

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

APPLE INC.,  
Petitioner

v.

PROXENSE, LLC  
Patent Owner

---

*Inter Partes* Review No.: IPR2025-00562

---

**PETITION FOR *INTER PARTES* REVIEW OF  
U.S. PATENT NO. 9,049,188**

## TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION .....	1
II. MANDATORY DISCLOSURES .....	2
A. Grounds for Standing (37 C.F.R. § 42.104(a)) .....	3
B. Real Party in Interest .....	3
C. Related Matters .....	3
D. Lead and Back-Up Counsel (37 C.F.R. § 42.8(b)(3)) and Service Information (37 C.F.R. § 42.8(b)(3)-(4)) .....	4
III. LEVEL OF SKILL IN THE ART .....	5
IV. OVERVIEW OF THE '188 PATENT .....	5
V. PROSECUTION OF THE '188 PATENT .....	6
VI. CLAIM CONSTRUCTION .....	7
VII. CITED ART .....	9
A. Giobbi '157 .....	9
B. Giobbi '139 .....	11
C. Broadcom .....	13
D. Dua .....	14
VIII. DISCRETIONARY FACTORS .....	17
A. Discretionary Denial Not Warranted Under <i>General         Plastic</i> .....	17
B. Discretionary Denial Not Warranted Under <i>Fintiv</i> .....	19
C. Discretionary Denial Not Warranted Under §325(d) .....	19

IX.	GROUND 1: GIOBBI '157, GIOBBI '139 AND DUA RENDER OBVIOUS CLAIMS 1-20.....	21
A.	Claim 1 .....	21
B.	Claim 2 The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on the hybrid device. ....	42
C.	Claim 3 The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on a device external to the hybrid device and communicatively coupled to the external RDC. ....	42
D.	Claim 4 The hybrid device of claim 1, wherein the local, secured biometric information for authenticating a user is based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a photograph, a signature, a voice sample, DNA and RNA.....	43
E.	Claim 5 The hybrid device of claim 1, wherein the integrated PDK stores local, secured financial information. ....	43
F.	Claim 6 The hybrid device of claim 1, wherein the integrated PDK stores local, secured financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information. ....	44
G.	Claim 7. The hybrid device of claim 1, wherein the hybrid device is a cell phone.....	44
H.	Claim 8. The hybrid device of claim 1, wherein the external PDK is included in jewelry. ....	44
I.	Claim 9. The hybrid device of claim 1, comprising a storage for inheritance information.....	44
J.	Claim 10 .....	45

K.	Claim 11 The method of claim 10 further comprising: sending the enablement signal to the hybrid device, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on the hybrid device. ....	47
L.	Claim 12 The method of claim 10 further comprising: sending the enablement signal to the hybrid device, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on a device external to the hybrid device and communicatively coupled to the external RDC. ....	47
M.	Claim 13 The method of claim 10, wherein the local, secured biometric information for authenticating a user is based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a photograph, a signature, a voice sample, DNA and RNA. ....	47
N.	Claim 14 The method of claim 10, wherein the integrated PDK stores local, secured financial information. ....	47
O.	Claim 15 The method of claim 10, wherein the hybrid device is a cell phone. ....	48
P.	Claim 16 The method of claim 10, wherein the external PDK is included in jewelry. ....	48
Q.	Claim 17 .....	48
R.	Claim 18 The method of claim 10, wherein the first signal includes inheritance information. ....	50
S.	Claim 19 The method of claim 10, wherein the external PDK is included in a watch. ....	50
T.	Claim 20 The hybrid device of claim 1, wherein the external PDK is included in a watch. ....	50
X.	GROUND 2: BROADCOM RENDERS OBVIOUS CLAIMS 1-7, 9-15 AND 17-18 .....	50
A.	Claim 1 .....	50

B.	Claim 2 The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on the hybrid device. ....	63
C.	Claim 3 The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on a device external to the hybrid device and communicatively coupled to the external RDC. ....	63
D.	Claim 4 The hybrid device of claim 1, wherein the local, secured biometric information for authenticating a user is based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a photograph, a signature, a voice sample, DNA and RNA. ....	63
E.	Claim 5 The hybrid device of claim 1, wherein the integrated PDK stores local, secured financial information. ....	64
F.	Claim 6 The hybrid device of claim 1, wherein the integrated PDK stores local, secured financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information. ....	64
G.	Claim 7. The hybrid device of claim 1, wherein the hybrid device is a cell phone. ....	65
H.	Claim 9. The hybrid device of claim 1, comprising a storage for inheritance information. ....	65
I.	Claim 10 .....	65
J.	Claim 11 The method of claim 10 further comprising: sending the enablement signal to the hybrid device, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on the hybrid device. ....	67

K.	Claim 12 The method of claim 10 further comprising: sending the enablement signal to the hybrid device, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on a device external to the hybrid device and communicatively coupled to the external RDC. ....	67
L.	Claim 13 The method of claim 10, wherein the local, secured biometric information for authenticating a user is based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a photograph, a signature, a voice sample, DNA and RNA. ....	67
M.	Claim 14 The method of claim 10, wherein the integrated PDK stores local, secured financial information. ....	67
N.	Claim 15 The method of claim 10, wherein the hybrid device is a cell phone. ....	68
O.	Claim 17 .....	68
P.	Claim 18 The method of claim 10, wherein the first signal includes inheritance information. ....	68
XI.	GROUND 3: BROADCOM AND GIOBBI '157 RENDER OBVIOUS CLAIMS 8, 16 AND 19-20 .....	69
A.	Claim 8. The hybrid device of claim 1, wherein the external PDK is included in jewelry. ....	69
B.	Claim 16 The method of claim 10, wherein the external PDK is included in jewelry. ....	70
C.	Claim 19 The method of claim 10, wherein the external PDK is included in a watch. ....	70
D.	Claim 20 The hybrid device of claim 1, wherein the external PDK is included in a watch. ....	70
XII.	SECONDARY CONSIDERATIONS .....	70
XIII.	CONCLUSION .....	71

## LIST OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 9,049,188 (the “’188 patent”)
1002	File History for U.S. Patent No. 9,049,188
1003	Declaration of Andrew Wolfe, Ph.D.
1004	U.S. Patent Pub. No. 2007/0245157 A1 (“Giobbi ’157”)
1005	U.S. Patent Pub. No. 2004/0255139 A1 (“Giobbi ’139”)
1006	U.S. Patent No. 9,042,819 (“Dua”)
1007	European Patent No. 1536306 A1 (“Broadcom”)
1008	Complaint, <i>Proxense, LLC v Apple Inc.</i> , 6:24-cv-00143, W.D. Tex., filed March 18, 2024
1009	Plaintiff’s Unopposed Motion for Leave to File Amended Complaint, <i>Proxense, LLC v Apple Inc.</i> , 6:24-cv-00143, W.D. Tex., filed October 28, 2024
1010	Order Granting Motion to Amend Complaint, <i>Proxense, LLC v Apple Inc.</i> , 6:24-cv-00143, W.D. Tex., issued November 13, 2024
1011	Claim Construction Order, <i>Samsung Electronics Co., Ltd. et al.</i> , 6:21-cv-00210, W.D. Tex., issued January 18, 2022
1012	Applications and patents related to the ’188 patent

## LIST OF CHALLENGED CLAIMS

Claim	U.S. Patent No. 9,049,188
1pre	A hybrid device comprising:
1A	an integrated personal digital key (PDK) for storing local, secured biometric information for authenticating a user and capable of communicating wirelessly with an external receiver-decoder circuit (RDC); and
1B	an integrated RDC for communicating wirelessly with at least one external PDK within a proximity zone,
1C	the integrated RDC coupled to the integrated PDK by a first signal line for communication,
1D	the integrated RDC coupled to at least one other component of the hybrid device by a second signal line,
1E	one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service.
2	The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on the hybrid device.
3	The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on a device external to the hybrid device and communicatively coupled to the external RDC.
4	The hybrid device of claim 1, wherein the local, secured biometric information for authenticating a user is based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a photograph, a signature, a voice sample, DNA and RNA.
5	The hybrid device of claim 1, wherein the integrated PDK stores local, secured financial information.
6	The hybrid device of claim 1, wherein the integrated PDK stores local, secured financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information.

7.	The hybrid device of claim <b>1</b> , wherein the hybrid device is a cell phone.
8.	The hybrid device of claim <b>1</b> , wherein the external PDK is included in jewelry.
9.	The hybrid device of claim <b>1</b> , comprising a storage for inheritance information.
10pre	A method comprising:
10A	creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external personal digital key (PDK),
10B	the hybrid device including an integrated PDK and the integrated RDC,
10C	wherein the integrated PDK stores local, secured biometric information for authenticating a user,
10D	receiving a first signal at the integrated RDC via the first wireless link from the external PDK;
10E	generating an enablement signal enabling one or more of an application, a function and a service.
11	The method of claim <b>10</b> further comprising: sending the enablement signal to the hybrid device, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on the hybrid device.
12	The method of claim <b>10</b> further comprising: sending the enablement signal to the hybrid device, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on a device external to the hybrid device and communicatively coupled to the external RDC.
13	The method of claim <b>10</b> , wherein the local, secured biometric information for authenticating a user is based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a photograph, a signature, a voice sample, DNA and RNA.
14	The method of claim <b>10</b> , wherein the integrated PDK stores local, secured financial information.

15	The method of claim <b>10</b> , wherein the hybrid device is a cell phone.
16	The method of claim <b>10</b> , wherein the external PDK is included in jewelry.
17A	The method of claim <b>10</b> , wherein the integrated PDK is electrically coupled to the integrated RDC, and the method further comprises: creating a second wireless link between the integrated PDK and an external RDC; and
17B	sending the enablement signal from the integrated PDK to the external RDC using the second wireless link,
17C	the enablement signal based on financial information stored locally and securely on the integrated PDK and used to complete a financial transaction.
18	The method of claim <b>10</b> , wherein the first signal includes inheritance information.
19	The method of claim <b>10</b> , wherein the external PDK is included in a watch.
20	The hybrid device of claim <b>1</b> , wherein the external PDK is included in a watch.

**GROUNDS OF CHALLENGE (37 C.F.R. § 42.204(b)(2))**

<b>No.</b>	<b>Ground for Challenge</b>
1	Giobbi '157, Giobbi '139 and Dua render obvious claims 1-20
2	Broadcom renders obvious claims 1-7, 9-15 and 17-18
3	Broadcom and Giobbi '157 render obvious claims 8, 16 and 19-20

## I. INTRODUCTION

Petitioner Apple Inc. (“Petitioner”) requests *inter partes* review (IPR) of claims 1-20 of U.S. Patent No. 9,049,188 (the “’188 patent,” Ex. 1001). This is Petitioner’s first IPR directed to the challenged claims. This Petition is substantially similar to the petition in *Samsung Electronics America, Inc. v. Proxense, LLC*, IPR2021-01438, filed on August 26, 2021 (the “Samsung IPR”), which was instituted on February 28, 2022 and terminated by agreement of the parties on February 24, 2023 before any final written decision. IPR2021-01438, Papers 1, 12, 33.

The claims of the ’188 patent recite a “hybrid device” (*e.g.*, a cell phone) that uses a Personal Digital Key (PDK) in conjunction with a Receiver Decoder Circuit (RDC) to access secure data on the hybrid device. Essentially, the claimed RDC acts as a digital lock protecting secured data on a device like a phone, and the PDK functions as a digital key: when an authorized PDK makes an access request to a corresponding RDC, the secured data is made available. The claimed hybrid device includes both an internal PDK (key) and an internal RDC (lock), and these integrated components communicate with external PDKs and external RDCs in other devices.

But this type of digital lock-and-key system was known years before the ’188 patent was filed. For example, in 2004—three years before the ’188

patent's earliest filing date—the Giobbi '139 system disclosed a hybrid device (also a cell phone) that used a PDK and an RDC to secure data in the exact same manner. Likewise, the Giobbi '157 reference also expressly discloses using a PDK and an RDC to access secured data on a hybrid device like a phone.

In fact, numerous prior art patents teach the same concept of using a digital lock-and-key to secure a data or service. For example, Dua discloses an RFID system in portable devices, such as phones, that uses the same type of digital lock-and-key recited in the claims '188 patent. Likewise, the Broadcom reference uses a digital key (referred to as a “token”) and a digital lock (referred to as a “reader”) to secure access to a wireless network. Thus, the challenged claims merely recite the well-known concept of securing data or services with a digital lock and key which was known in the art years before the '188 patent was filed. Accordingly, the challenged claims should be held unpatentable.

## **II. MANDATORY DISCLOSURES**

Pursuant 37 C.F.R. § 42.8(a)(1), the following mandatory notices are provided as part of this Petition.

**A. Grounds for Standing (37 C.F.R. § 42.104(a))**

Petitioner respectfully requests *inter partes* review (“IPR”) of Claims 1-20 (“Challenged Claims”) of the ’188 patent (Ex. 1001), which is indicated as assigned to Proxense LLC (“Patent Owner” or “Proxense”).

Petitioner certifies that the ’188 Patent is available for *inter partes* review and Petitioner is not barred or estopped from requesting review of the Challenged Claims on the grounds identified in this Petition.

**B. Real Party in Interest**

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner certifies Apple Inc. is the real party-in-interest.

**C. Related Matters**

As of the filing date of this Petition, the ’188 patent is or has been involved in the following matters:

- *Proxense, LLC v. Apple Inc.*, No. 6:24-cv-00143 (W.D. Tex. March 18, 2024) (pending, but dismissed with prejudice regarding the ’188 Patent);
- *Proxense, LLC v. Samsung Electronics, Co., Ltd. et al.*, No. 6.21-CV-00210 (W.D. Tex. March 5, 2021) (terminated); and
- *Samsung Electronics America, Inc. v. Proxense, LLC*, IPR2021-01438 (PTAB August 26, 2021) (terminated).

Exhibit 1012 lists the applications and patents related to the '188 patent according to the Patent Center.

**D. Lead and Back-Up Counsel (37 C.F.R. § 42.8(b)(3)) and Service Information (37 C.F.R. § 42.8(b)(3)-(4))**

Petitioner provides the following counsel and service information.

Pursuant to 37 C.F.R. § 42.10(b), a Power of Attorney accompanies this Petition. Petitioner agrees to accept electronic service at the email addresses listed below.

LEAD COUNSEL	BACK-UP COUNSEL
PHILIP W. WOO USPTO Reg. No. 39,880 DUANE MORRIS LLP, 260 Homer Avenue #202 Palo Alto, CA 94301 P: (650) 847-4145 F: (650) 644-0150 <a href="mailto:PWWoo@duanemorris.com">PWWoo@duanemorris.com</a>	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 <a href="mailto:MTSquire@duanemorris.com">MTSquire@duanemorris.com</a>
	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 <a href="mailto:DSBartow@duanemorris.com">DSBartow@duanemorris.com</a>
	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](mailto:PHBelnap@duanemorris.com)

### **III. LEVEL OF SKILL IN THE ART**

Petitioner proposes that a Person of Ordinary Skill in the Art (“POSITA”) would have had a bachelor’s degree in computer or electrical engineering (or an equivalent degree) with at least three years of experience in the field of encryption and security (or equivalent experience). Petitioner further proposes that more education could compensate for less experience and vice versa. Ex. 1003, ¶ 23.

### **IV. OVERVIEW OF THE ’188 PATENT**

The ’188 patent is directed towards a “hybrid device” that includes an integrated personal digital key (PDK) and an integrated receiver-decoder circuit (RDC) that are coupled in communication with each other. Ex. 1001 at 1:66-2:3. 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. Ex. 1001 at 21:50-56. The specification discloses that the integrated PDK is capable of storing local, secured financial information or secured biometric information for authenticating a user. Ex. 1001 at 22:25-27, 22:48-49. Similarly, the external

PDK is also capable of storing information. Ex 1001 at 16:34-36. *See also*, Ex. 1003, ¶ 24

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. Ex. 1001 at 16:23-25. 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. Ex. 1003, ¶ 25

## **V. PROSECUTION OF THE '188 PATENT**

On September 22, 2014, the Examiner issued a Non-Final rejection based on non-statutory double-patenting and obviousness based on patents Finn and Hochstein. Ex. 1002 at 104. On December 22, 2014, the applicant withdrew pending claim 1 to avoid the non-statutory double-patenting rejection as well as the 103 rejection, proposing new independent claims which added more details regarding the components of the hybrid device. *Id.* at 423-24. In response, the Examiner issued a Notice of Allowance with an Examiner's Amendment, amending the independent claims to require that the information stored on the PDK be "biometric" information "for authenticating

a user.” Ex. 443-444. These claims issued as amended by the Examiner. *See also* Ex. 1003, ¶ 26.

