

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

APPLE INC.,  
Petitioner

v.

PROXENSE, LLC  
Patent Owner

---

IPR2025-00562  
Patent 9,049,188 B1

---

**DECLARATION OF ANDREW WOLFE IN SUPPORT OF PETITION FOR  
*INTER PARTES* REVIEW OF U.S. PATENT NO. 9,049,188**

**TABLE OF CONTENTS**

	<b><u>Page</u></b>
I. INTRODUCTION .....	1
II. EDUCATION AND WORK EXPERIENCE .....	1
III. COMPENSATION.....	7
IV. LEGAL PRINCIPLES.....	7
V. LEVEL OF SKILL IN THE ART.....	9
VI. OVERVIEW OF THE '188 PATENT .....	9
VII. PROSECUTION OF THE '188 PATENT.....	10
VIII. CLAIM CONSTRUCTION .....	11
IX. CITED ART .....	12
A.    Giobbi '157 .....	12
B.    Giobbi '139 .....	14
C.    Broadcom .....	16
D.    Dua .....	17
X.    GROUND 1: GIOBBI '157, GIOBBI '139 AND DUA RENDER OBVIOUS CLAIMS 1-20.....	20
A.    Claim 1 .....	20
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. ....	41
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.....	41

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.....	42
E.	Claim 5 The hybrid device of claim 1, wherein the integrated PDK stores local, secured financial information.....	42
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.....	43
G.	Claim 7. The hybrid device of claim 1, wherein the hybrid device is a cell phone.....	43
H.	Claim 8. The hybrid device of claim 1, wherein the external PDK is included in jewelry.....	43
I.	Claim 9. The hybrid device of claim 1, comprising a storage for inheritance information.....	43
J.	Claim 10.....	44
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.....	45
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.....	46

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.....	46
N.	Claim 14 The method of claim 10, wherein the integrated PDK stores local, secured financial information. ....	46
O.	Claim 15 The method of claim 10, wherein the hybrid device is a cell phone. ....	46
P.	Claim 16 The method of claim 10, wherein the external PDK is included in jewelry. ....	46
Q.	Claim 17 .....	47
R.	Claim 18 The method of claim 10, wherein the first signal includes inheritance information. ....	48
S.	Claim 19 The method of claim 10, wherein the external PDK is included in a watch.....	48
T.	Claim 20 The hybrid device of claim 1, wherein the external PDK is included in a watch.....	49
XI.	GROUND 2: BROADCOM RENDERS OBVIOUS CLAIMS 1-7, 9-15 AND 17-18 .....	49
A.	Claim 1 .....	49
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. ....	61
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. ....	61

- 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..... 61
- E. Claim 5 The hybrid device of claim 1, wherein the integrated PDK stores local, secured financial information..... 62
- 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..... 62
- G. Claim 7. The hybrid device of claim 1, wherein the hybrid device is a cell phone..... 63
- H. Claim 9. The hybrid device of claim 1, comprising a storage for inheritance information..... 63
- I. Claim 10..... 63
- 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..... 64
- 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..... 65
- 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.....	65
M.	Claim 14 The method of claim 10, wherein the integrated PDK stores local, secured financial information. ....	65
N.	Claim 15 The method of claim 10, wherein the hybrid device is a cell phone. ....	65
O.	Claim 17 .....	66
P.	Claim 18 The method of claim 10, wherein the first signal includes inheritance information. ....	66
XII.	GROUND 3: BROADCOM AND GIOBBI '157 RENDER OBVIOUS CLAIMS 8, 16 AND 19-20 .....	67
A.	Claim 8. The hybrid device of claim 1, wherein the external PDK is included in jewelry. ....	67
B.	Claim 16 The method of claim 10, wherein the external PDK is included in jewelry. ....	68
C.	Claim 19 The method of claim 10, wherein the external PDK is included in a watch.....	68
D.	Claim 20 The hybrid device of claim 1, wherein the external PDK is included in a watch.....	68
XIII.	SECONDARY CONSIDERATIONS.....	68
XIV.	CONCLUSION .....	69

**LIST OF EXHIBITS**

Exhibit	Description
1001	U.S. Patent No. 9,049,188 (“’188 patent”)
1002	File History for U.S. Patent No. 9,049,188
1003	Declaration of Andrew Wolfe
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”)

**LIST OF APPENDICES**

Appendix A      *Curriculum Vitae* of Andrew Wolfe, Ph.D.

**LIST OF CHALLENGED CLAIMS**

<b>Claim</b>	<b>U.S. Patent No. 9,049,188</b>
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 FOR CHALLENGE (37 C.F.R. § 42.204(b)(2))**

No.	Ground for Challenge
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**

1. I have been retained by Petitioner Apple Inc. (“Apple”) to provide an opinion on the validity of U.S. Patent No. 9,049,188 B1 (the “’188 patent”), owned by Patent Owner Proxense, LLC (“Proxense” or “Patent Owner”). My opinions are based on information currently available to me. To the extent that additional information becomes available, I reserve the right to continue my investigation and study, which may include a review of documents and information that recently have been or may be produced, as well as testimony from depositions that may yet be taken in this case. I may thus expand or modify my opinions as my investigation and study continues. I may also supplement my opinions in response to any additional information that becomes available to me or that Patent Owner makes available, any matters raised by Patent Owner and/or opinions provided by Patent Owner’s experts, or in light of any relevant orders from the Patent Trial and Appeal Board.

## **II. EDUCATION AND WORK EXPERIENCE**

2. Attached to this declaration is a copy of my curriculum vitae that fully sets forth my qualifications. Below is a summary of my education, work experience, and other qualifications.

3. In 1985, I earned a Bachelor's degree in Electrical Engineering and Computer Science from The Johns Hopkins University. In 1987, I received an Master's degree in Electrical and Computer Engineering from Carnegie Mellon University. In 1992, I received a Ph.D. in Computer Engineering from Carnegie Mellon University. My doctoral dissertation proposed a new approach for the architecture of a computer processor.

4. I have more than 35 years of experience as a computer architect, computer system designer, personal computer graphics designer, educator, and executive in the electronics industry.

5. In 1983, I began designing touch sensors, microprocessor-based computer systems, and I/O (input/output) cards for personal computers as a senior design engineer for Touch Technology, Inc. During the course of my design projects with Touch Technology, I designed I/O cards for PC-compatible computer systems, including the IBM PC-AT, to interface with interactive touch-based computer terminals that I designed for use in public information systems. I continued designing and developing related technology as a consultant to the Carroll Touch division of AMP, Inc., where in 1986 I designed one of the first custom touch-screen integrated circuits. I designed the touch/pen input system for the Linus WriteTop, which many believe to be the first commercial tablet computer.

6. From 1986 through 1987, I designed and built a high-performance computer system as a student at Carnegie Mellon University. From 1986 through early 1988, I also developed the curriculum and supervised the teaching laboratory for processor design courses.

7. In the latter part of 1989, I worked as a senior design engineer for ESL-TRW Advanced Technology Division. While at ESL-TRW, I designed and built a bus interface and memory controller for a workstation-based computer system, and also worked on the design of a multiprocessor system.

8. At the end of 1989, I (along with some partners) reacquired the rights to the technology I had developed at Touch Technology and at AMP and founded The Graphics Technology Company. Over the next seven years, as an officer and a consultant for The Graphics Technology Company, I managed the company's engineering development activities and personally developed dozens of touch screen sensors, controllers, and interactive touch-based computer systems.

9. I have consulted, formally and informally, for a number of fabless semiconductor companies. In particular, I have served on the technical advisory boards for two processor design companies: BOPS, Inc., where I chaired the board; and Siroyan Ltd., where I served in a similar role for three

networking chip companies—Intellon, Inc., Comsilica, Inc., and Entridia, Inc.—and one 3D game accelerator company, Ageia, Inc.

10. I have also served as a technology advisor to Motorola and to several venture capital funds in the U.S. and Europe. Currently, I am a director of Turtle Beach Corporation, providing guidance in its development of premium audio peripheral devices for a variety of commercial electronic products.

11. From 1991 through 1997, I served on the Faculty of Princeton University as an Assistant Professor of Electrical Engineering. At Princeton, I taught undergraduate and graduate-level courses in Computer Architecture, Advanced Computer Architecture, Display Technology, and Microprocessor Systems, and conducted sponsored research in the area of computer systems and related topics. I was also a principal investigator for DOD research in video technology and a principal investigator for the New Jersey Center for Multimedia Research. From 1999 through 2002, while a Consulting Professor, I taught a Computer Architecture course to both undergraduate and graduate students at Stanford University. At Princeton, I received several teaching awards, both from students and from the School of Engineering. I have also taught advanced microprocessor architecture to industry professionals in seminars sponsored by the Institute of Electrical and

Electronics Engineers (“IEEE”) and the Association for Computing Machinery (“ACM”). I am currently an Assistant Teaching Professor at Santa Clara University teaching courses on Microprocessor Systems, IC Design, PCB Design, Real-Time Computing, and Mechatronics.

12. From 1997 through 2002, I held a variety of executive positions at a publicly-held fabless semiconductor company originally called S3, Inc. and later called SonicBlue Inc. I held the positions of Chief Technology Officer, Vice President of Systems Integration Products, Senior Vice President of Business Development, and Director of Technology, among others. At the time I joined S3, the company supplied graphics accelerators for more than 50% of the PCs sold in the United States. At S3 I supervised the design of several PC graphics accelerators. During my time at SonicBlue we launched more than 30 new consumer electronics products including devices to support copy-protected video and many of the first commercial products to support copy-protected internet audio content. These included some of the first consumer products to support playback of encrypted content using digital rights management (DRM) based security. I also worked with Universal Music Group and Sony Entertainment on the development of systems for distribution and management of secure, encrypted content.

13. I have published more than fifty peer-reviewed papers in computer architecture and computer systems and IC design. I also have chaired IEEE and ACM conferences in microarchitecture and integrated circuit design and served as an associate editor for IEEE and ACM journals. I served on the IEEE Computer Society Awards committee. I am an IEEE Fellow, an IEEE Computer Society Distinguished Contributor, and a Member of ACM. I am a named inventor on at least fifty-seven U.S. patents and thirty-seven foreign patents, which are listed in my curriculum vitae. Some of these patents relate to encryption systems.

14. In 2002, I was the invited keynote speaker at the ACM/IEEE International Symposium on Microarchitecture and at the International Conference on Multimedia. From 1990 through 2005, I have also been an invited speaker on various aspects of technology and the PC industry at numerous industry events including the Intel Developer's Forum, Microsoft Windows Hardware Engineering Conference, Microprocessor Forum, Embedded Systems Conference, Comdex, and Consumer Electronics Show, as well as at the Harvard Business School and the University of Illinois Law School. I have been interviewed on subjects related to computer graphics and video technology and the electronics industry by publications such as the Wall Street Journal, New York Times, Los Angeles Times, Time, Newsweek,

Forbes, and Fortune as well as on CNN, NPR, and the BBC. I have also spoken at dozens of universities including MIT, Stanford, University of Texas, Carnegie Mellon University, UCLA, University of Michigan, Rice University, and Duke University.

### **III. COMPENSATION**

15. I am being compensated at my usual and customary hourly rate of \$750 for my expert services in connection with this proceeding. My compensation does not depend in any way upon the outcome of this proceeding, the opinions I express, or the content of my testimony.

### **IV. LEGAL PRINCIPLES**

16. I am informed that “prior art” includes patents and printed publications that existed before the earliest applicable filing date of the '188 patent.

17. I am informed that in order for a claim to be anticipated, each and every requirement of the claim must be found, expressly or inherently, in a single prior art reference as recited in the claim.

18. I am informed that a claimed invention is not patentable if the claimed invention would have been obvious to a person of ordinary skill in the field of the invention at the time the invention was made.

19. I am informed that in order to show obviousness based on a combination of references, a particular motivation to combine the teachings in the references must be shown.

20. I am informed that claim terms are generally given their ordinary and customary meaning, which is the meaning that the term would have to a person of ordinary skill in the art at the time of the invention. I further understand that a person of ordinary skill in the art must read the claim term not only in the context of the particular claim in which the term appears but in the context of the entire patent, including the specification.

21. I am informed that the obviousness inquiry should not be done in hindsight, and depends on the scope and content of the prior art, the differences between the prior art and the claims at issue, the knowledge of a person of ordinary skill in the pertinent art at the time of invention, and any other objective factors indicating obviousness or non-obviousness.

