LLC v. Apple Inc.</i> , Case No. 6-24-cv-00143 (W.D. Tex)
EX-1029	Patents and Applications related to the '042 Patent

LISTING OF CHALLENGED CLAIMS

Claim 1	
[1.pre]	A hybrid device comprising:
[1.1]	an integrated personal digital key (PDK) for storing information and capable of communicating wirelessly with at least one external receiver-decoder circuit (RDC); and
[1.2]	an integrated RDC for communicating wirelessly with at least one external PDK within a proximity zone, the integrated RDC coupled to the integrated PDK by a first signal line for communication,
[1.3]	the integrated RDC coupled to at least one other component of the hybrid device by a second signal line,
[1.4]	one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service on one or more of the hybrid device and a device associated with the external RDC.
Claim 5	
[5]	The hybrid device of claim 1, wherein the one or more of the hybrid device and the device associated with the external RDC are enabled subsequent to the external PDK entering the proximity zone of the integrated RDC and based on the information stored by one or more of the external PDK and the integrated PDK.
Claim 6	
[6]	The hybrid device of claim 1, wherein the hybrid device is a cell phone and the hybrid device is enabled to provide cell phone service subsequent to the external PDK entering the proximity zone of the integrated RDC and based on the information stored by one or more of the external PDK and the integrated PDK.
Claim 8	
[8]	The hybrid device of claim 1, wherein the integrated PDK communicates with the external RDC subsequent to the external PDK entering the proximity zone of the integrated RDC.
Claim 9	

[9]	The hybrid device of claim 1, comprising storage for inheritance information.
Claim 10	
[10.pre]	A method comprising:
[10.1]	creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external personal digital key (PDK), the hybrid device including an integrated PDK and the integrated RDC;
[10.2]	receiving a first signal at the integrated RDC via the first wireless link from the external PDK;
[10.3]	generating an enablement signal enabling one or more of an application, a function and a service on one or more of the hybrid device and a device associated with an external RDC; and
[10.4]	sending the enablement signal to one or more of the hybrid device and the device associated with an external RDC.
Claim 11	
[11]	The method of claim 10, wherein the hybrid device is a cell phone and the enablement signal is sent to the cell phone enabling one or more of a service, a feature and a functionality of the cell phone.
Claim 13	
[13.1]	The method of claim 10, wherein the integrated PDK is electrically coupled to the integrated RDC, and the method comprises:
[13.2]	sending the enablement signal from the integrated RDC to the integrated PDK;
[13.3]	creating a second wireless link between the integrated PDK and an external RDC; and
[13.4]	sending the enablement signal from the integrated PDK to the external RDC using the second wireless link.
Claim 14	
[14]	The method of claim 11, wherein the integrated PDK modifies the enablement signal to produce a modified enablement signal, and the modified enablement signal is sent from the integrated PDK to the external RDC.

Apple Inc. (“**Petitioner**” or “**Apple**”) petitions for *Inter Partes* Review (“**IPR**”) of claims 1, 5-6, 8-11, 13-14 (“**the Challenged Claims**”) of U.S. Patent No. 8,646,042 (“**the ’042 Patent**”). Compelling evidence presented in this Petition demonstrates at least a reasonable likelihood that Apple will prevail with respect to at least one of the Challenged Claims.

I. REQUIREMENTS FOR IPR

A. Grounds for Standing

Petitioner certifies that the ’042 Patent is available for IPR. This petition is being filed within one year of service of a complaint against Apple. Apple is not barred or estopped from requesting review of the Challenged Claims on the below-identified grounds.

B. Challenge and Relief Requested

Apple requests an IPR of the Challenged Claims on the grounds noted below. Dr. Patrick Traynor provides supporting testimony in his Declaration. MS-1003, ¶¶[1-20]. Notably, these grounds are 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.

Ground	Claim(s)	35 U.S.C. § 102/103
1A	1, 5-6, 8-11, and 13-14	Giobbi-157 in view of Giobbi-139
1B	1, 5-6, 8-11, and 13-14	Giobbi-157 in view of Giobbi-139 and Dua
2	10-11 and 13-14	Broadcom

The '042 Patent claims priority to a number of provisional applications, the earliest of which was filed 12/6/2007. MS-1001, Cover. While Apple does not concede that 12/6/2007 is the priority date that should be afforded to the '042 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 '042 Patent.

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
Broadcom	Sep. 30, 2004	Jun. 1, 2005

¹ Dua relies upon previous applications which claim priority to May 12, 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 notes below constructions adopted in previous proceedings before WDTX (case number 6:21-CV-00210-ADA) where family members of the ’042 patent were asserted. MS-1009; MS-1003, ¶¶[23]-[24].³

1. Hybrid Device

For the purposes of the present proceeding, this term, which appears in claims 1-11 and 15, should be construed to mean “a device comprising an

² Microsoft Corporation has advanced modified constructions in claim construction pleadings in co-pending litigation. MS-1013. The asserted references of this petition additionally satisfy those proposed constructions, as explained in the petition. *Id.*

³ See also EX-1023, EX-1024, and EX-1025.

integrated personal digital key (PDK) and an integrated receiver-decoder circuit [(RDC)].” This definition is consistent with the use of the term in the specification of the ’042 patent⁴. *See, e.g.*, MS-1001, Abstract, 1:65-2:20, 13:15-40. For purposes of this proceeding, Petitioner adopts this construction of “hybrid device,” which, as noted above, was adopted in 6:21-CV-00210-ADA. MS-1009; MS-1003, ¶[25].

2. Personal Digital Key (“PDK”)

For the purposes of the present proceeding, this term, which appears in claims 1-3, 5-8, 10, 12-16, and 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 controller and memory for storing information particular to a user.” This definition is consistent with the use of the term in the specification of the ’042 patent. *See, e.g.*, MS-1001, 13:40-54. For purposes of this proceeding, Petitioner adopts this construction of “personal digital key,” which, as noted above, was adopted in 6:21-CV-00210-ADA. MS-1009; MS-1003, ¶[26].

⁴ This construction is based on the recitation of “PDK” in the Challenged Claims, which is distinct from the recitation of “integrated, secure memory” in the claims of other patents in the same family.

3. Receiver-decoder circuit (“RDC”)

For the purposes of the present proceeding, this term, which appears in claims 1-8, 10, 13-16, and 20 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 definition is consistent with the use of the term in the specification of the ’042 patent. *See, e.g.*, MS-1001, 7:10-22. For purposes of this proceeding, Petitioner adopts this construction of “receiver-decoder circuit,” which, as noted above, was adopted in 6:21-CV-00210-ADA. MS-1009; 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 ’042 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 ’042 PATENT

A. Brief Description

The ’042 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, Abstract, 1:20-26. 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, 3:62-4:20. 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, 3:20-32, 16: 20-38. Similarly, the external PDK is also capable of storing information. MS-1001, 3:62-4:20. 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, 4:63-5:24. 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 '042 Patent was allowed after a single office action that presented only a double-patenting rejection. MS-1002, 380-386. 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, 5-6, 8-11, and 13-14 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, ¶¶[31]-[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**⁵. 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]. An example of Giobbi-157’s PDK and Reader configuration is shown in the annotated version of Figures 2 and 3 below. MS-1003, ¶[34].

⁵ Bolding and italicized font added for emphasis here and throughout this reply.

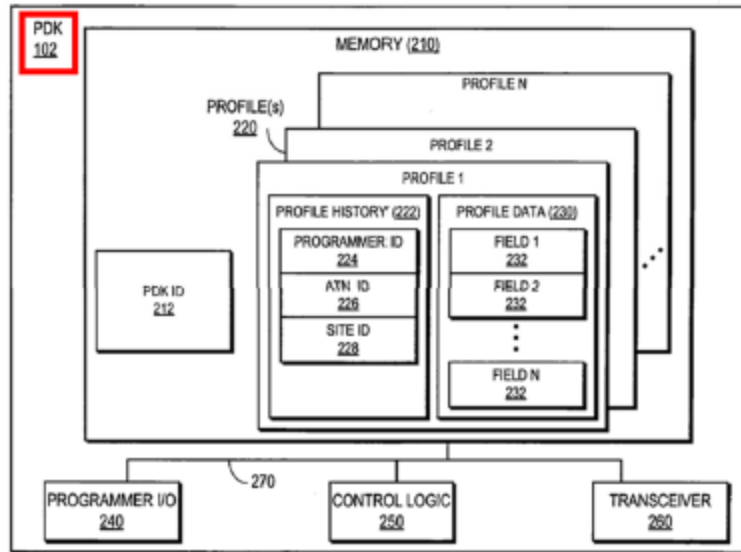


FIG. 2

MS-1005, FIG. 2.⁶

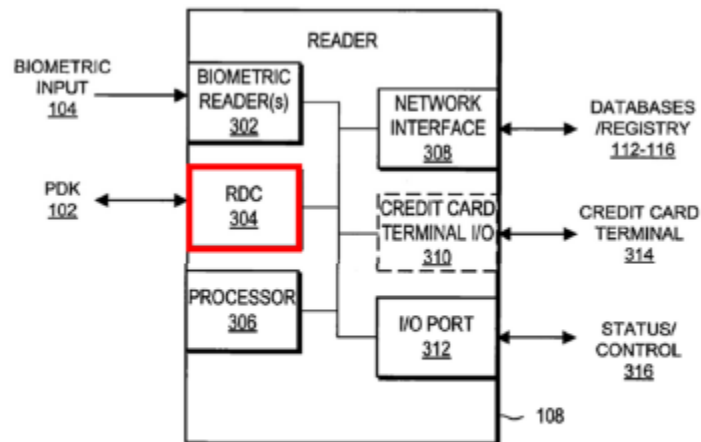


FIG. 3

MS-1005, FIG. 3.

⁶ All annotations added to figures are 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.” MS-1005, ¶¶[0057]-[0058], [0063], FIG. 4; MS-1003, ¶[35].

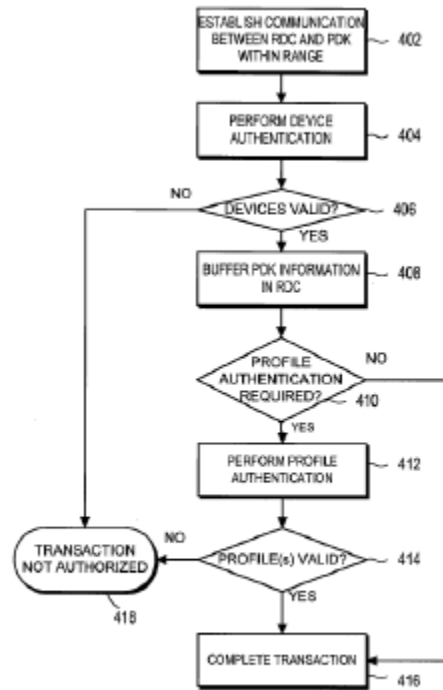


FIG. 4

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-1010⁷, 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” that 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 the use of 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]; MS-1005, ¶[0035]; MS-1003, ¶[38].

⁷ Although the document is marked confidential, this document was filed by the applicant as a provisional application, is incorporated by reference into Giobbi-157, and is publicly available through the USPTO's Patent Center website.

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. 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].

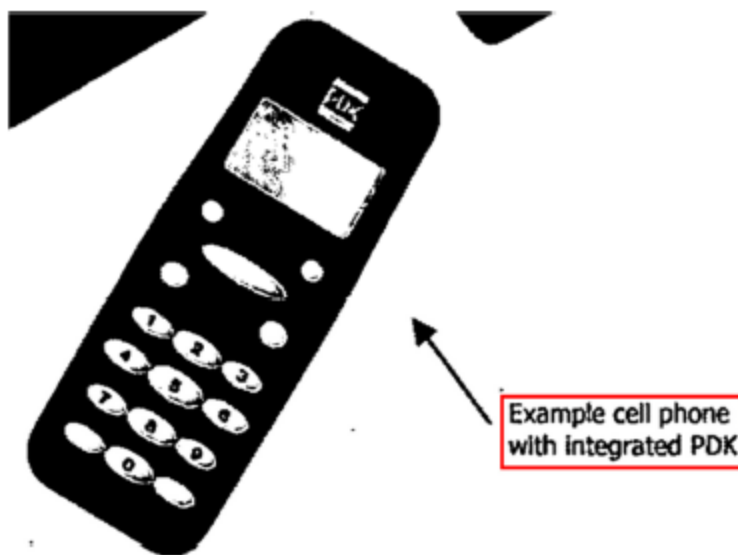
Giobbi-139 also discloses the scalability of RDC and PDK architecture. MS-1006, ¶¶[0091]-[0096]. For example, Giobbi-139 teaches that a user can “assign (or remove)” additional PDKs to a device with an integrated RDC. MS-1006, ¶¶[0092], [0095]; MS-1003, ¶[40].

Giobbi-139 further discloses a version of communication between a PDK and RDC that is not wireless. MS-1006, ¶¶[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

- (i) *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]; 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-1010, p. 28 (image cropped).

- (ii) *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].

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]. Notably, Giobbi-139 identifies such a configuration as an “enhancement.” MS-1006, ¶¶[0087]-[0088]. 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 enhance the security of the data stored on the cell phone. MS-1003, ¶[46].

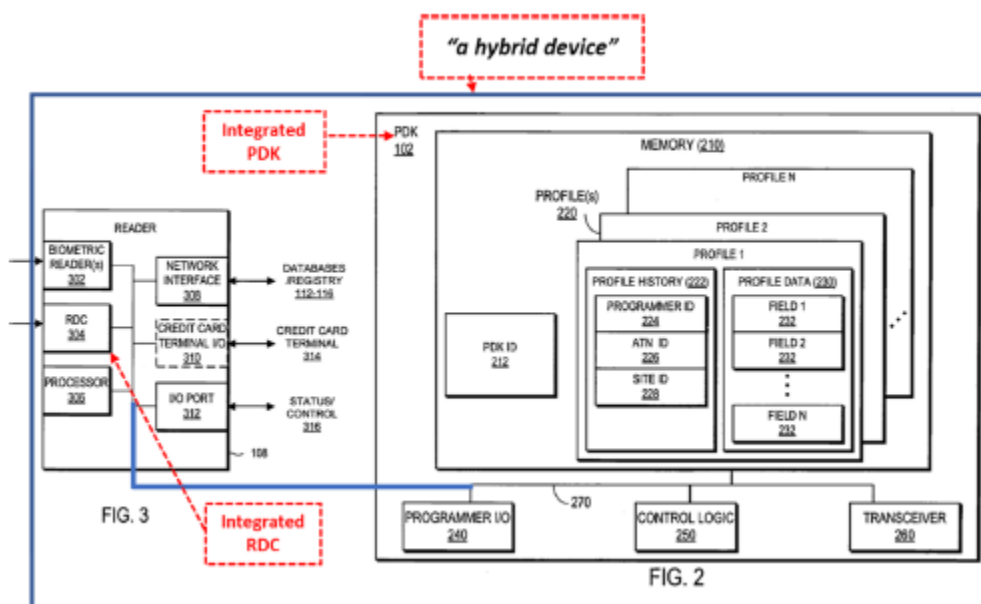
Giobbi-139 additionally teaches a broader way to secure data on a cell phone and discloses that an RDC integrated into a cellphone can be used with a PDK to “effectively enable[]/disable[] the device itself.” MS-1006, ¶¶[0088]-[0089]. In this configuration, the cell phone with the integrated RDC can enable or disable the device through authentication with a PDK. *Id.*; MS-1003, ¶¶[47]-[48].

(iii) *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 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).

(iv) 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 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 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, in this manner and 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 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]. 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].

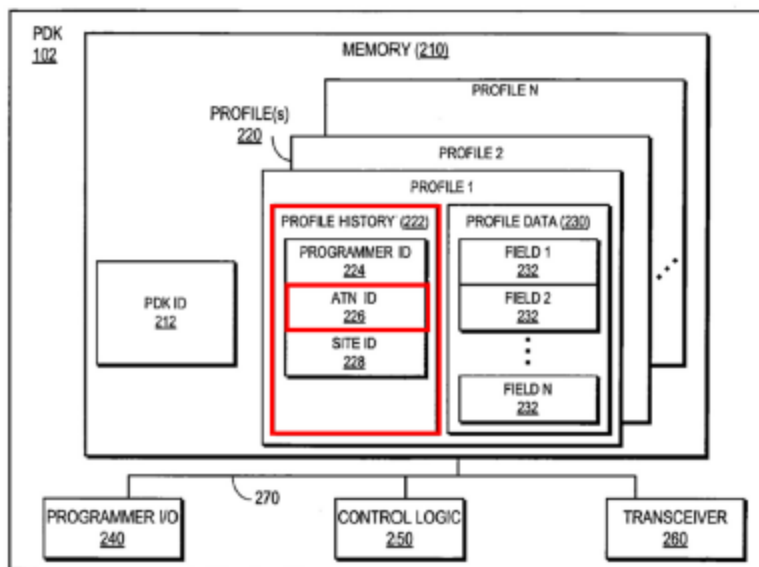


FIG. 2

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]; MS-1003, ¶[53].