## **VI. CLAIM CONSTRUCTION<sup>1</sup>**

The challenged claims of the ’188 patent are construed herein “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. § 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. § 42.100(b). “[C]laim terms need only be construed to the extent necessary to resolve the controversy.” *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011). Other than any terms expressly construed herein, Petitioner maintains that no specific construction of any claim term is required because the prior art references relied on in this Petition meet or disclose each of the claim terms under any reasonable construction. Petitioner reserves its right to respond to any claim

---

<sup>1</sup> Petitioner does not concede that any term not construed herein meets the statutory requirements of 35 U.S.C. § 112, or that the Challenged Claims recite patentable subject matter under 35 U.S.C. § 101.

constructions raised by the Patent Owner or the Board in the future. Ex. 1003, ¶ 27.

“Personal Digital Key (PDK)” (claims 1, 10)

In the Samsung IPR, the only term that the Board found necessary to construe was “Personal Digital Key (PDK).” IPR2021-01438, Paper 12, 16. The Board determined that “the term ‘PDK’ for ‘storing local, secured biometric information’ for authenticating a user, as claimed, encompasses a local memory for storing biometric information for authenticating a user, wherein the information is secured.” IPR2021-01438, Paper 12, 18-19.

In the litigation between Samsung and Proxense, *Proxense, LLC v. Samsung Electronics Co., Ltd. et al.*, No. 6:21-CV-00210-ADA (W.D. Tex) (the “Samsung Litigation”), the district court construed the term “Personal digital key” consistent with Proxense’s proposal as “[a]n operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for storing information particular to a user.” Ex. 1011 (claim construction Order, *Proxense, LLC v. Samsung Electronics Co., Ltd. et al.*, No. 6:21-CV-00210-ADA (W.D. Tex) January 18, 2022).

Under either the Board’s construction from the Samsung IPR or the district court’s construction from the corresponding litigation, the prior art

discloses or teaches a “Personal Digital Key (PDK),” as discussed in more detail below.

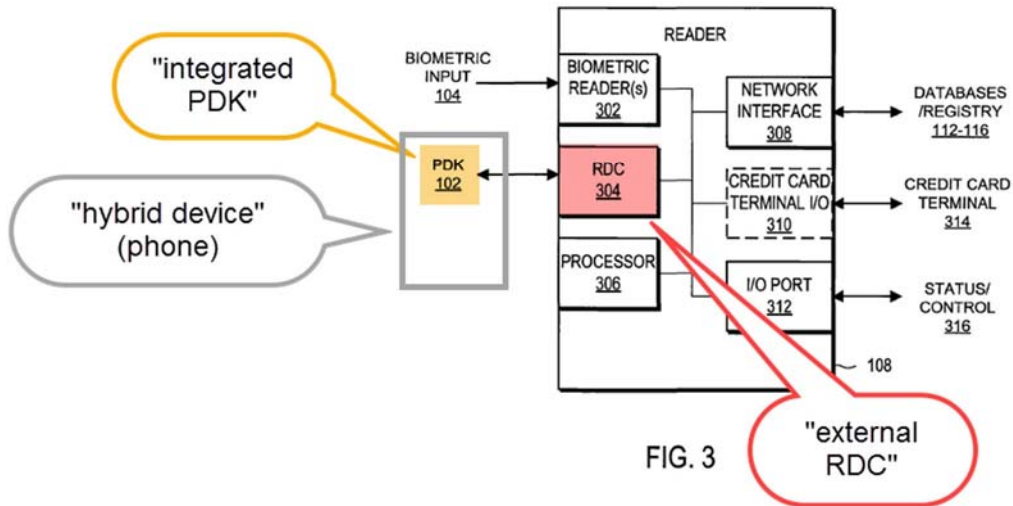
## **VII. CITED ART**

### **A. Giobbi ’157**

U.S. Patent Pub. No. 2007/0245157 A1 to Giobbi et al. (“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.” Ex. 1004 at Abstract. *See also*, Ex. 1003, ¶ 28.

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.” *Id.* Giobbi ’157 further teaches that the PDK may be integrated into a hybrid device, such as a cell phone. Ex. 1004 at ¶ 35 (“a portable electronic device such as a cell phone”), ¶ 12. *See also*, Ex. 1003, ¶ 29.

Giobbi ’157 teaches that its integrated PDK is capable of communicating wirelessly with an external receiver-decoder circuit (RDC). In particular, Giobbi ’157 teaches that information stored on a PDK, such as fingerprint information, is transmitted to an external RDC located on a “Reader 108.” *Id.* at ¶ 49. Giobbi ’157’s hybrid device is shown in the annotated version of Figure 3 below:



Ex. 1004 at Fig. 3 (annotated). Giobbi '157 teaches that its external RDC is communicatively coupled to an external database which is used for enabling an application/function/service:

For example, in one type of authentication, information is received from the PDK 102 at the RDC 304, processed by the processor 306, and transmitted to an external database 112-116 through the network interface 308.

Ex. 1004 at 53. This is shown, for example, in annotated Figure 3:

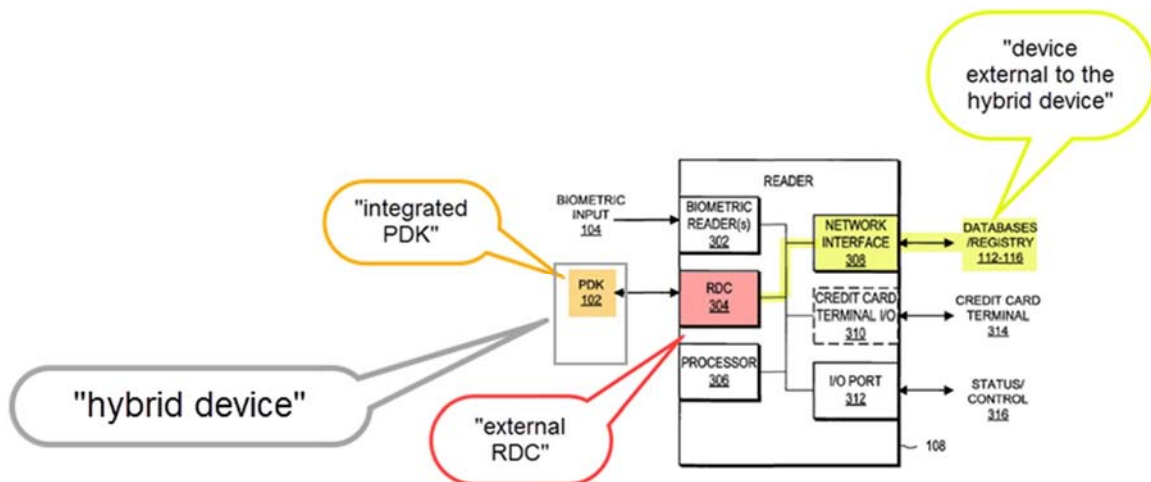


FIG. 3

Ex. 1004 at Fig. 3. Ex. 1003, ¶ 30.

Giobbi '157 teaches that its hybrid device, which contains the PDK, enables an application/function/service to take place. For example, Giobbi '157 teaches that its hybrid device's PDK is used to enable a financial transaction, such as an ATM withdraw:

Additionally, 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.

Ex. 1004 at ¶¶ 11, 65. *See also*, Ex. 1003, ¶ 31.

### B. Giobbi '139

U.S. Patent Pub. No. 2004/0255139 A1 to Giobbi ("Giobbi '139") is directed towards a "Personal Digital Key Digital Content Security System" which is aimed at protecting "unauthorized use and protect[ing] the digital content stored on computers from being wrongfully accessed, copied, and/or

distributed.” Ex. 1005 at Abstract. Like the Giobbi ’157 publication, Giobbi ’139 further teaches communicating with an receiver decoder circuit (RDC), and discloses that an RDC can be incorporated into a cell phone: “This embodiment involves integrating RDCs into...*PDA*s, *cell phones* [etc.]”). Ex. 1005 at ¶ 88, *compare with* Ex. 1004 at ¶ 35 (“The PDK **102** can be standalone as a portable, physical device or can be integrated into commonly carried items. . . such as a *cell phone [or] Personal Digital Assistant (PDA)*[.]”). Ex. 1003, ¶ 32.

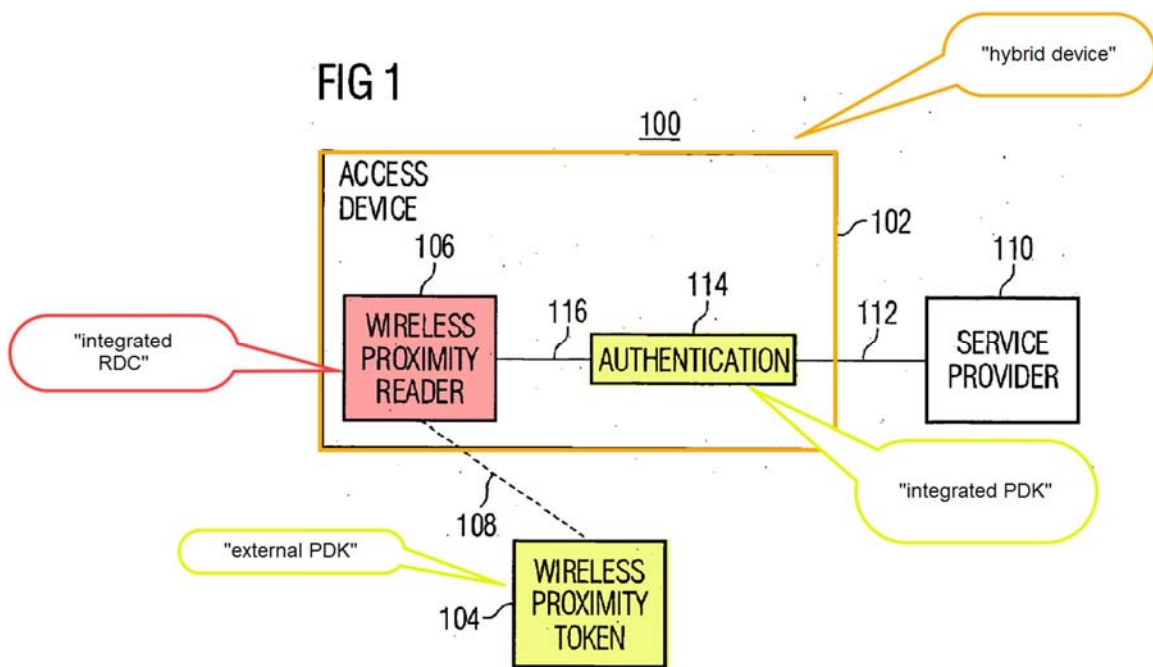
Giobbi ’139 expressly teaches coupling an integrated RDC and an integrated PDK by a signal line for communication. In particular, Giobbi ’139 teaches:

In other alternative embodiments, the communication between the user’s physical electronic key [*i.e.*, PDK] and the playing device is not wireless. Rather, in one alternative embodiment, ***the user’s physical electronic key [i.e., PDK] communicates the activation code to the playing device [i.e., the RDC on the playing device] via a transmission line such as a serial cable*** that plugs into the key at one end and the playing device at the other end. In another alternative embodiment, the key is a smart card or magnetic card into which the activation code is encoded, and the key is configured to physically fit into a card reader slot on the playing device.

Ex. 1005 at ¶¶ 41, 71-73. *See also*, Ex. 1003, ¶ 33.

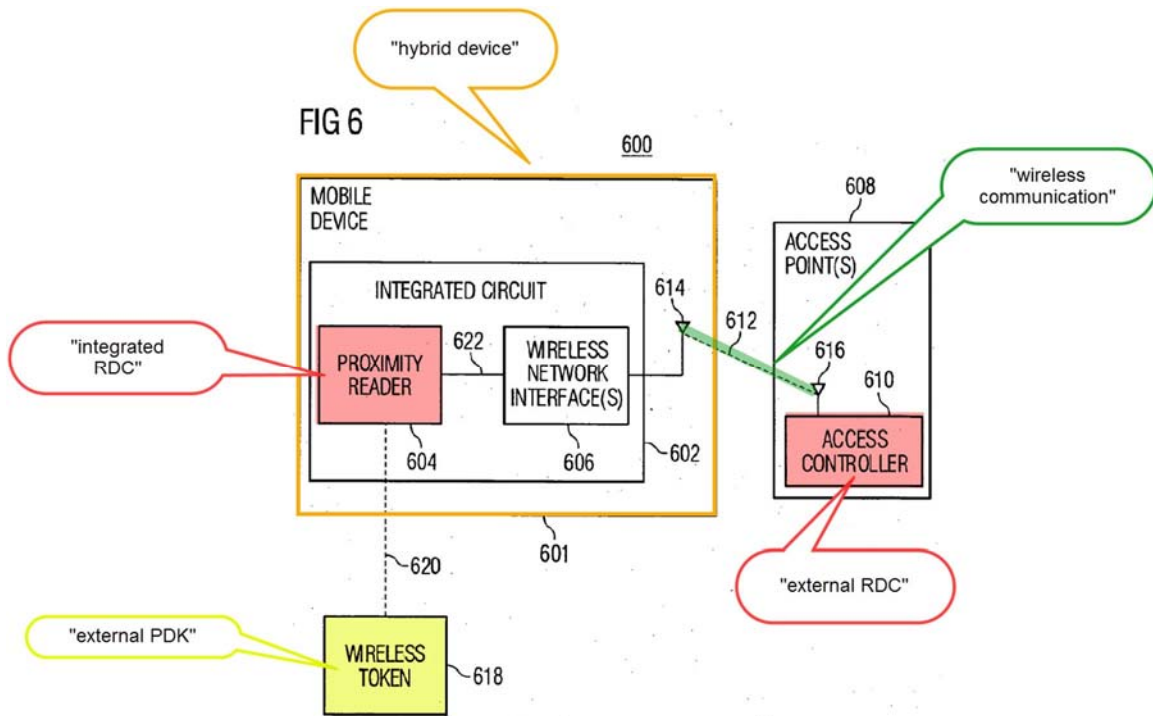
### C. Broadcom

E.P. Pub. No. 1536306 A1 (“Broadcom”) teaches a system for secured access to a service. Ex. 1007 at Abstract. In particular, Broadcom teaches that a user’s credentials may be stored on an RFID token, and this token may be read by an RFID reader in an Access Device. *Id.* The device including the RFID reader may authenticate the RFID token and permit access to the secured service after authentication. *Id.* This system is shown, for example, in Figure 1:



Ex. 1007 at Fig. 1. As shown in the figure, Access Device 102 will request access to a service provider 110 after “verifying that the information sent from the token 104 includes a credential associated with an authorized user and or access device.” Ex. 1007 at ¶¶ 119, 113-118. Broadcom confirms

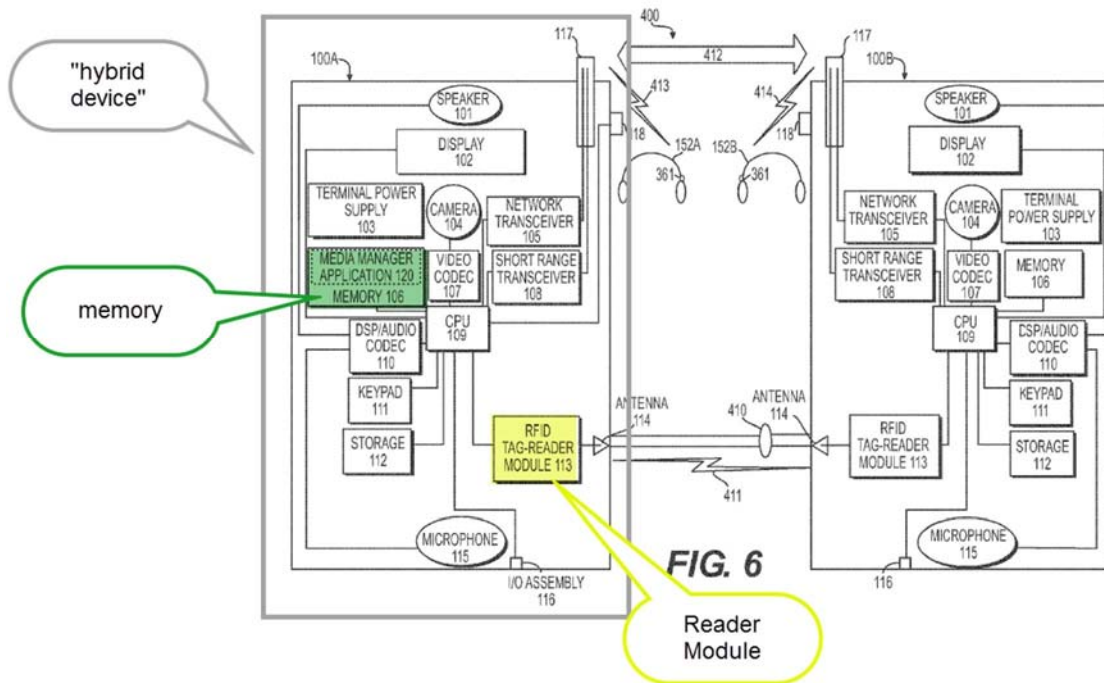
that, in some embodiments, the Access Device 102 can be a mobile phone which facilitates access to an access point for mobile communications, as shown, for example, in Figure 6:



Ex. 1007 at Fig. 6. Ex. 1003, ¶ 34.