22. I am informed that in order to rely on a reference for obviousness, the reference must be analogous art. I also understand that to be analogous art, the reference must be either (1) from the same field of endeavor as the claimed subject matter, regardless of the problem addressed, or (2) if not in the same field of endeavor, reasonably pertinent to the particular problem with which the inventor is involved. I am also familiar with the premise that for a

reference to be reasonably pertinent, it must have logically commended itself to an inventor's attention at the time of invention.

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

23. In my opinion a Person of Ordinary Skill in the Art 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). This level of skill is approximate, and more experience in one area would compensate for less experience in another area and vice versa.

## **VI. OVERVIEW OF THE '188 PATENT**

24. 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.

25. 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.

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

26. 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. 1002, at 443-444. These claims issued as amended by the Examiner.

## VIII. CLAIM CONSTRUCTION

27. It is my understanding that Petitioner submits that express interpretations of the challenged claims are not required to resolve this petition because the prior art references relied on in this Petition meet or disclose each of the claim terms under any reasonable construction. I currently see no reason to disagree with this position. I understand that in a prior proceeding—i.e., *Samsung Electronics America, Inc. v. Proxense, LLC*, IPR2021-01438, filed on August 26, 2021 (the “Samsung IPR”)—the Board determined that the term “Personal Digital Key (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. I further understand that 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.” 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).” I reserve the right to modify my opinions in light of to any claim constructions established by the Board or any Court in the future.

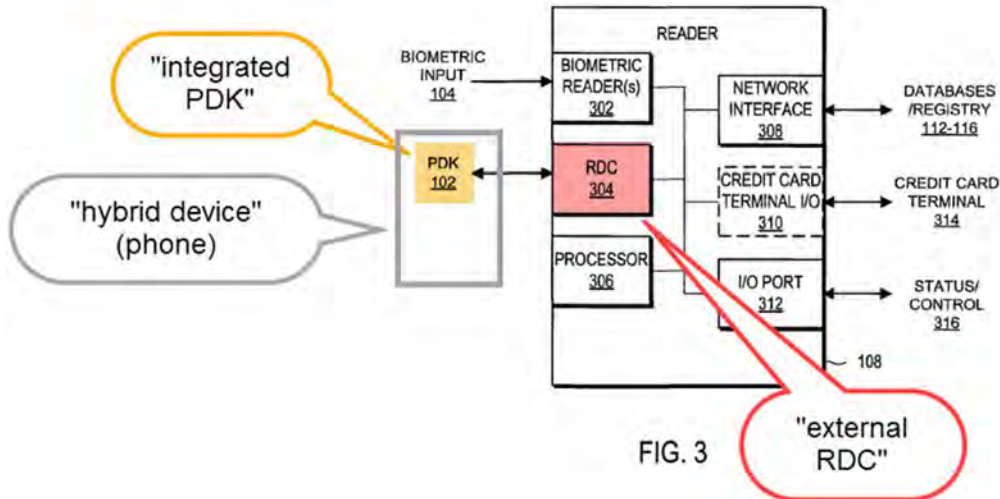
## **IX. CITED ART**

### **A. Giobbi ’157**

28. 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.

29. 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.

30. 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 I prepared:



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:

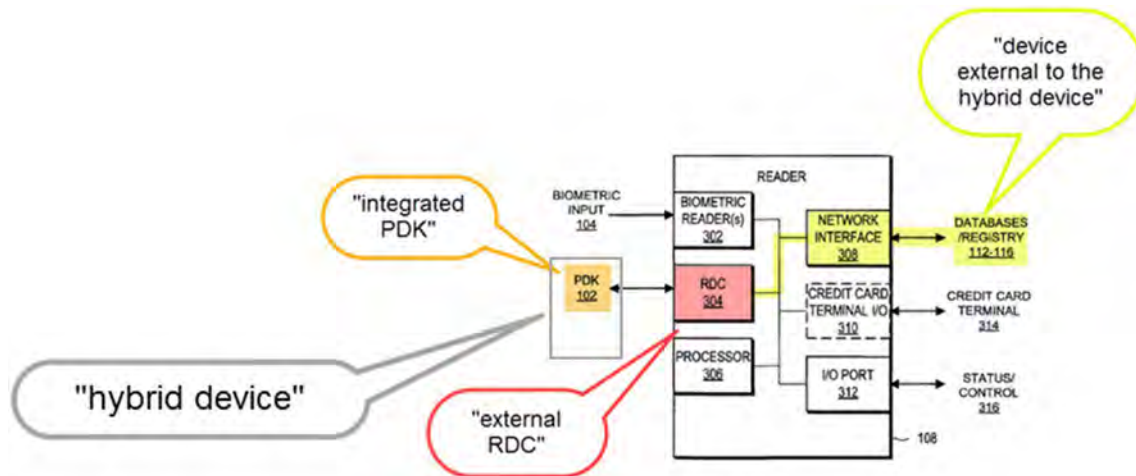


FIG. 3

Ex. 1004 at Fig. 3.

31. 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.

## B. Giobbi '139

32. 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 a receiver decoder circuit (RDC) and discloses that a 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)*[.]”).

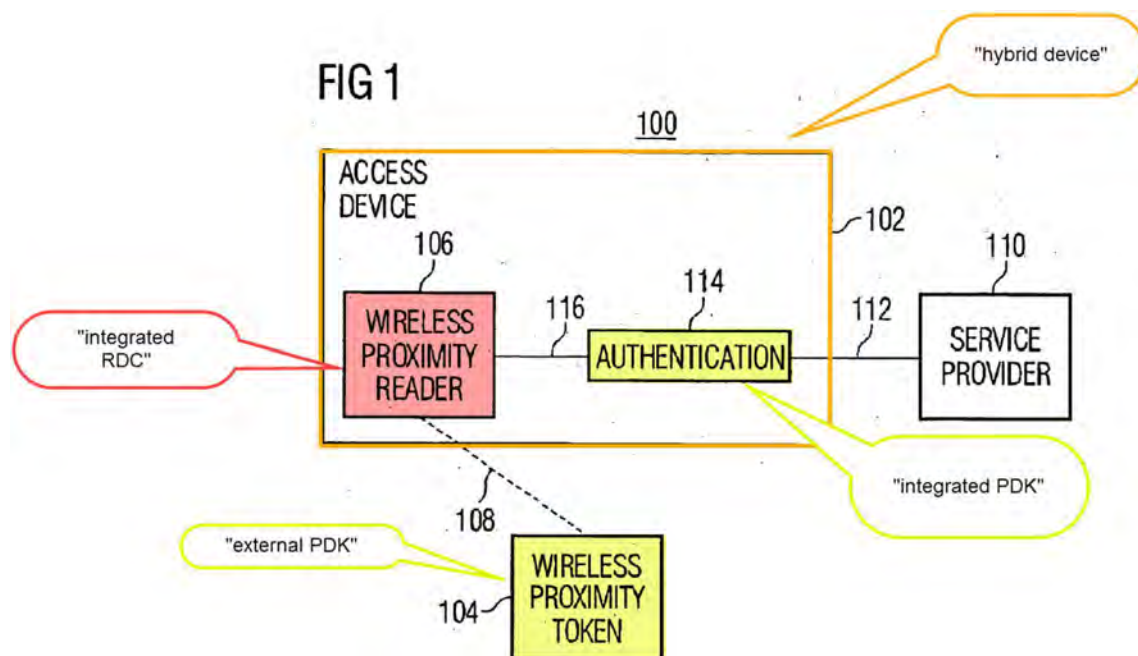
33. Giobbi ’139 expressly teaches coupling an integrated RDC and an integrated PDK by a signal line for communication. In particular, Giobbi ’139 teaches:

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.

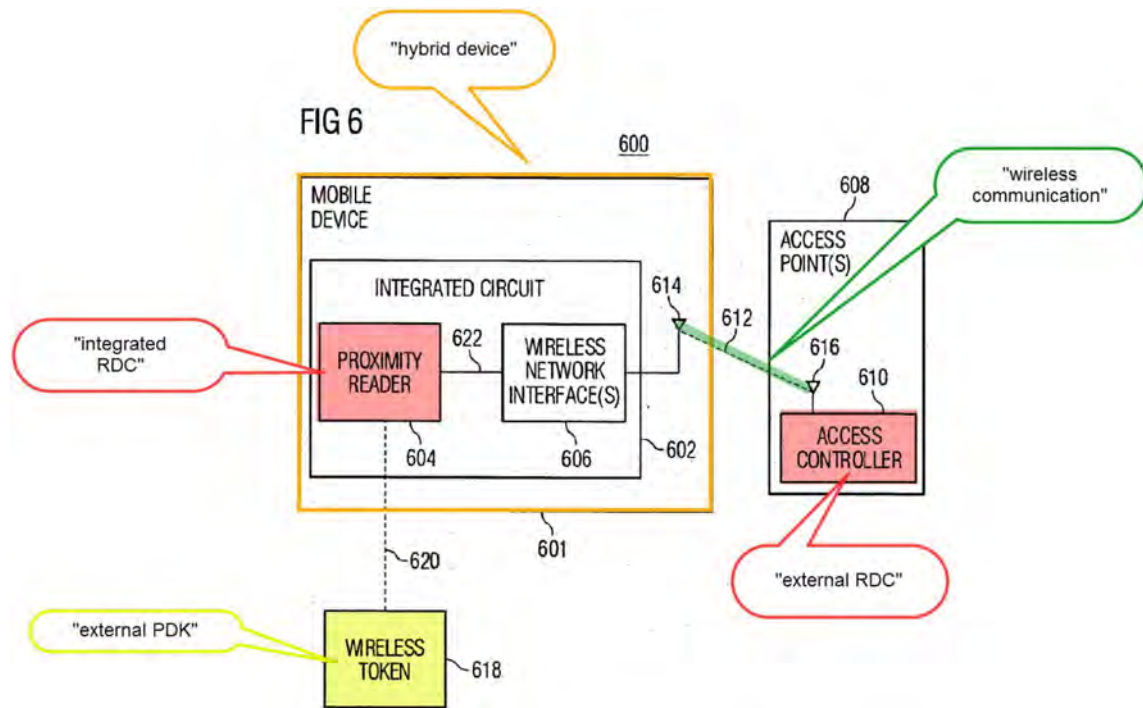
### C. Broadcom

34. 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

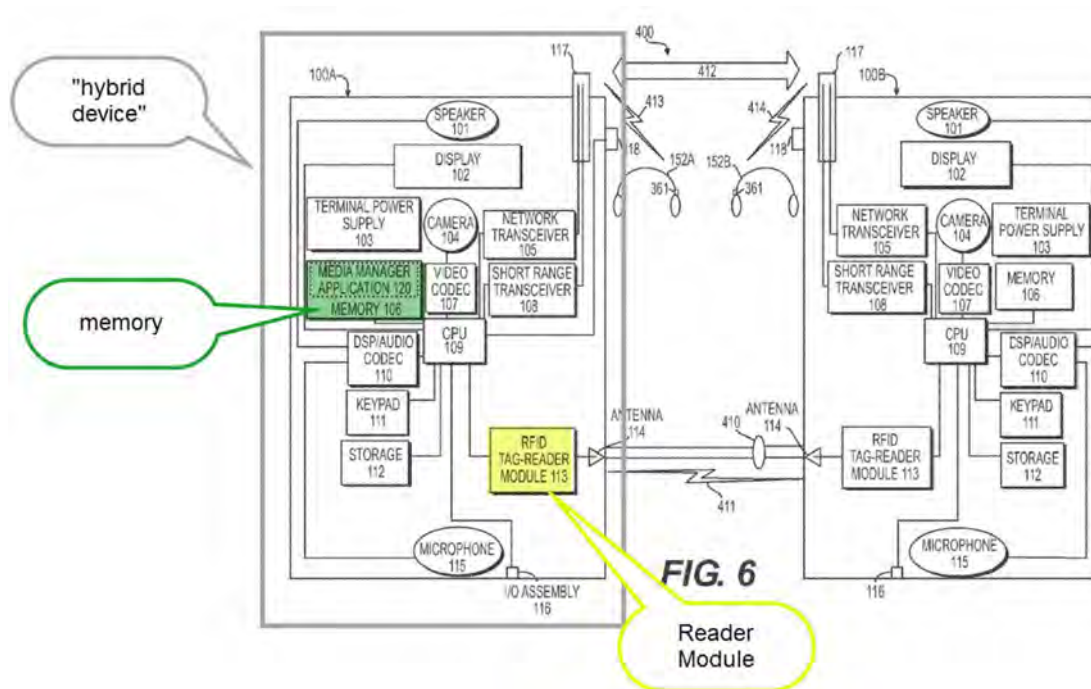
some embodiments, the Access Device 102 can be a mobile phone which facilitates access to an access point for mobile communications, as shown, for example, in Figure 6:



Ex. 1007 at Fig. 6.