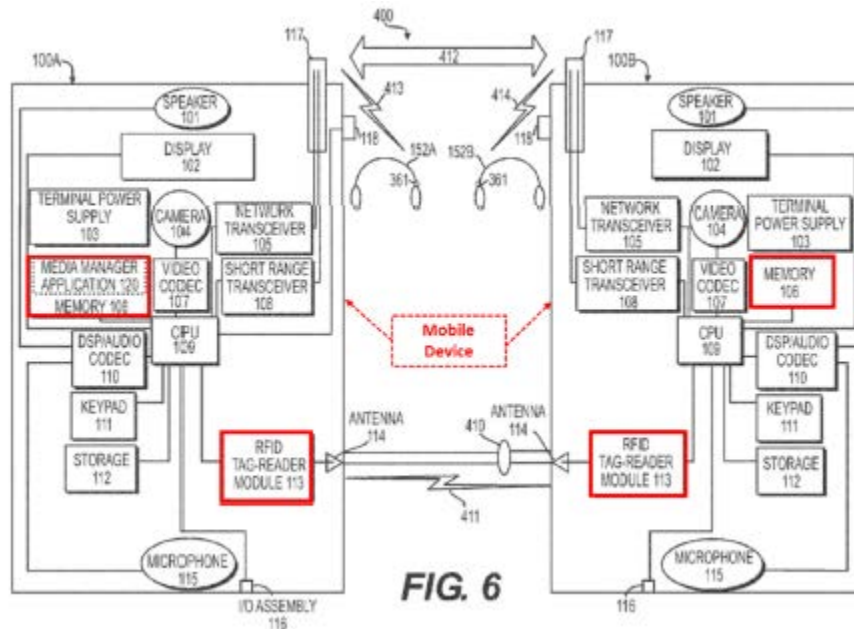
Dr. Traynor explains that, for at least the aforementioned reasons, a POSITA would have found it obvious to modify Giobbi-157's portable electronic device to include an RDC as taught by Giobbi-139 (thus creating a "**hybrid device**"). MS-1003, ¶[54]. Combining Giobbi-157 and Giobbi-139 would have involved (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; MS-1003, ¶[54].

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,

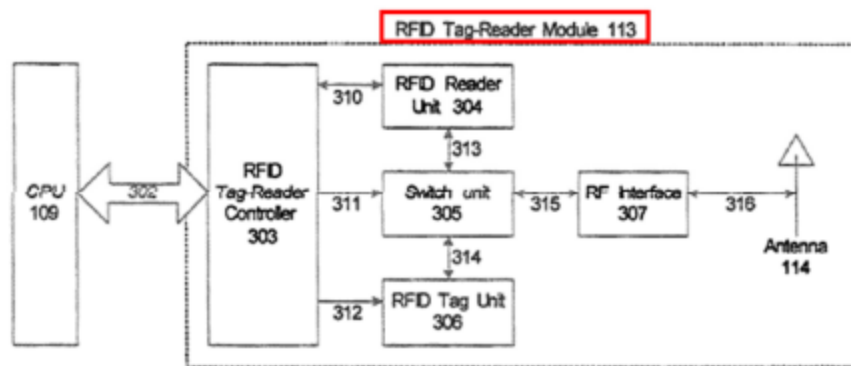
given that both were filed by the same applicant and describe similar techniques; and (iv) combining the techniques of Giobbi-157 and Giobbi-139 would have worked in the same manner already described in the references. MS-1005, ¶[0011]; MS-1006, ¶[0090]; MS-1003, ¶[55].

4. Overview of Dua

Dua discloses a wireless media player or related system (e.g., a cell phone) that 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.” 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].

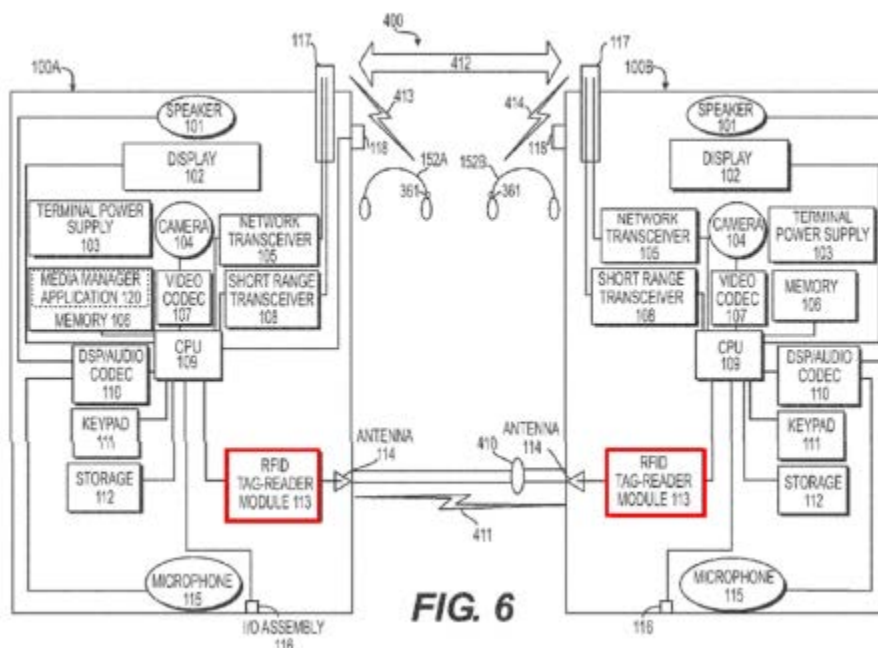
Dua’s RFID Tag Unit 306 stores information necessary to gain access to an external device in an encrypted internal tag memory and transmits this information to an external Reader when establishing a connection. MS-1007, 13:9-18, 14:53-64, 15:42-56, 16:31-34. As shown in FIG. 4A above, Dua also discloses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

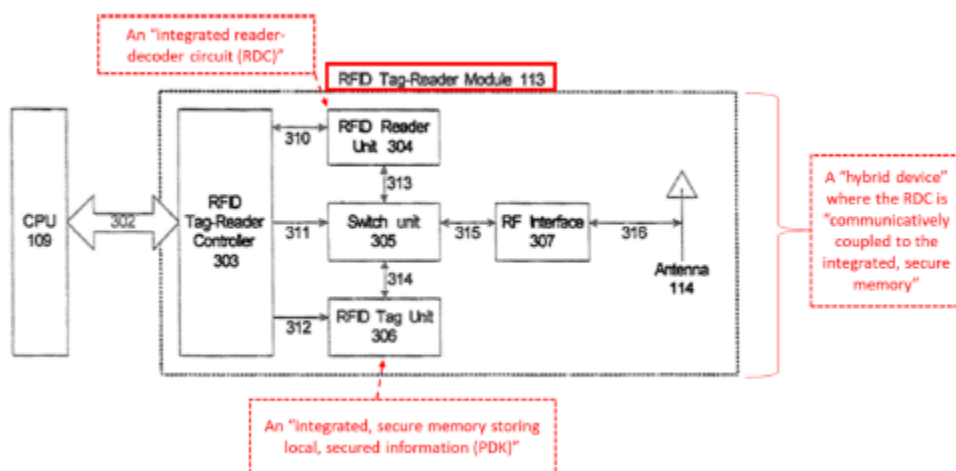
Dua further corroborates the teachings of the Giobbi references and provides implementation details for integrating an RDC and PDK into the same device.

MS-1003, ¶[56]. As Dr. Traynor explains, first, that a POSITA would recognize the similarity between 1) the RFID Tag in Dua and the PDK in Giobbi; and 2) the RFID Reader in Dua and the RDC in Giobbi. 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. MS-1005, Abstract, ¶¶[0011]-[0014]; MS-1006, Abstract, ¶[0010]; MS-1007, Abstract, 6:46-65, FIGS. 4A, 6.; MS-1001, Abstract, claim 1. 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.

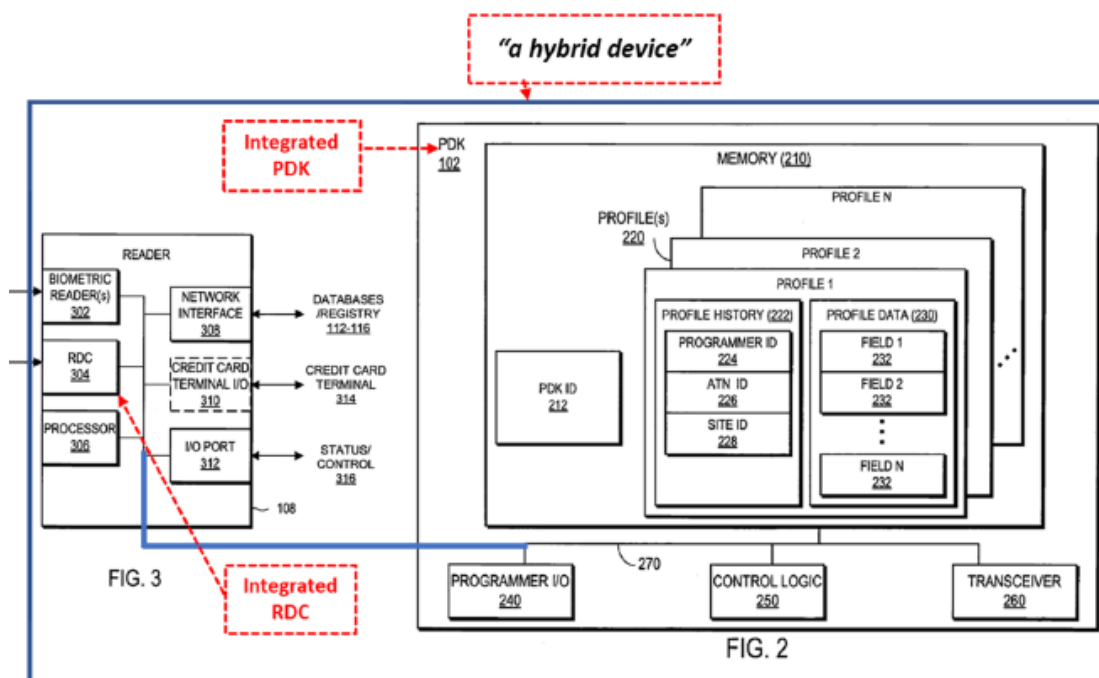


MS-1007, FIG. 4A.

6. Analysis

[1.pre]

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 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. 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 [a PDK] and an integrated [RDC].” *See supra*, §I.C.1, 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 all within a *hybrid device*. *Id.*



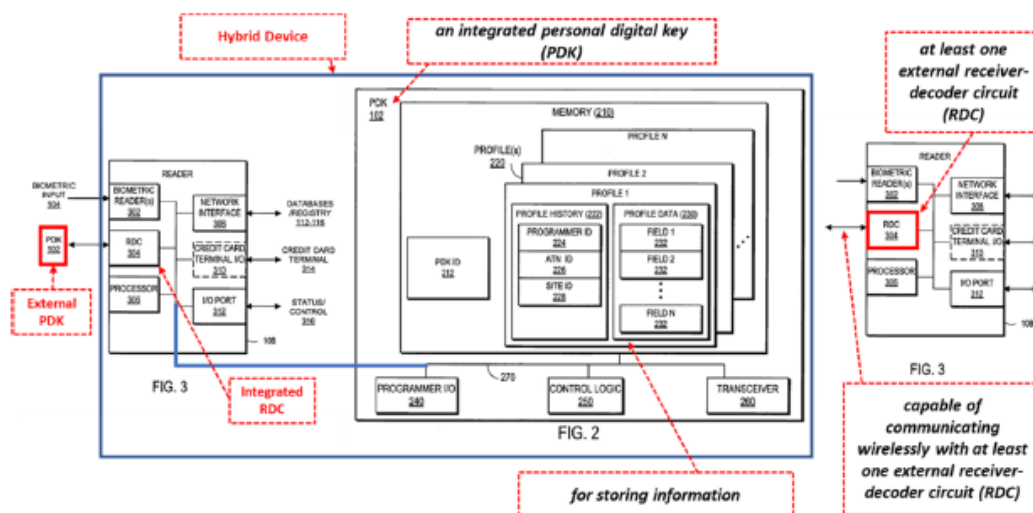
MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139's teachings).

[1.1]

Ground 1A

Giobbi-157 discloses a “*Personal Digital Key (PDK)*,” which is an example of an *integrated* secure memory *for storing information*. 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) [*“information”*] in a tamperproof 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]; *see supra*, §III.A.1, [1.pre]. Accordingly, the hybrid device of the Giobbi-157-Giobbi-139 combination includes an integrated PDK for storing information. 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, ¶[59].



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

Finally, Giobbi-157 teaches that PDKs “can wirelessly transmit [(“*communicating wirelessly*”)] the identification information including a unique PDK identification number and the biometric profile over a secure wireless channel for use in an authentication process,” and that the RDC is specially designed to receive information from the PDK. MS-1005, ¶[0050]. For example, “[t]he RDC 304 provides the wireless interface to the PDK 102 [(“*with at least one external receiver-decoder circuit (RDC)*”)]. Generally, the RDC 304 wirelessly receives data from the PDK 102 in an encrypted format and decodes the encrypted data for processing by the processor 306.” MS-1005, ¶¶[0050], [0059] (“When a PDK 102 comes within range of a Reader 108, communication is automatically established 402 between the RDC 304 of the Reader 108 and the PDK 102.”).

Thus, a PDK by its definition can “*communicat[e] wirelessly with at least one external receiver-decoder circuit (RDC).*” MS-1003, ¶[60].

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 a “*PDK*” *for storing information and capable of communicating wirelessly with at least one external receiver-decoder circuit (RDC)* (RFID reader). 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 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 PDK 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*

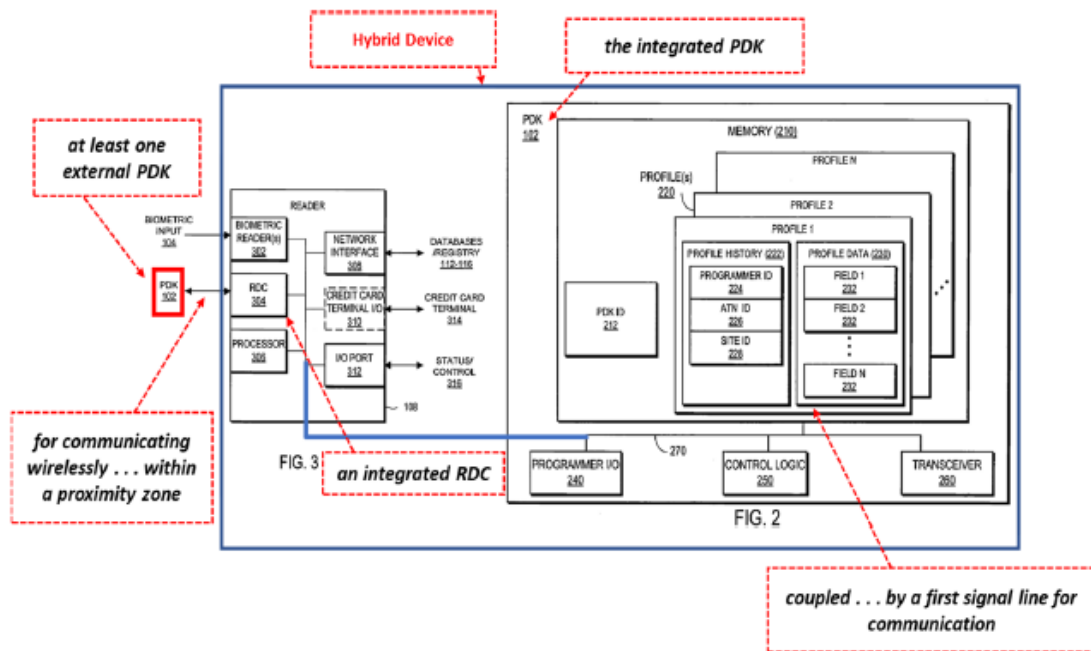
§III.A.1. As described above, the hybrid device includes an *integrated RDC* that is

coupled to the integrated PDK by a first signal line for communication. 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.



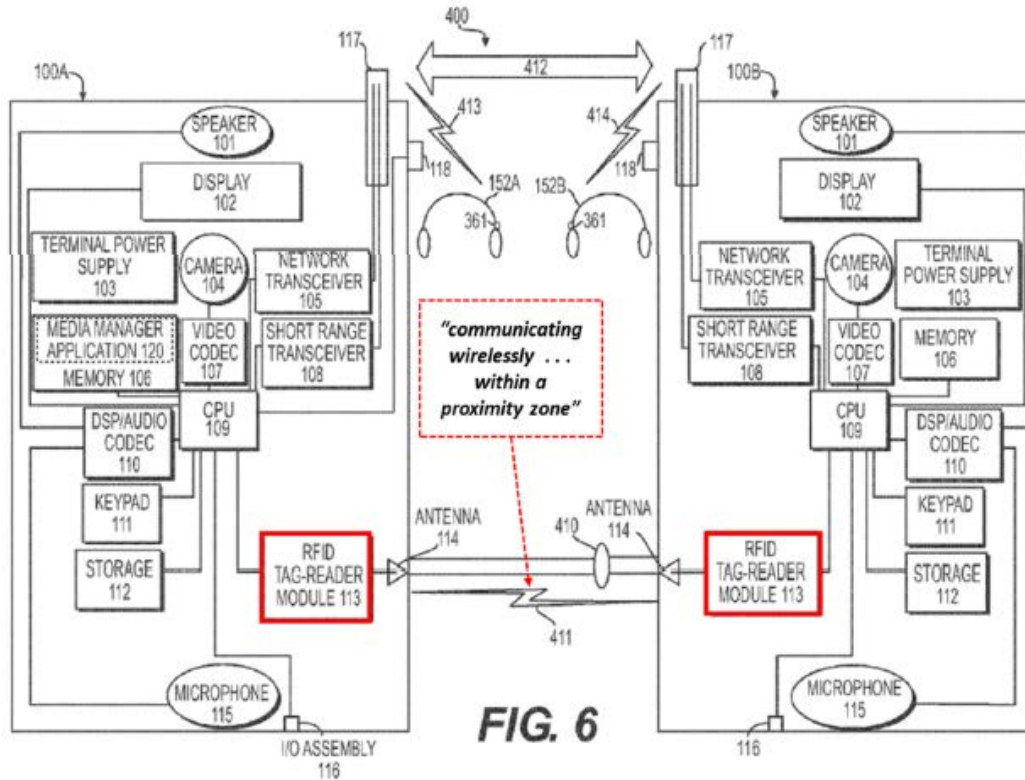
MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139’s teachings).

