

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,

Petitioner,

v.

PROXENSE, LLC,

Patent Owner.

Case No. IPR2024-00783
U.S. Patent No. 9,679,289
Filing Date: December 7, 2015
Issue Date: June 13, 2017

**DECLARATION OF ANDREW WOLFE IN SUPPORT OF PETITION FOR
INTER PARTES REVIEW OF U.S. PATENT NO. 9,679,289**

(Exhibit 1003)

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Education and Work Experience	2
III.	Compensation	7
IV.	Legal Principles	7
	A. Anticipation Analysis: 35 U.S.C. § 102.....	8
	B. Obviousness Analysis: 35 U.S.C. § 103	9
V.	Level of Ordinary Skill.....	14
VI.	Field of Art and Related Art.....	14
VII.	Cited Art Prior to the '289 Patent.....	15
	A. Dua	17
	B. Buer	22
	C. Giobbi '157.....	26
	D. Lee	28
	E. Nishikawa.....	31
VIII.	Overview of the '289 Patent.....	32
	A. Overview	32
	B. Claim Construction.....	36
IX.	Grounds 1 and 2: Claims 1-6, 8-11, And 14-19 Would Have Been Obvious Over Dua In View Of Giobbi '157 or Dua In View of Giobbi '157 and Kotola	38
	A. Independent Claims.....	38
	1. Independent Claim 14.....	38

a.	[14pre] “A method comprising:”	39
b.	[14a] “creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external device,”	39
c.	[14b] “the hybrid device including an integrated, secure memory and the integrated RDC, wherein the integrated, secure memory stores local, secured information;”	48
d.	[14c] “receiving a first signal, at the integrated RDC, via the first wireless link, from the external device; and”	50
e.	[14d] “generating an enablement signal enabling one or more of an application, a function and a service.”	51
2.	Independent Claim 1	55
a.	[1pre] “A hybrid device comprising:”	55
b.	[1a] “an integrated, secure memory storing local, secured information; and”	55
c.	[1b] “an integrated reader-decoder circuit (RDC) for communicating wirelessly with at least one external device within a proximity zone,”	56
d.	[1c] “the integrated RDC communicatively coupled to the integrated, secure memory for communication with the integrated, secure memory,”	56
e.	[1d] “wherein one or more of (a) the integrated RDC communicating wirelessly with the at least one external device within the proximity zone and (b) the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and a service.”	58
B.	Dependent Claims	59

1. 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 is enabled, at least in part, on the hybrid device.” ..59
2. 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 is enabled, at least in part, external to the hybrid device using an external RDC, the hybrid device communicatively coupled to wirelessly communicate with the external RDC.” 60
3. Claim 4: “The hybrid device of claim 1, wherein the local, secured information includes biometric information for authenticating a user.” 62
4. Claim 5: “The hybrid device of claim 1, wherein the local, secured information includes biometric information based on a biometric scan of a finger, the biometric information for authenticating a user.” 63
5. Claim 6: “The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information.” 64
6. Claim 8: “The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on an authorization of the financial information using an external authentication database, the financial information transmitted to the external authentication database.” 65
7. Claim 9: “The hybrid device of claim 8, wherein the external authentication database is separate from a merchant providing a sale in the financial transaction.” 67
8. Claim 10: “The hybrid device of claim 1, wherein the one or more of the application, the function and the service

	enabled based on the local, secured information stored by the integrated, secure memory includes a first application, function or service based on a first subsets of local, secured information stored by the integrated, secure memory and a second application, function or service based on a second subset of local, secured information, the first and second subset of local, secured information having different accessibility.”	67
9.	Claim 11: “The hybrid device of claim 1, wherein the hybrid device is a cell phone.”	69
10.	Claim 15: “The method of claim 14, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on the hybrid device.”	70
11.	Claim 16: “The method of claim 14 further comprising: sending the enablement signal, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on a device external to the hybrid device and communicatively coupled to an external RDC.”	70
12.	Claim 17: “The method of claim 14, wherein the local, secured information includes biometric information for authenticating a user.”	70
13.	Claim 18: “The method of claim 14, wherein the local, secured information includes financial information and wherein the one or more of the application, the function and the service completes a financial transaction.”	71
14.	Claim 19: “The method of claim 14, wherein the hybrid device is a cell phone.”	71
X.	Ground 3: Claims 1-7, 11, and 14-19 Would Have Been Obvious Over Buer.....	71
A.	Independent Claims.....	71
1.	Independent Claim 14.....	71
a.	[14pre] “A method comprising:”	71