#### D. Dua

35. 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.

36. 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.”

37. 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:

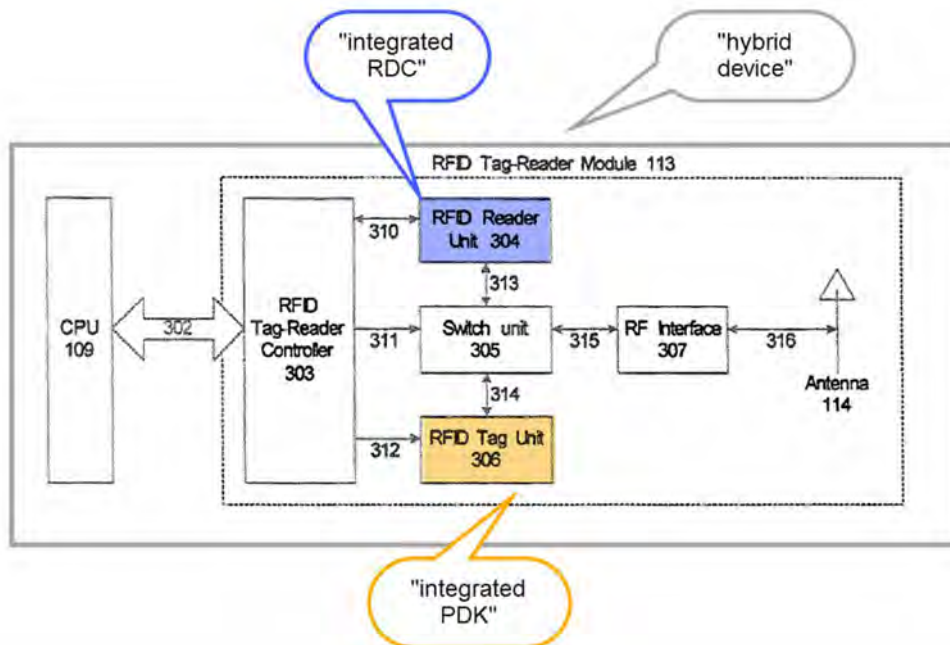


FIG. 4A

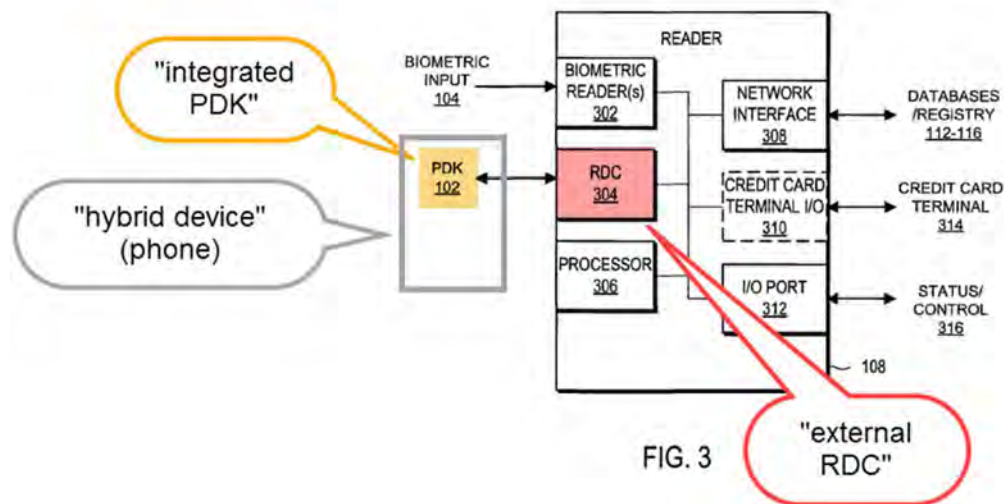
Ex. 1006 at Fig. 4A. Dua's **Tag** Unit 306 stores information necessary to gain access to an external device. In particular, Dua explains that its **Tag** Unit 306 stores information in internal tag memory. Ex. 1006 at 15:42-56. This information may be encrypted. Ex. 1006 at 16:31-34. Dua transmits 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.

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

**A. Claim 1**

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

38. 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 I prepared:

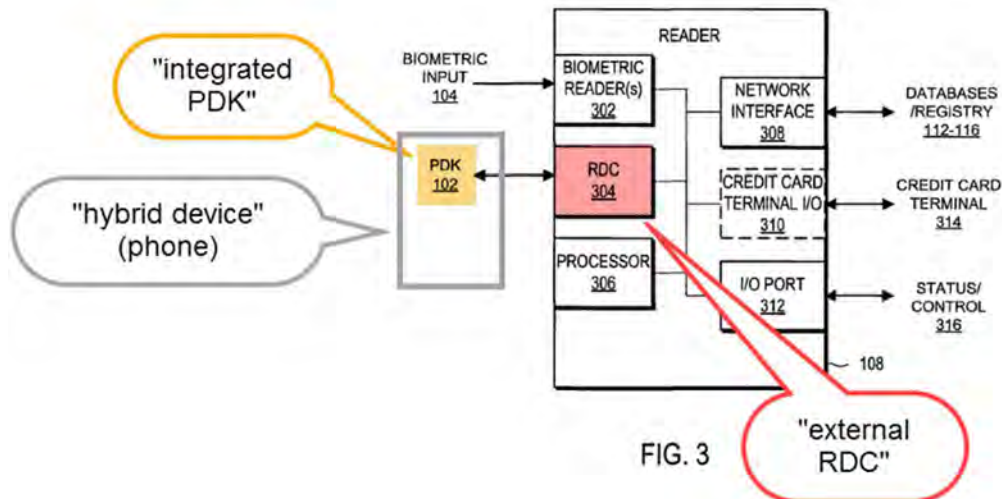


Ex. 1004 at Fig. 3 (annotated). As shown above, Giobbi’s hybrid device (cell phone) carries an integrated PDK. This PDK communicates with an external RDC, as discussed below.

**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**

39. *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,’ stores one or more profiles (e.g., a biometric profile) in a tamper-proof memory.”). 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.” *Id.* 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. 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[.]” *Id.* 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 I prepared:



Ex. 1004 at Fig. 3 (annotated). 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:

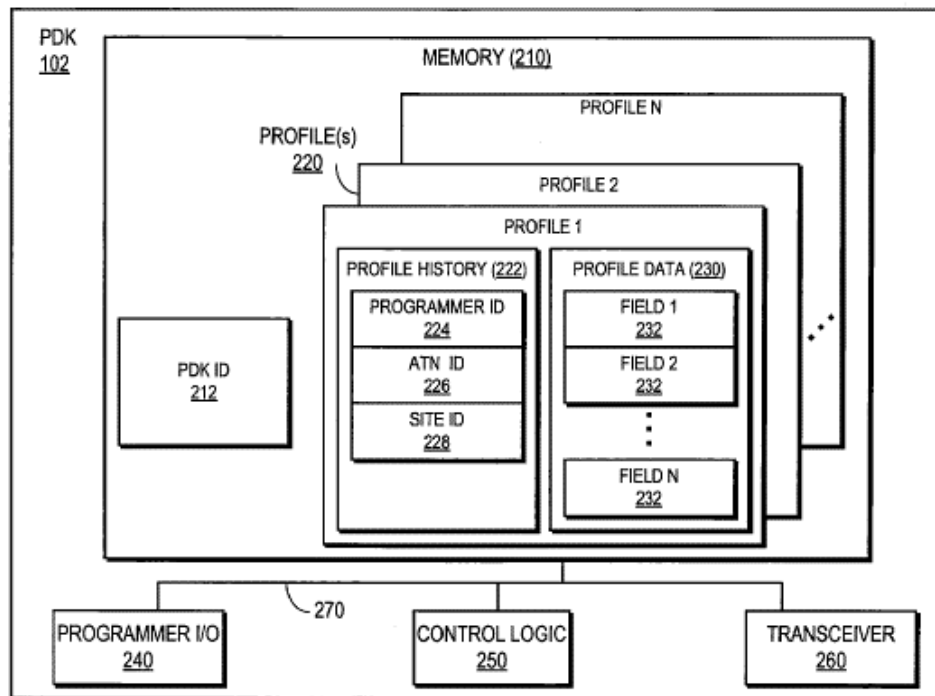


FIG. 2

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).

40. *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:

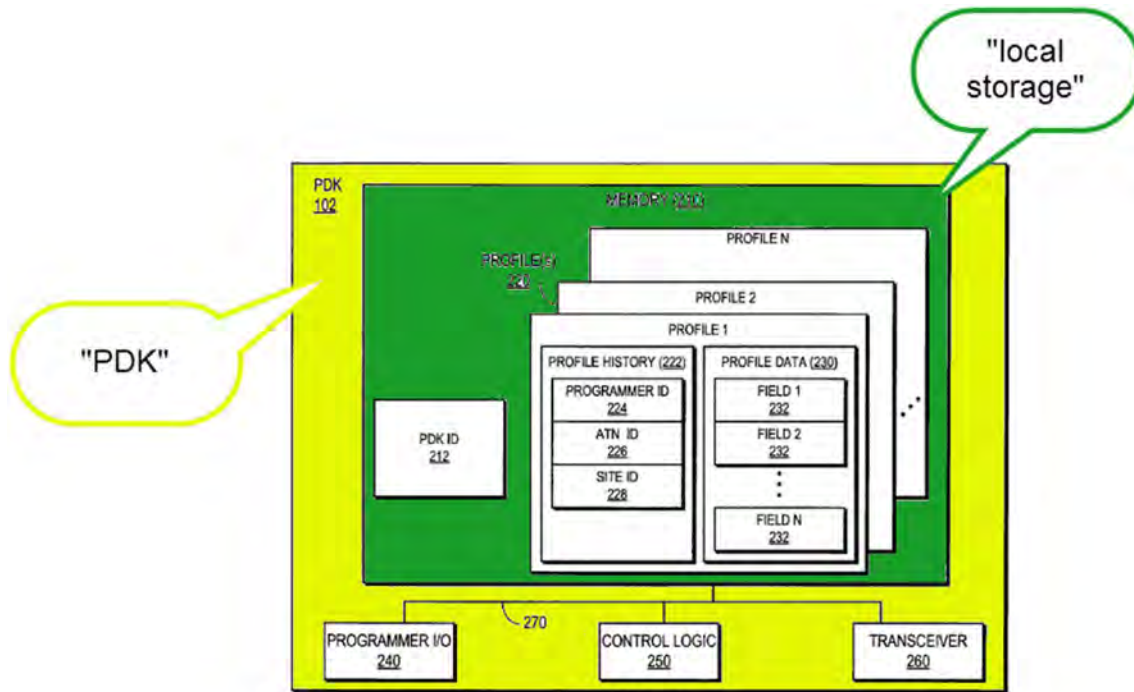


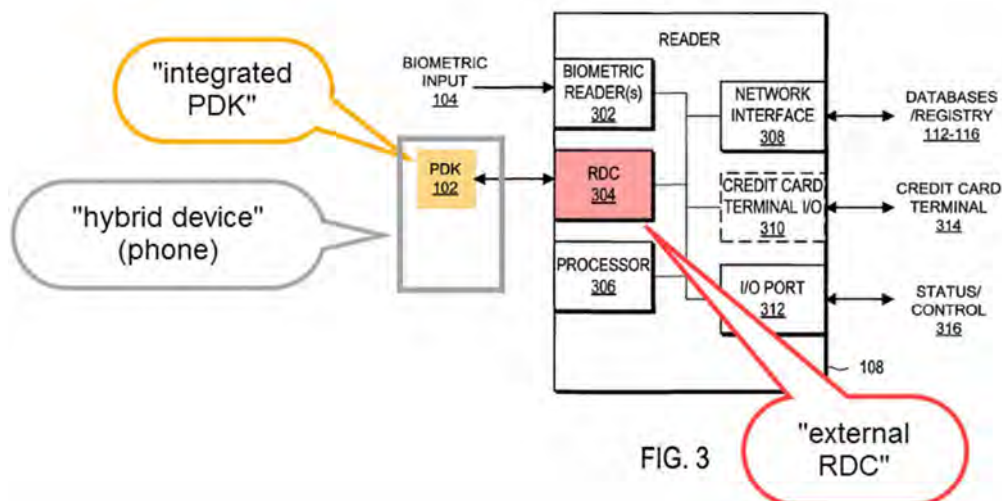
FIG. 2

Ex. 1004 at Fig. 2, ¶ 35.

41. *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.”).

42. *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, I annotated:



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*[.]”).