Giobbi-139 also discloses an integrated RDC “communicating wirelessly with the at least one external device within a proximity zone.” MS-1006,

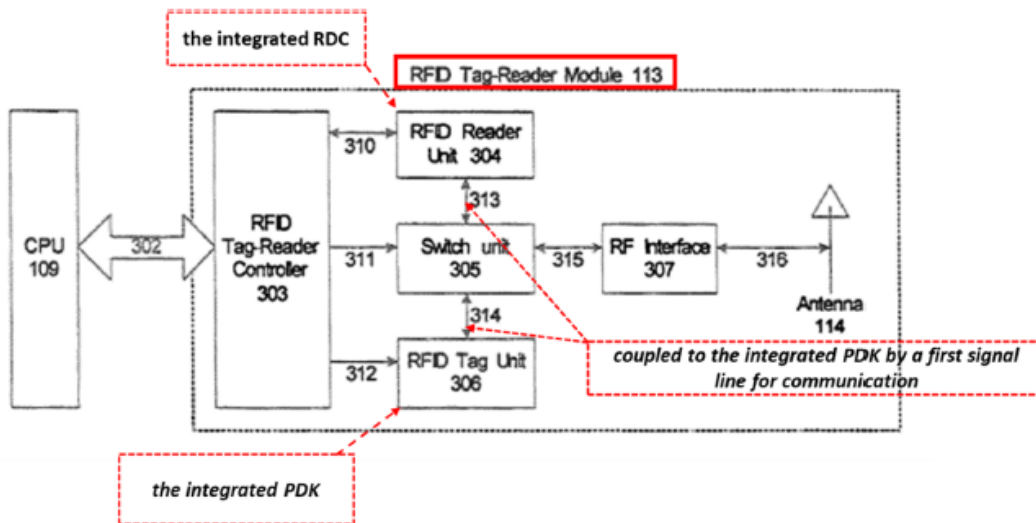
¶¶[0026]-[0044]; MS-1003, ¶[63].

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 . . . (PDK)*” of [1.1]). 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 PDK*” (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.

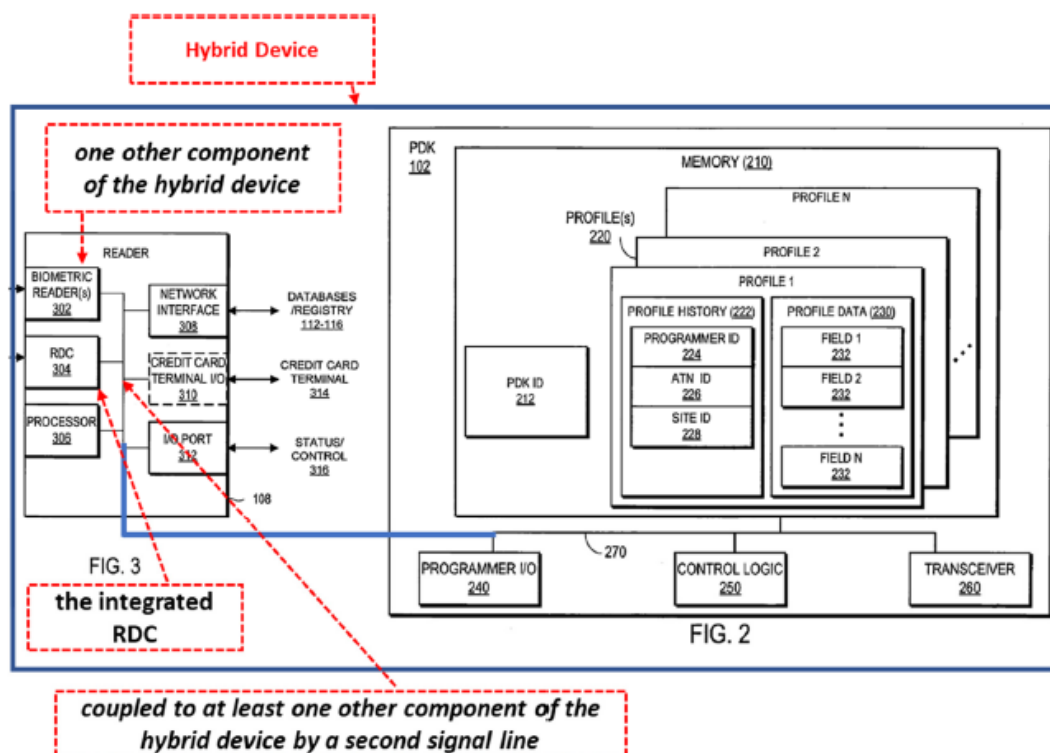
[1.3]

Ground 1A

First, Giobbi-139 teaches that a device can be controlled utilizing signals that are sent from or controlled by the RDC within the device. MS-1006, ¶¶[0041], [0088]-[0089]. For example, a storage device (“*at least one other component*”) “*of the hybrid device*” (such as a portion of the memory of a cell phone) can be controlled by a signal line from the RDC to the storage device (“*the integrated RDC coupled to at least one other component of the hybrid device by a second signal line*”). MS-1006, ¶¶[0041], [0088]-[0090]. Using the example of digital storage, Giobbi-139 teaches that the integrated RDC provides “multiple methods of securing digital content.” MS-1006, ¶[0071]. For example, Giobbi-139 teaches that the “bus structure that provides the communications path between storage mechanisms and their hosting devices” is controlled to secure portions of a device. MS-1006, ¶¶[0078], [0089]. In this way a controller (under direction of an RDC) can control “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, FIG. 11-13; ¶¶[0078], [0089]. Giobbi-139 gives a specific example of the use case where “[t]he [hard]drive’s controller 334 [(*at least one other component*)] is disabled whenever the PDK-Key 336 is not present.” (in reference to FIGS 12 and

13) MS-1006, ¶[0078]. Therefore, a POSITA would have found obvious that to control an application, function, or service on the device, “*a second signal line*” would connect the RDC to the “*at least one other component of the hybrid device.*” MS-1003, ¶[65].

Alternatively, Giobbi-157 teaches that both RDCs and PDKs can include biometric readers (“*at least one other component of the hybrid device*”). MS-1005, FIG. 3, ¶¶[0030], [0048]-[0049], [0051]-[0052], [0071]. Indeed, Giobbi-157 shows the *integrated RDC* 304 *coupled* by *a second signal line* to the biometric reader 302 (*at least one other component of the hybrid device*) in FIG. 3. MS-1005, FIG. 3. The *integrated RDC* compares the biometric input at the biometric reader to the biometric profile data received from a PDK. MS-1005, FIG. 3, ¶¶[0030], [0048]-[0049], [0051]-[0052], [0071]. Therefore, a POSITA would have found it obvious that in order for the data of the biometric reader to be compared to the data of the PDK, the “*the integrated RDC [is] coupled to at least one other component of the hybrid device by a second signal line.*” MS-1003, ¶[66].



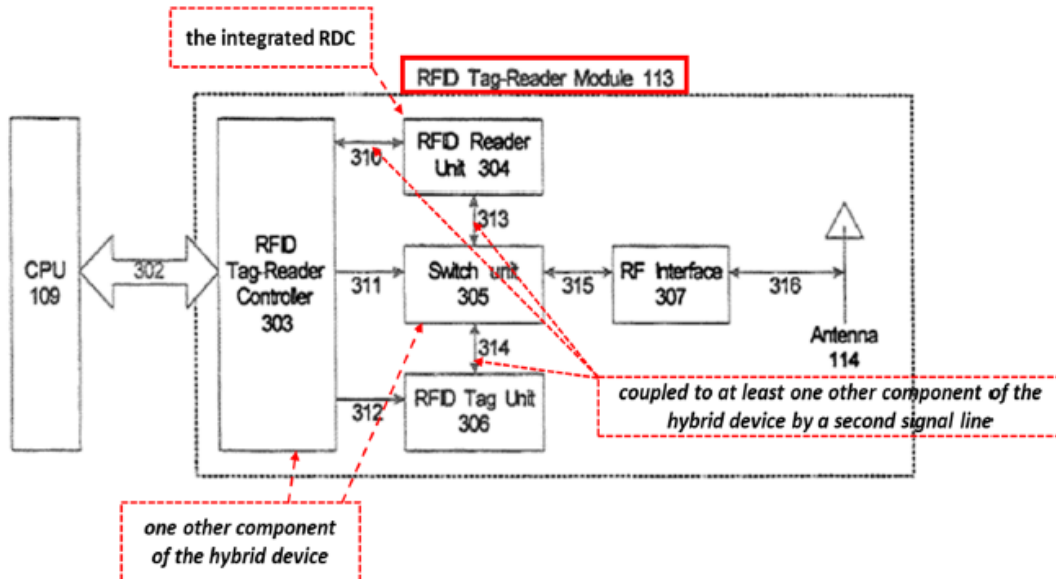
MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139's teachings).

Finally, both Giobbi-157 and Giobbi-139 teach a network interfacing component (*at least one other component of the hybrid device*) connected to an RDC, thus allowing the RDC to “relay” authorization information to an external device (Giobbi-157’s “network interface 308” connected to the RDC 304 in FIG.3). MS-1006, ¶[0085]. For example, Giobbi-139 teaches that “Network-Level protection, File-Level Protection can be expanded to a network environment by employing a centralized software application/database called a PDK Document Controller (DC) 340 running on a server 342.” MS-1006, ¶[0084]. “An RDC located in the requester’s workstation 346 acquires information from the user’s PDK-Key 344 and relays that information to the DC 340. The DC then enables

appropriate access.” MS-1006, ¶[0085]. Here the *integrated RDC* is *coupled to at least one other component of the hybrid device* (a network interface component) *by a second signal line* that allows communication with a component outside the hybrid device. MS-1003, ¶[67].

Ground 1B

FIG. 6 of Dua illustrates a hybrid device that includes an RFID Tag-Reader Module (an “RDC) Unit 306 (the “PDK”). 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.* Dr. Traynor explains that through Dua’s teachings it is obvious that *the integrated RDC* is *coupled to at least one other component of the hybrid device by a second signal line*, so that the RDC can enable that component or for the mere fact that the RDC must be connected to a processor, transmitter, memory, or power to function in the mobile device. MS-1007, FIG. 4A. 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, ¶[68].



MS-1007, FIG. 4A.

[1.4]

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]” 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 external PDK is valid and authenticated, the *integrated 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.)” (“*enabling one or more of an application, a function, and service*”). MS-1006, ¶[0063]. More specifically, the external PDK

can enable functions on *the hybrid device*, including “effectively enabling/disabling the device itself.” MS-1006, ¶[0089]; MS-1003, ¶[69].

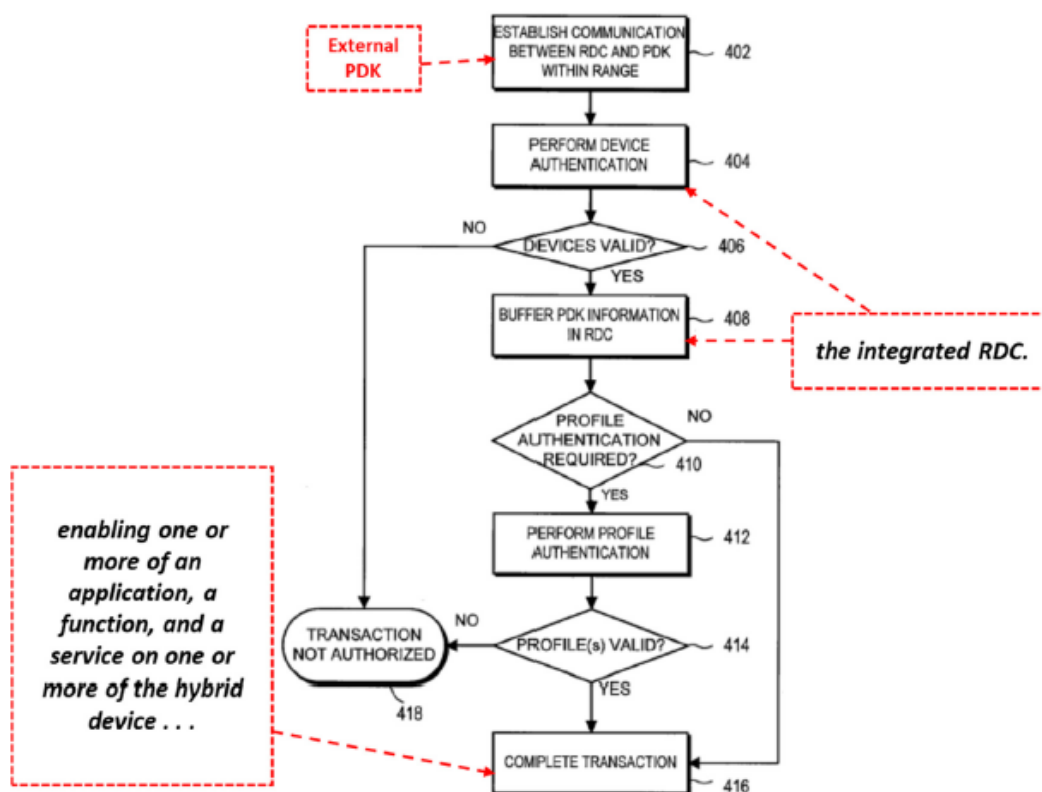


FIG. 4
MS-1005, FIG. 4.

Additionally, the integrated PDK of the hybrid device “*enabl[es] one or more of an application, a function, and service on. . . a device associated with the external RDC.*” MS-1005, Abstract, ¶[0011]. Transactions in Giobbi-157 are performed by transmitting authenticating information from a PDK (“*the integrated PDK*” of the hybrid device) to an RDC (*the external RDC*), for example, when completing a withdrawal from an ATM (*a device associated with the external*

RDC). MS-1005, ¶[0065]. An example authentication process and function enablement is shown below in FIG. 4; MS-1003, ¶[70].

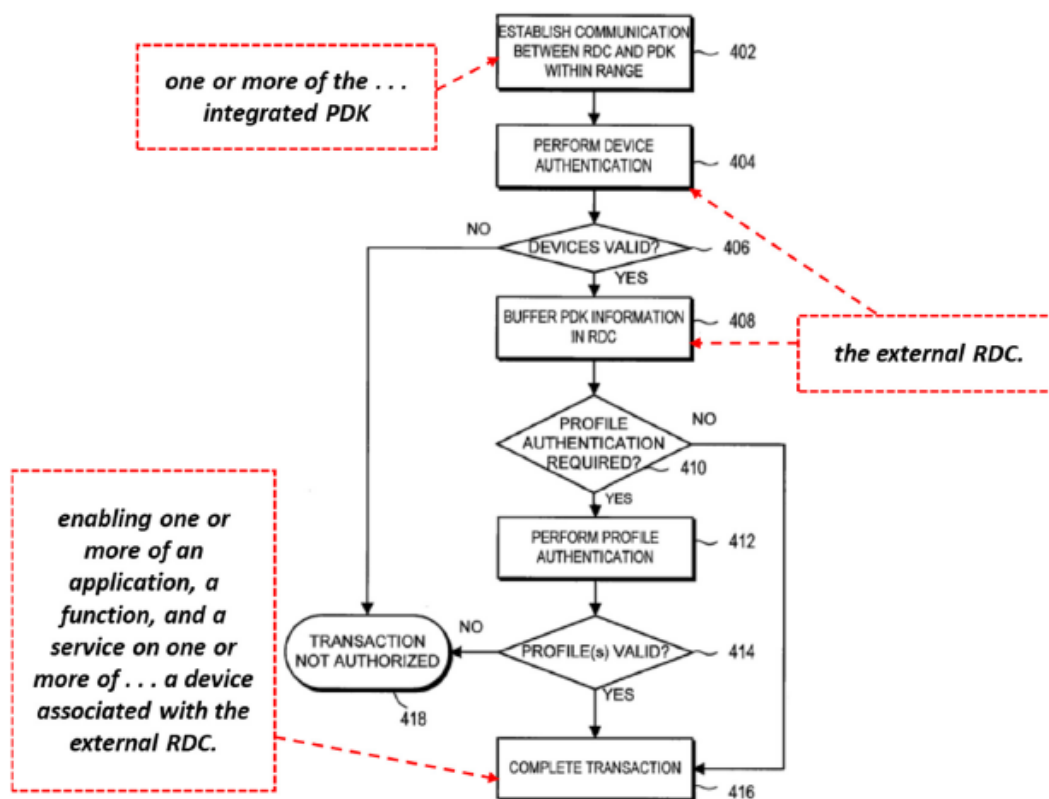


FIG. 4

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, ¶[71].

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 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, ¶[72].

[5]

Ground 1A/1B

See supra [1.4]. As discussed above, Giobbi-157 provides an example use of a Notary PDK used to initialize other PDKs, such as the PDK of the hybrid device. *See supra* §III.A.3.iv. The Notary PDK (***the external PDK***) when initializing the hybrid device’s PDK would ***enter[]the proximity zone of the integrated RDC*** and provide the Notary PDK ID in “a process that is trusted, audited, and easily verified.” MS-1005, ¶[0029], [0037], [0043]-[0044]. Then any subsequent use of the hybrid device to enable functionality would be ***subsequent to the external PDK*** (Notary PDK) ***entering the proximity zone of the integrated RDC***. MS-1003, ¶¶[73]-[74].