#### D. Dua

U.S. Patent No. 9,042,819 (“Dua”) teaches a hybrid device—*e.g.*, a cell phone—which establishes wireless connections with other devices to enable functions and exchange data. Ex. 1006 at 6:46-65. Dua’s hybrid device is shown, for example, in annotated Figure 6:



Ex. 1006 at Fig. 6. Ex. 1003, ¶ 35.

Dua employs an RFID system to secure data and applications on its hybrid device. Dua teaches that its RFID setup may act as an “electronic key,” e.g., for point-of-sale transactions. Ex. 1006 at 12:60-61. Dua uses an RFID Tag as an electronic “key” and an RFID Reader as the electronic “lock.” Ex. 1003, ¶ 36.

Specifically, Dua teaches that its hybrid device uses RFID Tag-Reader Module (shown above in Fig. 6 in yellow), that includes both an RFID *Reader* Unit 304 and RFID *Tag* Unit 306:

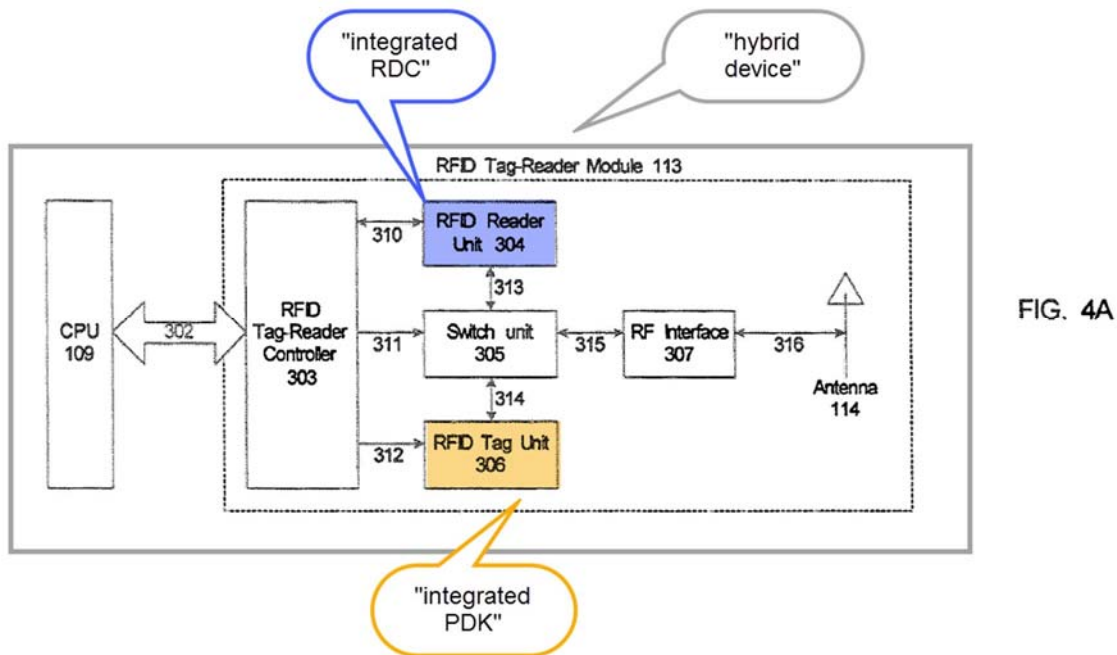


FIG. 4A

Ex. 1006 at Fig. 4A. Dua's **Tag** Unit 306 stores information necessary to gain access to an external device. In particular, Dua explains that its **Tag** Unit 306 stores information in internal tag memory. Ex. 1006 at 15:42-56. This information may be encrypted. Ex. 1006 at 16:31-34. Dua transmits this information to an external Reader. Ex. 1006 at 14:53-64. The external Reader reads the information transmitted by the Tag, *i.e.*, the key, to establish a secure connection. *Id.*; *see also id.* at 13:9-18. As shown in the figure, Dua also teaches an **integrated Reader** Unit 304 for reading information transmitted by external Tag Units. Ex. 1006 at 14:53-64. Ex. 1003, ¶ 37.

## VIII. DISCRETIONARY FACTORS

### A. Discretionary Denial Not Warranted Under *General Plastic*

In *General Plastic*, the Board “recognize[d] the potential for abuse of the review process by repeated attacks on patents,” and set forth a series of factors that may be analyzed for follow-on petitions to help conserve the finite resources of the Board. IPR2016-01357, Paper 19. The *General Plastic* factors weigh in favor of institution.

As already mentioned, this is Petitioner’s first IPR directed to the challenged claims of the ’188 patent. This Petition is substantially similar to the Samsung IPR Petition challenging the same claims. *See* IPR2021-01438, Paper 1. The Samsung IPR does not preclude institution.

**Factor 1 favors institution.** Petitioner was not a party to the Samsung IPR and Petitioner does not have a “significant relationship” with Samsung. Indeed, Petitioner is a direct market competitor with Samsung.

**Factors 2 and 5 have limited relevance or favor institution.** Petitioner was not aware of Patent Owner’s infringement allegations against Apple at the time of the Samsung IPR. The Samsung IPR Petition was filed on August 26, 2021, over two and a half years before Patent Owner filed its complaint against Apple on March 18, 2024 in *Proxense, LLC v. Apple Inc.*, No. 6:24-cv-00143 (W.D. Tex) (“the Pending Litigation”). Ex. 1008, 50-59.

Petitioner had no reason to perform any prior art searches when the Samsung IPR Petition was filed and did not perform any prior art searches at that time. Nor did Petitioner have reason to challenge the '188 patent until Patent Owner alleged infringement in the Pending Litigation.

**Factor 3 favors institution.** This Petition is substantially similar to the Samsung IPR Petition challenging claims of the '188 patent. Petitioner does not present any new grounds. There is no evidence of road mapping, and the mere fact that the preliminary patent owner response and decision instituting the Samsung IPR issued more than two years before the filing of this Petition, is insufficient to establish otherwise. The filing of multiple petitions here is the result of Proxense filing serial district court actions.

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

**Factors 6-7 favor institution.** The merits of this Petition are strong, as reflected in the Board's decision instituting the Samsung IPR to which this Petition is substantially similar. IPR2021-01438, Paper 12. While the Samsung IPR was instituted, that proceeding was terminated by the parties before the Board could issue a final written decision. *Id.*, Paper 33. There is significant value for the Board to consider the invalidity grounds in this

petition “to improve patent quality and restore confidence in the presumption of validity that comes with issued patents.” *Code200, UAB v. Bright Data, Ltd.*, IPR2022-00861, Paper 18, 5 (PTAB Aug. 23, 2022) (citations omitted). Furthermore, there is no risk that the Petition would undermine the Office’s ability to complete this proceeding in a timely manner. To the contrary, because the Samsung IPR Petition was instituted, the Board’s ability to issue a final determination not later than one year after granting institution of this IPR is enhanced.

**B. Discretionary Denial Not Warranted Under *Fintiv***

In *Apple Inc. v. Fintiv, Inc.*, the Board articulated a set of nonexclusive factors that it will consider in determining whether to institute an AIA post-grant proceeding where there is parallel district court litigation. IPR2020-00019, Paper 11. The *Fintiv* analysis is inapplicable here because Proxense has amended its original complaint and dismissed with prejudice the ’188 patent from the Pending Litigation. *See* Ex. 1009, Ex. 1010. As such there is no parallel litigation involving the ’188 patent.

**C. Discretionary Denial Not Warranted Under §325(d)**

Considering the two-part framework discussed in *Advanced Bionics*, IPR2019-01469, Paper 6, the Board should not exercise its §325(d) discretion to deny institution.

With respect to the first part of the *Advanced Bionics* framework, the '188 patent was issued over rejections in view of Finn and Hochstein. None of the prior art in this petition—Giobbi '157, Giobbi '139 or Broadcom—was cited or addressed by either the Examiner or Applicant during original prosecution. This weighs in favor of institution. *See, e.g., Digital Check Corp. d/b/a ST Imaging v. E-Imagedata Corp.*, IPR2017-00178, Paper 6 at 12-13 (PTAB. April 25, 2017) (instituting where: “[T]here is no indication in the record that the Examiner rejected any claims based on either reference or that the Examiner or applicant substantively discussed either reference during prosecution[.]”). Furthermore, while the Giobbi '157, Giobbi '139 or Broadcom were cited in the Samsung IPR, that proceeding was terminated before any final written decision. IPR2021-01438, Paper 33

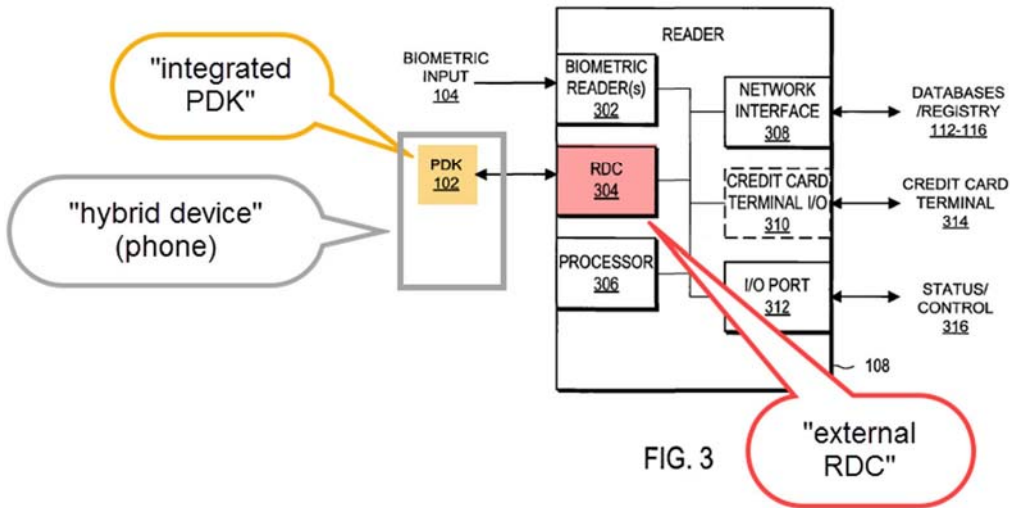
Because the first part of the *Advanced Bionics* framework is not satisfied, the Board need not consider the second part. To the extent the Board determines otherwise, Petitioner submits that the Grounds presented herein demonstrate that the examiner erred in determining the claims are allowable over the prior art. The merits of the petition are especially strong, as reflected in the Board’s decision instituting the Samsung IPR to which this Petition is substantially similar. IPR2021-01438, Paper 12.

**IX. GROUND 1: GIOBBI '157, GIOBBI '139 AND DUA RENDER OBVIOUS CLAIMS 1-20**

**A. Claim 1**

**1. 1pre A hybrid device comprising:**

To the extent that the preamble is limiting, Giobbi '157 discloses a hybrid device, such as a cell phone. Ex. 1004 at ¶ 35 (“a portable electronic device such as a cell phone”), ¶ 12. Giobbi '157's hybrid device is shown in the annotated version of Figure 3 below:

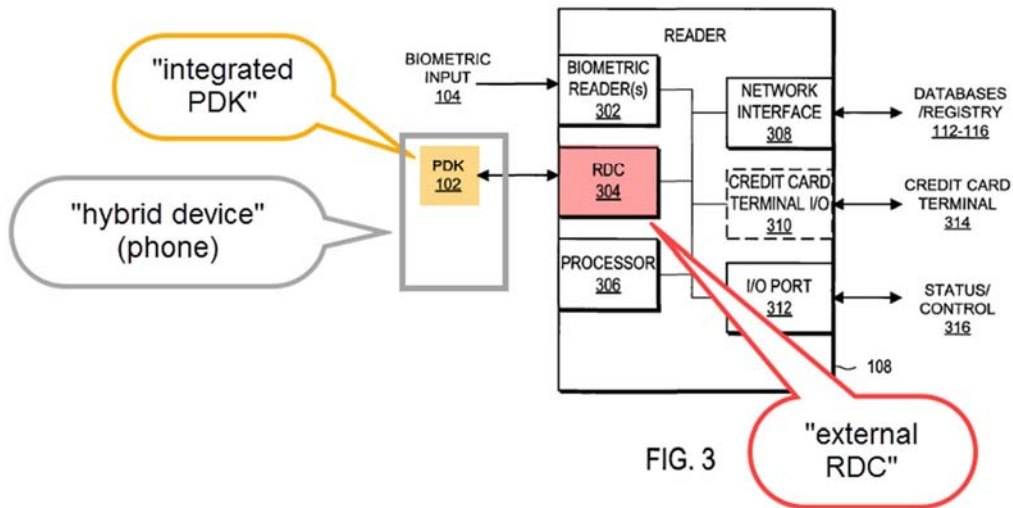


Ex. 1004 at Fig. 3 (annotated). As shown above, Giobbi's hybrid device (cell phone) carries an integrated PDK. This PDK communicates with an external RDC, as discussed below. Ex. 1003, ¶ 38.

**2. 1A an integrated personal digital key (PDK) for storing local, secured biometric information for authenticating a user and capable of communicating**

**wirelessly with an external receiver-decoder circuit (RDC); and**

*an integrated personal digital key (PDK):* Giobbi '157 expressly discloses a “Personal Digital Key (PDK).” Ex. 1004 at ¶ 11 (“[a] portable physical device, referred to herein as a *Personal Digital Key* or ‘PDK’”). Consistent with the Board’s construction of the term “PDK” for “storing local, secured biometric information” as encompassing a local memory for storing biometric information for authenticating a user, wherein the information is secured, Giobbi '157’s PDK 102 locally stores digital information “*in a tamper-proof format* that uniquely associates the PDK 102 with an individual.” Ex. 1004 at ¶ 28. A POSITA would understand this disclosed storage of digital information to be in a local memory. A POSITA would also understand the disclosure to refer to biometric information being secured in a tamper-proof (i.e., secured) format. Ex. 1003, ¶ 39. As discussed above, Giobbi '157 further teaches that its PDK is integrated into a hybrid device, such as a cell phone: “The PDK 102 can be standalone as a portable, physical device or can be *integrated* into commonly carried items. . . such as a cell phone[.]” Ex. 1004 at ¶ 35. Thus, Giobbi '157 teaches an integrated personal digital key, *i.e.*, a PDK integrated into a cell phone. This is shown, for example, in the annotated version of Figure 3 below prepared by Petitioner’s expert, Dr. Wolfe:



Ex. 1004 at Fig. 3 (annotated). *See also*, Ex. 1003, ¶ 39.

Consistent with the court’s construction in the Samsung Litigation of the term “Personal digital key” as meaning “[a]n operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for storing information particular to a user,” *Giobbi ’157* discloses that its PDK 102 includes a “**transceiver 260**,” “**memory 210**,” “**control logic 250**,” as seen in Figure 2 below:

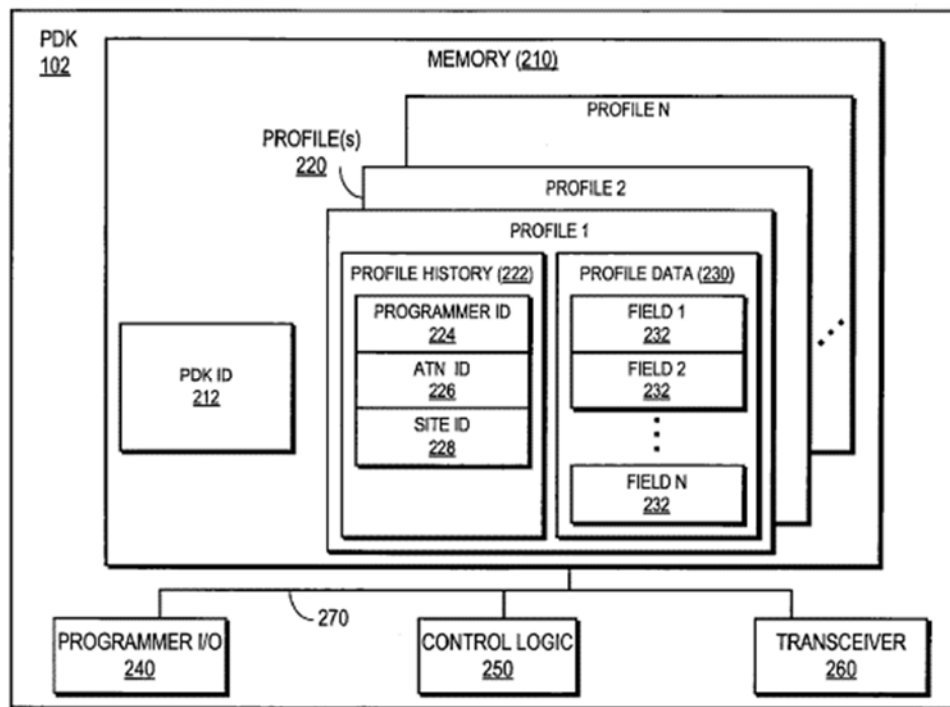


FIG. 2

Ex. 1004 at Fig. 2, ¶ 46. Giobbi '157 describes that a “**RDC 304 wirelessly receives data from the PDK 102,**” which a POSITA would have understood means that the PDK 102 includes an antenna for the wireless communication. Ex. 1004, ¶ 50 (emphasis added); Ex. 1003, ¶ 39.