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

43. 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 a RDC into Giobbi '157's hybrid device for communication with external PDKs based, in part, on the teachings of Giobbi '139.

44. In particular, Giobbi '139 *expressly* teaches integrating a 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 a 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.

45. 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 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. Thus, it would have been a natural fit to integrate an RDC into Giobbi '157's cell phone.

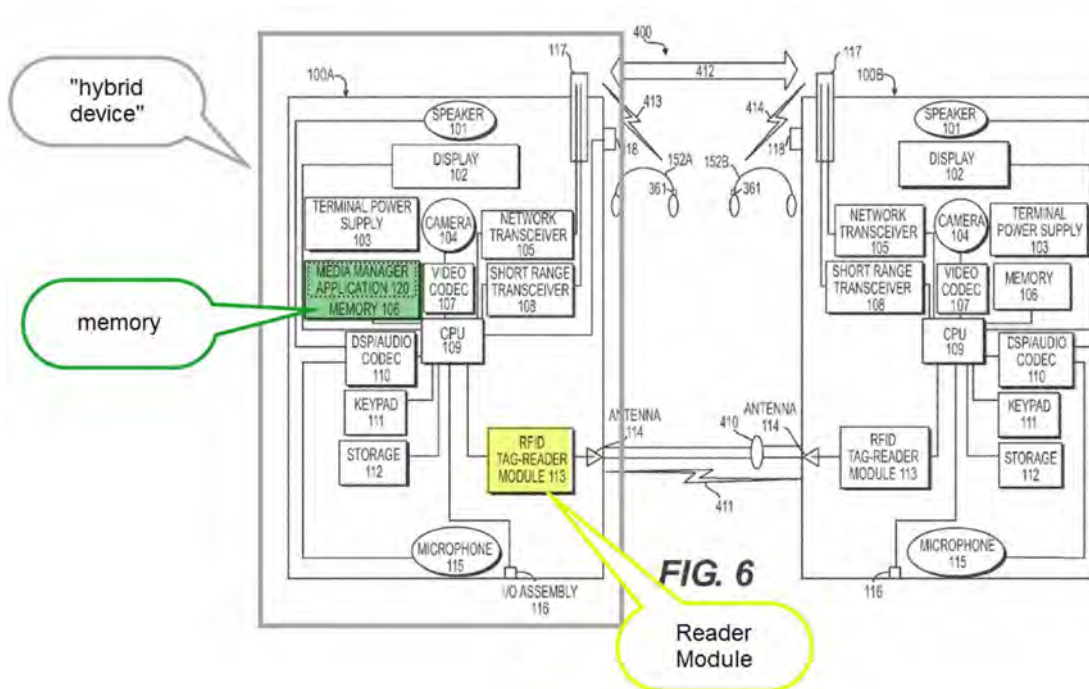
46. In addition, Giobbi '157 touts that its invention improves transactions. Ex. 1004 at ¶ 27 (describing the benefits of the claimed invention on transaction flexibility and efficiency). Integrating a RDC into Giobbi '157's cell phone would further this goal by allowing the phone to take part in both 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.

47. 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 a

RDC onto a hybrid device would be desirable since it would provide security for the data stored on the hybrid device.

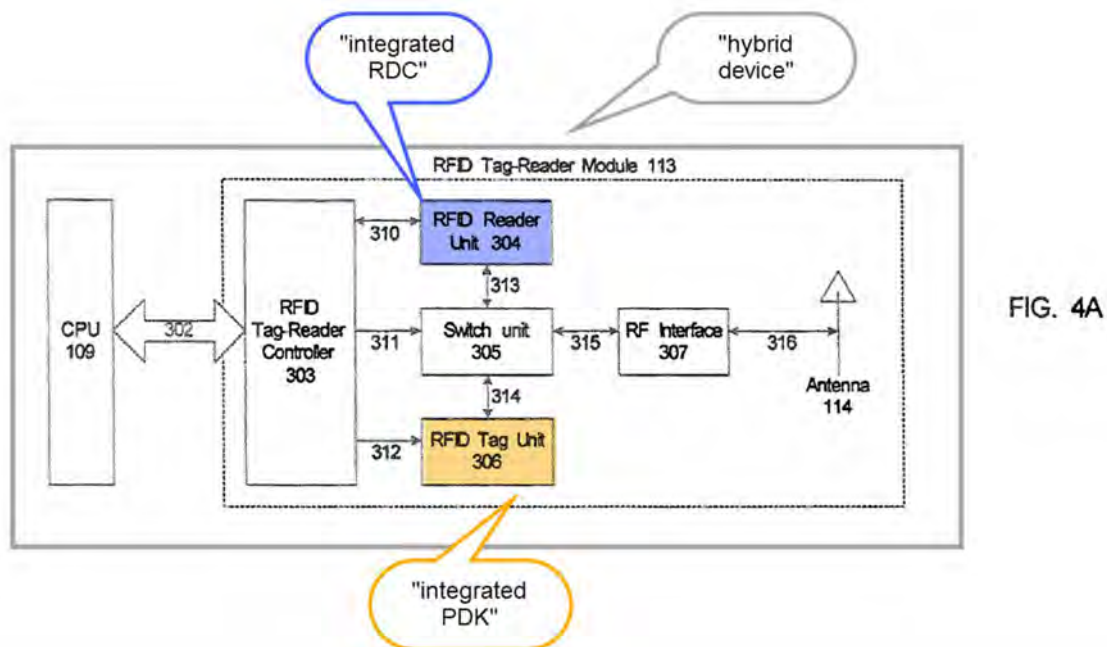
48. Further, Giobbi '157 teaches that it is advantageous to incorporate PDKs into “commonly carried items,” like phones, since it would eliminate the need for a user to carry a separate PDK device and would reduce the risk of loss. Ex. 1005 at ¶ 35. This added convenience would similarly motivate a POSITA to integrate a 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. 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.*

49. In addition to Giobbi '139, the Dua patent's RFID system configuration also provides motivation to integrate a 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 a RFID Tag as an electronic “key” and a RFID Reader as the electronic “lock.”

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



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.

51. 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.

52. 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.

***Additional Motivations to Combine:***

53. A POSITA would also be motivated to combine the teachings of Giobbi '139 and Dua with the Giobbi '157 system because, at least, because 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 a RDC into the Giobbi ’157 hybrid device.

54. This reasonable expectation of success is further bolstered by the teachings of Dua, which, as discussed above, also teaches integrating a RDC and PDK into the same type of device. Ex. 1006 at Fig. 4A, 13:19-14:64.

55. I generated an annotated version of Figure 3 which adds an integrated RDC (blue) into Giobbi ’157’s cell phone hybrid device:

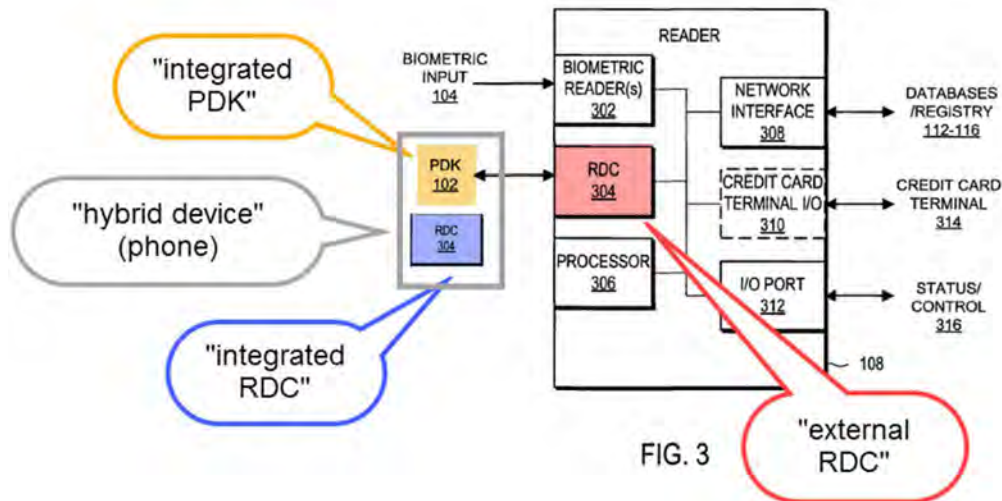


FIG. 3

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

56. 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.

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

57. 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.

58. 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.

59. 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.

60. 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. 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.

61. 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.

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

62. 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. 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). 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.**

63. 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:

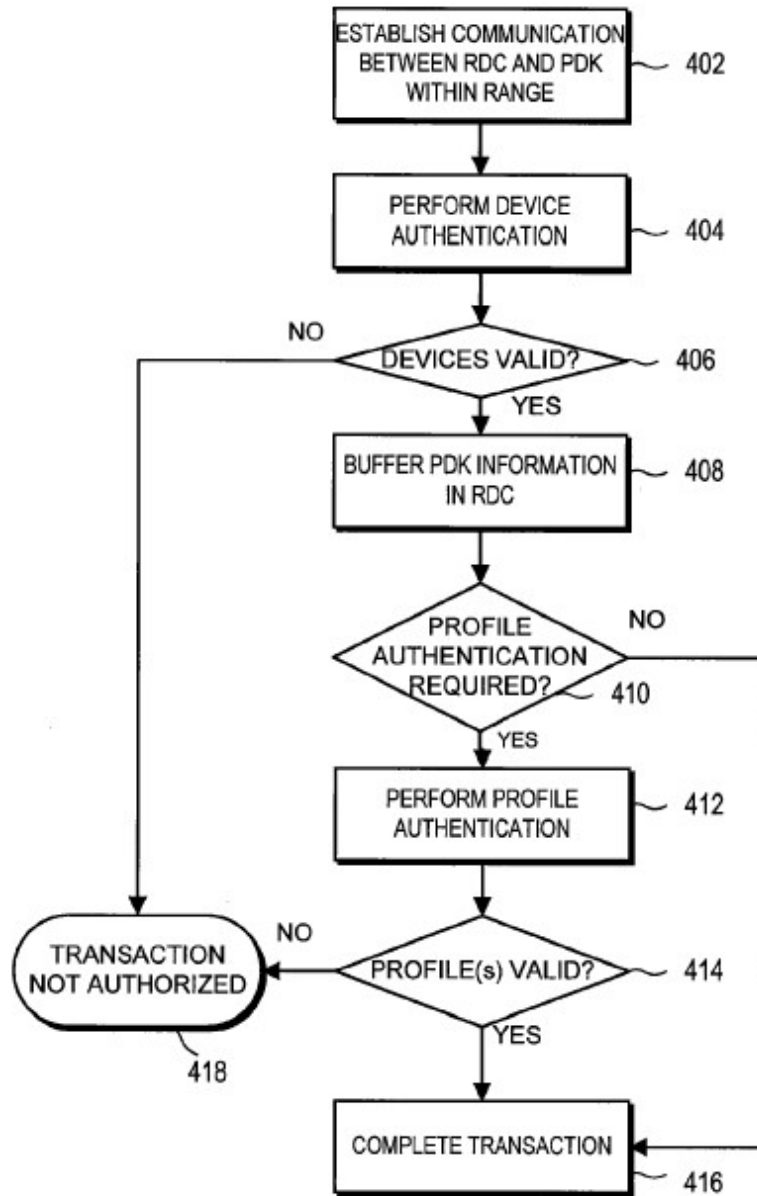


FIG. 4

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.

64. 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.

**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.**

65. 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.

**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.**

66. 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.

**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.**

67. 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.

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

68. 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.

**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.**

69. 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.

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

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

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

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

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

72. 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.

**J. Claim 10**

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

73. *See* claim 1.

**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),**

74. *See* claim 1.

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

75. *See* claim 1.

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

76. *See* claim 1.

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

77. *See* claim 1.

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

78. As discussed with respect to claim 1, a 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.

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

**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.**

80. 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.

- 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.

81. 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.

- 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.

82. *See* claim 4.

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

83. *See* claim 1, 2, 5.

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

84. *See* claim 1.

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

85. *See* claim 8.

**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**

86. 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.*

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

87. 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.

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

88. 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.

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

89. *See* claim 9.

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

90. *See* claim 8.