Both Giobbi-139 and Giobbi-157 teach proximity-based enablement of applications, functions, and services on a ***device associated with an external RDC***. MS-1005, ¶¶[0030], [0059], [0062]; MS-1006, ¶¶[0036]-[0037], [0087]-[0090]. For example, Giobbi-157 teaches that “[w]hen a PDK 102 comes within range of a Reader 108 [a device with an integrated RDC], communication is automatically

established 402 between the RDC 304 of the Reader 108 and the PDK 102.” MS-1005, ¶[0059]. A user can then “initiate” or “trigger” a transaction. MS-1005, ¶[0065]; MS-1003, ¶[75]. Then, the RDC “transmits 604 profile authentication requests to the PDK 102 requesting transmission of one or more stored profiles over the secure channel” to authenticate the user (“*based on the information stored by one or more of the external PDK and the integrated PDK*”). MS-1005, FIG. 4, ¶¶[0064]-[0068]. If the transmitted profiles are valid, the transaction is completed at the ATM (*the device associated with the external RDC [is] enabled*). MS-1005, FIG. 4, ¶¶[0064]-[0068]; MS-1003, ¶[75].

Both Giobbi-139 and Giobbi-157 teach proximity-based enablement of applications, functions, and services on *the hybrid device*. MS-1005, ¶¶[0049]-[0058], [0064]-[0068]; MS-1003, ¶[76]. For example, a shop owner can carry a hybrid device and utilize the integrated PDK to enable functions within the store such as enabling a cash register or unlocking a storeroom. *Id.* When a customer carrying a PDK requests to initiate a purchase, the merchant can utilize the hybrid device to both receive input from the user, and receive, via the integrated RDC, the external PDK’s information to compare to the input to authenticate the customer. MS-1005, FIG. 3, 5, ¶¶[0049]-[0058], [0064]-[0068]; MS-1003, ¶[76]. Thus, the *hybrid device* carried by the merchant is *enabled* to complete a purchase transaction *subsequent to the external PDK* of the customer *entering the*

proximity zone of the integrated RDC of the merchant's hybrid device *and based on the information stored by . . . external PDK*. MS-1003, ¶[76].

Of note, both the external PDK and the integrated PDK can connect to the integrated RDC, as taught by Giobbi-157: “Thus, if multiple PDKs 102 enter the proximity zone, the Reader 108 automatically determines which PDKs 102 are valid and buffers the received information from each valid PDK 102.” MS-1005, ¶[0062]. In some cases, the enablement can occur automatically, based on proximity alone such as “situations where the mere presence of a PDK 102 [(“*the external PDK*”)] within range of the Reader 108 is by itself a clear indication of the PDK owner's desire to complete a transaction.” MS-1005, ¶[0067]. Here, the RDC “detects the PDK 102 within range, authenticates the user [(“*based on the information stored by . . . the external PDK*”)], and executes a transaction.” MS-1005, ¶[0067]. Alternatively, if using the *integrated PDK*, the user of the hybrid device can “trigger” the authentication process to request profile information from the integrated PDK for the enablement of the hybrid device *based on the information stored by . . . the integrated PDK*. MS-1003, ¶[77]. Thus, a POSITA would have found obvious that with multiple PDKs having communications with the integrated RDC, the “transaction” is completed using information from either PDK. *Id.* Giobbi-157 teaches that “completing 416 the transaction includes enabling access to secure physical or digital assets” [(“*one or more of the hybrid*

device . . . are enabled”). and Giobbi-139 teaches that a PDK can “effectively enabling/disabling the device itself” (“*one or more of the hybrid device . . . are enabled*”). MS-1005, ¶[0063]; MS-1006, ¶[0089]; MS-1003, ¶[77].

Therefore, a POSITA would have found it obvious that the hybrid device is enabled *subsequent to the external PDK entering the proximity zone of the integrated RDC and based on the information stored by one or more of the external PDK and the integrated PDK*. MS-1003, ¶[78].

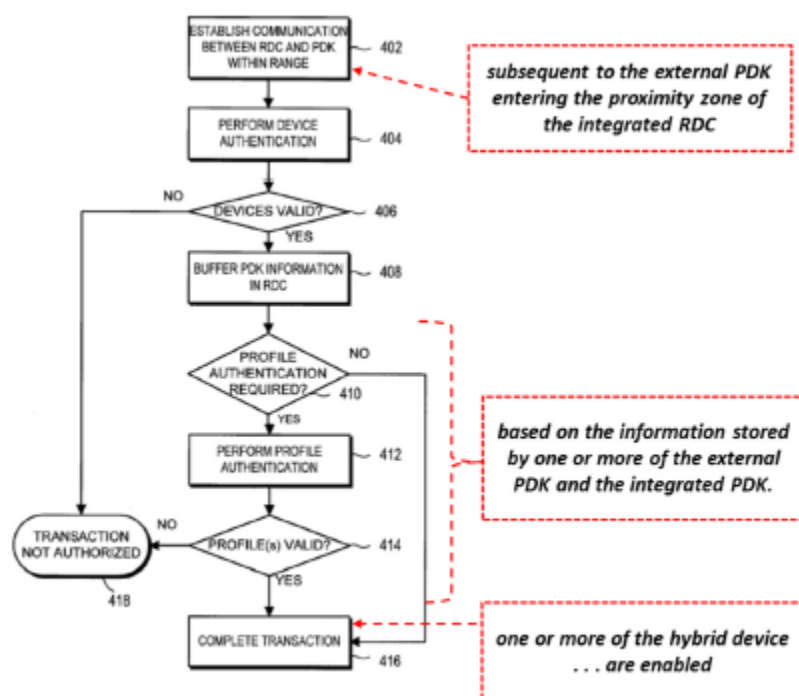


FIG. 4

MS-1005, FIG. 4.

[6]

Ground 1A/1B

See supra [5]; MS-1003, ¶[79]. As discussed above, Giobbi-157 also discloses that its PDK is integrated into a hybrid device, such as a cell phone. MS-1005, ¶[0035]; *see supra*, §III.A.1, [1.pre]. Giobbi-139 teaches integrating an RDC into the same type of device disclosed in Giobbi-157. MS-1006, ¶[0088]; MS-1005, ¶[0035]. Therefore, a POSITA would have found obvious that by integrating each device according to their teachings, a hybrid device is created, ***wherein the hybrid device is a cell phone***. MS-1003, ¶¶[79]-[80].

Giobbi-139 teaches that the use of PDKs and RDCs can “effectively enabl[e]/disabl[e] the device itself,” thus an ***external PDK enable[s] a cell phone***. MS-1006, ¶[0089]; MS-1003, ¶[81]. By enabling the cell phone, the device would then be able ***to provide cell phone service***. *Id.* A POSITA would have found obvious that the enablement of the entire device would subsequently enable the device to ***provide cell phone service***. *Id.* Alternatively, a POSITA would have found obvious that the integrated RDC connected to other components of the cell phone (such as a cellular modem), would control a component of the hybrid device to enable the device to ***provide cell phone service***. *Id.* Thus, the hybrid device being ***enabled to provide cell phone service subsequent to the external PDK entering the proximity zone of the integrated RDC (hybrid device) and based on***

the information stored by one or more of the external PDK and the integrated PDK,” would have been obvious to a POSITA. *See supra* [5]; MS-1003, ¶[81].

[8]

Ground 1A/1B

See supra [5]; MS-1003, ¶[82]. Giobbi-157 teaches that when PDKs come within range of RDCs an initial communication occurs and the RDCs retain connected PDKs in buffer memory. MS-1005, ¶[0062]. Giobbi states that communications “are automatically initiated each time a PDK 102 enters the proximity zone of the Reader 108. Thus, if multiple PDKs 102 enter the proximity zone, the Reader 108 automatically determines which PDKs 102 are valid and buffers the received information from each valid PDK 102.” MS-1005, ¶[0062]. Thus, a POSITA would have found obvious that *the integrated PDK* of the hybrid device *communicates with the external RDC* of a device (e.g., a credit card terminal, an ATM, a second hybrid device) *subsequent to the external PDK* (the Notary PDK) *entering the proximity zone of the integrated RDC* (during initialization). MS-1007, FIGS. 4A, 4B, and 6; 18:60-22:6; MS-1003, ¶[83].

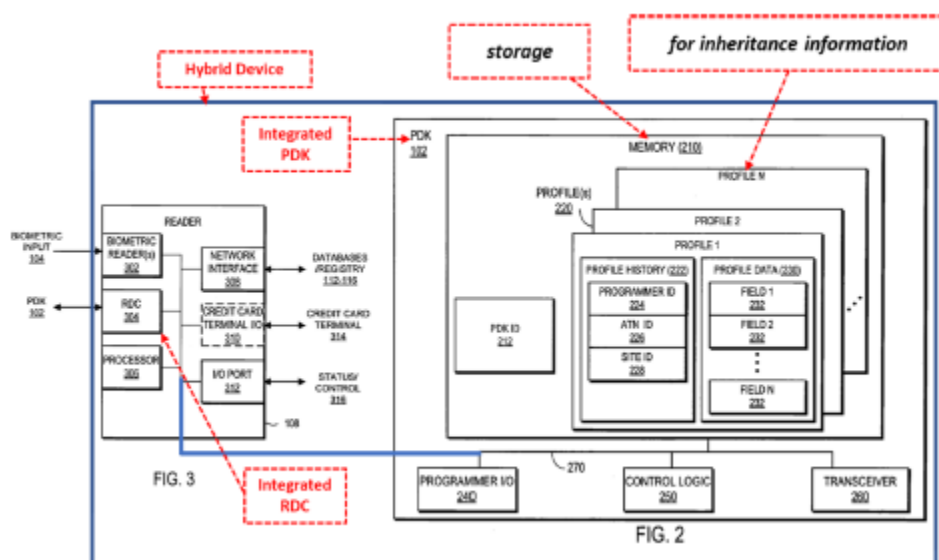
[9]

Ground 1A/1B

The '042 describes “inheritance” as the transfer of some information such as “authorization inheritance.” MS-1001, 2: 52-55; 17:46-60; MS-1003, ¶[84].

The profile information within a PDK contains authentication information.

MS-1005, ¶¶[0011]-[0012]. When the profiles are copied to another PDK, the other PDK effectively “inherits” the information from the first PDK, thereby enabling the second PDK to “inherit” the permissions of the first PDK. MS-1005, ¶[0043]. Giobbi-157 teaches that a “user can make copies of the PDK 102 or move profiles from one PDK 102 to another once the PDK 102 is unlocked.” MS-1005, ¶[0043]. Thus, a POSITA would have found obvious that 1) the storage within the PDK that is within *the hybrid device compris[es] storage for inheritance information* and 2) that when a profile is copied from one PDK to another—the information is inherited. MS-1003, ¶[85].



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

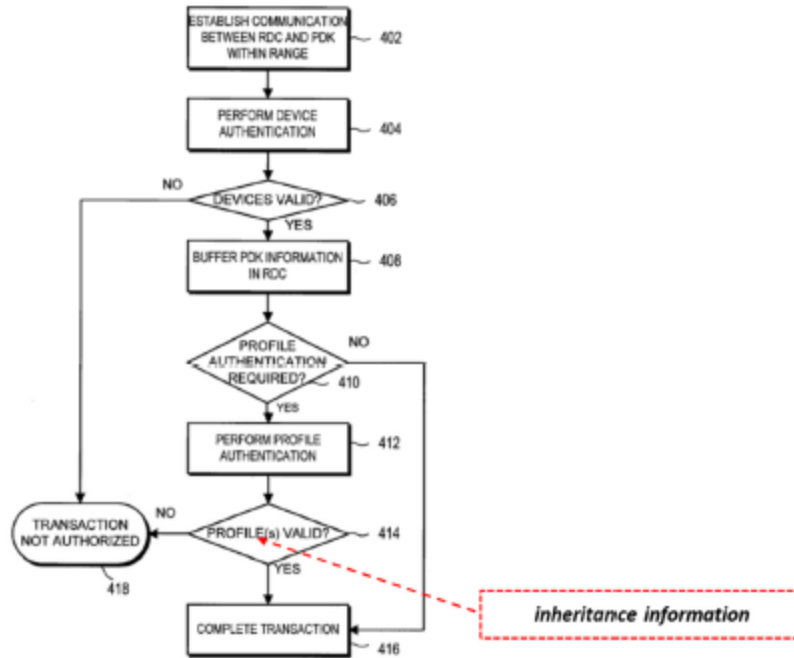


FIG. 4

MS-1005, FIG. 4.

[10.pre]

Grounds 1A/IB

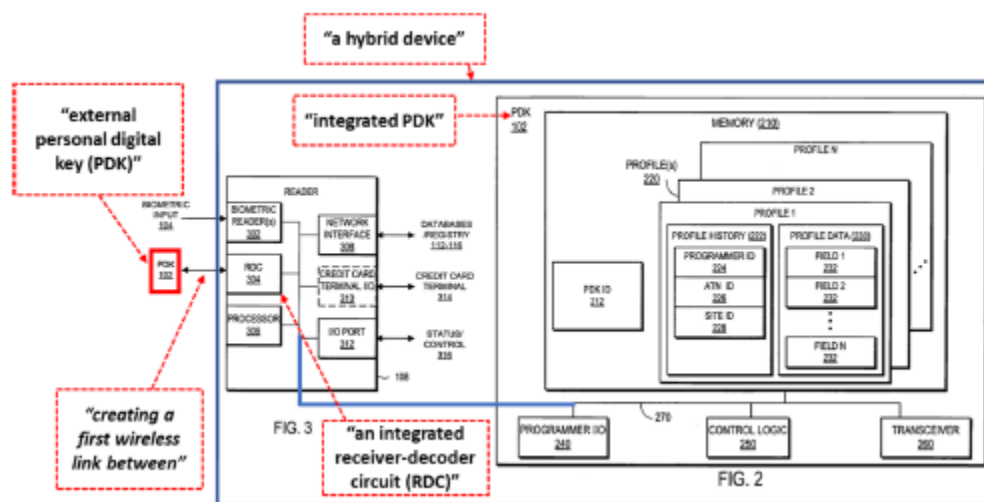
See supra [1.pre]. Giobbi-157 discloses that its techniques can be implemented as a “method.” MS-1005, Abstract, ¶[0011]; MS-1003, ¶[86].

[10.1]

Grounds 1A/IB

As described above in [1.1] and [1.2], the Giobbi-157-Giobbi-139 combination includes both an RDC and a PDK (“*the hybrid device including an integrated PDK and the integrated RDC*”). MS-1005, ¶¶[0011], [0027]-[0028], [0050]; *see supra* §III.A.3, [1.1]-[1.2]. Additionally, Giobbi-157 discloses that, “[w]hen a PDK 102 [“(an external personal digital key (PDK))”] comes within

range . . . communication is automatically established 402 between the RDC 304 [(“*integrated receiver-decoder circuit (RDC)*”)] . . . 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 personal digital key (PDK)*”). MS-1005, ¶[0059]. 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, ¶[87].



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

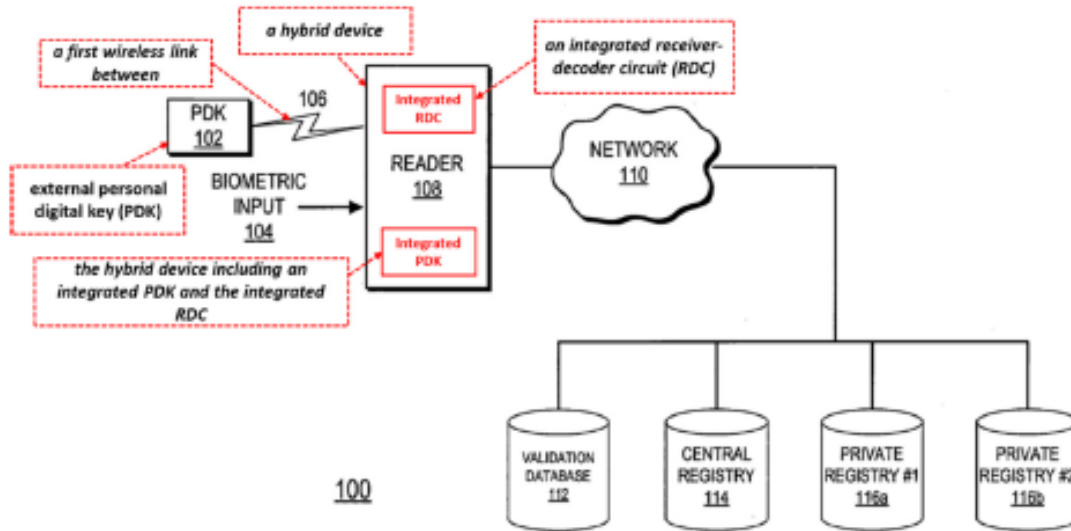


FIG. 1

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

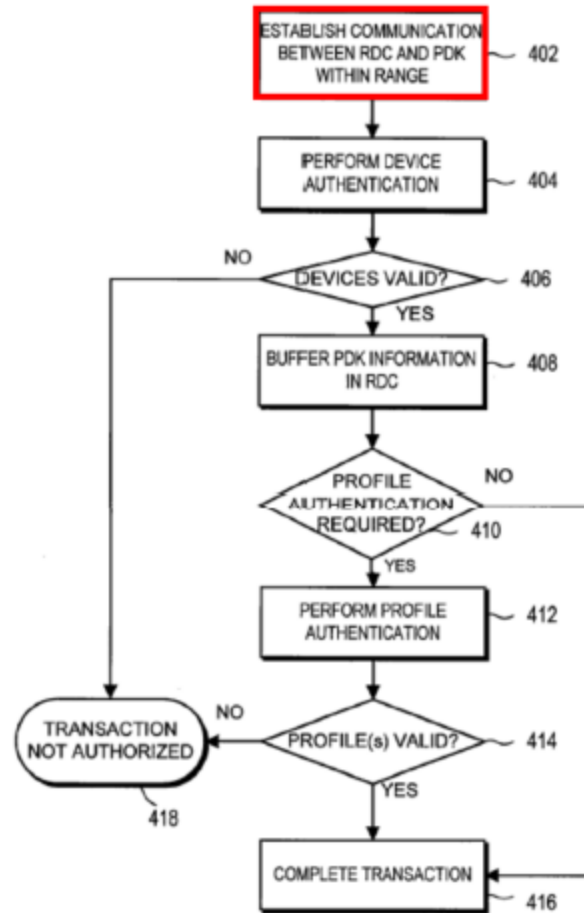


FIG. 4

MS-1005, FIG. 4.