b.	[14a] “creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external device,”	72
c.	[14b] “the hybrid device including an integrated, secure memory and the integrated RDC, wherein the integrated, secure memory stores local, secured information;”	85
d.	[14c] “receiving a first signal, at the integrated RDC, via the first wireless link, from the external device; and”	86
e.	[14d] “generating an enablement signal enabling one or more of an application, a function and a service.”	87
2.	Independent Claim 1	93
a.	[1pre] “A hybrid device comprising:”	93
b.	[1a] “an integrated, secure memory storing local, secured information; and”	93
c.	[1b] “an integrated reader-decoder circuit (RDC) for communicating wirelessly with at least one external device within a proximity zone,”	93
d.	[1c] “the integrated RDC communicatively coupled to the integrated, secure memory for communication with the integrated, secure memory,”	94
e.	[1d] “wherein one or more of (a) the integrated RDC communicating wirelessly with the at least one external device within the proximity zone and (b) the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and a service.”	96
B.	Dependent Claims	98

1. 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 is enabled, at least in part, on the hybrid device.” ..98
2. 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 is enabled, at least in part, external to the hybrid device using an external RDC, the hybrid device communicatively coupled to wirelessly communicate with the external RDC.” 98
3. Claim 4: “The hybrid device of claim 1, wherein the local, secured information includes biometric information for authenticating a user.” 102
4. Claim 5: “The hybrid device of claim 1, wherein the local, secured information includes biometric information based on a biometric scan of a finger, the biometric information for authenticating a user.” 103
5. Claim 6: “The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information.” 103
6. Claim 7: “The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on a signal received from the at least one external device by the integrated RDC.” 104
7. Claim 10: “The hybrid device of claim 1, wherein the one or more of the application, the function and the service enabled based on the local, secured information stored by the integrated, secure memory includes a first application, function or service based on a first subsets of local, secured information stored by the integrated, secure memory and a second application, function or service based on a second subset of local, secured information, the first and second

	subset of local, secured information having different accessibility.”	105
8.	Claim 11: “The hybrid device of claim 1, wherein the hybrid device is a cell phone.”	106
9.	Claim 15: “The method of claim 14, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on the hybrid device.”	106
10.	Claim 16: “The method of claim 14 further comprising: sending the enablement signal, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on a device external to the hybrid device and communicatively coupled to an external RDC.” ..	107
11.	Claim 17: “The method of claim 14, wherein the local, secured information includes biometric information for authenticating a user.”	107
12.	Claim 18: “The method of claim 14, wherein the local, secured information includes financial information and wherein the one or more of the application, the function and the service completes a financial transaction.”	107
13.	Claim 19: “The method of claim 14, wherein the hybrid device is a cell phone.”	108
XI.	Ground 4: Buer in view of Giobbi ’157 further renders obvious claims 4, 8-10, 12, 13, 17, and 20.	108
A.	Claim 4: “The hybrid device of claim 1, wherein the local, secured information includes biometric information for authenticating a user.”	108
B.	Claim 8: “The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on an authorization of the financial information using an external	

	authentication database, the financial information transmitted to the external authentication database.”	110
C.	Claim 9: “The hybrid device of claim 8, wherein the external authentication database is separate from a merchant providing a sale in the financial transaction.”	112
D.	Claim 10: “The hybrid device of claim 1, wherein the one or more of the application, the function and the service enabled based on the local, secured information stored by the integrated, secure memory includes a first application, function or service based on a first subsets of local, secured information stored by the integrated, secure memory and a second application, function or service based on a second subset of local, secured information, the first and second subset of local, secured information having different accessibility.”	113
E.	Claim 12: “The hybrid device of claim 1, wherein the at least one external device is included in jewelry.”	115
F.	Claim 13: “The hybrid device of claim 1, wherein the at least one external device is a watch.”	116
G.	Claim 20: “The method of claim 14, wherein the external PDK is included in a watch.”	116
XII.	Ground 5: Claim 4 Would Have Been Obvious Over Buer And Nishikawa	117
A.	Claim 4: “The hybrid device of claim 1, wherein the local, secured information includes biometric information for authenticating a user.”	117
XIII.	Conclusion	119