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

91. See claims 8, 19.

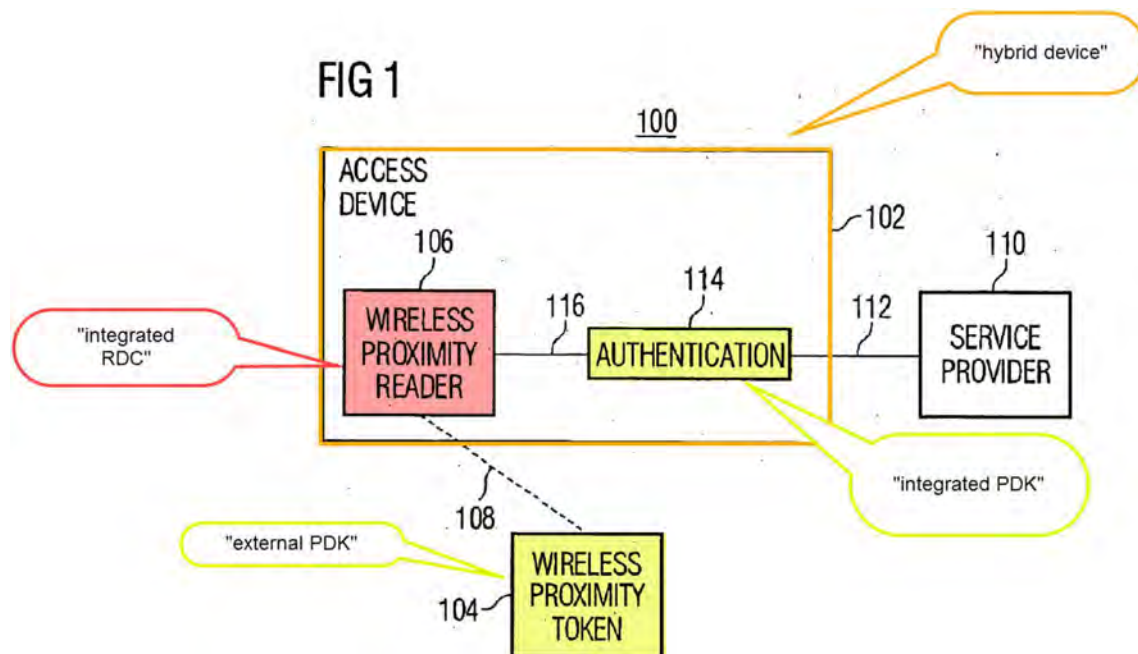
**XI. GROUND 2: BROADCOM RENDERS OBVIOUS CLAIMS 1-7, 9-15 AND 17-18**

**A. Claim 1**

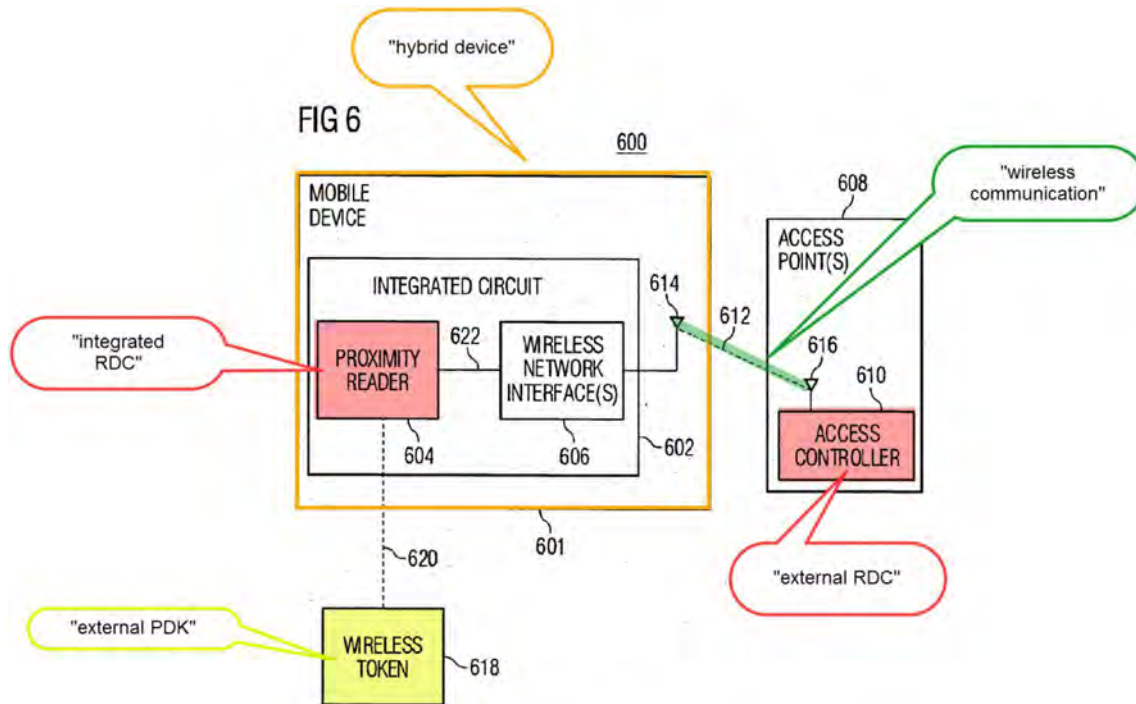
**1. 1pre A hybrid device comprising:**

92. 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.*

93. 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:

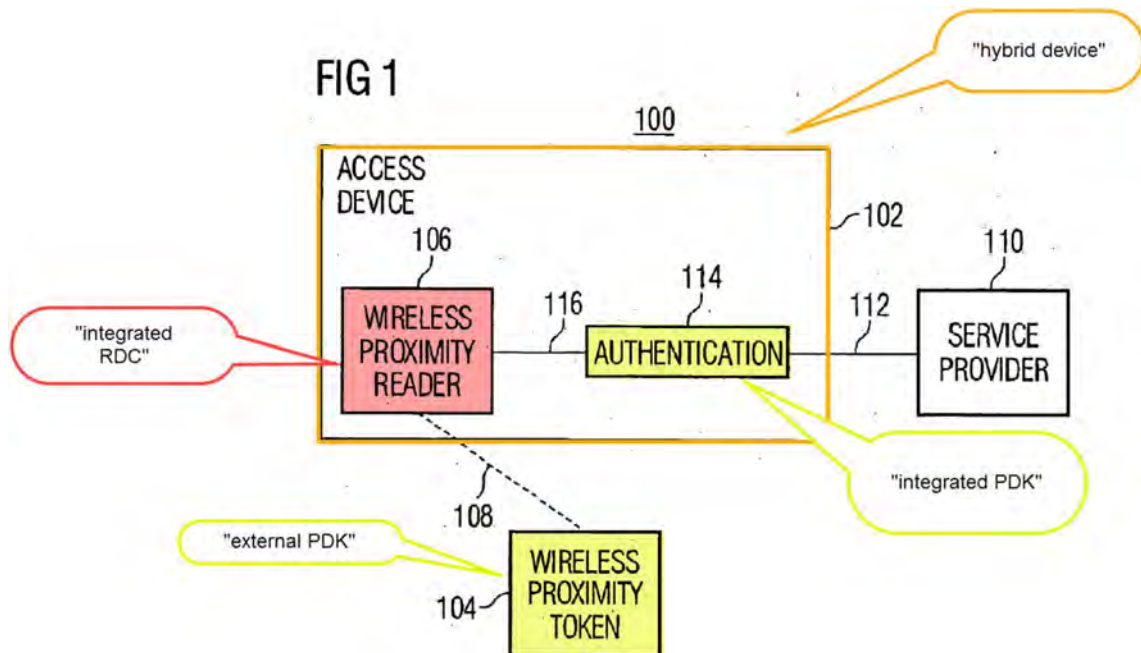


Ex. 1007 at Fig. 6.

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

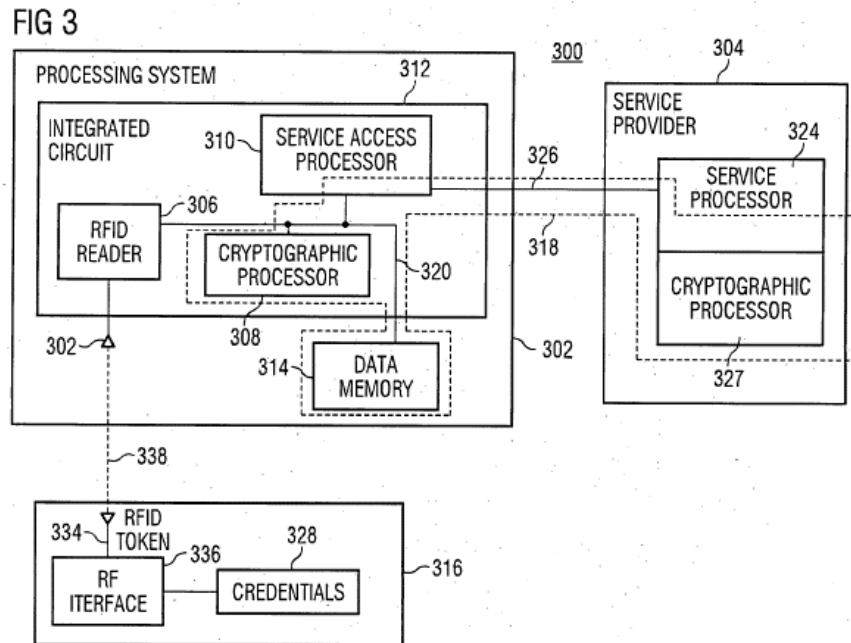
**wirelessly with an external receiver-decoder circuit (RDC); and**

94. *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):



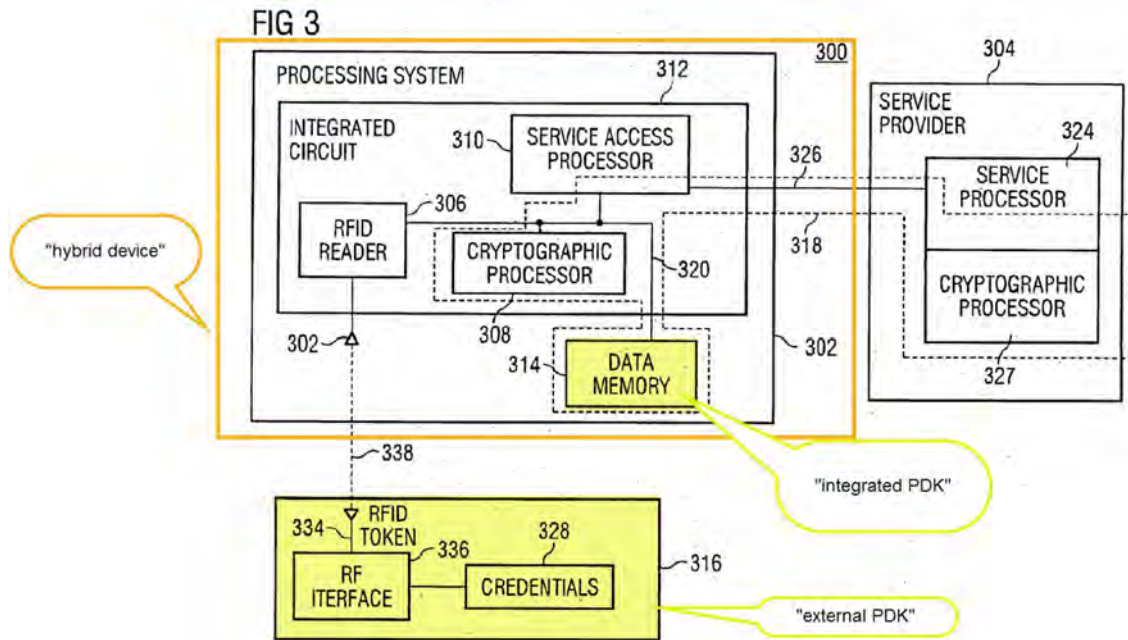
Nonetheless, a POSITA would understand the access device 102 to include internal memory for storing at least the disclosed database which would contain biometric information.

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. 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. RF signals from the access device “are broadcast via an antenna 332.” Ex. 1007, ¶ 146.