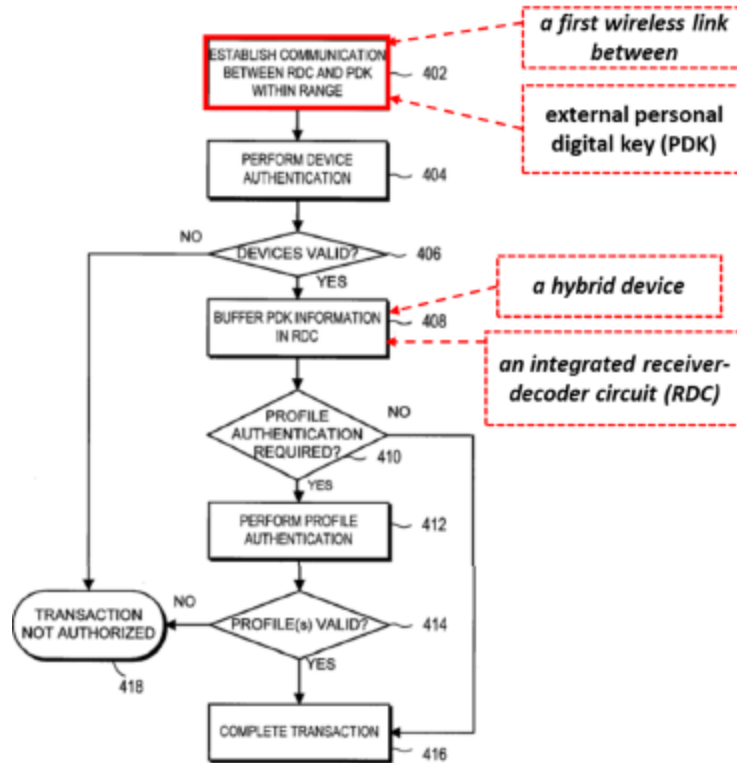


FIG. 4

MS-1005, FIG. 4.

[10.2]

Ground 1A/1B

Giobbi-157 discloses that, when an external “PDK 102 [(“*the external PDK*”)] comes within range of a Reader 108, communication [(“*receiving a first signal . . . via the first wireless link*”)] is automatically established 402 between the RDC 304[(“*at the integrated RDC*”)] . . . and the PDK 102 . . . when it enters a proximity zone of the [RDC]”. MS-1005, ¶[0059], FIGS. 4-5; *see supra* [1.1], [1.2]. 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 PDK”)*]” (*“receiving a first signal, at the integrated RDC via the first wireless link from the external device”*). MS-1005, ¶[0061].

Additionally, Giobbi-157 provides an 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, ¶[88].

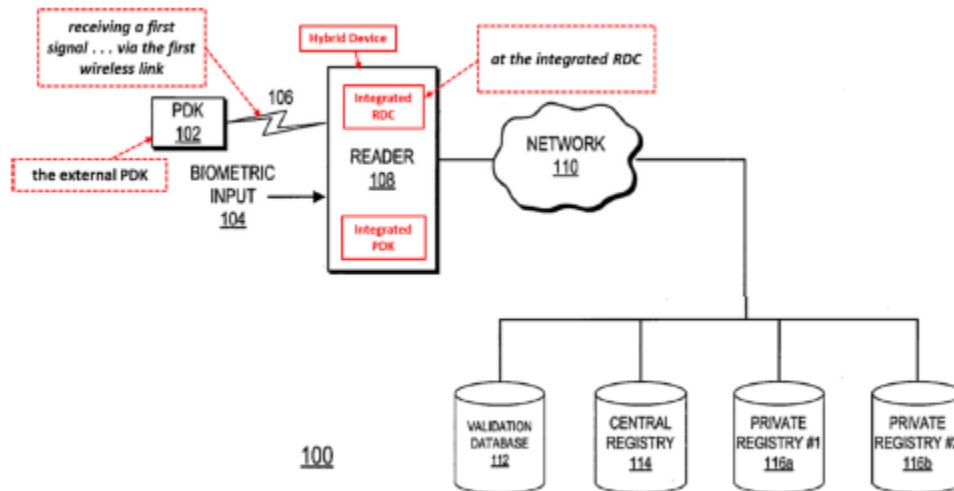


FIG. 1

MS-1005, FIG. 1 (modified to show the hybrid device of Giobbi-157/139).

Alternatively, a POSITA would have found obvious from the teachings of Giobbi-157/139, especially from FIG. 1 above and FIG. 4 below, that “[w]hen a PDK 102[*(“the external PDK”)*] comes within range of a Reader 108 communication [*“receiving a first signal ... via the first wireless link from the external PDK”*] is automatically established 402 between the RDC 304 [*“the*

integrated RDC”), of the Reader 108 and the PDK 102.” MS-1005, ¶[0059]; MS-1003, ¶[89].

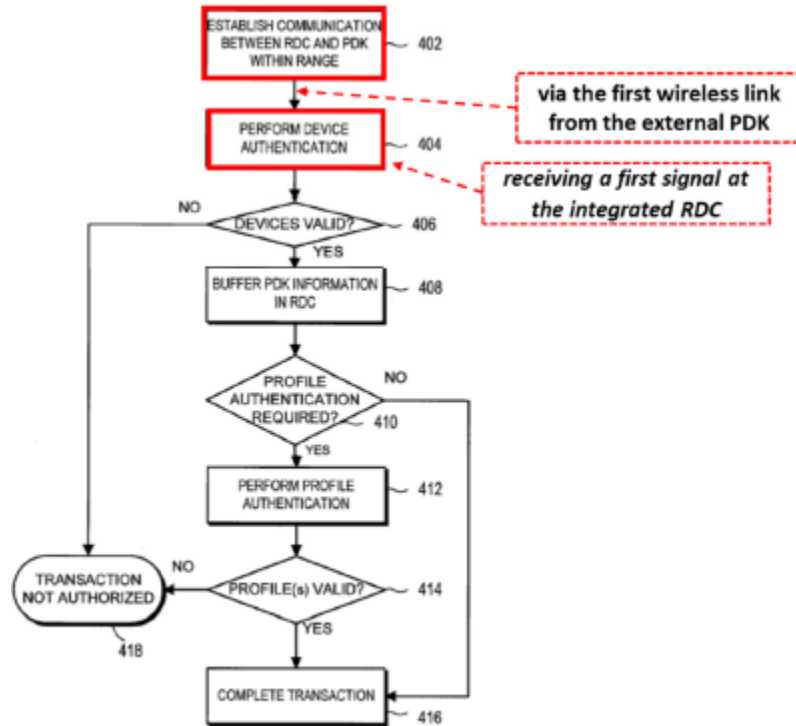


FIG. 4

MS-1005, FIG. 4.

[10.3]

Ground 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. 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.)” (“*enabling one or more of an application, a function, and service on . . . a device associated with an external RDC*”). 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” (“*enabling one or more of an application, a function, and service on . . . the hybrid device*”).

MS-1006, ¶[0089]. Accordingly, a POSITA would have found 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*”)) or “enabling/disabling the device itself” would require an electronic signal to be *generated* (“*an enablement signal*”). MS-1003, ¶[90]. Specifically, a POSITA would have understood from the PDK/RDC architecture that when PDKs and RDCs communicate for the purpose of *enabling one or more of an application, a function and a service on one or more of the hybrid device and a device associated with an external RDC*, that the *enablement signal* is first *generated* prior to transmission between the PDK and RDC. *Id.*

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 *generated* by a biometric scanner, 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.* Giobbi-139 further teaches that signals between PDKs and RDCs can “enable/disable” functions on the device with the integrated RDC (“***enabling one or more of an application, a function and a service on one or more of the hybrid device***”). MS-1006, ¶[0089]-[0091]; *see supra* §III.A.3. As seen in FIG. 4 below, because the RDC of the hybrid device or the external RDC can perform the “profile authentication” with the biometric input, the ***enablement signal*** can ***enable[] . . . on one or more of the hybrid device and a device associated with an external RDC***. MS-1005, FIG. 4; MS-1003, ¶[91].

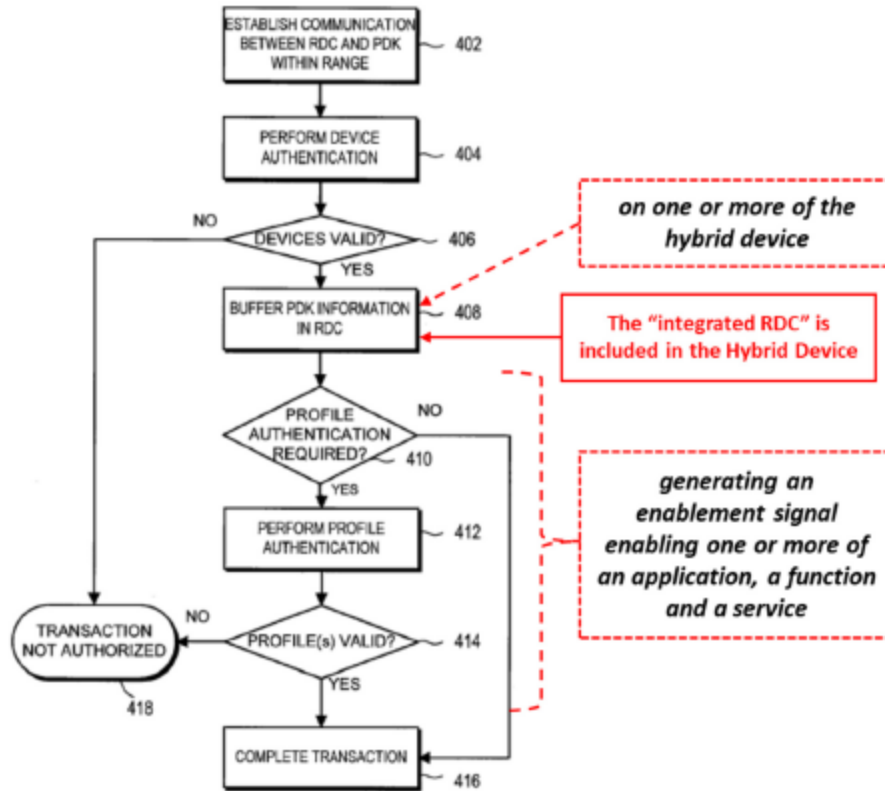


FIG. 4

MS-1005, FIGS. 4.

Furthermore, a POSITA would have found obvious from the teachings of Giobbi-139 that the connection between a PDK and RDC can authenticate or enable functionality associated with an RDC. MS-1006, ¶[0067]-[0069], [0087]-[0091]; MS-1003, ¶[92]. For example, Giobbi-157 teaches situations where the mere presence of a PDK 102 within range of the Reader 108 is by itself a clear indication of the PDK owner's desire to complete a transaction." MS-1005, ¶[0067]. Thus, the generation of these communication signals between a PDK and RDC are the *generat[ion]* of *an enablement signal enabling one or more of an*

application, a function and a service on . . . a device associated with an external RDC”). MS-1003, ¶[92].

[10.4]

Grounds 1A/IB

As discussed above, Giobbi-157 discloses a wireless authentication process (“*sending the enablement signal*”) between the PDK and RDC that “completes a transaction.” MS-1005, FIG.4. The authentication is first performed after a PDK has connected to an RDC (either the hybrid device’s integrated RDC or second device that includes an external RDC). (“*sending the enablement signal to one or more of the hybrid device and the device associated with an external RDC.*”). MS-1005, ¶[0074], FIGS. 3, 7D; *see supra* [14.1]-[14.3]. Giobbi-157 teaches that authentication of a PDK is used for “authorizing a transaction to be processed at the Reader 108 [device containing an RDC]” (“*the hybrid device*” or “*the device associated with an external RDC.*”). MS-1005, ¶[0033], FIG. 3; MS-1003, ¶[93].

Giobbi-139 teaches that a PDK (external to the hybrid device) can enable functions on a device or the device itself. MS-1006, ¶¶[0088-0090]. For example, Giobbi-139 teaches that the authentication process can enable the playing of music on a device. MS-1006, ¶[0037]; MS-1003, ¶[94].

Thus, a POSITA would have found obvious that an external PDK causes the RDC of the hybrid device to send the enablement signal to a component within the

hybrid device itself to enable a function within the hybrid device (“*sending the enablement signal to one or more of the hybrid device*”). See *supra* [1.3], [4]; MS-1006, ¶¶[0037], [0088-0090]; MS-1003, ¶[95].

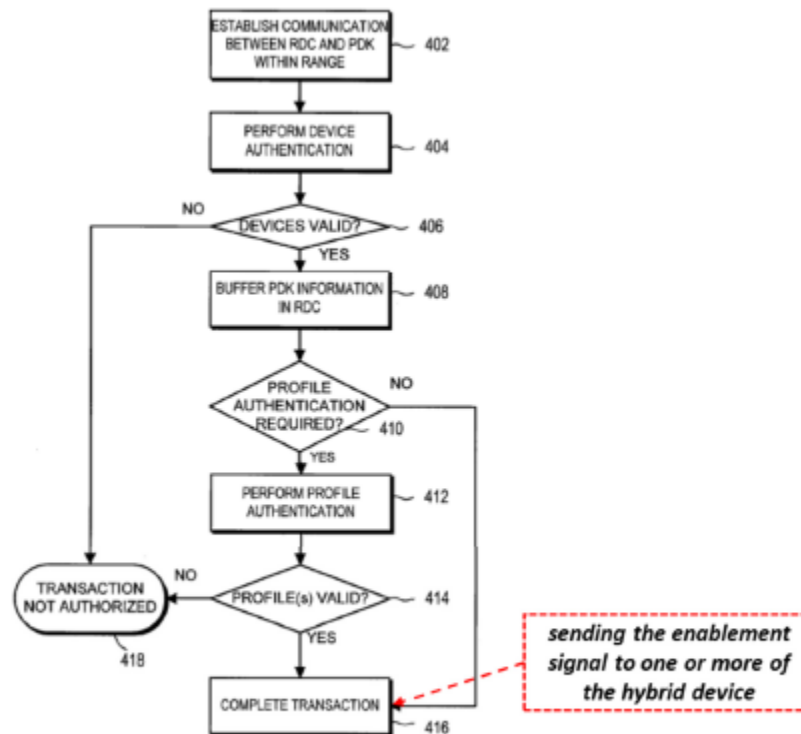


FIG. 4

MS-1005, FIG. 4.

Additionally, the hybrid device can use the integrated PDK to *send[] the enablement signal to . . . the device associated with an external RDC* and enable “an application, a function and a service” on the device associated with “*an external RDC.*” MS-1005, ¶¶[0057], [0061-0063]; MS-1006, ¶¶[0037], [0088-0090]; MS-1003, ¶[96]. For example, Giobbi-157 teaches that this can occur automatically, when “the mere presence of a PDK 102 within range of the Reader

108 is by itself a clear indication of the PDK owner's desire to complete a transaction." MS-1005, ¶[0067]. As seen below in FIG. 14, Giobbi-139 also teaches this architecture such that, a hybrid device within range of an external RDC (through the integrated PDK) can "*send[] the enablement signal to one or more of . . . the device associated with an external RDC*" MS-1005, ¶¶[0057], [0061-0063]; MS-1006, ¶[0037], [0081-0083], [0088-0090]; MS-1003, ¶[96]. A POSITA would have understood that the automatic communication and authentication of a PDK that completes the "transaction" would include *sending the enablement signal to . . . the device associated with an external RDC*. MS-1003, ¶[96].

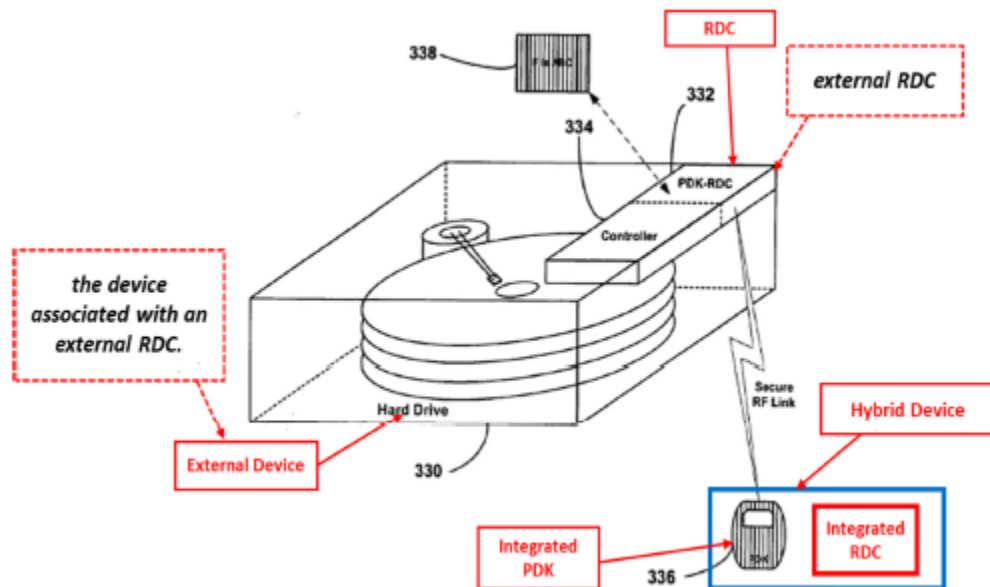


FIG. 14

MS-1006, FIG. 14.