*for storing local [information]:* Giobbi '157 further discloses that its integrated PDK is used for storing information in local storage: “The PDK 102 *stores* digital information *in a tamper-proof format* that uniquely associates the PDK 102 with an individual.” *Id.* at ¶ 28 (emphasis added). In particular, the PDK is disclosed as including memory 210 for storage:

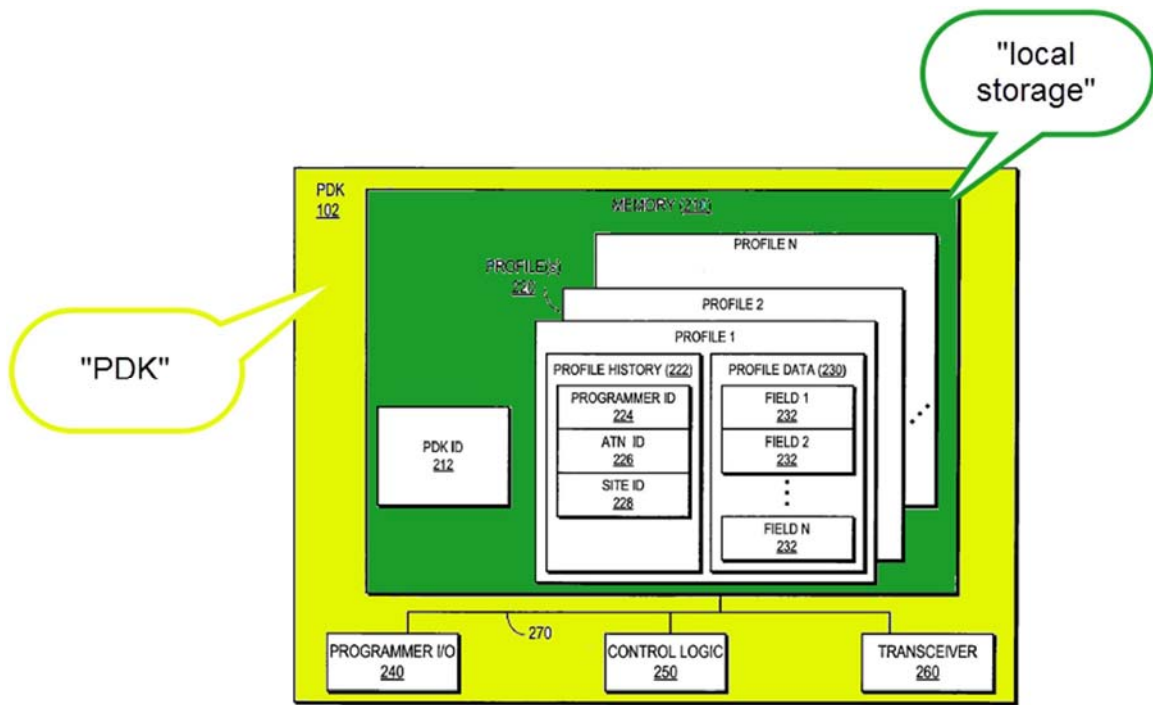


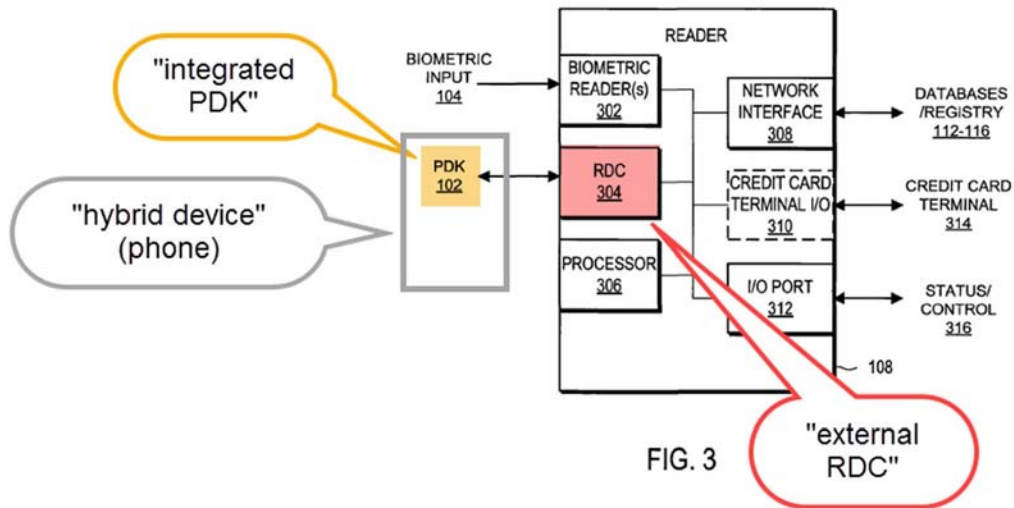
FIG. 2

Ex. 1004 at Fig. 2, ¶ 35. Ex. 1003, ¶ 40.

**secured biometric information for authenticating a user:** Giobbi '157 explains that the information stored locally on its integrated PDK is secured information for authenticating a user: “The PDK 102 *stores* digital information in a *tamper-proof* format that uniquely associates the PDK 102 with an individual.” *Id.* at ¶ 28 (emphasis added). Giobbi '157 further teaches that this information may be biometric information, *i.e.*, a “biometric profile.” *Id.* at ¶¶ 37-38 (“A PDK 102 can store multiple biometric profiles, each comprising a different type of biometric information.”). Giobbi '157 teaches that this biometric information is used for authentication, *e.g.*, fingerprint authentication. *Id.* at ¶ 38 (“In one embodiment the PDK 102 also stores one

or more biometric profile ‘samples’ associated with each biometric profile. . .  
 In the case of fingerprint authentication, for example, the biometric profile sample may represent only small portion area of the full fingerprint image.”).  
 Ex. 1003, ¶ 41.

*and capable of communicating wirelessly with an external receiver-decoder circuit (RDC):* Giobbi ’157 teaches that its integrated PDK is capable of communicating wirelessly with an external receiver-decoder circuit (RDC). In particular, Giobbi ’157 teaches that information stored on a PDK, such as fingerprint information, is transmitted to an external “RDC” located, for example, on a “Reader 108.” *Id.* at ¶ 49. This is shown, for example, in Figure 3, annotated by Dr. Wolfe:



Ex. 1004 at Fig. 3. Giobbi '157 further teaches that this communication between the integrated PDK and external RDC (on the Reader) is done wirelessly. *Id.* at ¶ 50 (“The RDC 304 provides the wireless interface to the PDK 102. Generally, the RDC 304 *wirelessly* receives data from the PDK 102[.]”). Giobbi 157 further teaches that an integrated PDK may communicate with an external RDC even if these two components are meters away. *Id.* at ¶ 30 (“The Reader 108 wirelessly communicates with the PDK 102 when the PDK 102 is within a proximity zone of. . .for example, *several meters*[.]”). Ex. 1003, ¶ 42.

**3. 1B an integrated RDC for communicating wirelessly with at least one external PDK within a proximity zone,**

As discussed above, Claim limitation 1A requires an integrated PDK communicate with an external RDC. Claim limitation 1B further requires the reverse—an *integrated* RDC (*i.e.*, an RDC integrated within the cell phone hybrid device) in communication with an external PDK (*i.e.*, a PDK in a device external to the cell phone hybrid device). A POSITA would have been motivated to integrate an RDC into Giobbi '157's hybrid device for communication with external PDKs based, in part, on the teachings of Giobbi '139.

In particular, Giobbi '139 *expressly* teaches integrating an RDC into the same type of hybrid device disclosed in Giobbi '157, a cell phone. Specifically, Giobbi '139 discloses a “Personal Digital Key Digital Content Security System (PDK-DCSS) is used to protect computers from unauthorized use and protect the digital content stored on computers from being wrongfully accessed, copied, and/or distributed.” Ex. 1005 at Abstract. Like Giobbi '157, Giobbi '139 teaches that in its system the PDK is used to request access to data secured via an RDC. Ex. 1005 at ¶¶ 22-44. Giobbi '139 further teaches that its RDC may be integrated in its hybrid device, *e.g.*, a cell phone: “This embodiment involves *integrating RDCs into...PDAs, cell phones* [etc.]”). Ex. 1005 at ¶ 88, *compare with* Ex. 1004 at ¶ 35 (“The PDK 102 can be standalone as a portable, physical device or can be integrated into commonly carried items. . . such as a *cell phone [or] Personal Digital Assistant (PDA)*[.]”). Giobbi '139 also discloses that its integrated RDC may communicate with an external PDK. Ex. 1005 at ¶¶ 22-44. Thus, Giobbi '139 expressly teaches “an integrated RDC for communicating wirelessly with at least one external PDK within a proximity zone” as required by claim limitation 1B. A POSITA would have been motivated by this express teaching to integrate an RDC into the hybrid device of Giobbi '157.

Further, Giobbi '139 teaches that RDCs *should* be incorporated into hybrid devices like cell phones because these devices “commonly included” data storage, and, in fact, Giobbi '139 identified such a configuration as an “enhancement.” Ex. 1005 at ¶¶ 87-88. This makes sense, because, as Dr. Wolfe explains, it would be desirable to include an RDC in a device holding the data that is meant to be secured to permit the use of hardware-key-based security. Ex. 1003, ¶ 45. Thus, it would have been a natural fit to integrate an RDC into Giobbi '157's cell phone.

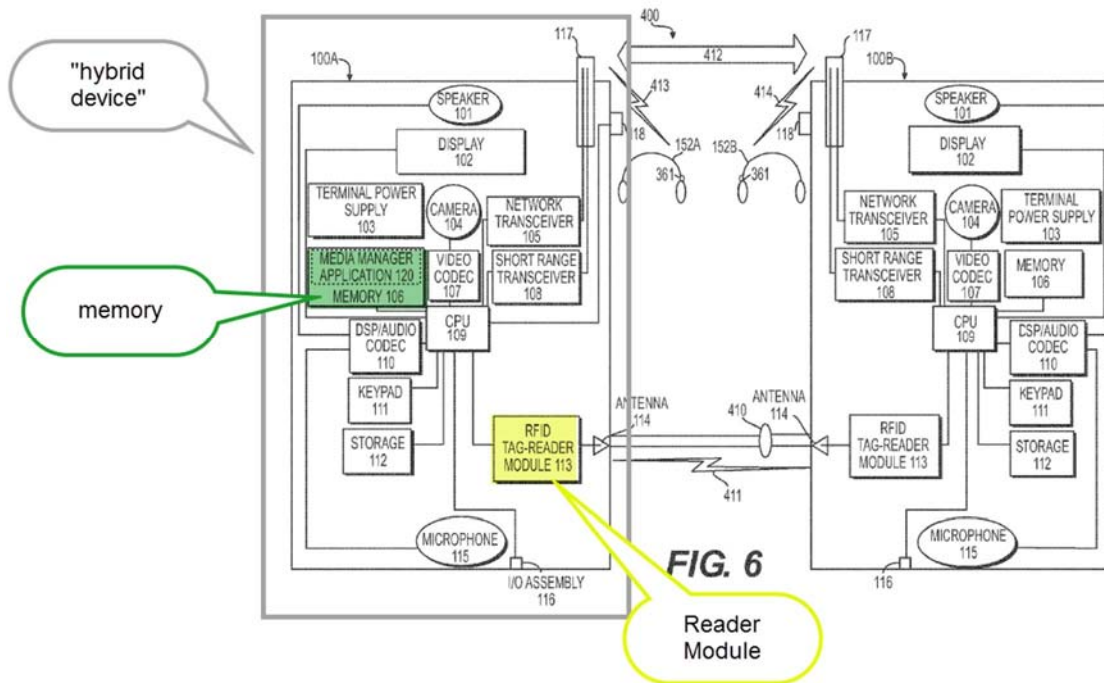
In addition, Giobbi '157 touts that its invention improves transactions. Ex. 1004 at ¶ 27 (describing the benefits of the claimed invention on transaction flexibility and efficiency). Integrating an RDC into Giobbi '157's cell phone would further this goal by allowing the phone to take part in both sides of a transaction. That is, a phone having both an integrated RDC and PDK could both make requests and respond to requests to access data. This would allow a user greater flexibility in a single device, consistent with Giobbi '157's teachings. Ex. 1003, ¶ 46.

Likewise, the main focus of both Giobbi '157 and Giobbi '139 is secure access. As discussed above, Giobbi '157 and Giobbi '139 teach securing data using an RDC. Thus, in view of these teachings, integrating an RDC onto a

hybrid device would be desirable since it would provide security for the data stored on the hybrid device. Ex. 1003, ¶ 47.

Further, Giobbi '157 teaches that it is advantageous to incorporate PDKs into “commonly carried items,” like phones, since it would eliminate the need for a user to carry a separate PDK device and would reduce the risk of loss. Ex. 1005 at ¶ 35; Ex. 1003, ¶ 48. This added convenience would similarly motivate a POSITA to integrate an RDC into a hybrid device like a cell phone, since doing so would eliminate the need for a separate device and likewise reduce the risk of loss. *Id.* Indeed, Giobbi '157's teachings that PDKs can be integrated into wearables such as jewelry would further motivate a POSITA to incorporate a matching RDC into other portable devices carrying data, such as a phone. *Id.*

In addition to Giobbi '139, the Dua patent's RFID system configuration also provides motivation to integrate an RDC into Giobbi '157's hybrid device. Specifically, like Giobbi '157 and Giobbi '139, Dua teaches a hybrid device—*e.g.*, a cell phone—which establishes wireless connections with other devices to enable functions and exchange data. Ex. 1006 at 6:46-65. Dua's hybrid device is shown, for example, in annotated Figure 6:



Ex. 1006 at Fig. 6. Similar to Giobbi '157 and Giobbi '139, Dua uses its an RFID system to secure data and applications on its hybrid device. Dua teaches that its RFID setup may act as an “electronic key,” *e.g.*, for point-of-sale transactions. Ex. 1006 at 12:60-61. Dua uses an RFID Tag as an electronic “key” and an RFID Reader as the electronic “lock.”

Specifically, Dua teaches that its hybrid device uses RFID Tag-Reader Module (shown above in Fig. 6 in yellow), that includes both an RFID *Reader* Unit 304 and RFID *Tag* Unit 306:

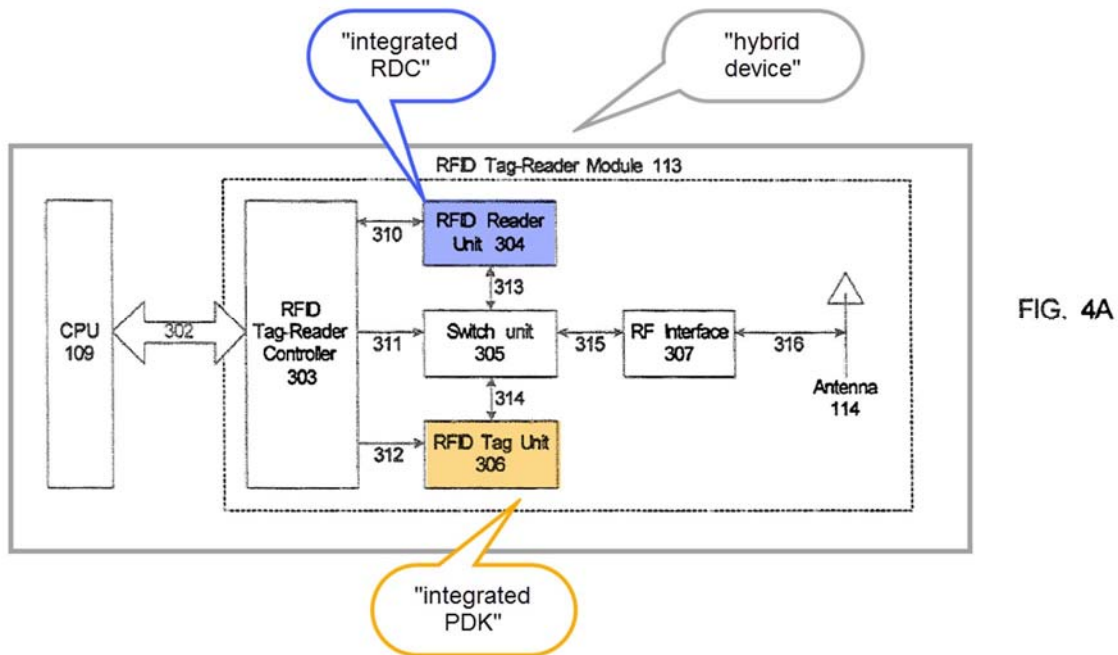


FIG. 4A

Ex. 1006 at Fig. 4A. Dua's Tag Unit 306 stores information necessary to gain access to an external device. In particular, Dua explains that its Tag Unit 306 stores information in internal Tag memory. Ex. 1006 at 15:42-56. This information may be encrypted. Ex. 1006 at 16:31-34. Dua transmits this information to an external Reader. Ex. 1006 at 14:53-64. The external Reader reads the information transmitted by the Tag, *i.e.*, the key, to authenticate the device and establish a secure connection. *Id.*; see also *id.* at 13:9-18. As shown in the figure, Dua also teaches an *integrated Reader* Unit 304 for reading information transmitted by external Tag Units. Ex. 1006 at 14:53-64. Ex. 1003, ¶ 50.