95. *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:



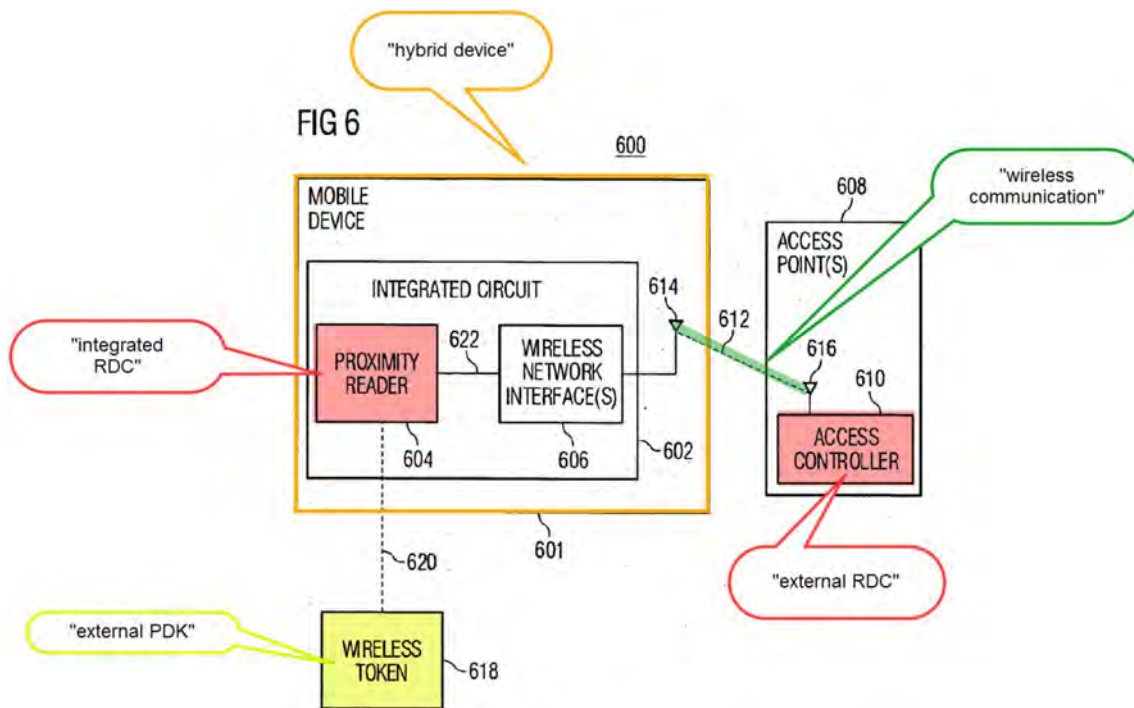
Ex. 1007 at Fig. 3.

96. *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).

97. 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.”).

98. *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:

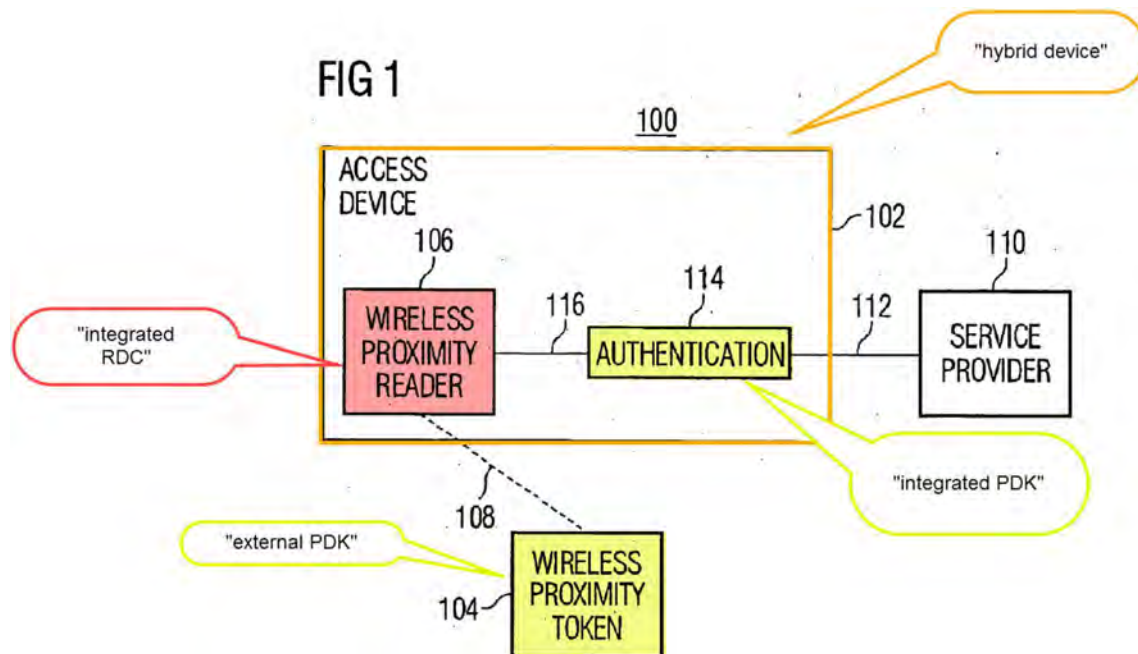


99. Ex. 1007 at Fig. 6. Broadcom explains that a token may send authentication information to an integrated RDC (*i.e.*, the proximity reader). Ex. 1007 at 165. As discussed above, this information is passed to local memory and authentication circuitry. Broadcom teaches that a wireless network interface 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.

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

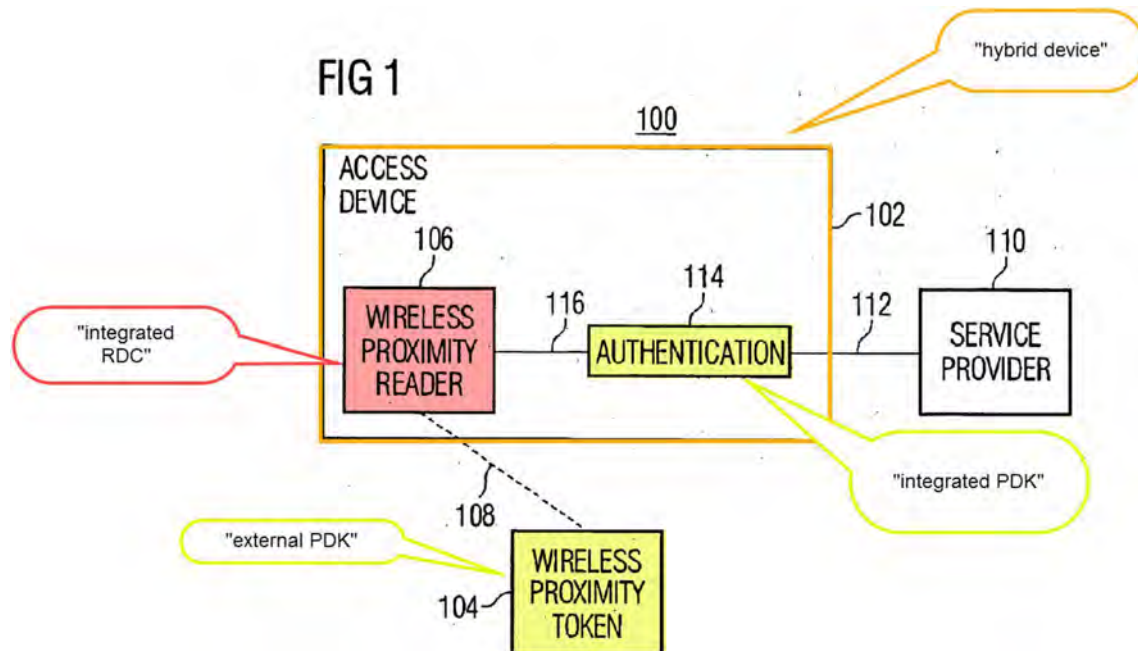
100. As discussed with respect to claim limitation 1A, Broadcom's hybrid device includes an integrated RDC, the wireless proximity reader:



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.

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

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



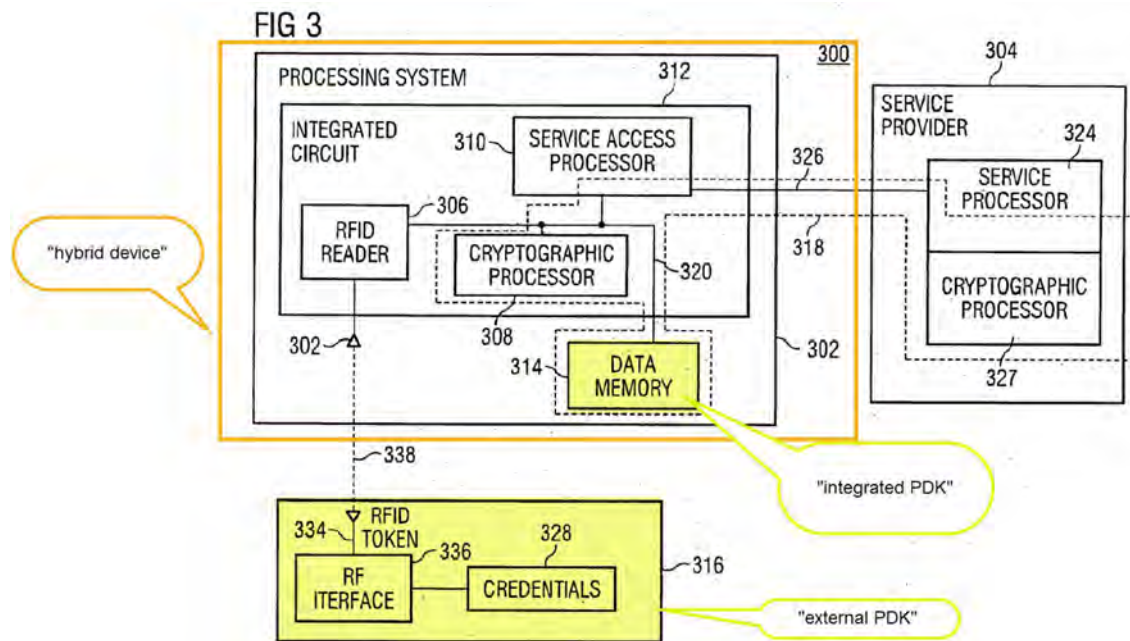
Ex. 1007 at Fig. 1 (annotated). Broadcom explains:

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.

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

102. 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

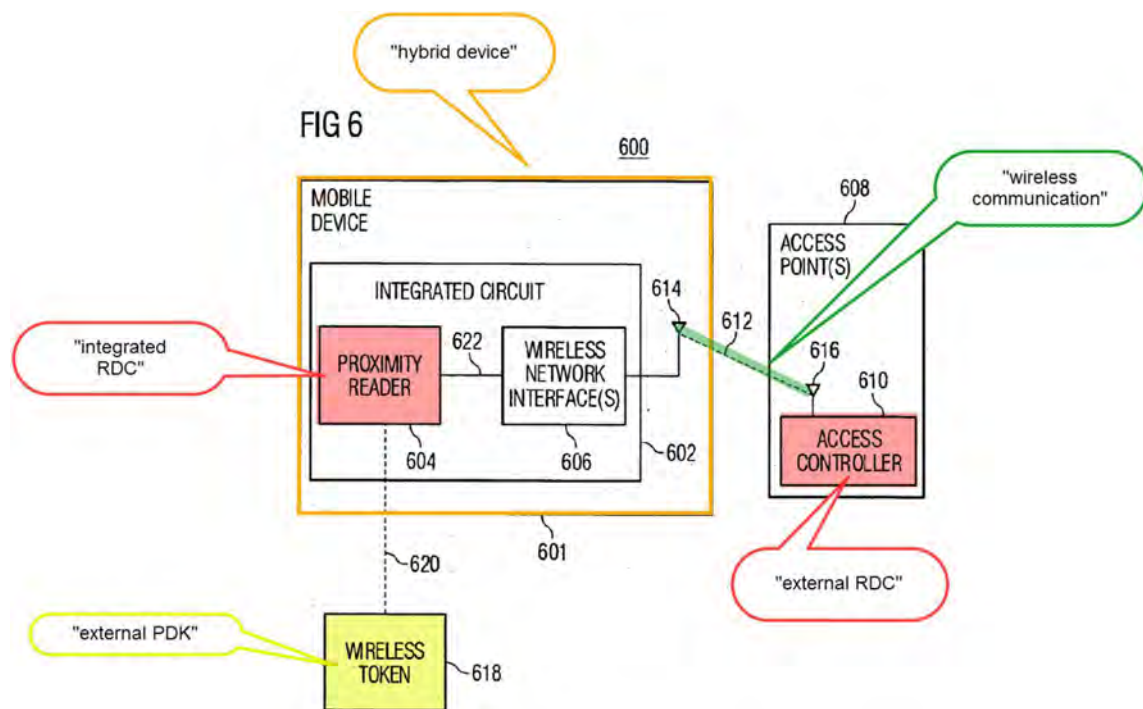
would be connected to an application processor as well as various input and output devices such as buttons, a touch sensor, and a vibrator motor. This allows processing of credentials as well as interactions with a user in response to the presentation of credentials.

103. 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. 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.

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

104. 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.

105. 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.

106. 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.*

**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.**

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

**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.**

108. 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.

**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.**

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

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

110. 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.

**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.**

111. 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.

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

112. *See* claim 1.

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

113. 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.