TABLE OF EXHIBITS

Exhibit	Description
Ex-1001	U.S. Patent No. 9,679,289 to David L. Brown (“the ’289 patent”)
Ex-1002	Prosecution history of U.S. Patent No. 9,679,289
Ex-1003	Declaration of Andrew Wolfe, Ph.D., including his Curriculum Vitae
Ex-1004	U.S. Patent Application Publication No. 2006/0258289 to Dua (“Dua”)
Ex-1005	European Patent Application Publication No. EP 1536306 to Buer et al. (“Buer”)
Ex-1006	U.S. Patent Application Publication No. 2007/0245157 to Giobbi et al. (“Giobbi ’157”)
Ex-1007	U.S. Patent Application Publication No. 2004/0255139 to Giobbi (“Giobbi ’139”)
Ex-1008	PCT Application Publication No. WO 90/06633 to Lee et al. (“Lee”)
Ex-1009	Order, <i>Proxense, LLC v. Samsung Elecs. Co., Ltd.</i> , No. 6:21-cv-00210-ADA (W.D. Tex. Jan. 18, 2022)
Ex-1010	Memorandum in Support of Claim Construction Order, <i>Proxense, LLC v. Samsung Elecs. Co., Ltd.</i> , No. 6:21-cv-00210-ADA (W.D. Tex. Dec. 28, 2022)
Ex-1011	Scheduling Order, <i>Proxense, LLC v. Google LLC</i> , No. 6:23-cv-00320-ADA (W.D. Tex. March 18, 2024)
Ex-1012	U.S. Patent Application Publication No. 2005/0116050 to Jei et al. (“Jei”)
Ex-1013	PCT Application Publication No. WO 2005/104584 to Bella et al. (“Bella”)

Ex-1014	European Patent Application Publication No. EP 1600885 to Nishikawa et al. (“Nishikawa”)
Ex-1015	Google’s Proposed Constructions, <i>Proxense, LLC v. Google LLC</i> , No. 6:23-cv-00320-ADA (W.D. Tex October 17, 2023)
Ex-1016	Proxense’s Proposed Constructions, <i>Proxense, LLC v. Google LLC</i> , No. 6:23-cv-00320-ADA (W.D. Tex October 17, 2023)
Ex-1017	U.S. Patent Application Publication No. 2004/0176032 to Kotola et al. (“Kotola”)
Ex-1018	Preliminary Infringement Contentions Exhibit E, <i>Proxense, LLC v. Google LLC</i> , No. 6:23-cv-00320 (W.D. Tex)
Ex-1019	U.S. Patent Application Publication No. 2005/0151623 to Von Hoffmann (“Von Hoffmann”)
Ex-1020	Claim Construction Order, <i>Proxense, LLC v. Google LLC</i> , No. 6:23-cv-00320-ADA (W.D. Tex. January 23, 2024)
Ex-1021	Bluetooth Specification, Profiles of the Bluetooth System, Version 1.0 B (December 1999)
Ex-1022	Comparison of District Courts (December 31, 2023)

LIST OF APPENDICES

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

LIST OF CHALLENGED CLAIMS

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

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

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

	application, the function and the service completes a financial transaction.
Claim 19	
[19]	The method of claim 14, wherein the hybrid device is a cell phone.
Claim 20	
[20]	The method of claim 14, wherein the external PDK is included in a watch.