Thus, Reader Unit 304 is another example of the claimed integrated RDC in the prior art, and Tag Unit 306 is another example of the claimed

integrated PDK in the prior art. And, together, as taught by Dua, these integrated RDCs and PDKs are used to secure and share information across devices in the same manner claimed by the '188 patent. Indeed, the '188 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. Ex. 1003, ¶ 51.

Further, in addition to the motivations discussed above, Dua also evidences other known motivations for integrating both a PDK and an RDC into a hybrid device. For example, Dua teaches “[i]t is often desirable to interact on a frequent basis with multiple electronic devices that contain different types of digital media.” Ex. 1006 at 1:41-51. Dua likewise teaches that, since wireless devices such as cell phones have become more popular, “it is increasingly desirable to provide interconnection between these devices for convenience and to take advantage of the rich feature sets available.” *Id.* at 2:22-37. Dua explains that its invention achieves these goals by including both an integrated RDC and PDK in its RFID Tag-Reader Module 113, allowing its hybrid devices to both send and receive requests for data access: “RFID-Tag Reader Module 113 may be adapted, for example, to allow communication in passive and active communication modes with

reading/writing functionality[.]” *Id.* at 13:23-38. This further underscores the obviousness of the claimed invention. Ex. 1003, ¶ 52.

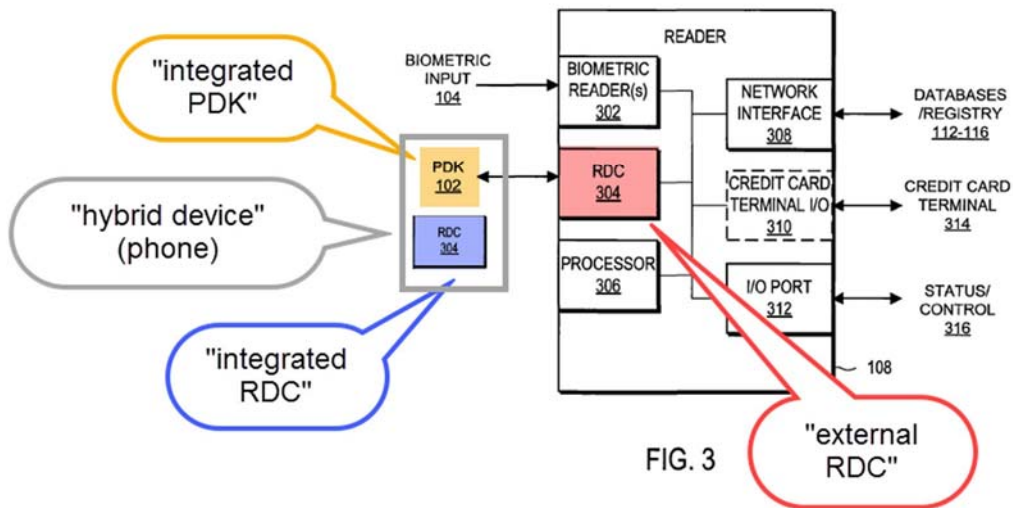
***Additional Motivations to Combine:***

A POSITA would also be motivated to combine the teachings of Giobbi ’139 and Dua with the Giobbi ’157 system because, at least, Giobbi ’157, Giobbi ’139 and Dua are in the *same field of endeavor* as the ’188 patent—the field of incorporating RDC/PDK technology into hybrid devices to allow secure data sharing and services. Ex. 1004 at Abstract; Ex. 1005 at Abstract; Ex. 1006 at Abstract, Fig. 4A; Ex. 1001 at Abstract, claim 1. Likewise, a POSITA would recognize that Giobbi ’157, Giobbi ’139 and Dua use *similar techniques to solve the same problem* as the ’188 patent. Indeed, as discussed above and throughout this petition, the Giobbi references and Dua integrate PDKs and RDCs into hybrid devices in the same manner claimed by the ’188 patent. A POSITA would further have had *a reasonable expectation of success* in integrating an RDC into Giobbi ’157’s hybrid device. As discussed above, Giobbi ’139 already teaches that an RDC can be incorporated into a hybrid device for communication with external PDKs, and it explains how to do so. For example, in one embodiment Giobbi ’139 teaches that external RDCs can be incorporated into devices such as “PDAs, cell phones [etc.]...in which case *the RDC is either directly installed on the device*, or integrated

into the device in which the memory cards/sticks are inserted.” Ex. 1005 at ¶ 88. Giobbi ’139 further explains that external PDKs can be used to unlock content stored on hybrid devices with integrated RDCs, such that when the corresponding PDK “is not present, these devices and their storage means are locked and disabled.” *Id.* at ¶ 90. Further, Giobbi ’139 specifically teaches that both an RDC and PDK can be integrated in the *same* device, as discussed below with respect to claim limitation 1C. Thus, Giobbi ’139 itself confirms that an RDC and PDK can both be integrated into the same hybrid device. Accordingly, a POSITA would have had a reasonable expectation of success integrating an RDC into the Giobbi ’157 hybrid device. Ex. 1003, ¶ 53.

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. Ex. 1006 at Fig. 4A, 13:19-14:64. Ex. 1003, ¶ 54.

Petitioner’s expert, Dr. Wolfe, generated an annotated version of Figure 3 which adds an integrated RDC (blue) into Giobbi ’157’s cell phone hybrid device:



Ex. 1004 at Fig. 3 (annotated—RDC 304 and gray box added). Ex. 1003, ¶ 55.

The integrated RDC could communicate with an external PDK stored in another portable device, such as another cell phone, watch or the like according to the teachings of Giobbi '157, Giobbi '139 and Dua. Ex. 1004 at ¶ 35 (disclosing PDKs stored in hybrid devices, such as phones); Ex. 1005 at ¶¶ 88-90 (disclosing integrated RDCs communicating with external PDKs in other devices); Ex. 1006 at 13:19-14:64. *See also*, Ex. 1003, ¶ 56.

**4. 1C the integrated RDC coupled to the integrated PDK by a first signal line for communication,**

Claim limitation 1C requires that the integrated RDC and PDK be connected via a first signal line for communication. A POSITA would have

been motivated to couple the integrated RDC and PDK with a signal line for communication based on the teachings of Giobbi '139 and Dua. Ex. 1003, ¶ 57.

Indeed, Giobbi '139 *expressly* teaches coupling an integrated RDC and an integrated PDK by a signal line for communication. In particular, Giobbi '139 teaches:

In other alternative embodiments, the communication between the user's physical electronic key [*i.e.*, PDK] and the playing device is not wireless. Rather, in one alternative embodiment, ***the user's physical electronic key [i.e., PDK] communicates the activation code to the playing device [i.e., the RDC on the playing device] via a transmission line such as a serial cable*** that plugs into the key at one end and the playing device at the other end. In another alternative embodiment, the key is a smart card or magnetic card into which the activation code is encoded, and the key is configured to physically fit into a card reader slot on the playing device.

Ex. 1005 at ¶ 41, 71-73. Thus, Giobbi '139 teaches that a PDK could be integrated into the playing device and connected to the playing device's integrated RDC using, for example, "a serial cable." *Id.* A POSITA would have been motivated by this express teaching in Giobbi '139 to likewise couple the integrated RDC and PDK in Giobbi '157 by a signal line for communication. Ex. 1003, ¶ 58.

Further, a POSITA would be motivated to couple the integrated RDC with the integrated PDK in the Giobbi '157 device for security reasons.

Indeed, Giobbi '157, Giobbi '139 and Dua teach that to gain access to content on a device one uses a PDK to request access through an integrated RDC. Indeed, the entire purpose of both Giobbi references and Dua is to secure access to data or services via PDK-RDC pairing. Notably, Giobbi '139 expressly teaches that even an authorized user must use a PDK to access her own files. *See, e.g.*, Ex. 1005 at ¶ 41 (requiring a wired connection between a user's PDK and the RDC). Dua discloses a similar configuration. *See* Ex. 1006 at Fig. 4A. Thus, to maintain security, a POSITA would have been motivated to couple Giobbi '157's integrated PDK with the integrated RDC, as taught by Giobbi '139 and Dua. Ex. 1003, ¶ 59.

Patent Owner may argue that an integrated RDC could be programmed to freely grant local access to data without being coupled to an integrated PDK, and, thus, a POSITA would have no reason to couple the integrated PDK with the integrated RDC. Such an argument should be rejected for several reasons. First, the prior art consistently teaches accessing RDC-protected data by using a PDK; indeed, that is the entire focus of the Giobbi references and Dua. Ex. 1005 at Abstract, Ex. 1004 at Abstract; Ex. 1006 at Abstract. Second, allowing a user to access data without a PDK would present a major security risk, since external users could attempt to gain access to data by pretending to be the user. Ex. 1003, ¶ 60. This runs contrary to a central

focus of both Giobbi references and Dua, security. *See, e.g.*, Ex. 1004 at Abstract; Ex. 1005 at Abstract; Ex. 1006 Abstract. Third, Giobbi '139 expressly teaches coupling integrated PDKs and RDCs using a cable—a POSITA considering these two references would thus naturally be motivated to use the approach that is expressly disclosed in the prior art. Ex. 1005 at 41. A POSITA would be further motivated by Dua, which teaches the same configuration. Ex. 1006 at Fig. 4A. Ex. 1003, ¶ 60.

For at least these reasons, and the reasons discussed above with respect to claim limitation 1B, a POSITA would have been motivated to couple the hybrid device's internal components, including the coupling of the integrated PDK and RDC with a first signal line. Ex. 1003, ¶ 61.

**5. 1D the integrated RDC coupled to at least one other component of the hybrid device by a second signal line,**

As discussed above, Giobbi '139 teaches that an RDC may be integrated into a hybrid device. Giobbi '139 further teaches that the integrated RDC is coupled to a variety of other components on the hybrid device. For example, Giobbi '139 discloses coupling the integrated RDC to memory (Ex. 1005 at ¶ 88), as well as “storage mechanisms” (*id.* at ¶ 89) or to a hard drive (*id.* at ¶ 97, Figs. 11, 12 14). Indeed, a POSITA would readily understand that such signal lines would permit the integrated RDC to function as described in

Giobbi '139. Ex. 1003, ¶ 62. Further, a POSITA would understand that an integrated RDC in Giobbi '157's hybrid device would require at least a processor and a network interface to function (just as in external Reader 108).

*Id.* These signals lines are the claimed “second signal line.”

**6. 1E one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service.**

To the extent that this limitation does not require that application/function/service to run on the hybrid device, Giobbi '157 discloses this limitation. In particular, Giobbi '157 enables a function or service for providing “efficient, secure, and highly reliable authentication for transaction processing” using a PDK in conjunction with an RDC. Ex. 1004 at Abstract, ¶ 11. This transaction is made possible by transmitting authenticating information from the integrated PDK to the external RDC. Thus, the integrated PDK enables this application/function/service. This authentication process is shown, for example, in Figure 4:

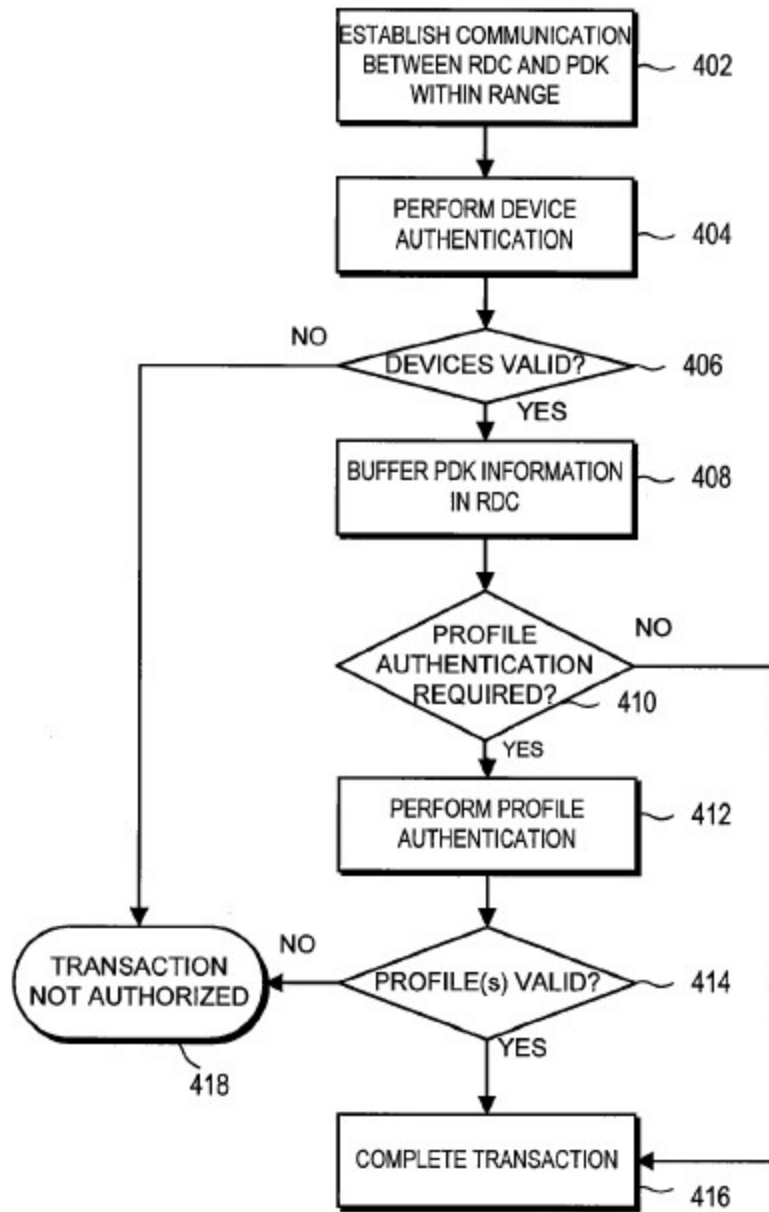


FIG. 4

Ex. 1004 at Fig. 4, ¶¶ 59-63; *see also id.* at ¶¶ 27, 63; Ex. 1005 at ¶¶ 10, 20-25 and 72. This may include, for example, a withdrawal from an ATM.  
 Ex. 1004 at ¶ 65; *see also*, Ex. 1003, ¶ 63.

To the extent that this limitation requires that the application/service/function run on the hybrid device itself, Giobbi '139 teaches this limitation. For example, Giobbi '139 teaches that the integrated RDC may be incorporated into cell phones, PDAs and MP3 players. Ex. 1005 at 88. 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. Ex. 1005 at ¶ 37; *see also*, Ex. 1003, ¶ 64.

**B. Claim 2 The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on the hybrid device.**

As discussed with respect to claim limitation 1E, Giobbi '139 teaches that the application/function/service is enabled at least in part on the hybrid device, such as playing music. Ex. 1003, ¶ 65.

**C. Claim 3 The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on a device external to the hybrid device and communicatively coupled to the external RDC.**

As discussed with respect to claim limitation 1E, Giobbi '157 teaches that its external RDC may be communicatively coupled to an external database (the claimed “device external to the hybrid device”) which is used

for enabling an application/function/service external to the hybrid device. *See* claim limitation 1E. Ex. 1003, ¶ 66.

**D. Claim 4 The hybrid device of claim 1, wherein the local, secured biometric information for authenticating a user is based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a photograph, a signature, a voice sample, DNA and RNA.**

Giobbi '157 teaches that the local, secured biometric information for authenticating a user can be based on a fingerprint:

For example, in biometric authentication, the authentication process cannot continue until the Reader detects a biometric contact and receives biometric information. It is noted that biometric contact is not limited to physical contact and can be, for example, 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.

Ex. 1004 at ¶ 65; Ex. 1003, ¶ 67.

**E. Claim 5 The hybrid device of claim 1, wherein the integrated PDK stores local, secured financial information.**

Giobbi '157 teaches that the integrated PDK stores local, secured financial information, such as:

Alternatively, *bank information, debit/check/ATM card information*, coupon codes, or *any other purchasing means information* (typically stored in a profile memory field 232) can be transmitted by the PDK 102 in place of credit card information.

Ex. 1004 at ¶ 63. Giobbi '157 teaches that the information is secured in “tamper proof” memory. Ex. 1004 at Abstract. Ex. 1003, ¶ 68.