[11]

Grounds 1A/IB

See supra §III.A.3, [6], [10.3], [10.4]; MS-1003, ¶[97] (“***wherein the hybrid device is a cell phone***”).

As discussed above, claim 10 recites “*sending the enablement signal to ... the hybrid device.*” *See supra* [10.4]. Here, claim 11 recites a “cell phone” as an example of a “hybrid device.” Thus, for the reasons stated above, “***the enablement signal is sent to the cell phone***” (the “*hybrid device*”). *See supra* [10.3]-[10.4]; MS-1003, ¶[98].

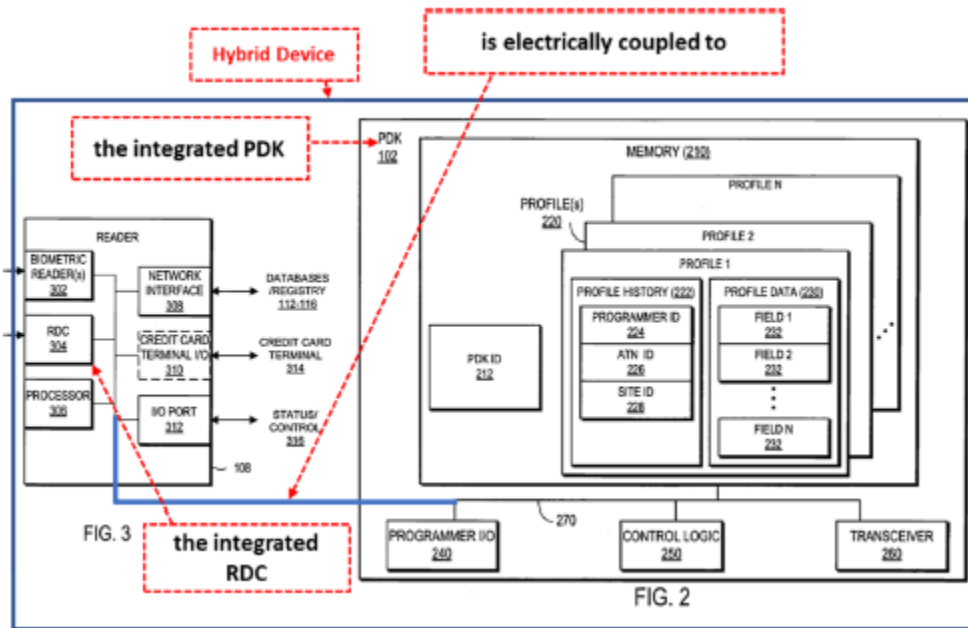
Giobbi-139 teaches that a device including an RDC (the hybrid device cell phone) can be “effectively enabl[ed]/disabl[ed]” using a PDK (“***enabling one or more of a service, a feature and a functionality of the cell phone***”). MS-1006, ¶[0089]. Giobbi-157 teaches that the entire “system and method provide[s] efficient, secure and highly reliable authentication for transaction processing and/or access control ***applications.***” MS-1005, ¶[0011]. Giobbi-157 further details the enablement of a “transaction” that “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-1003, ¶[99]. (“***enabling one or more of a service, a feature and a functionality of the cell phone***”)

[13.1]

Grounds 1A/IB

See *supra* [1.2]; MS-1003, ¶[100].

The hybrid device includes an *integrated PDK* that *is electrically coupled to the integrated RDC*. See *supra* [1.2]; §III.A.3; MS-1003, ¶[101].



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

[13.2]

Grounds 1A/IB

See *supra* [1.2]; [5], [6], and [8]; MS-1003, ¶¶[102]-[103].

Giobbi-157 teaches that the PDK profiles store information including “the specific hardware, Notary, and site used at the time the profile data was created and stored to the PDK.” MS-1005, FIG.2, ¶[0044]. During the initialization process a RDC must be used to communicate with the Notary PDK. MS-1005,

¶[0050]. A POSITA would have found obvious that during the initialization process, that the integrated RDC is *sending the enablement signal from the integrated RDC* (received from the Notary PDK) *to the integrated PDK*. MS-1003, ¶[104]. For example, during the initialization process the Notary PDK “administers [(enables)] the acquisition and storage of information in the PDK.” MS-1005, ¶[0029]. During this process, the Notary PDK signs the PDK being initialized with the Notary’s PDK ID number. MS-1005, ¶[0044]. Based on the discussed PDK/RDC architecture, a POSITA would have found obvious the use of an RDC (the integrated RDC) to retrieve the Notary PDK’s ID through standard PDK/RDC communication methods discussed. MS-1003, ¶[104]. In this example, the RDC then *send[s] the enablement signal* (at least some of which includes the Notary PDK’s ID) *from the integrated RDC* (communicating with the Notary PDK) *to the integrated PDK* that is being initialized. MS-1005, ¶[0044]; MS-1003, ¶[104].

Alternatively, Giobbi-139 teaches “enabling/disabling” a device entirely, or that “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,’” (*“sending the enablement signal”*). MS-1006, ¶¶[0087-0090]. Therefore, an external PDK can be used to protect digital storage (an integrated PDK’s memory) within the hybrid device. MS-1003, ¶[105] (citing MS-1006, ¶[0090]).

Giobbi-139, therefore, teaches the protection of data within the hybrid device from theft, or when left unattended, or if the user wishes to purposefully disable the integrated PDK, through use of an external PDK. MS-1006, ¶[0090]; MS-1003, ¶[106]. Giobbi-139 also teaches that a component or device controlled by an RDC (“*the integrated RDC*”) “will only function when the associated PDK-Key 336 is within range,” showing that individual components of a device (at least some portions of *the integrated PDK*) can be controlled with an external PDK. MS-1006, ¶[0071]. For example, a POSITA would have understood that during an authentication process that relies on an external PDK to access components within a hybrid device, the integrated RDC of the hybrid device, upon successfully authenticating the external PDK, *sends the enablement signal from the integrated RDC* to one or more internal components of the hybrid device to enable access to those components. MS-1006, ¶¶[0071], [0090]; MS-1003, ¶[106]. A POSITA would have understood that, in some implementations, the integrated PDK could be one of these internal components and, therefore, that, in this circumstance, the integrated RDC *sends the enablement signal from the integrated RDC to the integrated PDK*. MS-1003, ¶[106].

[13.3]

Grounds 1A/IB

The “first wireless link” of claim 10 is between the integrated RDC and an external PDK. *See supra* [10.1]; MS-1003, ¶[107].

Giobbi-157 teaches that RDCs automatically communicate with multiple, distinct PDKs that are within the proximity zone. MS-1005, ¶[0062]. Therefore, when *the integrated PDK* “comes within range of a Reader 108[(“*external RDC*”)], communication is automatically established[(“*create[es] a second wireless link*”)] 402 between the RDC 304 [(“*the external RDC*”)] of the Reader 108 and the PDK 102 [(“*the integrated PDK*”)].” MS-1005, ¶[0059]; MS-1003, ¶[108].

As Giobbi-157 repeatedly shows, communication between a PDK and an RDC is automatic within range. MS-1005, FIG. 4, ¶[0059]. In Giobbi-157’s examples, the PDK and RDC *creat[e] a second wireless link between the integrated PDK and an external RDC* to begin the PDK/RDC communication and authentication process. MS-1005, ¶¶[0011]-[0012], [0026]-[0028], [0030], FIGS. 1-4; MS-1003, ¶[109].

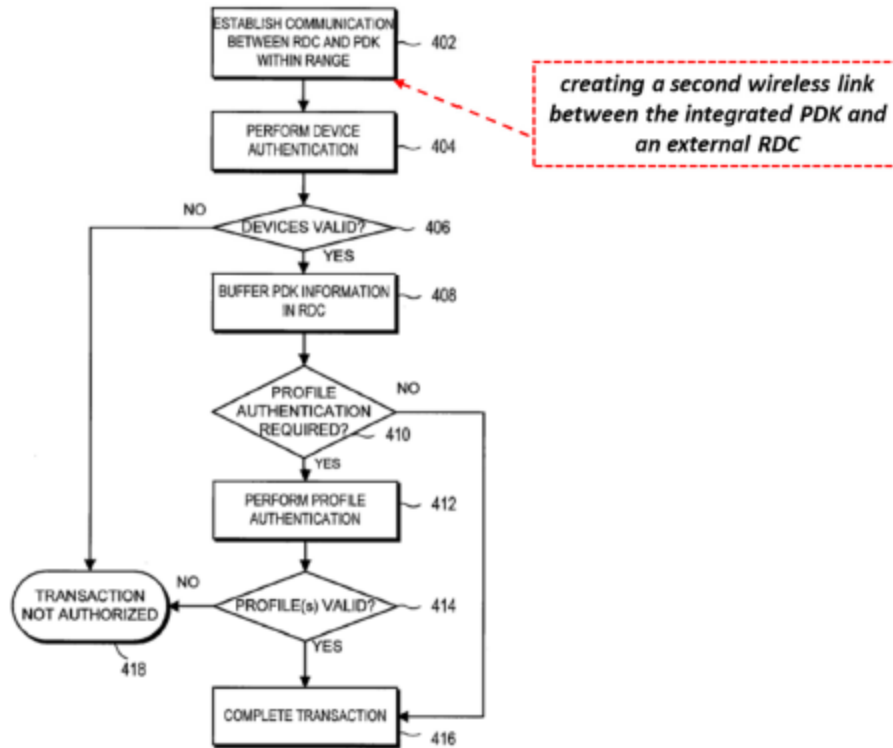


FIG. 4

MS-1005, FIG. 4

[13.4]

Grounds 1A/IB

See supra [10.4]. Giobbi-157 teaches that authentication of a PDK is used for “authorizing a transaction to be processed at the Reader 108 [(device containing an external RDC)].” MS-1005, ¶[0033], [0059], FIG. 3-4. Giobbi-139 teaches that a PDK can enable functions on a device or the device itself. MS-1006, ¶¶[0088-0090]. For example, Giobbi-139 teaches that the authentication process can enable the playing of music on a device. MS-1006, ¶[0037] ; MS-1003, ¶¶[110]-[111].

Thus as both Giobbi-157 and Giobbi-139 describe, the integrated PDK of the hybrid device can automatically establish a wireless link with an external RDC. MS-1005, ¶[0033], [0059], FIG. 3-4; MS-1006, ¶¶[0088-0090]. The hybrid device can then *send[] the enablement signal from the integrated PDK to the external RDC using the second wireless link*. MS-1005, ¶[0033], [0059], FIG. 3-4; MS-1006, ¶¶[0088]-[0090]; MS-1003, ¶[112].

[14]

Grounds 1A/IB

Giobbi-157 first teaches that signals between a PDK and RDC can be unencrypted stating that “[g]enerally, initial communication between the Reader 108 and the PDK 102 is not encrypted to provide faster and more power efficient communication.” MS-1005, ¶[0059]; MS-1003, ¶[113].

Giobbi-157 then teaches that the data sent from a PDK to an RDC is encrypted prior to transmission. MS-1005, ¶¶[0037], [0050], claim 30. Giobbi-139 further states that broadcasted content can be modified where the “[t]he modification is that the broadcast content is transmitted in a copy protected format.” MS-1006, ¶[0055]. For example, the *integrated PDK* can encrypt data (*modifies the enablement signal to produce a modified enablement signal*) for transmission over a secure link (*and the modified enablement signal is sent from the integrated PDK to the external RDC*). MS-1005, ¶[0047]. Then the RDC

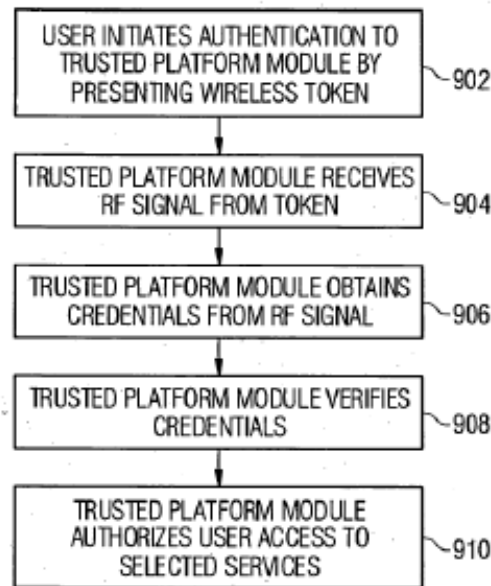
“provides the wireless interface to the PDK 102. Generally, the RDC 304 wirelessly receives data from the PDK 102 in an encrypted format and decodes the encrypted data for processing by the processor 306.” MS-1005, ¶[0050]; MS-1003, ¶[114].

B. [GROUND 2] – Claims 10-11 and 13-14 are rendered obvious by Broadcom

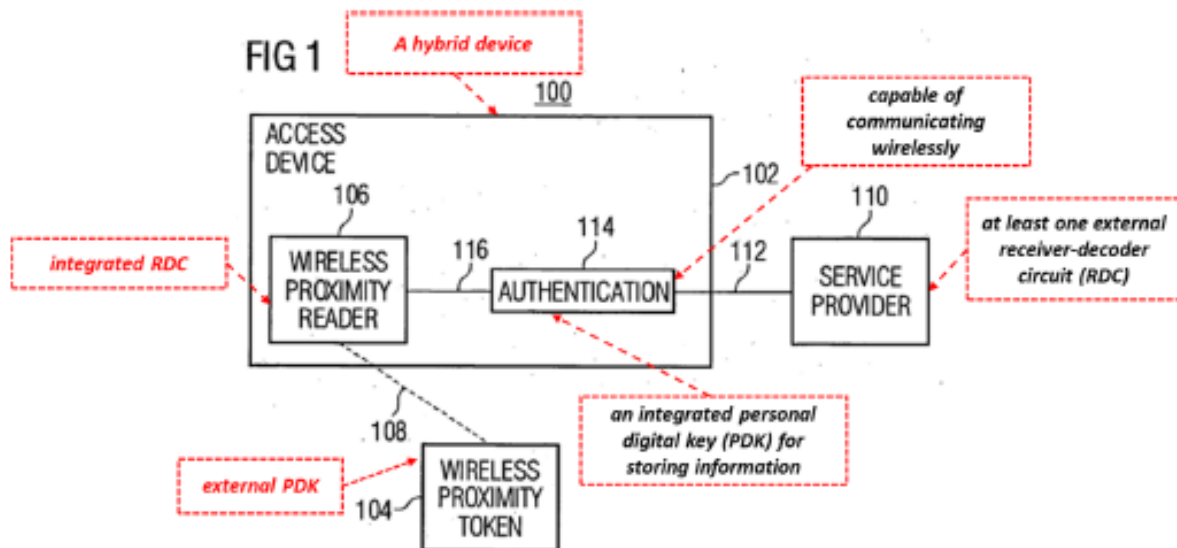
1. Overview of Broadcom

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, ¶[115].

FIG 9



MS-1008, FIG. 9.



MS-1008, FIG. 1 (annotated).

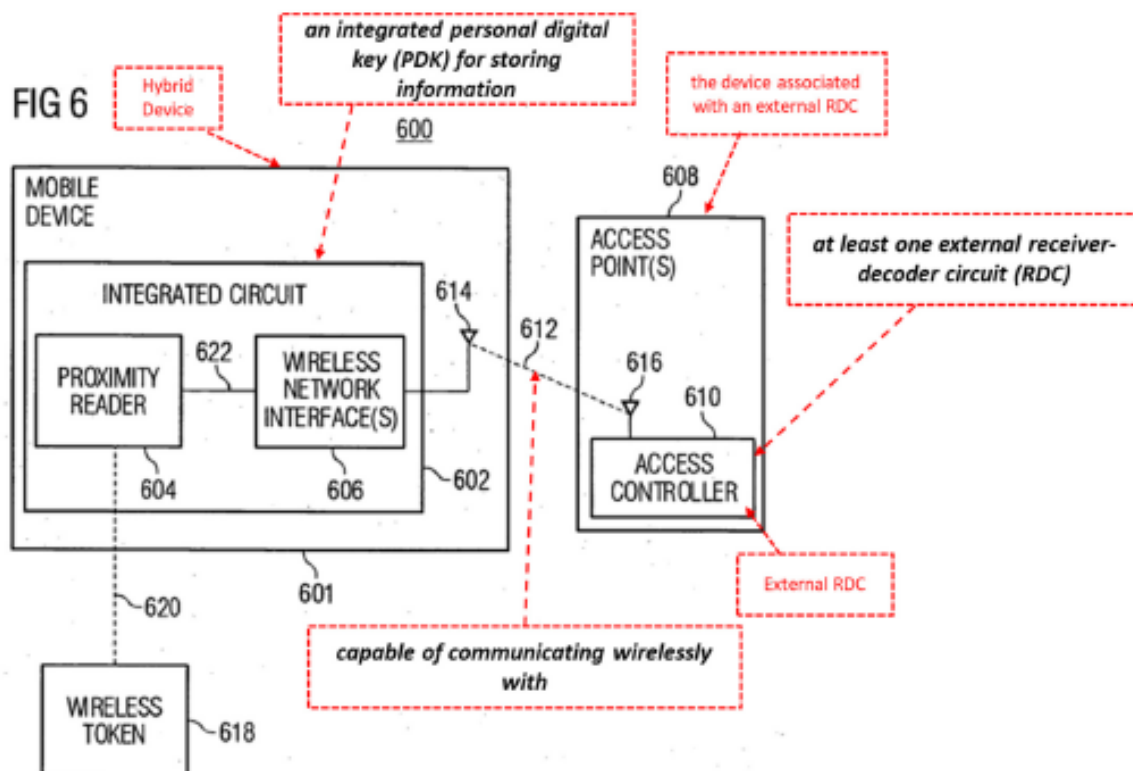
The authentication information is stored securely within memory that is “tamper resistant,” and “is not exposed in the mobile device.” MS-1008, ¶¶[0013], [0134], [0167], [0187]. The “authentication information” and “credentials” are

secured in this memory. MS-1008, ¶¶[0013], [0134], [0167], [0187], [0192]; MS-1003, ¶[116].