GROUND(S) FOR CHALLENGE (37 C.F.R. § 42.204(b)(2))

Ground	Claim(s) Challenged	35 U.S.C. §	Reference(s)
1	1-6, 8-11, and 14-19	103	Dua, Giobbi '157
2	1-6, 8-11, and 14-19	103	Dua, Giobbi '157, Kotola
3	1-7, 10-11, and 14-19	103	Buer
4	4, 8-10, 12, 13, 17, and 20	103	Buer, Giobbi '157
5	4	103	Buer, Nishikawa

I, Dr. Andrew Wolfe, declare as follows:

I. Introduction

1. My name is Andrew Wolfe, and I have been retained by Finnegan, Henderson, Farabow, Garrett & Dunner, LLP, counsel for Google LLC (“Google”), as an expert witness in the case Google LLC v. Proxense LLC, Case No. IPR2024-00783 with respect to U.S. Patent No. 9,679,289 (“the ’289 patent”), Ex-1001.¹

2. My opinions are based on my years of education, research, and experience, as well as my investigation and study of relevant materials. The materials that I have studied for this declaration include the documents identified in the table of exhibits.

3. I may rely upon these materials, my knowledge and experience, and/or additional materials to rebut arguments raised by the patent owner. Further, I may also consider additional documents and information in forming any necessary opinions, including documents that may not yet have been provided to me.

4. My analysis of the materials produced in this investigation is ongoing, and I will continue to review any new material as it is provided. This declaration represents only those opinions I have formed to date. I reserve the right to revise,

¹ All references to “Ex” in this declaration refer to the Google Exhibits concurrently filed with Google’s petition.

supplement, and/or amend my opinions stated herein based on new information and my continuing analysis of the materials already provided.

5. I understand that the Petition for *Inter Partes Review* involves the '289 patent, Ex-1001, '289 patent.

II. Education and Work Experience

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

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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 a lecturer at Santa Clara University teaching courses on Microprocessor Systems, Integrated Circuit Design, Real-Time Computing, and Mechatronics and currently serve as Faculty Senate President.

16. 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.

17. 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.

18. 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.

19. Additional details about my employment history, fields of expertise, and publications are further included in my curriculum vitae, attached herewith as Appendix A.

III. Compensation

20. I am being compensated at my usual and customary hourly rate of \$650 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

21. For purposes of this declaration, I have been informed about certain aspects of the law as it relates to my opinions.

22. I understand that for an invention claimed in a patent to be found patentable, it must be (among other things) new and not obvious based on what was known before the invention was made.

23. I understand that the information that is used to evaluate whether an invention was new and not obvious when made is generally referred to as “prior art.”

I understand that the prior art includes patents and printed publications that existed before the earliest filing date of the patent (which I have been informed is called the “effective filing date”). I also understand that a patent or published patent application is prior art if it was filed before the effective filing date of the claimed invention and that a printed publication is prior art if it was publicly available before the effective filing date.

24. I understand that in this *inter partes review* proceeding, the information that may be evaluated is limited to patents and printed publications. My analysis, which is set out in detail below, compares the claims to printed publications that I understand are prior art to the claims.

A. Anticipation Analysis: 35 U.S.C. § 102

25. I understand that a person cannot obtain a patent on an invention if the prior art included that invention. If an invention is not new, then the invention has been “anticipated” by the prior art. A claim is “anticipated” by the prior art if each and every limitation of the claim is disclosed, expressly or inherently, in a single item of prior art, from which a person of ordinary skill in the art could practice the invention. I have applied this standard in my evaluation of whether claims of the ’289 patent are anticipated in light of the prior art.

B. Obviousness Analysis: 35 U.S.C. § 103

26. It is my understanding that a claim is unpatentable if the claimed subject matter as a whole would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. I also understand that an obviousness analysis takes into account the scope and content of the prior art, the differences between the claimed subject matter and the prior art, and the level of ordinary skill in the art at the time of the invention.

27. I understand that a claimed invention is not patentable if it would have been “obvious” to a person of ordinary skill in the field of the invention at the time the invention was made. This means that even if all the requirements of a claim are not found in a single prior art reference, the claim is not patentable if the differences between the subject matter in the prior art and the subject matter in the claim would have been obvious to a person of ordinary skill in the art at the time the application was filed.

28. In determining the scope and content of the prior art, it is my understanding that a reference is considered relevant prior art to the '289 patent if it falls within the field of the inventor's endeavor. In addition, a reference is prior art if it is reasonably pertinent to the particular problem with which the inventor was involved. A reference is reasonably pertinent if it logically would have commended itself to an inventor's attention in considering his problem. Thus, if a reference

relates to the same problem as the claimed invention, that supports the use of the reference as prior art in an obviousness analysis.