**F. Claim 6 The hybrid device of claim 1, wherein the integrated PDK stores local, secured financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information.**

As discussed with respect to claim 5, the PDK stores bank information, debit/check/ATM card information. *See* claim 5. Further, as discussed with respect to claim limitation 1E, this enables the user to, *e.g.*, make a withdraw from an ATM. Ex. 1003, ¶ 69.

**G. Claim 7. The hybrid device of claim 1, wherein the hybrid device is a cell phone.**

Giobbi '157 teaches that its hybrid device may be a cellular phone. Ex. 1004 at ¶¶ 35, 12. *See also*, Ex. 1003, ¶ 70.

**H. Claim 8. The hybrid device of claim 1, wherein the external PDK is included in jewelry.**

Giobbi '157 teaches that its external PDK may be included in jewelry, including: “watches, rings, necklaces or bracelets.” Ex. 1004 at ¶ 35; Ex. 1003, ¶ 71.

**I. Claim 9. The hybrid device of claim 1, comprising a storage for inheritance information.**

The '188 patent teaches several types of inheritance information: service inheritance, feature inheritance and personality inheritance:

**Service inheritance** is authorization of the second device for any functionality provided by a given service. **Feature inheritance** is similar to service inheritance but for a limited set of features offered by a given service. **Personality inheritance** is where the preferences of a user or holder of a first device are shared with a user or holder of a second device.

Ex. 1001 at 18:14-20 (emphasis added). The '188 patent teaches that there are a variety of types of information that fall under these categories. For example, it teaches that service inheritance information can be “a first credit card account.” Ex. 1001 at 18:51. As discussed with respect to claims 5-6, the PDK on the hybrid device stores credit card information, which is service inheritance information and, thus, Giobbi '157 stores the claimed “inheritance information.” *See* claim 5; *see also*, Ex. 1003, ¶ 72.

**J. Claim 10**

**1. 10pre A method comprising:**

*See* claim 1. Ex. 1003, ¶ 73.

**2. 10A creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external personal digital key (PDK),**

*See* claim 1. Ex. 1003, ¶ 74.

**3. 10B the hybrid device including an integrated PDK and the integrated RDC,**

*See* claim 1. Ex. 1003, ¶ 75.

4. **10C wherein the integrated PDK stores local, secured biometric information for authenticating a user,**

*See* claim 1. Ex. 1003, ¶ 76.

5. **10D receiving a first signal at the integrated RDC via the first wireless link from the external PDK;**

*See* claim 1. Ex. 1003, ¶ 77.

6. **10E generating an enablement signal enabling one or more of an application, a function and a service.**

As discussed with respect to claim 1, an RDC transmits information received by a PDK to, for example, a remote server, which in turn responds by permitting access to a function, application or service, such as ATM access.

*See also* claims 2, 3, 5. Giobbi '157 teaches that a “validation decision” signal is sent back to the RDC by, for example, an external server: “[i]n one embodiment, the information is processed remotely at the registry 114-16 and the registry 114-116 *returns a validation decision to the Reader 108.*” Thus, Giobbi 157 teaches generating the claimed “enablement signal,” *e.g.*, the validation signal. Ex. 1003, ¶ 78.

As discussed with respect to claim 1, it would have been obvious to incorporate an RDC with such functionality into the hybrid device of Giobbi '157. Ex. 1003, ¶ 79.

- K. Claim 11 The method of claim 10 further comprising: sending the enablement signal to the hybrid device, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on the hybrid device.**

As discussed in claim 10, remote servers transmit an enablement signal back to the integrated RDC (located in the hybrid device according to the proposed combination) which in turn enables a function. Ex. 1003, ¶ 80.

- L. Claim 12 The method of claim 10 further comprising: sending the enablement signal to the hybrid device, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on a device external to the hybrid device and communicatively coupled to the external RDC.**

As discussed for claim 11, Giobbi '157 teaches sending an enablement signal to the hybrid device. *See* claim 11. Further, as discussed above, Giobbi '157 teaches that at least one or more functions are enabled on a device external to the hybrid device, for example, an ATM. *See* claim 1, 2, 5. Ex. 1003, ¶ 81.

- M. Claim 13 The method of claim 10, wherein the local, secured biometric information for authenticating a user is based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a photograph, a signature, a voice sample, DNA and RNA.**

*See* claim 4. Ex. 1003, ¶ 82.

- N. Claim 14 The method of claim 10, wherein the integrated PDK stores local, secured financial information.**

*See* claim 1, 2, 5. Ex. 1003, ¶ 83.

**O. Claim 15 The method of claim 10, wherein the hybrid device is a cell phone.**

*See* claim 1. Ex. 1003, ¶ 84.

**P. Claim 16 The method of claim 10, wherein the external PDK is included in jewelry.**

*See* claim 8. Ex. 1003, ¶ 85.

**Q. Claim 17**

**1. 17A The method of claim 10, wherein the integrated PDK is electrically coupled to the integrated RDC, and the method further comprises: creating a second wireless link between the integrated PDK and an external RDC; and**

As discussed with respect to claim 1, Giobbi '157 in view of Giobbi '139 renders obvious incorporated both an integrated PDK and RDC into a single hybrid device, such that they can communicate with external PDK and RDCs. *See* claim 1. Such communication between a PDK and RDC can be wireless. *Id.*; *see also*, Ex. 1003, ¶ 86.

**2. 17B sending the enablement signal from the integrated PDK to the external RDC using the second wireless link,**

Claim 17B is similar to Claim 10E, except that it requires the enablement signal to originate from the *integrated PDK* and be sent to an external RDC. Giobbi '157 discloses this limitation, for example, in its disclosure of transmitting credit card information. In particular, Giobbi '157 discloses that in one embodiment, in order to enable a financial transaction,

credit card information is required. Accordingly, the PDK transmits the enabling credit card information from the integrated PDK to the external RDC, which enables the financial transaction to take place:

FIG. 7D illustrates a process for authentication with a private registry 114 or the Central Registry 116. If the Reader 108 determines that registry authentication is requested, a secure communication channel is established 762 over the network 110 between the Reader 108 and one or more registries (e.g., the Central Registry 114, any private registry 116, or other validation database 112). *If any additional information is needed to process the registry authentication (e.g., a credit card number), the Reader 108 requests and receives the additional information from the PDK 102.* Identification information is transmitted 764 from the Reader 108 to the registry 114-116 through the network interface 308. The PDK status is received 766 from the registry to determine 768 if the status is valid 772 or invalid 770. In one embodiment, the information is processed remotely at the registry 114-116 and the registry 114-116 returns a validation decision to the Reader 108.

Ex. 1004 at ¶ 74; Ex. 1003, ¶ 87.

**3. 17C the enablement signal based on financial information stored locally and securely on the integrated PDK and used to complete a financial transaction.**

As discussed with respect to claim 17B, the enablement signal is based on financial information stored locally and securely on the integrated PDK—credit card information—which is used to complete the financial transaction.

See claim 17B. Ex. 1003, ¶ 88.

**R. Claim 18 The method of claim 10, wherein the first signal includes inheritance information.**

*See* claim 9. Ex. 1003, ¶ 89.

**S. Claim 19 The method of claim 10, wherein the external PDK is included in a watch.**

*See* claim 8. Ex. 1003, ¶ 90.

**T. Claim 20 The hybrid device of claim 1, wherein the external PDK is included in a watch.**

*See* claims 8, 19. Ex. 1003, ¶ 91.

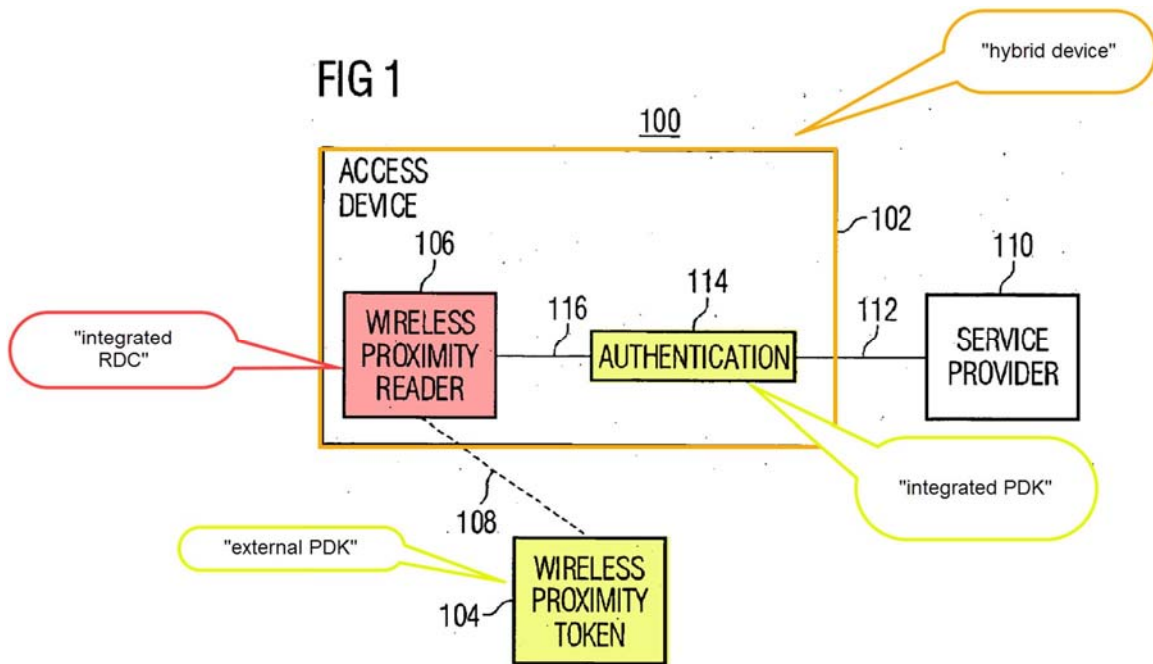
**X. GROUND 2: BROADCOM RENDERS OBVIOUS CLAIMS 1-7, 9-15 AND 17-18**

**A. Claim 1**

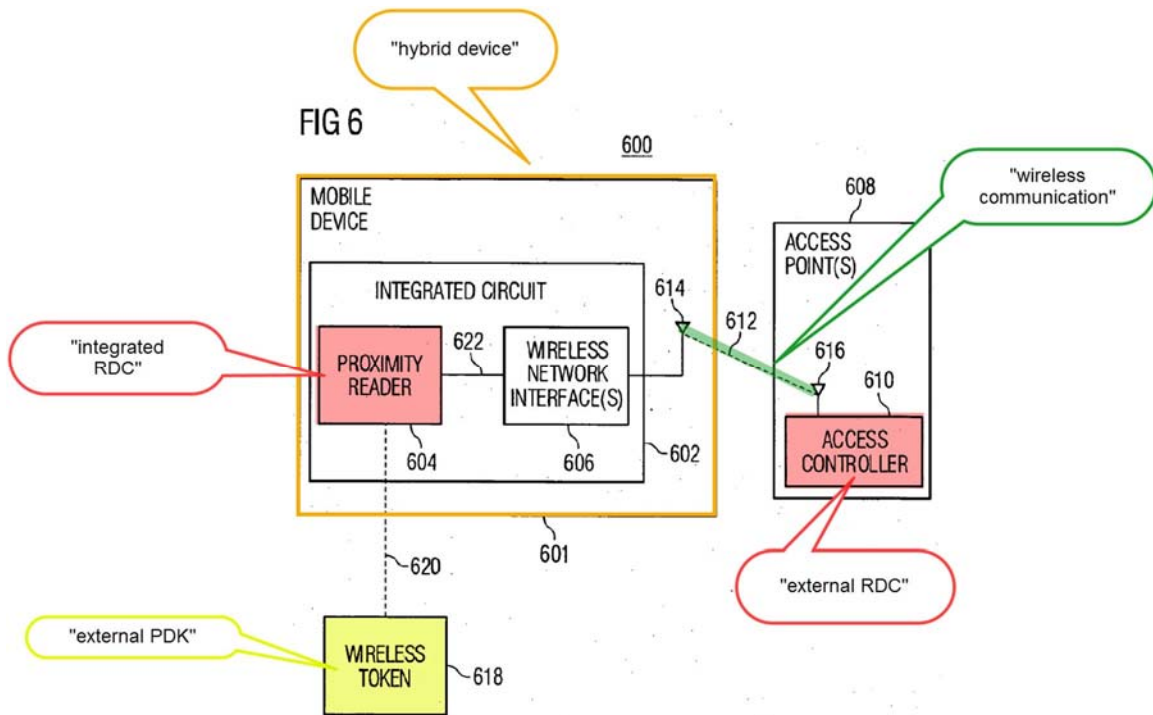
**1. 1pre A hybrid device comprising:**

Broadcom teaches a system for secured access to a service. Ex. 1007 at Abstract. In particular, Broadcom teaches that a user's credentials may be stored on an RFID token, and this token may be read by an RFID reader. *Id.* The device including the RFID reader may authenticate the RFID token and permit access to the secured service after authentication. *Id.*; Ex. 1003, ¶ 92.

This system is shown, for example, in Figure 1:



Ex. 1007 at Fig. 1. As shown in the figure, Access Device 102 will request access to a service 110 after “verifying that the information sent from the token 104 includes a credential associated with an authorized user and or access device.” Ex. 1007 at ¶¶ 119, 113-118. This Access Device 102 is the claimed “hybrid device.” Broadcom confirms that, in some embodiments, the Access Device 102 can be a mobile device, such as a phone, as shown, for example, in Figure 6:

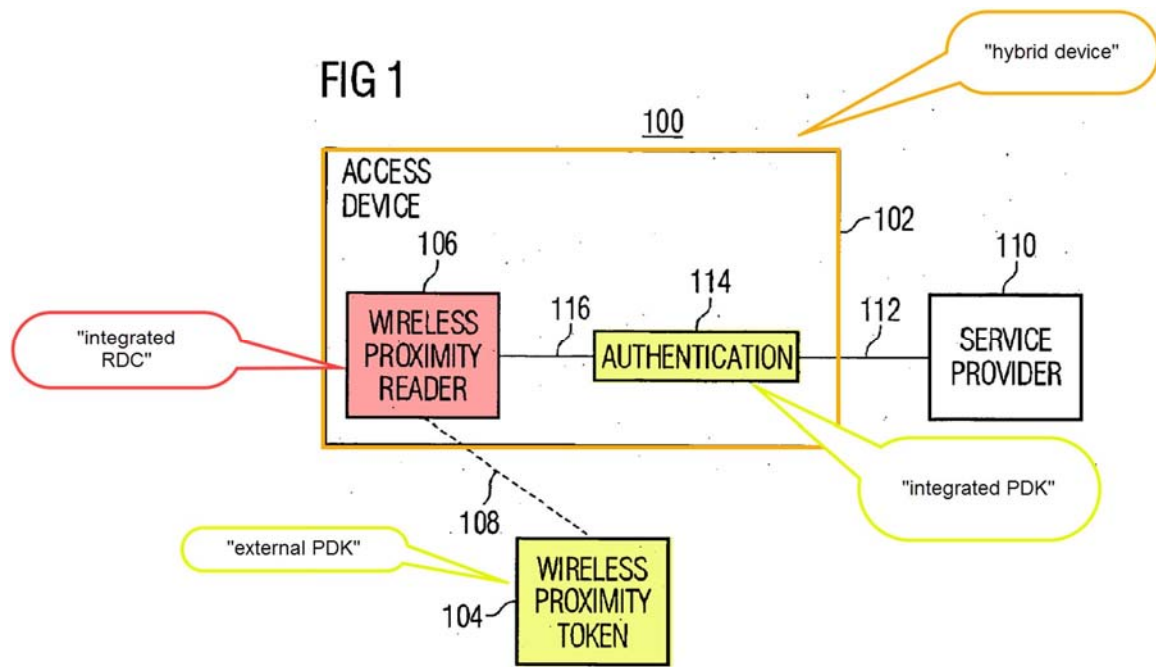


Ex. 1007 at Fig. 6; Ex. 1003, ¶ 93.