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, ¶[117].

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, ¶[118].

Broadcom discloses that the Access Device 102 can be a mobile phone that facilitates access to an access point for mobile communications, as illustrated below in FIG 6. MS-1008, ¶¶[0123]-[0124], [0191]; MS-1003, ¶[119].



MS-1008, FIG. 6 (annotated).

2. Analysis

[10.pre]

Broadcom discloses that its techniques can be embodied in a “method.” MS-1008, ¶¶[0009]-[0010]; MS-1003, ¶[120].

[10.1]

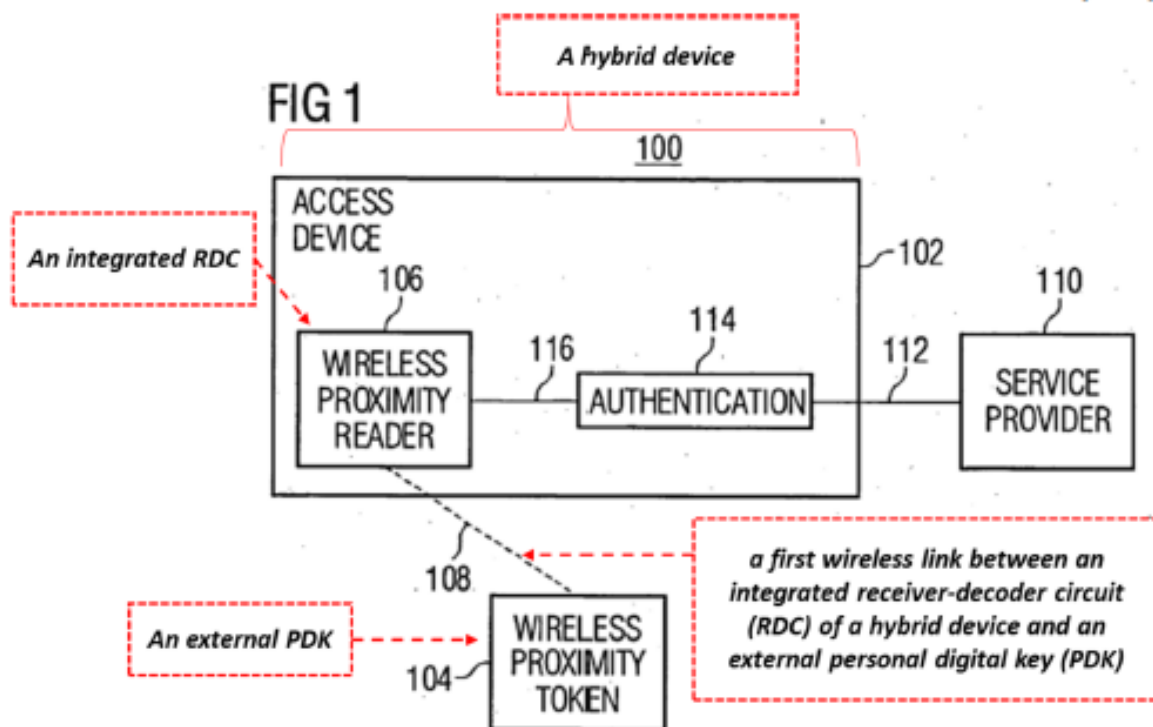
Broadcom discloses a “*hybrid device*,” (“a device comprising an integrated, secure memory storing local, secured information and an integrated receiver-decoder circuit” or “a device comprising an integrated personal digital key (PDK) and an integrated receiver-decoder circuit”). MS-1008, ¶¶[0110]-[0119], FIGS. 1, 6, MS-1003, ¶[121]; *see supra* §I.C.1. Broadcom’s “access device 102” reads

credentials stored on a “wireless proximity token 104,” (“an external PDK”) 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 . . . (PDK) and an integrated . . . (RDC)” for the reasons discussed above. *See supra*, §§I.C.1, III.B.1. As shown below in FIGS. 1 and 3, Broadcom’s cell phone includes an integrated PDK and an integrated RDC (a “*hybrid device*”). *Id*; MS-1003, ¶[121].

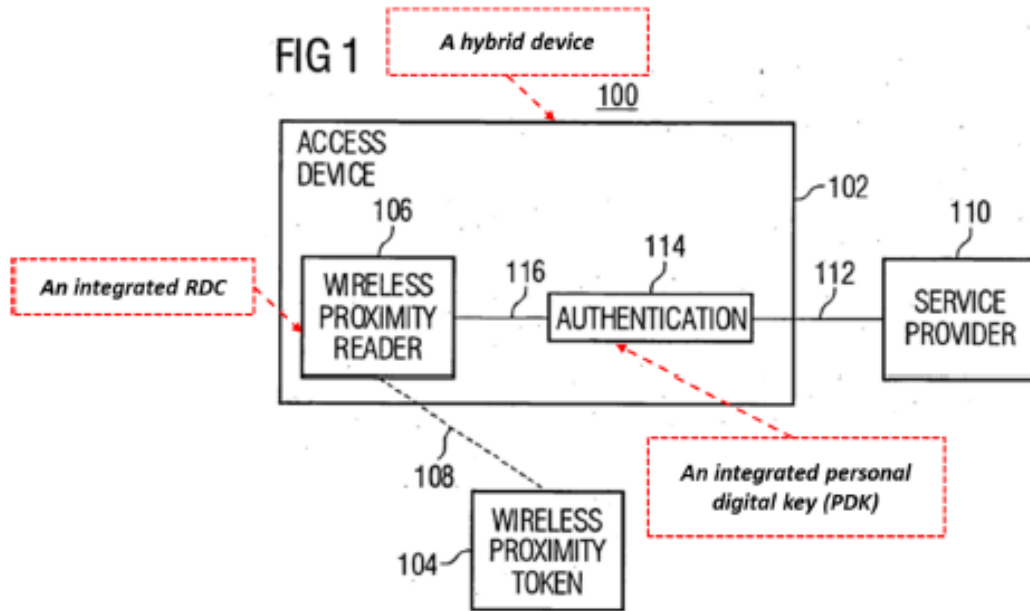


MS-1008, FIG. 1.

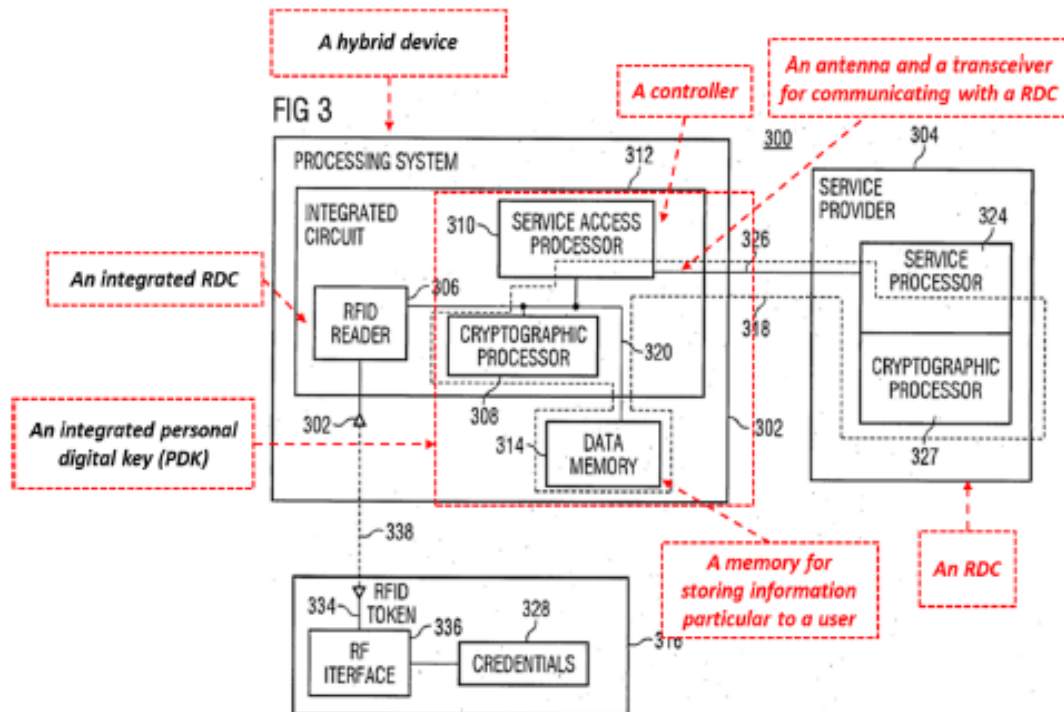
Broadcom also teaches “an operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for storing information particular to a user” as required by the above construction of a “**PDK**.” MS-1008, FIGS. 3, 6; *see supra*, §I.C.1. As Dr. Traynor explains, a POSITA would have recognized or found obvious that the “authentication component 114” would have included all of the features of a “PDK” (e.g., “an antenna ... a transceiver ... a controller and [a] memory ...”) because Broadcom discloses that the authentication component 114 performs functions that would have required these components. MS-1008, ¶¶[0116]-[0118] (“a cryptographically secured communication channel may be established between

the authentication component 114 and the service provider 110,” (“an antenna ... a transceiver”), “the authentication component 114 may process (e.g., encrypt or sign) the information before sending it to the service provider 110” (“a controller”), and “authentication information may include information from the token” (a “memory for storing information particular to a user”); MS-1003, ¶[122]. Dr. Traynor further explains that “a POSITA would have recognized that the subsequent figures of Broadcom (e.g., FIG. 3) provide implementation details for the overview presented in FIG. 1.” *Id.*

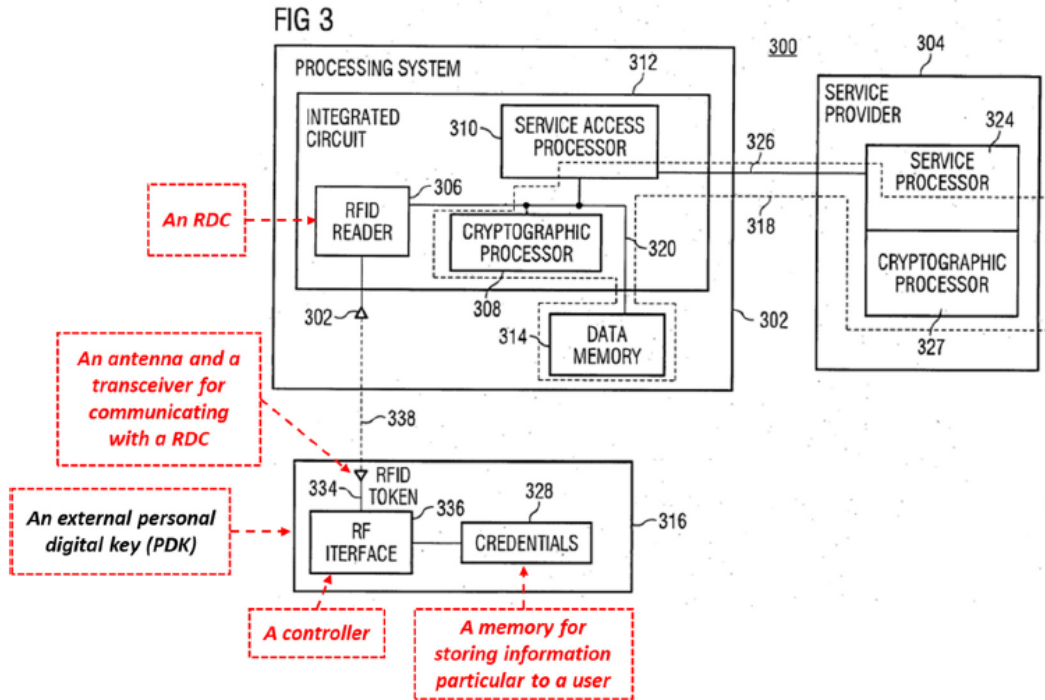
Additionally, Broadcom discloses that its access device 102 includes a “wireless proximity reader 106” (“*an integrated reader-decoder circuit (RDC)*”) to “receive signals 108” from a “wireless proximity token 104” that is “proximate to the access device 102.” MS-1008, ¶¶[0110]-[0119], FIGS. 1, 6. Broadcom also 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.” 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 also* MS-1008, ¶¶[0158], [0184] *and supra*, §§I.C.3; MS-1003, ¶[123].



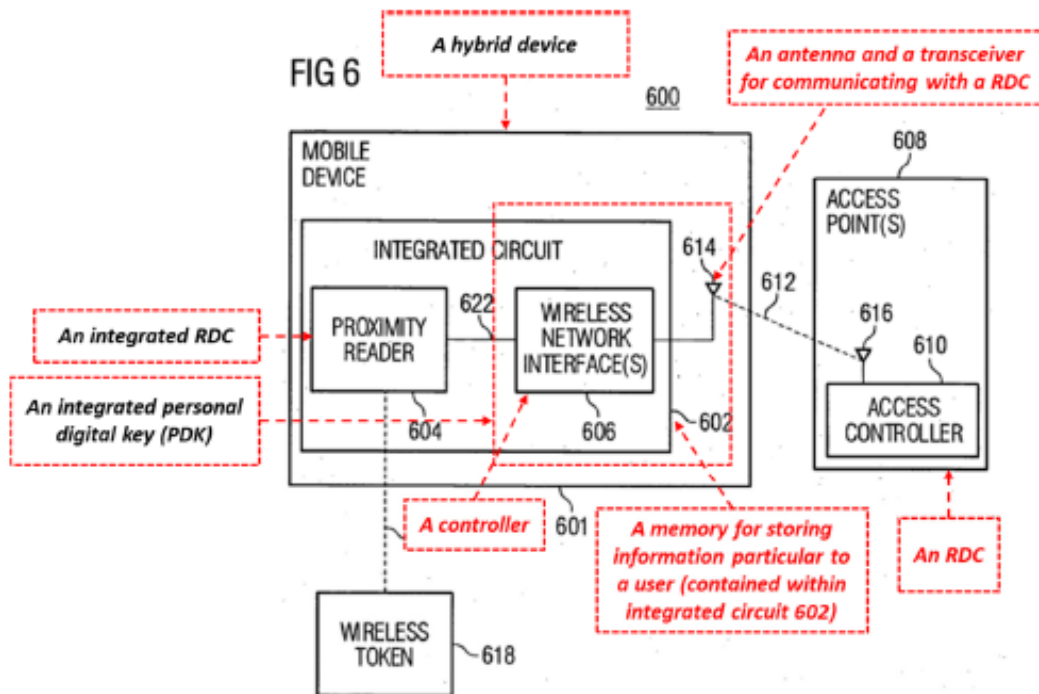
MS-1008, FIG. 1.



MS-1008, FIG. 3.



MS-1008, FIG. 3.



MS-1008, FIG. 6.

Broadcom discloses that “the access device 102 may automatically request a predefined service once the user places the token 104 [(“*an external personal digital key (PDK)*”)] 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 personal digital key (PDK)*”). MS-1008, ¶¶[0111]-[0117]; *see supra* §III.B.1, [1.1], [1.3]. As discussed above, the Broadcom’s *hybrid device includes* both “*an integrated PDK*” and an “*integrated RDC.*” MS-1008, ¶¶[0116]-[0119], [0135]-[0137], FIGS. 1, 3; MS-1003, ¶[124].

[10.2]

As discussed above in [10.1], 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 PDK*”). MS-1008, ¶[0111]; *see supra* [10.1]. For example, “[t]he proximity reader 501[(“*the integrated RDC*”)] may [] receive appropriate authentication information from the token 514 [(“*from the external PDK*”)]” MS-1008, ¶[0156]; MS-1003, ¶[125].

[10.3]

Broadcom discloses that “[a]ccess to secured services may be controlled based on the proximity of a wireless token.” MS-1008, ¶[0057]. Once the token is within proximity, the access device 102 sends “authentication-related information [(“**enablement signal**”)] 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 on ...one or more of the hybrid device and a device associated with an external RDC**”). MS-1008, ¶¶[0116]-[0119]. Specifically, the “term access may include, for example, acquiring, using, invoking, etc. Thus, data may be accessed by providing a copy of the data to the access device,” from **a device associated with an external RDC**. MS-1008, ¶[0122]; MS-1003, ¶[126].