**I. Claim 10**

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

114. *See* claim 1.

**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),**

115. *See* claim 1.

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

116. *See* claim 1.

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

117. *See* claim 1.

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

118. *See* claim 1.

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

119. As discussed with respect to claim 1, a 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.

- 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.**

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

**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.**

121. 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.

**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.**

122. *See* claim 4.

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

123. *See* claim 5.

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

124. *See* claim 1; claim 7.

**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**

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

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

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

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

127. *See* claim 2, 5.

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

128. *See* claim 9.

## **XII. 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.**

129. 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.

130. 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.

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

131. *See* claim 8.

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

132. *See* claim 8.

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

133. *See* claim 8, 19.

### **XIII. SECONDARY CONSIDERATIONS**

134. At this stage of these proceedings, it is my understanding that Petitioner has no burden to identify and rebut secondary considerations. Rather, it is my understanding that Patent Owner must first present a *prima facie* case for such consideration, which Petitioners should then have the chance to rebut. That said, I have considered evidence of secondary considerations that I am aware of at this time and I am currently unaware of any evidence of secondary considerations that would have any impact on my conclusions of obviousness as expressed above.

#### **XIV. CONCLUSION**

135. For at least the foregoing reasons, the listed claims are obvious in my opinion over the prior art.

I, Andrew Wolfe, do hereby declare and state, that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, under Section 1001 of Title 18 of the United States Code.

Dated: February 4, 2025



Andrew Wolfe

# Andrew Wolfe Ph.D.

2005 De La Cruz Blvd STE 142  
Santa Clara, CA 95050  
(408) 394-1096 (mobile)  
Email: awolfe@awolfe.org

## Education:

Ph.D. in Electrical and Computer Engineering, Carnegie Mellon University, 1992  
Visiting Graduate Student, Center for Reliable Computing, Stanford University, 1988-1989  
M.S. in Electrical and Computer Engineering, Carnegie Mellon University, 1987  
B.S.E.E. in Electrical Engineering and Computer Science, The Johns Hopkins University, 1985

## Recent Employment:

Lecturer, Asst. Teaching Professor [September 2013-present]  
**Santa Clara University**

Teaching graduate and undergraduate courses on embedded computing, mechatronics, real-time systems, computer architecture, design, and community service. Faculty Senate President 2023-24.

Consultant, [October 2002-present]  
**Wolfe Consulting**

Consultant on processor technology, computer systems, consumer electronics, software, design tools, and intellectual property issues. Testifying and consulting expert for IP and other technology-related litigation matters.

Sample clients include:

Google	Apple	Samsung
Sony	Huawei	HTC
AT&T	Verizon Mobile	T-Mobile
IBM	Motorola/Lenovo	Nintendo
Activision	AMD	Western Digital
Sonos	Qualcomm	LG
Netflix	Roku	Tivo
Synaptics	Sawstop	3M
Medigus	TCL	ZTE
Egnyte	Acer	Waymo

Chief Technical Officer, [1999-2002]; Sr. VP of Business Development, [2001-2002]; VP, Systems Integration, S3 Fellow, [1998 – 1999]; Director of Technology, S3 Fellow, [1997 - 1998]  
**SONIC|blue, Inc**, Santa Clara, CA (formerly S3 Inc.)

## Strategic Business Development:

Developed and implemented strategy to reposition S3 from PC graphics into the leading networked consumer electronics company.

- Acquired Diamond Multimedia and coordinated integration of communications, Rio digital music, and workstation graphics divisions into S3.
- Identified and negotiated acquisitions to grow digital media businesses including Empeg, ReplayTV, and Sensory Science.
- Identified and negotiated strategic investments including Comsilica, Intellon, KBGear Interactive, Entridia, DataPlay and others.

- Developed strategy for integrated graphics/core-logic products and established a joint venture with Via Technologies to design and market these products.
- Negotiated divestiture of graphics chip business to Via and the workstation graphics division to ATI.

**Product Planning and Development:**

- Drove roadmap development within SONICblue product divisions.
- Managed Business Development for all product lines.
- Led New Product Development and Corporate Vision processes.
- Acting co-General Manager of Rio digital music business in 2<sup>nd</sup> half of 2001. Responsible for all areas of product development, business development, and cost management.
- Managed development of the Savage/MX and Savage/IX mobile 3D graphics accelerators and Savage/NB system logic products.

**Public Relations, Public Policy and Investor Relations:**

- Present company products and strategy at industry events such as CES, Comdex, and Microprocessor Forum.
- Discuss new products and initiatives with the press.
- Promote issues of interest to SONICblue to industry groups and in Washington.
- Brief analysts, and investors on company progress. Participate in quarterly conference calls.

**IP Management and Licensing:**

- Negotiated and managed partnership agreements including a critical cross-licensing agreement with Intel.
- Renegotiated technology-licensing agreements with IBM for workstation graphics products.
- Evaluated outside technology opportunities, managed video research and development, and managed corporate IP strategy with legal staff including patent filings, cross licensing, and litigation.

Consulting Professor, [1999-2002]

**Stanford University**, Stanford, CA

Teaching computer architecture and microprocessor design.

Assistant Professor [1991 - 1997]

**Princeton University**, Princeton, NJ

Teaching and research in the Electrical Engineering department. Research in embedded computing systems, multimedia, video signal processors, compiler optimization, and high performance computer architecture. Principal investigator or project manager for ~\$6M in funded research.

Visiting Assistant Professor, [1992]

**Carnegie Mellon University**, Pittsburgh, PA

Research and preparation of teaching materials on advanced microprocessor designs including new superscalar and superpipelined processor architectures.

Founder and Vice President and Consultant, [1989 - 1995]

**The Graphics Technology Company, Inc.**, Austin, TX

Founded company to develop touch-sensitive components and systems for the first generation of PDA devices and interactive public systems. Obtained financing from Gunze Corp., Osaka, Japan. Company is now part of 3M.

Senior Electrical Engineer, [1989]

**ESL - TRW, Advanced Technology Division**, Sunnyvale, CA

Designed the architecture for an Intel i860-based multiple-processor digital signal processing system for advanced military applications. Designed several FPGA interface chips for VME-bus systems.

Design Consultant, [1986 -1987]

**Carroll Touch Division, AMP Inc.**, Round Rock, TX

Developed several new technologies for touch-screen systems. Designed the first ASIC produced for AMP, a mixed-signal interface chip for controlling touch-screen sensors. Developed the system electronics, system firmware, and customer utility software for numerous products including those based on the new ASIC.

Senior Design Engineer, [1983 -1985]

**Touch Technology Inc.**, Annapolis, MD

**Advisory Boards:**

Director, Turtle Beach Corporation (NASDAQ:HEAR) (formerly Parametric Sound Corporation), KBGear Interactive, Inc., Comsilica, Inc., Rioport.com, various S3 subsidiaries.

Technical Advisory Boards, Ageia, Inc., Intellon, Inc., Comsilica, Inc., Entridia, Inc., Siroyan, Ltd., BOPS, Inc, Qvester Venture Funds

Carnegie Mellon University Silicon Valley Advisory Board; Johns Hopkins University Tech Transfer Advisory Board

**Awards:**

IEEE Fellow - for contributions in hardware code compression of embedded software, power consumption analysis, and optimization, 2022  
IEEE Computer Society Distinguished Contributor - 2021  
Micro Test-of-Time Award (in recognition of one of the ten most influential papers of the first 25 years of the symposium), 2014  
Business 2.0 “20 Young Executives You Need to Know”, 2002  
Walter C. Johnson Prize for Teaching Excellence, 1997.  
Princeton University Engineering Council Excellence in Teaching Award, Spring 1996  
AT&T/Lucent Foundation Research Award, 1996.  
Walter C. Johnson Prize for Teaching Excellence, 1995  
IEEE Certificate of Appreciation, 1995, 2001.  
AT&T Foundation Research Award, 1993.  
Semiconductor Research Corporation Fellow, 1986 - 1991.  
Burroughs Corporation Fellowship in Engineering, 1985 - 1986.

**Professional Activities:**

Program Chair: Micro-24, 1991, Hot Chips 13, 2001.  
General Chair: Micro-26, 1993, Micro-33, 2000.  
Associate Editor: IEEE Computer Architecture Letters; ACM Transactions in Embedded Computing Systems  
Speaker at CES, WinHec, Comdex, Intel Dev. Forum, Digital Media Summit, Microprocessor Forum, etc.  
Keynote speaker at Micro-34, ICME 2002  
IEEE B. Ramakrishna Rau Award committee – 2012-2016  
IEEE Computer Society Awards Committee – 2015  
Director – IEEE Consultants Network of Silicon Valley – 2022-present  
CES Awards Judge – 2016  
Entrepreneurship Mentor – Draper University

**Over 50 refereed publications.****Publications since January 2006:**

Wolfe, A., “Retrospective on Code Compression and a Fresh Approach to Embedded Systems”, IEEE MICRO, July/Aug. 2016, Invited paper.

Michael Kreienkamp, Olivia McConaghy, Sally L. Wood, Andrew Wolfe, Julia A. Scott, 2024 NYC Neuromodulation Conference, Transcranial Photobiomodulation Control System Compatible with EEG, abstract and poster. June 2024 <https://neuromodec.org/nyc-neuromodulation-2024/poster-list.html#A83D>

**Patents:**

- U.S. Pat. 5,041,701 – *Edge Linearization Device for a Contact Input System*, Aug. 20, 1991.
- U.S. Pat. 5,438,168 – *Touch Panel*, Aug. 1, 1995.
- U.S. Pat. 5,736,688 – *Curvilinear Linearization Device for Touch Systems*, Apr. 7, 1998.
- U.S. Pat. 6,037,930 – *Multimodal touch sensitive peripheral device*, March 14, 2000.
- U.S. Pat. 6,408,421 – *High-speed asynchronous decoder circuit for variable-length coded data*, June 18, 2002.
- U.S. Pat. 6,865,668 – *Variable-length, high-speed, asynchronous decoder circuit*, March 8, 2005
- U.S. Pat. 7,079,133 – *Superscalar 3D Graphics Engine*, July 18, 2006
- EP 1 661 131 B1 – *PORTABLE ENTERTAINMENT APPARATUS*, Jan. 21, 2009
- U.S. Pat. 7,555,006 – *Method and system for adaptive transcoding and transrating in a video network*, June 30, 2009
- U.S. Pat. 7,996,595 – *Interrupt Arbitration for Multiprocessors*, Aug. 9, 2011
- EP 2 241 979 B1 – *Interrupt Arbitration for Multiprocessors*, Oct. 10, 2011
- U.S. Pat. 8,131,970 – *Compiler Based Cache Allocation*, March 6, 2012
- U.S. Pat. 8,180,963 – *Hierarchical read-combining local memories*, May 15, 2012
- U.S. Pat. 8,193,941 – *Snoring Treatment*, June 5, 2012
- U.S. Pat. 8,203,541 – *OLED display and sensor*, June 19, 2012
- U.S. Pat. 8,243,045 – *Touch-sensitive display device and method*, August 14, 2012
- U.S. Pat. 8,244,982 – *Allocating processor cores with cache memory associativity*, August 14, 2012
- U.S. Pat. 8,260,996 – *Interrupt Optimization for Multiprocessors*, Sept. 4, 2012
- 101185761 (KR) – *Noise Cancellation for Phone Conversation*, Sept. 19, 2012
- 101200740 (KR) – *OLED display and sensor*, November 7, 2012
- 101200741 (KR) – *Touch-sensitive display device and method*, November 7, 2012
- U.S. Pat. 8,321,614 – *Dynamic scheduling interrupt controller for multiprocessors*, Nov. 27, 2012
- U.S. Pat. 8,352,679 – *Selectively securing data and/or erasing secure data caches responsive to security compromising conditions*, Jan. 8, 2013
- U.S. Pat. 8,355,541 – *Texture Sensing*, Jan. 15, 2013
- U.S. Pat. 8,370,307 – *Cloud Data Backup Storage Manager*, Feb. 5, 2013
- U.S. Pat. 8,398,451 – *Tactile Input Interaction*, March. 19, 2013
- JP 5241032 B2 – *Routing Across Multicore Network Using Real World or Modeled Data*, April 13, 2013
- ZL201010124820.3 – *Interrupt Optimization for Multiprocessors*, April 17, 2013
- U.S. Pat. 8,428,438 – *Apparatus for Viewing Television with Pause Capability*, April 23, 2013
- JP 5266197 B2 – *Data Centers Task Mapping*, May 10, 2013
- U.S. Pat. 8,508,498 – *Direction and Force Sensing Input Device*, August 13, 2013
- U.S. Pat. 8,547,457 – *Camera Flash Mitigation*, October 1, 2013
- U.S. Pat. 8,549,339 – *Processor core communication in multi-core processor*, October 1, 2013
- 101319048 (KR) – *Camera Flash Mitigation*, October 10, 2013
- U.S. Pat. 8,628,478 – *Microphone for remote health sensing*, January 14, 2014
- 101362017 (KR) – *Thread Shift: Allocating Threads to Cores*, Feb. 5, 2014
- 101361928 (KR) – *Cache Prefill on Thread Migration*, Feb. 5, 2014
- 101361945 (KR) – *Mapping Of Computer Threads onto Heterogeneous Resources*, Feb. 5, 2014
- JP 5487307 B2 – *Mapping Of Computer Threads onto Heterogeneous Resources*, Feb. 28, 2014
- JP 5484580 B2 – *Task Scheduling Based on Financial Impact*, Feb. 28, 2014
- JP 5487306 B2 – *Cache Prefill on Thread Migration*, Feb. 28, 2014
- 101372623 (KR) – *Power Management for Processor*, March. 4, 2014
- 101373925 (KR) – *Allocating Processor Cores with Cache Memory Associativity*, March 6, 2014
- U.S. Pat. 8,676,668 – *Method for the determination of a time, location, and quantity of goods to be made available based on mapped population activity*, March 18, 2014
- U.S. Pat. 8,687,533 – *Energy Reservation in Power Limited Networks*, April 1, 2014
- 101388735 (KR) – *Routing Across Multicore Networks Using Real World or Modeled Data*, April 17, 2014
- U.S. Pat. 8,725,697 – *Cloud Data Backup Storage*, May 13, 2014
- U.S. Pat. 8,726,043 – *Securing Backing Storage Data Passed Through a Network*, May 13, 2014
- ZL201010124826.0 – *Dynamic scheduling interrupt controller for multiprocessors*, May 14, 2014
- JP 5547820 B2 – *Processor core communication in multi-core processor*, May 23, 2014
- U.S. Pat. 8,738,949 – *Power Management for Processor*, May 27, 2014