2. **1A an integrated personal digital key (PDK) for storing local, secured biometric information for authenticating a user and capable of communicating wirelessly with an external receiver-decoder circuit (RDC); and**

*an integrated personal digital key (PDK):* Broadcom teaches that its Access Device 102 includes an integrated PDK. Consistent with the Board’s construction of the term “PDK” for “storing local, secured biometric information” as encompassing a local memory for storing biometric information for authenticating a user, wherein the information is secured, the claimed integrated PDK is disclosed or taught by Broadcom’s disclosure of an “Authentication component 114” and internal memory of the Access

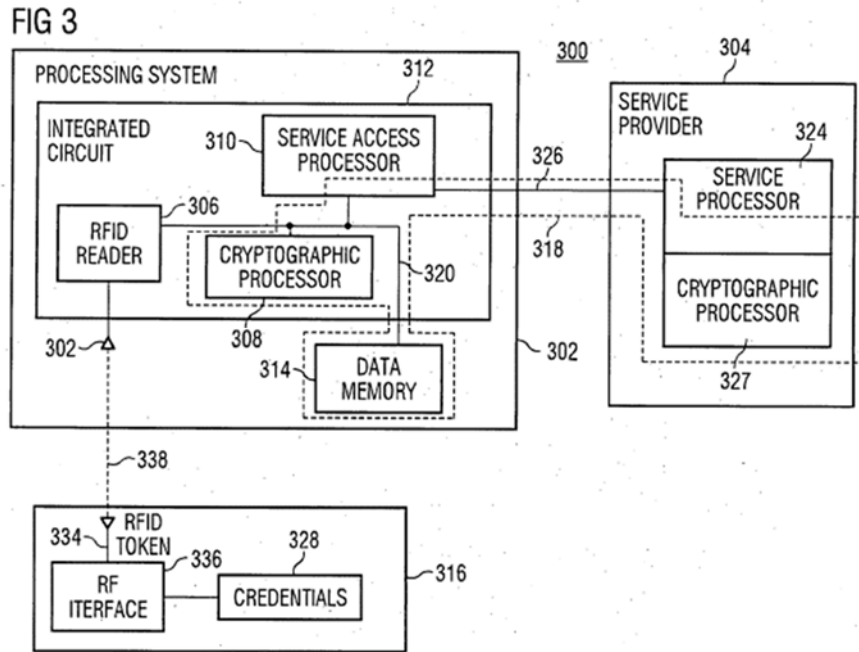
Device 102. Regarding internal memory, Broadcom describes that “the access device 102 may include a database (not shown) that matches a given token (or information from the token) with one or more default services.” Ex. 1007, ¶ 116. “[T]he authentication component 114...provides a cryptographically reliable authentication that the information is from a specific token that is proximate that particular access device.” Ex. 1007, ¶ 118. In a user’s interaction with the access device 102, “the user may be asked to input a password and/or provide a biometric (e.g., a fingerprint) to a biometric reader to further verify the authenticity of the user.” Ex. 1007, ¶ 114. The Authentication circuitry is shown in Figure 1 (the internal memory is not expressly shown in Figure 1):



Ex. 1003, ¶ 94. Nonetheless, a POSITA would understand the access device 102 to include internal memory for storing at least the disclosed database which would contain biometric information. *Id.*

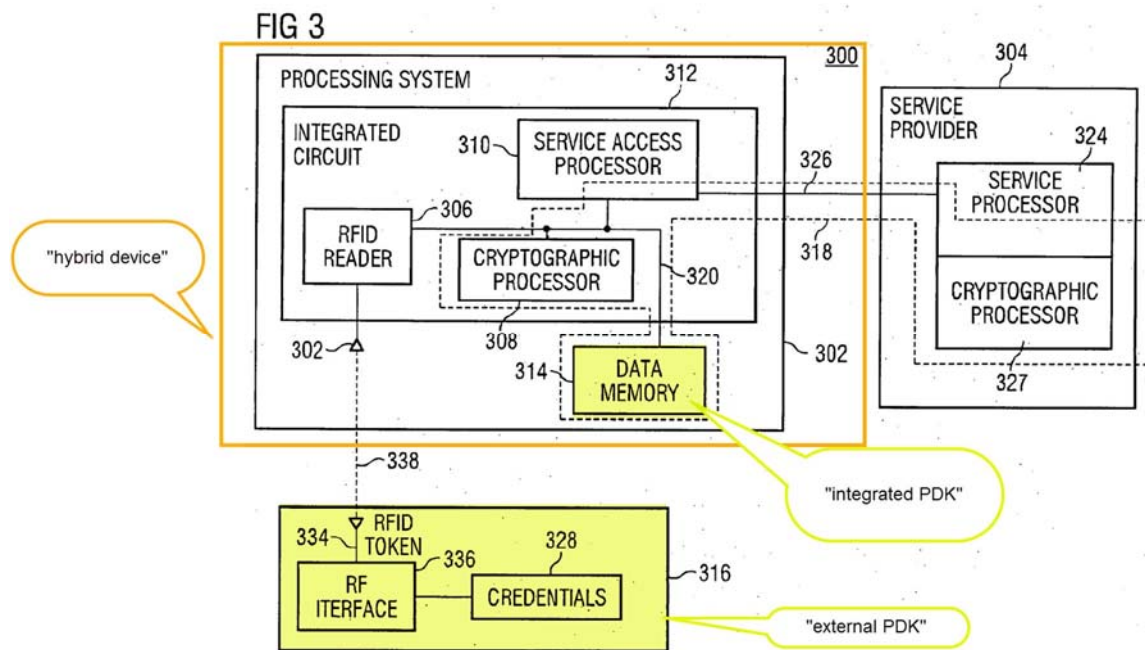
Consistent with the court’s construction in the Samsung Litigation of the term “Personal digital key” as meaning “[a]n operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for storing information particular to a user,” Broadcom discloses that its access device includes “antenna 332,” “RFID reader 306,” “data memory 314,” “cryptographic processor 308,” “service access processor 312,” as seen in

Figure 2 below:



Ex. 1007 at Fig. 3, ¶ 145; Ex. 1003, ¶ 94. Broadcom describes that “an RFID reader 306, a cryptographic processor 308 and a service access processor 310 may be incorporated into a single integrated circuit 312.” Ex. 1007, ¶ 133. A POSITA would have understood that RFID reader 306 is a transceiver because it both transmits and receives RF signals. Ex. 1007, ¶¶ 145-146; Ex. 1003, ¶ 94. RF signals from the access device “are broadcast via an antenna 332.” Ex. 1007, ¶ 146.

*for storing local [information]:* Broadcom’s internal memory—part the claimed PDK—is used for storing information locally. In particular, Broadcom teaches that Access Device includes “Data Memory 314” which stores, *e.g.*, security keys. Ex. 1007 at ¶¶ 135-137. This internal processing component within the hybrid device is shown, for example, in Figure 3:

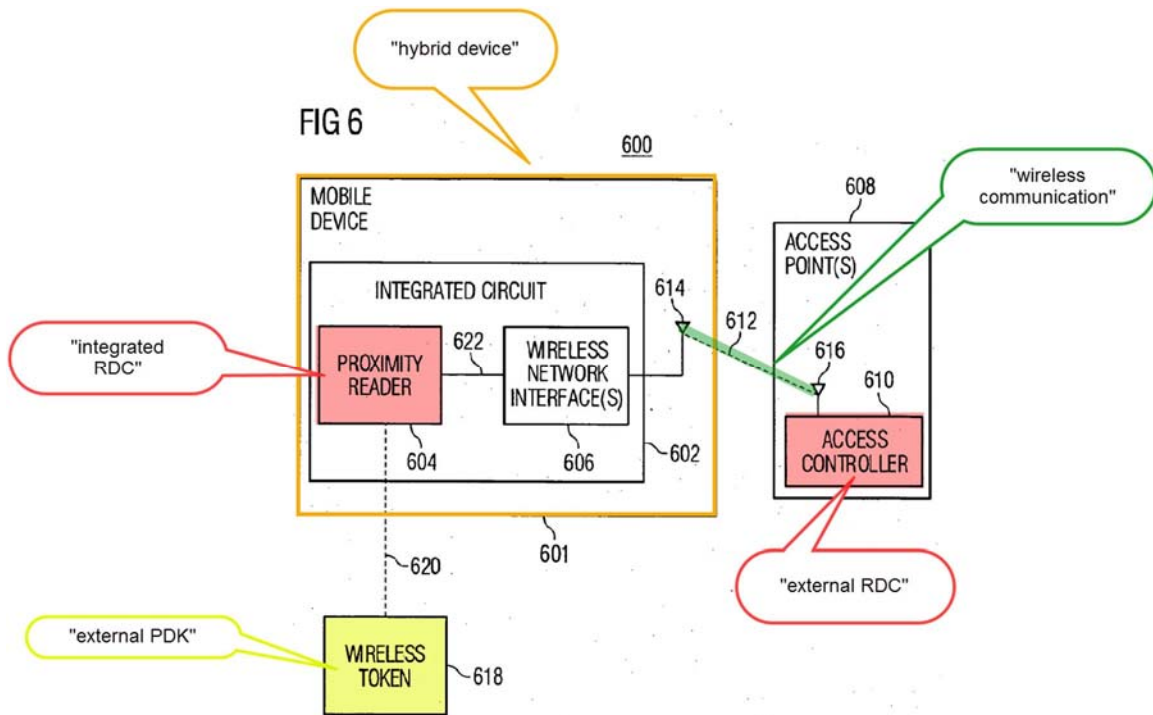


Ex. 1007 at Fig. 3; Ex. 1003, ¶ 95.

***secured biometric information for authenticating a user:*** Broadcom teaches that, besides a security key, a “biometric characteristic” can be used to authenticate a user: “Typically, access to the service will be initiated by the user's interaction with the access device 102. . .the user may be asked to input a password and/or provide a biometric (e.g., a fingerprint) to a biometric reader to further verify the authenticity of the user.” Ex. 1007 at ¶ 114. As discussed above, this secured biometric information is stored on data memory 314 (part of the integrated PDK). Ex. 1003, ¶ 96.

Information stored in memory is secured, in particular, it is encrypted. Ex. 1007 at 14 (“once the information from the RFID token is received by the RFID reader it may be ***encrypted*** within the chip.”). Ex. 1003, ¶ 97.

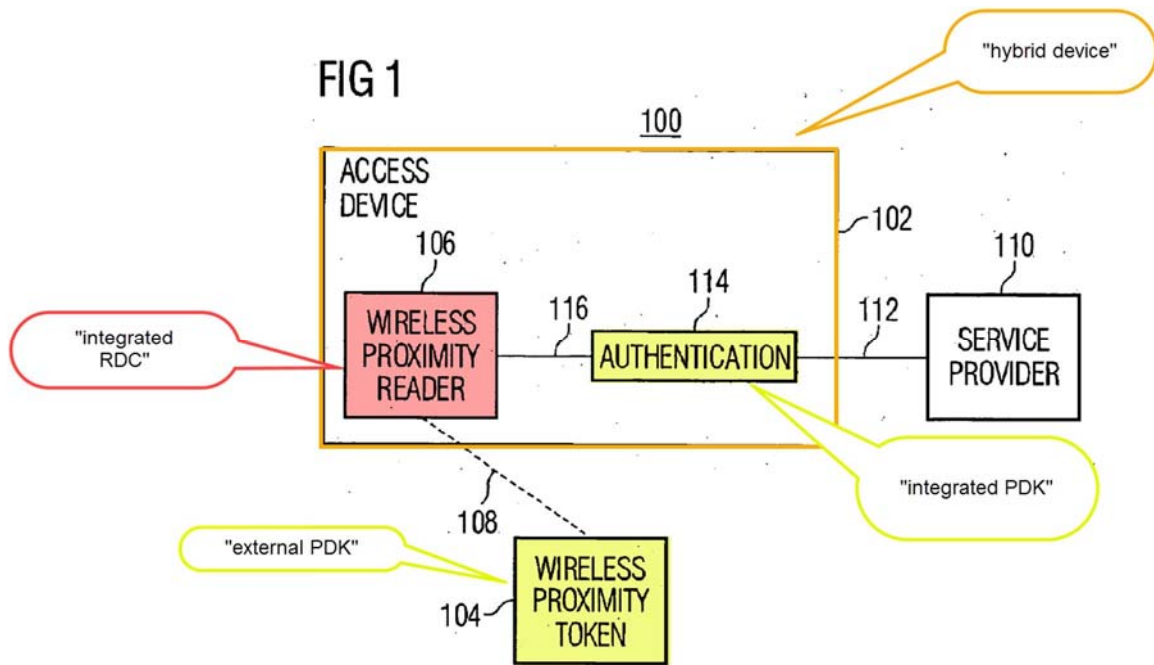
***and capable of communicating wirelessly with an external receiver-decoder circuit (RDC):*** Broadcom’s integrated PDK is capable of communicating wirelessly with an external receiver decoder circuit (RDC). In particular, Broadcom’s hybrid device communicates wirelessly through a network interface with an external access point as shown in Figure 6:



Ex. 1007 at Fig. 6; Ex. 1003, ¶ 98. Broadcom explains that a token may send authentication information to an integrated RDC (*i.e.*, the proximity reader). Ex. 1007 at 165. As discussed above, this information is passed to local memory and authentication circuitry. Broadcom teaches that a wireless network interface 606 may be used to wirelessly communicate signals to a service, for example, to an access controller 610 within an access point. Ex. 1007 at 164-66. The access controller, which is involved in the determination whether to grant access to the service, is the claimed external RDC. Ex. 1003, ¶ 99.

**3. 1B an integrated RDC for communicating wirelessly with at least one external PDK within a proximity zone,**

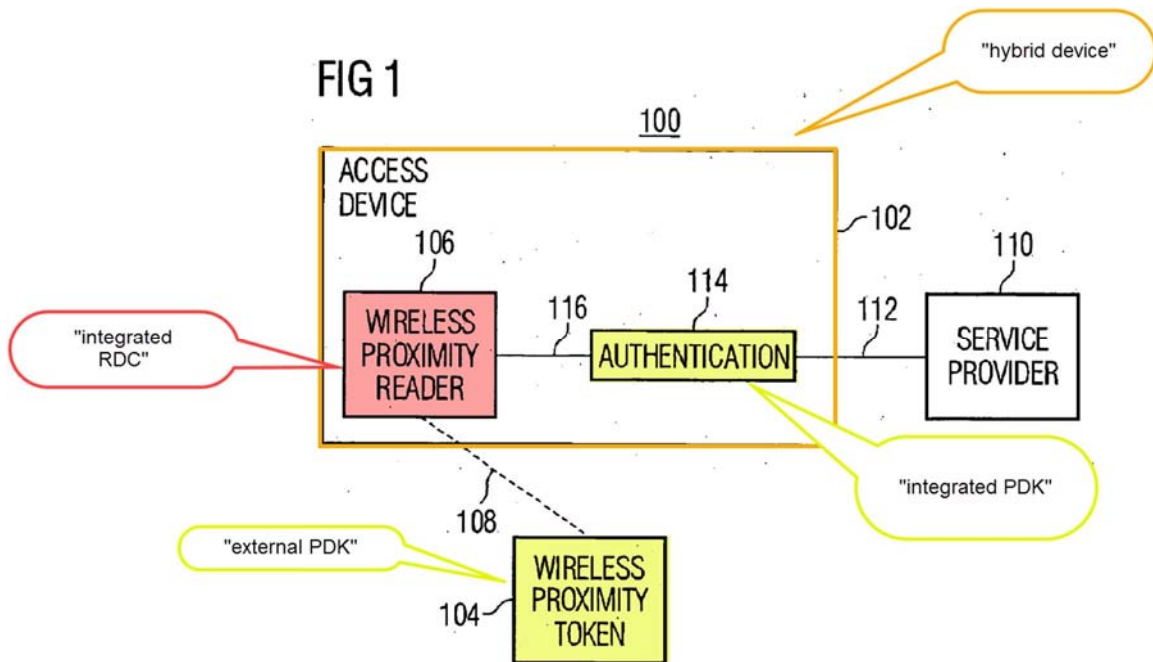
As discussed with respect to claim limitation 1A, Broadcom's hybrid device includes an integrated RDC, the wireless proximity reader:



Ex. 1007 at Fig. 1. As discussed above, the wireless proximity reader communicates with an external token seeking access to a service. This external token is the claimed external PDK. Ex. 1003, ¶ 100.