Alternatively, Broadcom discloses that the “service may enable an access device [(“**hybrid 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” (“**generating an enablement signal enabling one or more of an application, a function and a service on ... the hybrid device**”). MS-1008, ¶[0120]. “[F]or example, invoking, interacting with or

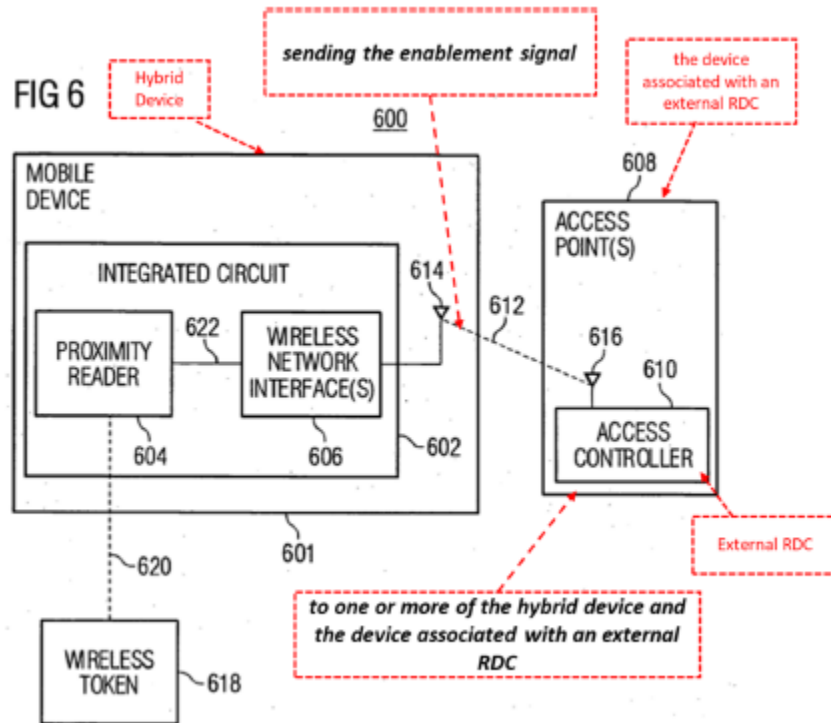
using the application or loading the application onto the access device” (“*on ... the hybrid device*”). MS-1008, ¶[0122]; MS-1003, ¶[127].

[10.4]

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 associated with an external RDC*”) returns an authentication decision to the access device 102 (“*sending the enablement signal 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.” MS-1008, ¶[0119]; MS-1003, ¶[128].

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, the user “use[s] the token 618 in a similar manner as discussed above” (e.g., as described in FIGS. 1 and 3) and “when a user moves the token 618 within relatively close proximity ... to the reader 604” it “send[s] authentication information to one or more wireless network interface(s) 606” which wirelessly communicates with a network access point 608. MS-1008, ¶¶[0164]-[0165]. In this embodiment, access to the network for a “mobile device 601” (“*the one or more of the application, the function, and the service*”) is enabled by

“communicating with a respective access controller 610 [*(the device associated with an external RDC)*] in [the] access point(s) 608 via RF signals 612 transmitted and received via one or more antennas 614 and 616” (*“sending the enablement signal”*). MS-1008, ¶[0165]; MS-1003, ¶[129].



MS-1008, FIG. 6.

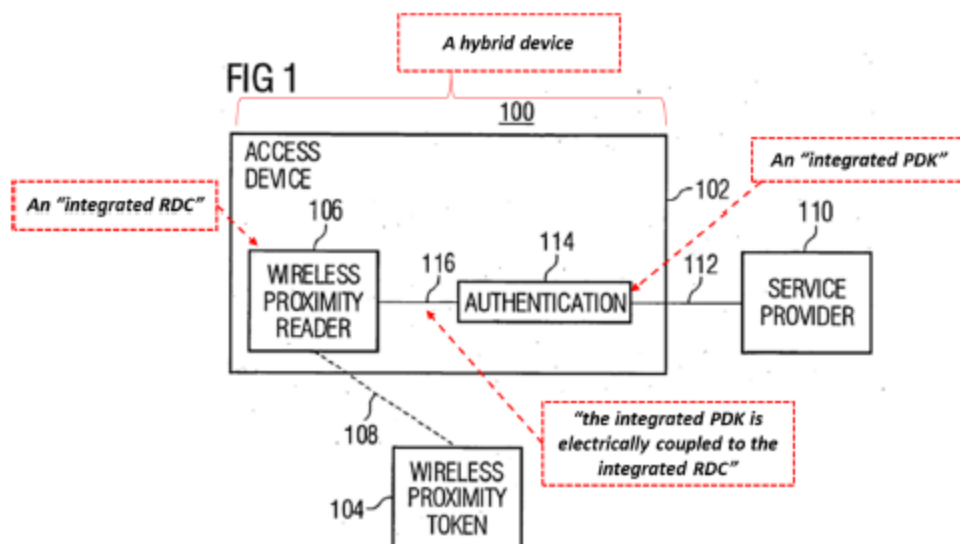
[11]

As described above in [10.3], one example access device is a “mobile device” and/or a “cellular phone” (*“the hybrid device is a cell phone”*) and that “access to the wireless network may be provided when a user moves the token 618 within relatively close proximity ... to the reader 604 [of mobile device 601]” (*“enabling one or more of a service, a feature and a functionality of the cell*

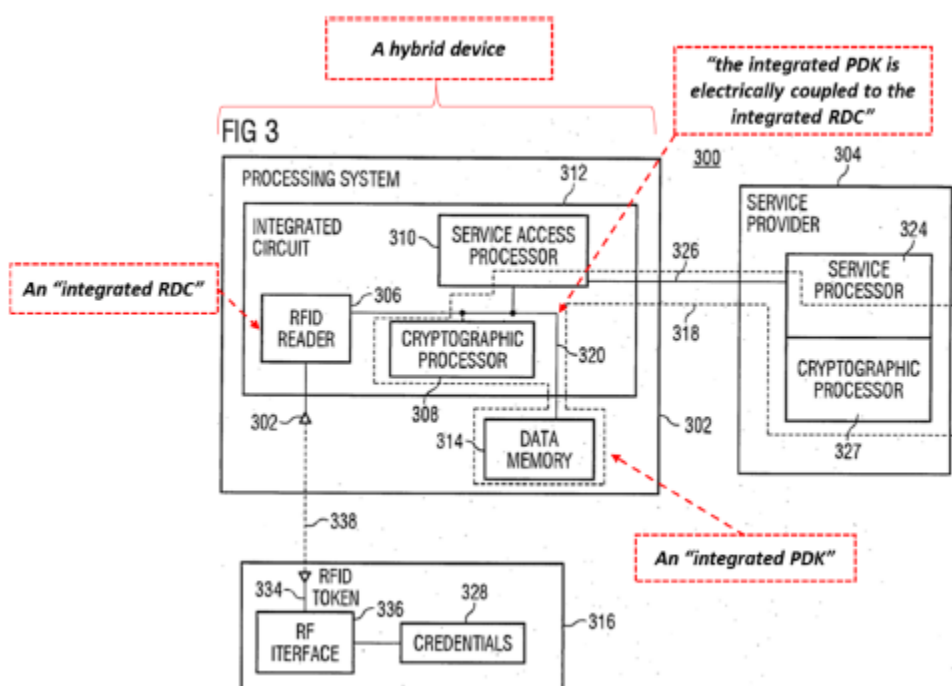
phone”). MS-1008, ¶¶[0125], [0163]-[0168], FIG. 6; *see supra* [10.3]. Broadcom discloses that this access is provided by an “access controller 610 in one or more access point(s) 608 via RF signals 612 transmitted and received via one or more antennas 614 and 616” (“*the enablement signal is sent to the cell phone*”). MS-1008, ¶¶[0164]-[0165], FIG. 6; MS-1003, ¶[130].

[13.1]

Broadcom discloses that “information may only pass between the reader 106 and the authentication component 114 via a connection 116” (“*the integrated PDK is electrically coupled to the integrated RDC*”). MS-1005, ¶[0116]. Additionally, Broadcom discloses, as part of its detailed FIG. 3 view, an “RFID reader 306” that is connected to a “data memory 314” via a “data bus 320” (“*the integrated PDK is electrically coupled to the integrated RDC*”). MS-1008, ¶¶[0133]-[0137], FIG. 3; *see supra* [1.2]; MS-1003, ¶[131].



MS-1008, FIG. 1.



MS-1008, FIG. 3.

[13.2]

As discussed above, Broadcom's wireless proximity reader 106 ("*integrated RDC*") is "configured to receive signals 108 (e.g., RF signals) from the wireless

proximity token 104” which include the “authentication information” (“***an enablement signal***”). MS-1008, ¶[0111]-[0118], [0148], [0156]-[0159], ; *see supra* [1.2]. Once received by the wireless proximity reader 106, the reader sends the information to the “authentication component 114” via a “cryptographically secured communication channel” such that the “determination of whether the token 104 is proximate the access device 102 is performed in a secure manner” (“***sending the enablement signal from the integrated RDC to the integrated PDK***”). MS-1008, ¶¶[0116]-[0117]; MS-1003, ¶[132]; *see supra* [1.2].

[13.3]

Broadcom discloses that the authentication component 114 is also “in secure communication with the service provider 110” and that “a cryptographically secured communication channel may be established[(“***creating***”)] between the authentication component 114 and the service provider 110” (“***a second wireless link between the integrated PDK and an external RDC***”). MS-1008, ¶[0117]; MS-1003, ¶[133].

[13.4]

Broadcom discloses that the access device 102 (particularly the authentication component 114) “request[s] access to a service from the service provider 110 by sending a signal over a communication media 112” which includes the “authentication-related information” (“***sending the enablement signal***”).

from the integrated PDK to the external RDC using the second wireless link”).

MS-1008, ¶¶[0113]-[0119]. After the service provider 110 receives the signal, “the service provider 110 may then enable access to the requested service.” MS-1008, ¶[0119]; MS-1003, ¶[134].

[14]

In its FIG. 3 detailed view, Broadcom discloses a “cryptographic processor 308” that is part of the integrated circuit 312 that implements Broadcom’s PDK. MS-1008, ¶¶[0137]-[0142], FIG. 3. This cryptographic processor 308 “perform[s] key exchange and encryption, decryption and/or authentication operations necessary to send and receive the encrypted information,” particularly, “[authentication] information ... received from an RFID token 316” (“*the integrated PDK modifies the enablement signal to produce a modified enablement signal*”). *Id.* Broadcom discloses that “[e]ncrypted [authentication] information [(“*the modified enablement signal*”)] also may be sent between the integrated circuit 312 and a cryptographic processor 322 and a service processor 324 in the service provider 304 via a communication link 326” (“*the modified enablement signal is sent from the integrated PDK to the external RDC*”). MS-1008, ¶[0138], FIG. 3; MS-1003, ¶[135].

IV. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION

A. 35 U.S.C. §325(d) – *Advanced Bionics*

Advanced Bionics and the *Becton* factors strongly favor institution.

Advanced Bionics LLC v. MED-EL Elektromedizinische Gerate GmbH, IPR2019-01469, Paper 6 (PTAB Feb. 13, 2020) (“*Advanced Bionics*”) (precedential);

Becton, Dickinson and Co. v. B. Braun Melsungen AG, IPR2017-01586, Paper 8 (PTAB Dec. 15 2017) (“*Becton*”) (precedential).

The Examiner never issued a prior art rejection during the ’042 Patent’s prosecution. MS-1002, 380-386. There is no indication that the Examiner substantively considered any of the prior art applied in this Petition. *Id.*

During prosecution, the applicant and the Examiner did not discuss the prior art applied in this Petition, so the prior art asserted in this Petition is not the same as, or substantially similar to, art and arguments previously presented to the Office. *See, generally*, MS-1002. Moreover, even if any of these references were somehow considered cumulative to references considered by the Examiner, none of the claims were examined in view of the asserted combinations applied in this petition. Accordingly, neither condition of the first prong of the *Advanced Bionics* framework is met, and there is no need to reach the second prong. *See, e.g., Oticon Medical AB et. al. v. Cochlear Ltd.*, IPR2019-00975, Paper 15 at 20 (PTAB Oct. 16, 2019) (precedential).

While Giobbi-139 is listed on the face of the '042 Patent, it is one of many references that were cited and, more critically, was not applied or discussed by the Examiner during prosecution. *See generally* MS-1002. Simply citing a reference on an information disclosure statement, with nothing more, does not favor denial. *See Navistar, Inc. v. Fatigue Fracture Tech., LLC*, IPR2018-00853, Paper 13 at 16-17 (PTAB Sept. 12, 2018) (“[T]he fact that [references] were of record, but not applied in any rejection by the Examiner . . . provides little impetus for us to exercise our discretion to deny institution under §325(d).”).

B. 35 U.S.C. §314(a) - *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. *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11, 6 (PTAB Mar. 20, 2020) (precedential) (“*Fintiv*”); MS-1012, 6-7, 9. As demonstrated below, a holistic analysis of the *Fintiv* framework favors institution.

Factor 1 is neutral because neither party has requested a stay. *Fintiv*, Paper 15, 12 (PTAB May 13, 2020). Moreover, the Board does “not attempt to predict” how a district court might adjudicate a future motion to stay, if/when filed. *See Fintiv*, 12; *Sand Revolution II, LLC v. Cont’l Intermodal Group – Trucking LLC*, IPR2019-01393, Pap. 24, 7 (June 16, 2020)(“*Sand Revolution*”)(informative);

Sotera Wireless Inc. v. Masimo Corporation, IPR2020-01019 Pap. 12, 14 (PTAB Dec. 1, 2020)(“*Sotera*”) (precedential).

Factor 2 weighs heavily against discretionary denial. The deadline for the PTAB’s Final Written Decision (FWD) in the proceeding that Apple seeks to join, IPR2024-00573 (the “Microsoft IPR”), is August 13, 2025. IPR2024-00573, Paper 12. In comparison, the District Court’s median time-to-trial of 32.7 months (EX-1026, p. 37) yields an estimated trial date in December 2026 (EX-1027, p. 4). Because the median time-to-trial projects a FWD before the projected trial dates, the discretionary denial is not merited.

In the co-pending District Court litigation, although a nominal trial date has been scheduled over 52 weeks after the *Markman* hearing (EX-1028, pp. 3, 5)), no firm trial date has been set. But the District Court schedule remains in flux, and even the *Director’s Guidance* recognizes that “scheduled trial dates are unreliable and often change.” MS-1012, 8. Here, the current schedule is unreliable because Apple has filed a Motion to Transfer Venue to transfer the case to the Northern District of California. EX-1027, p. 6-7). If this motion is successful, the FWD will likely issue substantially earlier than any trial date.

For these reasons, Factor 2 does not favor discretionary denial.

Factor 3 weighs against discretionary denial because Petitioner has diligently filed this Petition months ahead of the one-year time bar. Co-pending litigation is

in its early stages, with fact discovery not yet open and the scope of the infringement allegations unclear. EX-1028, p. 3. If an IPR is instituted, subsequent investments in the District Court litigation can further be minimized (*e.g.*, through a motion to stay).

Factor 4 weighs against discretionary denial. As noted above, the District Court schedule is far from certain and final invalidity grounds have yet to be determined. Given the uncertainty in the trial schedule⁸ and in the final invalidity grounds that will be at issue during trial in the District Court, Petitioner reserves the right to request further briefing and/or submit additional evidence after the parties gain more clarity regarding the District Court litigation schedule and grounds (*e.g.*, after a decision on the motion to transfer is issued). Because the amount of issue overlap between this petition and the litigation is unclear, Factor 4 does not merit discretionary denial.

Further, Petitioner hereby stipulates that if the PTAB institutes IPR2024-01398 and joins it with the Microsoft IPR,⁹ Petitioner will not pursue the grounds

⁸ In addition to uncertainty around the trial date, there is still uncertainty regarding the venue and subsequent scheduling if the pending motion to transfer is granted.

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

raised in this Petition in the parallel district court litigation with respect to the claims for which trial is instituted. *See Sand Revolution II, LLC v. Continental Intermodal Group–Trucking LLC*, IPR2019- 01393, Paper 24 at 7 (PTAB Jun. 16, 2020).

For Factor 5, Petitioner is a defendant in the co-pending litigation.

Factor 6 heavily weighs against discretionary denial due to the particularly strong merits of this Petition. As demonstrated in the Petition with reference to Dr. Traynor’s testimony and additional evidence, and institution of the proceeding that Apple seeks to Join (EX-1025) a finding of unpatentability of the Challenged Claims, which are obvious based on prior art references that were not utilized by the Examiner during prosecution is likely. The strength of the merits alone outweigh any inefficiencies born of parallel litigation. Additionally, Petitioner is concurrently filing a Motion for Joinder seeking to join this Petition to the instituted Microsoft IPR.

V. CONCLUSION

The Challenged Claims are unpatentable.

VI. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1)

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

Apple Inc. is the real party-in-interest.

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

The '042 Patent is the subject of the following civil actions: *Proxense, LLC v. Microsoft Corporation*, 6:23-cv-00319, W.D. Tex., filed May 2, 2023 (MS-1004), *Proxense, LLC v. Google LLC et al*, 6-23-cv-00320 (WDTX) filed May 2, 2023, and *Proxense, LLC v. Apple Inc.*, 6-24-cv-00143 (WDTX) filed March 18, 2024.

Additionally, Microsoft filed IPR2024-00573, and Google has filed IPR2024-00782 and IPR2024-01318 (seeking to join IPR2024-00573) against the '042 Patent. Petitioner is also concurrently filing a petition challenging the '042 Patent in IPR2024-01399 in which Petitioner seeks to join Google's challenge in IPR2024-00782. Patent and Applications related to the '042 Patent are found in EX-1029.

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

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

Petitioner provides the following designation of counsel.

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

D. Service Information

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

Date: September 12, 2024

Respectfully submitted,

DUANE MORRIS LLP

BY: /Philip W. Woo/

Philip W. Woo

USPTO Reg. No. 39,880

Duane Morris LLP

260 Homer Avenue #202

Palo Alto, CA 94301

ATTORNEY FOR PETITIONER

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 13,202 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Date: September 12, 2024

BY: /Philip W. Woo/

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

ATTORNEY FOR PETITIONER

CERTIFICATE OF SERVICE

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

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

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

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

Date: September 12, 2024

BY: /Philip W. Woo/

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

ATTORNEY FOR PETITIONER