29. In my opinion, the prior art references identified herein seek to solve the same types of problems as the '289 patent and logically would have commended themselves to an inventor's attention considering the problems of the '289 patent.

30. I understand that a determination as to whether a claim would have been obvious should be based on four factors (though not necessarily in the following order): (i) the level of ordinary skill in the art at the time the application was filed; (ii) the scope and content of the prior art; (iii) the differences between the claimed invention and the prior art; and (iv) any objective factors indicating obviousness or non-obviousness that may exist in a particular case.

31. It is my understanding that an obviousness analysis cannot be based on hindsight, but it must be done using the perspective of a person of ordinary skill in the relevant art as of the effective filing date of the patent claim.

32. I understand the objective factors indicating obviousness or nonobviousness may include: commercial success of products covered by the patent claims; a long-felt but unaddressed need for the invention; failed attempts by others to make the invention; copying of the invention by others in the field; expressions of surprise by experts and those skilled in the art at the making of the invention; and the patentee having proceeded contrary to the accepted wisdom of the prior art. I

also understand that any of this evidence must be specifically connected to the invention rather than associated with the prior art or with marketing or other efforts to promote an invention.

33. I understand that the teachings of two or more prior art references may be combined in the manner disclosed in the claim if such a combination would have been obvious to one having ordinary skill in the art at the effective filing date. In determining whether a combination would have been obvious, I understand that the following exemplary rationales may support a conclusion of obviousness:

- Combining prior art elements according to known methods to yield predictable results;
- Simple substitution of one known element for another to obtain predictable results;
- Use of a known technique to improve similar devices (methods, or products) in the same way;
- Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
- “Obvious to try”—choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;
- Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design

incentives or other market forces if the variations are predictable to a person of ordinary skill in the art; and

- Some teaching, suggestion, or motivation in the prior art that would have led a person of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

34. I understand that the obviousness analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, but instead can take account of the ordinary innovation and experimentation in the relevant field that does no more than yield predictable results.

35. I understand that, in assessing whether there was an apparent reason to modify or combine known elements as claimed, it may be necessary to look to interrelated teachings of multiple patents or prior art references, the effects of commercial demands, and the background knowledge of a person of ordinary skill in the art. I further understand that any motivation that would have applied to a person of ordinary skill in the art, including motivation from common sense or derived from the problem to be solved, is sufficient to explain why references would have been combined.

36. I understand that modifications and combinations suggested by common sense are important and should be considered. Common sense suggests that

familiar items can have obvious uses beyond the particular application being described in a prior art reference, that if something can be done once it would be obvious to do it multiple times, and that in many cases a person of ordinary skill in the art can fit the teachings of multiple patents together in an obvious manner to address a particular problem. The prior art does not need to be directed to solving the same problem that is addressed in the patent.

37. I understand that a person of ordinary skill in the art is also a person of ordinary creativity. In many fields, it may be that there is little discussion of obvious techniques, modifications, and combinations, and it may be the case that market demand will drive a new design, rather than scientific research or literature. When there is market pressure or design need to solve a particular problem, and there are a finite number of identified, predictable solutions, a person of ordinary skill has a good reason to employ the known options. If this leads to the expected success, then it is likely the product of ordinary skill and common sense as opposed to patentable innovation. I understand that if a combination was obvious to try, that may show that it was obvious and therefore unpatentable. That a particular combination of prior art elements was obvious to try suggests that the combination was obvious even if no one made the combination.

V. Level of Ordinary Skill

38. In my opinion a person of ordinary skill in the art (“POSITA”) at the time of the purported invention would have had a bachelor’s degree in computer or electrical engineering or an equivalent degree, and at least three years of experience in the field of encryption and security or equivalent experience. It is my further opinion that additional education could substitute for professional experience, and significant work experience could substitute for formal education.

VI. Field of Art and Related Art

39. The ’289 patent generally relates to the use of keys and readers, such as RFID tags and RFID readers:

The invention generally relates to personal digital keys and corresponding sensors, capable of proximity detection/location determination and auxiliary data services/application services....