U.S. Pat. 8,751,854 – *Processor Core Clock Rate Selection*, June 10, 2014  
 JP 5559891 B2 – *Thermal Management in Multi-Core Processor*, June 13, 2014  
 101414033 (KR) – *Dynamic Computation Allocation*, June 25, 2014  
 JP 5571184 B2 – *Dynamic Computation Allocation*, July 4, 2014  
 101426341 (KR) – *Processor core communication in multi-core processor*, May 23, 2014  
 U.S. Pat. 8,799,671 – *Techniques for Detecting Encrypted Data*, Aug 5, 2014  
 101433485 (KR) – *Task Scheduling Based on Financial Impact*, Aug. 18, 2014  
 U.S. Pat. 8,824,666 – *Noise Cancellation for Phone Conversation*, Sept. 2, 2014  
 U.S. Pat. 8,836,516 – *Snoring Treatment*, Sept. 16, 2014  
 U.S. Pat. 8,838,370 – *Traffic flow model to provide traffic flow information*, Sept. 16, 2014  
 U.S. Pat. 8,838,797 – *Dynamic Computation Allocation*, Sept. 16, 2014  
 U.S. Pat. 8,854,379 – *Routing Across Multicore Networks Using Real World or Modeled Data*, Oct. 7, 2014  
 JP 5615361 B2 – *Thread Shift: Allocating Threads to Cores*, Oct. 15, 2014  
 U.S. Pat. 8,866,621 – *Sudden infant death prevention clothing*, Oct. 21, 2014  
 U.S. Pat. 8,881,157 – *Allocating threads to cores based on threads falling behind threads*, Nov. 4, 2014  
 ZL201080024755.5 – *Camera Flash Mitigation*, Nov 5, 2014  
 U.S. Pat. 8,882,677 – *Microphone for remote health sensing*, Nov. 11, 2014  
 U.S. Pat. 8,924,743 – *Securing Data Cache through Encryption*, December 30, 2014  
 U.S. Pat. 8,994,857 – *Camera Flash Mitigation*, March 31, 2015  
 JP 5699140 B2 – *Camera Flash Mitigation*, April 8, 2015  
 ZL201080035189.8 – *Thread Shift: Allocating Threads to Cores*, June 10, 2015  
 ZL201180005030.6 – *Processor core communication in multi-core processor*, June 10, 2015  
 U.S. Pat. 9,143,814 – *Method and system for adaptive transcoding and transrating in a video network*, Sept 22, 2015  
 ZL201080035177.5 – *Mapping Of Computer Threads onto Heterogeneous Resources*, Oct. 14, 2015  
 U.S. Pat. 9,178,694 – *Securing Backing Storage Data Passed Through a Network*, November 3, 2015  
 U.S. Pat. 9,189,282 – *Thread-to-core mapping based on thread deadline, thread demand, and hardware characteristics data collected by a performance counter*, November 17, 2015  
 U.S. Pat. 9,189,448 – *Routing image data across on-chip networks*, November 17, 2015  
 U.S. Pat. 9,208,093 – *Allocation of memory space to individual processor cores*, December 8, 2015  
 U.S. Pat. 9,239,994 – *Data Centers Task Mapping*, January 19, 2016  
 ZL201080036611.1 – *Allocating Processor Cores with Cache Memory Associativity*, January 20, 2016  
 EP2228779 B1 – *Traffic flow model to provide traffic flow information*, Jan. 27, 2016  
 U.S. Pat. 9,262,628 – *Operating System Sandbox*, February 16, 2016  
 GB2485682 – *Mapping Of Computer Threads onto Heterogeneous Resources*, Sept. 28, 2016  
 U.S. Pat. 9,330,137 – *Cloud Data Backup Storage Manager*, May. 3, 2016  
 ZL201080035185.X – *Cache Prefill on Thread Migration*, Aug. 24, 2016  
 U.S. Pat. 9,519,305 – *Processor Core Clock Rate Selection*, December 13, 2016  
 U.S. Pat. 9,569,270 – *Mapping thread phases onto heterogeneous cores based on execution characteristics and cache line eviction count*, February 14, 2017  
 GB2485683 – *Thread Shift: Allocating Threads to Cores*, Oct. 18, 2017  
 U.S. Pat. 9,852,435 – *Telemetrics based location and tracking*, December 26, 2017.  
 U.S. Pat. 9,915,994 – *Power management for processor*, March 13, 2018  
 U.S. Pat. 9,927,254 – *Traffic flow model to provide traffic flow information*, March 27, 2018  
 EP2254048 B1 – *Thread Mapping in Multi-Core Processors*, August 29, 2018  
 U.S. Pat. 10,860,432 – *Cloud Data Backup Storage Manager*, December 8, 2020

**Expert testimony by deposition or at trial – April 15, 2018 - -present**

<b>Case</b>	<b>Venue</b>	<b>Case Number</b>
Joe Andrew Salazar v HTC Corporation	E.D. Texas	2:16-cv-010986-JRG-RSP
Hitachi Maxell, Ltd. v. ZTE Corporation and ZTE (USA), Inc.	E.D. Texas	5:16-cv-00179 5:16-cv-00178
INTER PARTES REVIEW OF U.S. PATENT NO. 7,663,506 (Mediatek v AMD)	PTAB	IPR2017-00101 IPR2017-00102
Papst Licensing GmbH & Co. KG v. Samsung Electronics Co.,Ltd. and Samsung Electronics America, Inc.	E.D. Texas	6:15-CV-1102
HTC Corporation v. Telefonaktiebolaget LM Ericsson	E.D. Texas	6: 18-cv-00243-JRG
Seven Networks, LLC v ZTE (USA) Inc and ZTE Corporation	N. D. Texas - Dallas	3:17-CV-1495
AGIS Software Development, LLC v. HTC Corporation	E. D. Texas	2:17-cv-514
Barbaro Technologies, LLC v. Niantic, Inc	N.D. CA	3:18-cv-02955-RS
Immersion Corp. v. Samsung Electronics America, Inc. et al	E.D. Texas	2:17-cv-00572
INTER PARTES REVIEW OF U.S. PATENT NO. 7,171,526 (Northstar Innovations – Micron)	PTAB	IPR2018-01004 IPR2018-01005
CISCO SYSTEMS, INC., vs. UNILOC USA, INC., UNILOC 2017 LLC and UNILOC LICENSING USA LLC	N.D. CA	3:18-cv-04991-SI
INTER PARTES REVIEW OF U.S. PATENT NO. 8,020,014 (Intel/VLSI)	PTAB	IPR2018-01661 IPR2018-01312
INTER PARTES REVIEW OF U.S. PATENT NO Patent 9,294,799 (Comcast/Rovi)	PTAB	IPR2019-00299
Inter Partes Review of U.S. Patent No 7720929 (Unified Patents v Datascope)	PTAB	IPR2019-01115
Solas OLED Ltd., v. Samsung Display Co., Ltd., Samsung Electronics Co, Ltd., and Samsung Electronics America, Inc.,	PTAB	IPR2019-01668
INTER PARTES REVIEW OF U.S. PATENT NO Patent 8,973,069 (Comcast/Rovi)	PTAB	IPR2019-01434
U.S. Patent No. 8,448,215 IPR (Comcast v Rovi)	PTAB	IPR2019-01353
U.S. PATENT NO. 8,847,898 IPR filing (Samsung v Neodron)	PTAB	IPR2020-00234
U.S. PATENT NO. 8,610,009 IPR filing (Samsung v Neodron)	PTAB	IPR2020-00225
U.S. PATENT NO. 10,365,747 IPR filing (Samsung v Neodron)	PTAB	IPR2020-00308

AGIS Software Development LLC v. Google LLC, AGIS Software Development LLC v. WAZE Mobile Limited, and AGIS Software Development LLC v. Samsung Elecs. Co., Ltd. et al	E.D. Texas	2:19-cv-00361-JRG 2:19-cv-00359-JRG 2:19-cv-00362-JRG
Inter Partes Review of U.S. Patent No 8,112,670 (Sony)	PTAB	IPR2020-00726
U.S. Patent 8,819,505 IPR (Intel v PACT)	PTAB	IPR2020-00525
Inter Partes Review of U.S. Patent No 8,078,540 (Sony)	PTAB	IPR2020-00922
Inter Partes Review of U.S. Patent No 9,037,807 (Intel v PACT)	PTAB	IPR2020-00540
HONG KONG U-CLOUDLINK NETWORK TECHNOLOGY LIMITED AND U-CLOUDLINK (AMERICA), LTD., vs. SIMO HOLDINGS INC. AND SKYROAM, INC.,	N.D. CA	3:18-cv-05031-EMC
Joe Andrew Salazar v AT&T Mobility, LLC et al.	E.D. Texas	2:20-cv-00004-JRG
Innovative Memory Solutions Inc. v Micron, Inc	Delaware	14-1480 RGA
Inter Partes Review of U.S. Patent No. 6,411,941	PTAB	IPR2021-01338 IPR2021-01406
Maxell, Ltd. et al v. VIZIO, Inc	C.D. CA	2-21-cv-06758
Inter Partes Review of U.S. Patent No. 7,619,912	PTAB	IPR2022-00615
Inter Partes Review of U.S. Patent Nos. 11,016,918 and 11,232,054	PTAB	IPR2022-00996 IPR2022-00999
In the Matter of Certain Smart Televisions, - Maxell, Ltd. et al v. VIZIO, Inc	ITC	337-TA-1338
INTER PARTES REVIEW OF U.S. PATENT NOS. 8,787,060 and 9,318,160	PTAB	IPR2022-01427 IPR2022-01428
Sweat Equity Partners, LLC vs. Swoop Search, LLC, et al.,	San Francisco Superior Court	CGC-21-591702
Walter Kidde Portable Equipment, Inc. v. First Alert, Inc. and BRK Brands	W.D. Texas	6:22-cv-566-ADA
INTER PARTES REVIEW OF U.S. PATENT NO. 11,093,417	PTAB	IPR2023-00454
INTER PARTES REVIEW OF U.S. PATENT NO. 9,858,215	PTAB	IPR2023-00455
INTER PARTES REVIEW OF U.S. PATENTS NOS. 9,369,081 and 9,941,830	PTAB	IPR2023-00992 IPR2023-00993
FlatFrog Laboratories AB v. Chemtronics Co., Ltd.	E.D. Texas	2:23-cv-00306
INTER PARTES REVIEW OF U.S. PATENT NOS. 8,624,844	PTAB	IPR2024-00404
Topia Technology, Inc. v. EgnYTE, Inc.	District of Delaware	1-21-cv-01821-CJB