**4. 1C the integrated RDC coupled to the integrated PDK by a first signal line for communication,**

The integrated RDC (proximity reader) and integrated PDK (authentication circuitry and memory) are coupled via a signal line 116 for communication:



Ex. 1007 at Fig. 1 (annotated). Broadcom explains:

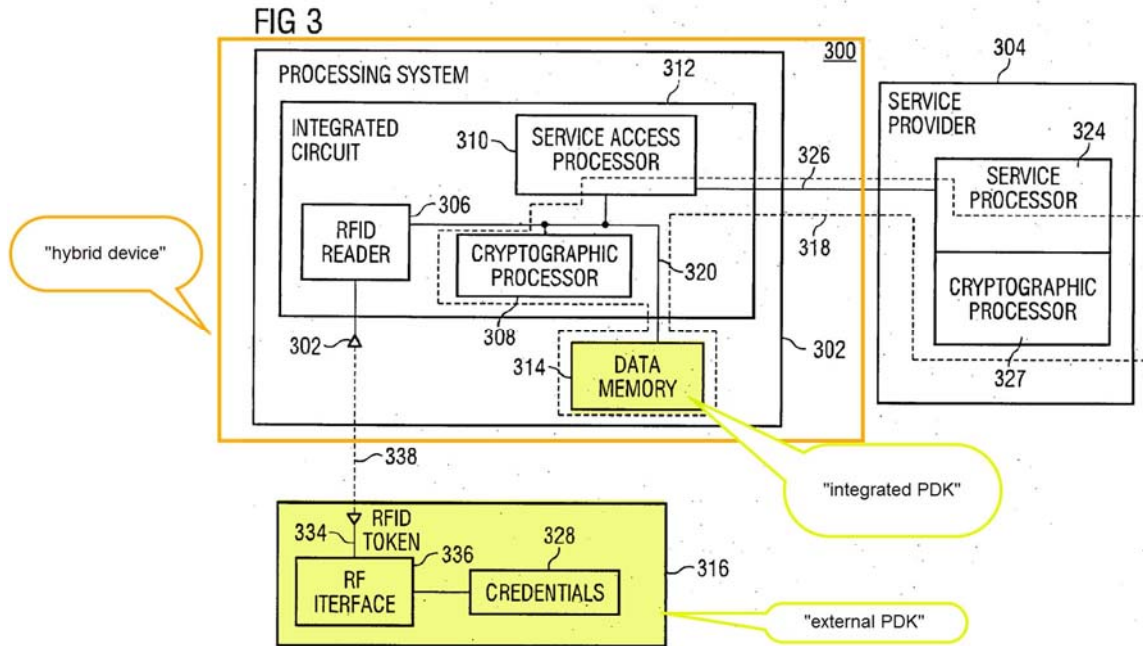
As represented by block 206, the access device 102 may send authentication-related information to the service provider 110 to indicate that the token 104 is proximate to the access device 102. For example, the access device 102 may include an authentication component 116 (sic – should be 114) such that the determination of whether the token 104 is proximate the access device 102 is performed in a secure manner. In addition, the Information provided by the token may be maintained within the access device 102 in a secure manner. For example, the information may only pass between the reader 106 and the authentication component 114 via a connection 116 within a common integrated circuit.

Ex. 1007 at 116; Ex. 1003, ¶ 101.

**5. 1D the integrated RDC coupled to at least one other component of the hybrid device by a second signal line,**

Broadcom teaches a variety of components within its hybrid device are connected to its integrated RDC (the proximity reader), including

cryptographic processor 306 and service access processor 312, as shown, for example, in Figure 3:

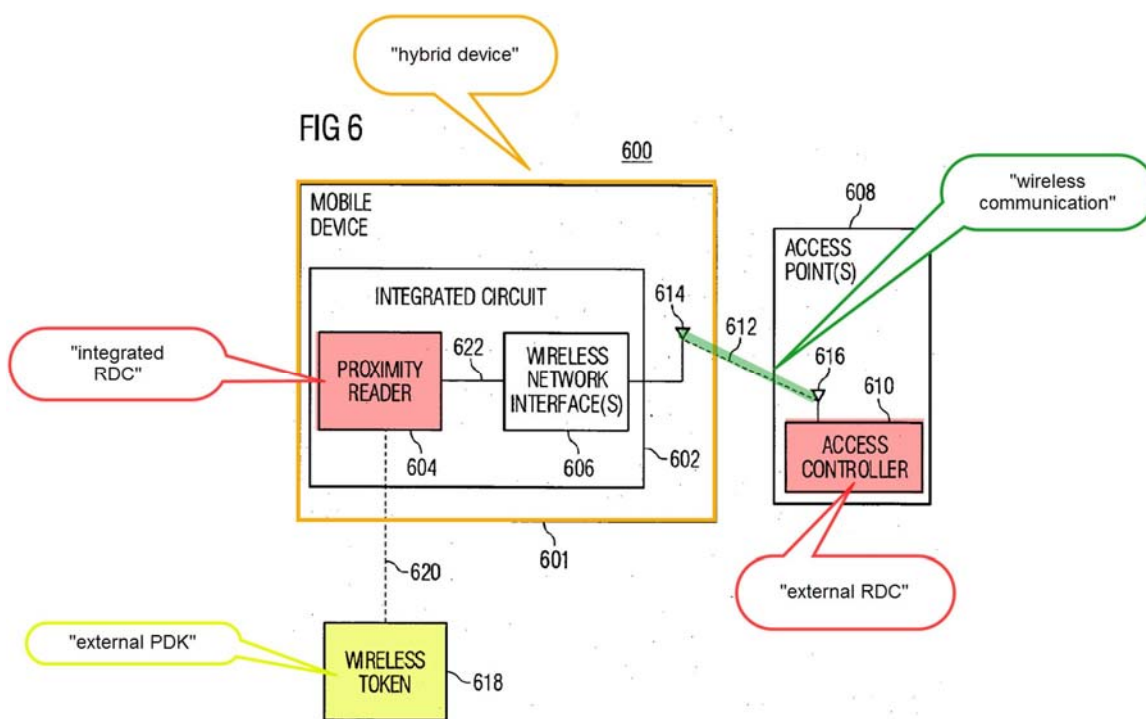


Ex. 1007 at Fig. 3. A POSITA would understand that additional circuitry in the hybrid device, for example, in a cell phone, would also need to be connected to the integrated RDC. For example, the integrated RDC would necessarily be connected to the phone's display screen to, at a minimum, provide confirmation of authorization. Ordinarily, an RDC in a mobile phone would be connected to an application processor as well as various input and output devices such as buttons, a touch sensor, and a vibrator motor. This allows processing of credentials as well as interactions with a user in response to the presentation of credentials. Ex. 1003, ¶ 102.

Broadcom further teaches that these components can be “connected/coupled in many different ways” and are not limited by the drawings. Ex. 1007 at ¶ 199. Broadcom notes that “one or more integrated circuits” can be used to house the internal components within a mobile phone. *Id.* at ¶ 198. Further, Broadcom teaches that its components may be “connected/coupled directly or indirectly” through intervening devices such as buffers. *Id.* at ¶ 204. Thus, Broadcom teaches that its internal components, including its integrated RDC, may be connected with a plurality of other components, including other circuits, either directly or indirectly. A POSITA would readily understand that multiple signal lines would be necessary to connect the integrated RDC directly to a plurality of integrated circuits. Ex. 1003, ¶ 103. Accordingly, Broadcom teaches using a second signal line to connect the integrated RDC to another component in the hybrid device. In a typical mobile phone in use at the time, a variety of such components would be connected by one or more system busses, I/O busses, and peripheral ports such as UART, SDI, and I<sup>2</sup>C ports. Any one or more of these would be the claimed second signal line. *Id.*

**6. 1E one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service.**

As discussed above, the integrated PDK communicates with an external RDC to enable a wide variety of applications/functions/services, including: “service may enable an access device to, for example, read or write data in a data memory, access encrypted data, use cryptographic keys, gain access to cryptographic material such as security associations and keys, access a web page, access a data network or access a processing application.” Ex. 1007 at ¶ 120. This is shown, for example, in Figure 6:



Ex. 1007 at Fig. 6. Ex. 1003, ¶ 1004.

To the extent this limitation requires that the service be run on the hybrid device itself, Broadcom discloses, for example, that the service may allow the hybrid device to view a webpage. Ex. 1007 at 120; Ex. 1003, ¶ 105.

To the extent this limitation requires that the service be run on a device external to the hybrid device, Broadcom discloses, for example, that the service may allow the hybrid device to access a processing application. *Id.*

Ex. 1003, ¶ 106.

**B. Claim 2 The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on the hybrid device.**

As discussed above, the integrated PDK communicates with an external RDC to enable a service, such as viewing a webpage. *See* claim limitation 1E. Ex. 1003, ¶ 107.

**C. Claim 3 The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on a device external to the hybrid device and communicatively coupled to the external RDC.**

As discussed above, the integrated PDK communicates with an external RDC to enable a service, such as access to a processing application. *See* claim limitation 1E. Ex. 1003, ¶ 108.

**D. Claim 4 The hybrid device of claim 1, wherein the local, secured biometric information for authenticating a user is based on one or more of a fingerprint, palm print, a retinal**

**scan, an iris scan, a photograph, a signature, a voice sample, DNA and RNA.**

As discussed above, Broadcom teaches that the secured biometric data may be a fingerprint scan. *See* claim 1; Ex. 1003, ¶ 109.

**E. Claim 5 The hybrid device of claim 1, wherein the integrated PDK stores local, secured financial information.**

Broadcom expressly teaches that its device solves a need for access to “sensitive information such as financial data or personal information.” Ex. 1007 at 8. A POSITA would understand this teaching to mean that the information stored in the PDK could be, for example, secured financial information. Broadcom further teaches that its device may store “credit card information,” which is also financial information. *Id.* at ¶ 195; *see also*, Ex. 1003, ¶ 110.

**F. Claim 6 The hybrid device of claim 1, wherein the integrated PDK stores local, secured financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information.**

As discussed with respect to claim 5, Broadcom’s PDK may store financial information. *See* claim 5. Broadcom discloses that its system solves the need for “improved techniques for providing access to secured services,” *i.e.*, providing access to a secured financial transaction based on the financial information. Ex. 1007 at 8. Indeed, Broadcom expressly teaches that its

system may be used to “perform a sales transaction.” *Id.* at ¶ 195; Ex. 1003, ¶ 111.

**G. Claim 7. The hybrid device of claim 1, wherein the hybrid device is a cell phone.**

*See* claim 1; Ex. 1003, ¶ 112.

**H. Claim 9. The hybrid device of claim 1, comprising a storage for inheritance information.**

As discussed in Ground 1, the ’188 patent teaches that storing inheritance information may include, *e.g.*, “service inheritance information” such as “a first credit card account.” Ex. 1001 at 18:12-42. As discussed above, the PDK on the hybrid device may store financial information. In fact, the external token may be a credit card. Ex. 1007 at ¶ 130. Accordingly, Broadcom’s hybrid device, which receives and stores information from the token, would store the claimed “inheritance information.” *See* claim 5; Ex. 1003, ¶ 113.

**I. Claim 10**

**1. 10pre A method comprising:**

*See* claim 1; Ex. 1003, ¶ 114.

**2. 10A creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external personal digital key (PDK),**

*See* claim 1; Ex. 1003, ¶ 115.

3. **10B the hybrid device including an integrated PDK and the integrated RDC,**

*See* claim 1; Ex. 1003, ¶ 116.

4. **10C wherein the integrated PDK stores local, secured biometric information for authenticating a user,**

*See* claim 1; Ex. 1003, ¶ 117.

5. **10D receiving a first signal at the integrated RDC via the first wireless link from the external PDK;**

*See* claim 1; Ex. 1003, ¶ 118.

6. **10E generating an enablement signal enabling one or more of an application, a function and a service.**

As discussed with respect to claim 1, an RDC transmits information received by a PDK to, for example, a remote server, which in turn responds by permitting access to a function, application or service, such as access to a wireless network. For example, Broadcom teaches: “Typically, access to the service will be initiated by the user's interaction with the access device 102. . .the user may be asked to input a password and/or provide a biometric (e.g., a fingerprint) to a biometric reader to further verify the authenticity of the user.” Ex. 1007 at ¶ 114. Thus, this user “input” is an example of the claimed enablement signal, since it enables one or more of an application, a function and a service. Ex. 1003, ¶ 119.

- J. Claim 11** The method of claim 10 further comprising: sending the enablement signal to the hybrid device, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on the hybrid device.

As discussed in claims 1 and 10, the integrated RDC enables a function, such as wireless network access. Ex. 1003, ¶ 120.

- K. Claim 12** The method of claim 10 further comprising: sending the enablement signal to the hybrid device, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on a device external to the hybrid device and communicatively coupled to the external RDC.

As discussed with respect to claim 1, Broadcom teaches that a network interface seeks access to a wireless network via “access controller 606,” which grants access to the network in response to the RDC’s request. Ex. 1003, ¶ 121.

- L. Claim 13** The method of claim 10, wherein the local, secured biometric information for authenticating a user is based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a photograph, a signature, a voice sample, DNA and RNA.

*See* claim 4; Ex. 1003, ¶ 122.

- M. Claim 14** The method of claim 10, wherein the integrated PDK stores local, secured financial information.

*See* claim 5; Ex. 1003, ¶ 123.

**N. Claim 15** The method of claim 10, wherein the hybrid device is a cell phone.

*See* claim 1; Ex. 1003, ¶ 124.

**O. Claim 17**

- 1. 17A** The method of claim 10, wherein the integrated PDK is electrically coupled to the integrated RDC, and the method further comprises: creating a second wireless link between the integrated PDK and an external RDC; and

As discussed with respect to claim 1, Broadcom teaches a wireless link between the integrated PDK and an external RDC. Ex. 1003, ¶ 125.

- 2. 17B** sending the enablement signal from the integrated PDK to the external RDC using the second wireless link,

As discussed with respect to claim 10E, an enablement signal (*e.g.*, biometric information) is sent from the integrated PDK to the external RDC.

Ex. 1003, ¶ 126.

- 3. 17C** the enablement signal based on financial information stored locally and securely on the integrated PDK and used to complete a financial transaction.

*See* claim 2, 5; Ex. 1003, ¶ 127.

**P. Claim 18** The method of claim 10, wherein the first signal includes inheritance information.

*See* claim 9; Ex. 1003, ¶ 128.

**XI. GROUND 3: BROADCOM AND GIOBBI '157 RENDER OBVIOUS CLAIMS 8, 16 AND 19-20**

**A. Claim 8. The hybrid device of claim 1, wherein the external PDK is included in jewelry.**

Broadcom broadly teaches that its external PDK (its “token”) may be included in “smart cards, credit cards, dongles, badges, biometric devices such as fingerprint readers, mobile devices such as cellular telephones, PDAs, etc.” Ex. 1007 at ¶ 130. It would have been obvious in view of Broadcom’s disclosure of including a PDK in a wearable, such as a badge, to include the external PDK in other wearables like jewelry. Indeed, as discussed with respect to Ground 1, Giobbi ’157 teaches doing just that. Ex. 1003, ¶ 129.

A POSITA would also be motivated to combine these references at least because Giobbi ’157 and Broadcom are in the *same field of endeavor* as the ’188 patent—the field of incorporating RDC/PDK technology into hybrid devices. Likewise, a POSITA would recognize that Giobbi ’157 and Broadcom use *similar techniques to solve the same problem* as the ’188 patent—as discussed throughout this petition, the Giobbi ’157 and Broadcom references integrate PDKs and RDCs into hybrid devices in the same manner claimed by the ’188 patent. A POSITA would further have had *a reasonable expectation of success* in the proposed combination—as discussed above, Giobbi ’157 already teaches that a PDK can be incorporated into a jewelry

such as watches and necklaces, and Broadcom already contemplates including its PDK in a wearable. Ex. 1003, ¶ 130.

**B. Claim 16 The method of claim 10, wherein the external PDK is included in jewelry.**

*See* claim 8; Ex. 1003, ¶ 131.

**C. Claim 19 The method of claim 10, wherein the external PDK is included in a watch.**

*See* claim 8; Ex. 1003, ¶ 132.

**D. Claim 20 The hybrid device of claim 1, wherein the external PDK is included in a watch.**

*See* claims 8, 19; Ex. 1003, ¶ 133.

## **XII. SECONDARY CONSIDERATIONS**

At this stage of these proceedings, Petitioner has no burden to identify and rebut secondary considerations. Rather, Patent Owner must first present a *prima facie* case for such consideration, which Petitioners should then have the chance to rebut. *Sega of Am., Inc. v. Uniloc USA, Inc.*, IPR2015-01453, at \*10 (Mar. 10, 2015). The Board typically rejects arguments against institution based on objective indicia, so that the Petitioners can have a fair opportunity to address any secondary indicia evidence on reply. *Petroleum Geo-Services Inc. v. WesternGeco LLC*, IPR2015-01478, at \*22 (Mar. 17, 2015); Ex. 1003, ¶ 134.

### **XIII. CONCLUSION**

For at least the foregoing reasons, the instant petition should be instituted.

Date: February 7, 2025

Respectfully submitted,

BY: /Philip W. Woo/  
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

*ATTORNEY FOR PETITIONER*

**CERTIFICATE OF COMPLIANCE**

Pursuant to 37 C.F.R. § 42.24 *et seq.*, the undersigned certifies that this document complies with the type-volume limitations. This document contains 12,969 words as calculated by the “Word Count” feature of Microsoft Word 2016, the word processing program used to create it.

Date: February 7, 2025

BY: /Philip W. Woo  
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

*ATTORNEY FOR PETITIONER*

**CERTIFICATE OF SERVICE**

Pursuant to 37 C.F.R. §§ 42.6(e), 42.8(b)(4) and 42.105, the undersigned certifies that on February 7, 2025, a complete copy of this petition and supporting exhibits were served via Federal Express, postage prepaid, to Patent Owner, by serving the correspondence address of record for the '188 patent:

Patent Law Works/Proxense  
Greg Sueoka  
310 East 4500 South, Suite 400  
Salt Lake City UT 84107  
UNITED STATES

and, by email, upon 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](mailto:bmelton@susmangodfrey.com)

Date: February 7, 2025

BY: /Philip W. Woo/  
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  
[pwoo@duanemorris.com](mailto:pwoo@duanemorris.com)

*ATTORNEY FOR PETITIONER*