Proximity sensors and location tracking are technologies with many applications. For example, proximity sensors can be used to provide secure access to physical and/or digital assets, based on biometrics, passwords, PINs, or other types of authentication. Proximity sensors typically have advantages of being less cumbersome, easier to use, and more flexible in form factor and implementation. Proximity sensors can be used to control access to resources and/or to authenticate individuals, for example.

One possible application that can take advantage of proximity sensors is location tracking. RFID tracking is one example. In RFID, RFID tags are attached to objects to be tracked. RFID readers then interact with the RFID tags to determine the location of the tag.

Ex-1001, '289 patent, 1:45-2:10.

40. In the '289 patent, the keys are each referred to as a “personal digital key (PDK)” and the readers are each referred to as a “receiver-decoder circuit (RDC).” Ex-1001, '289 patent, 1:45-52. These acronyms are not terms of art, but their meaning is clear in the context of the '289 specification and they have been previously construed.

VII. Cited Art Prior to the '289 Patent

41. Radio frequency identification (RFID) and near field communication (NFC) technologies were known well before the '289 patent's earliest priority date. *See, e.g.,* Ex-1017, Kotola, [0007] (“The rising use of RF-ID tags promotes standardization efforts to establish a broadly applicable communication framework between RF-ID tag readers and RF-ID tags. Such a standard is established by European Computer Manufacturers Association (ECMA) International, Geneva, Switzerland in a near field communication Standard (ECMA-340) dated December 2002.”); Ex-1004, Dua, [0015] (“[T]he present invention preferably includes integrated Radio Frequency Identification (RFID) technology,” and “allows

interoperability with all RF 13.56 MHz readers and tags compatible with existing international standards, including ISO 14443 A/B, ISO 15693, FeliCa™, and NFC.”).

42. These technologies enable two electronic devices to interact with each other when brought into close proximity. RFID tags, also known as RFID chips, are small electronic devices capable of storing information in its internal memory and of transmitting and receiving information via an antenna and microchip with other external devices, also known as RFID readers, using radio waves. These radio waves transmit data from the tag to the reader. The RFID tags could be passive or active RFID tags. *See, e.g.*, Ex-1004, Dua, [0053], [0092]; Ex-1017, Kotola, Abstract. Passive RFID tags are energized by a nearby RFID reader; active RFID tags, on the other hand, obtain energy from an internal battery or power source.

43. The '289 patent is directed to a “hybrid” device that includes both an internal key and reader. Hybrid devices having both key and reader were previously known years before the '289 patent was filed, however.

44. As an example, Dua discloses a cellular phone that includes both an RFID tag (PDK) and an RFID reader (RDC) in the form of an integrated RFID Tag-Reader Module to automatically set up and establish a wireless connection with an external device in the proximity of Dua’s cellular phone. Ex-1004, Dua, [0011]-[0016].

45. As another example, Buer also discloses a cellular phone that includes both an internal authentication component (PDK) and a proximity reader (RDC) to secure access to various services using external RFID tokens and readers that are in proximity with Buer's cellular phone. Ex-1005, Buer, [0010], [0014], [0130], [0163].

46. Numerous prior art patents also teach the same concept of using a digital key and reader to secure data or a service. *See, e.g.*, Ex-1006, Giobbi '157; Ex-1007, Giobbi '139; Ex-1008, Lee; Ex-1012, Jei; Ex-1013, Bella; Ex-1014, Nishikawa; Ex-1017, Kotola; Ex-1019, Von Hoffmann.

47. In my opinion, the challenged claims of the '289 patent merely recite the well-known concept of enabling applications, functions, or services with digital keys and readers that were well known in the art years before the '289 patent was filed.

48. In the following paragraphs, I provide an overview of the prior art in the following paragraphs.

A. Dua

49. U.S. Patent Application Publication No. 2006/0258289 ("Dua") is titled "Wireless Media System and Player and Method of Operation." Ex-1004, Dua, Cover.

50. Dua's Abstract states:

A wireless media player and a related system and methodology are disclosed. One aspect of the wireless media player system pertains to a virtual connector system, apparatus, and method for the automatic establishment of wireless connectivity with other electronic devices. In one embodiment, the media player device employs the use of integrated Radio Frequency Identification (RFID) technology to exchange communication settings, media capability, and other parameters with an external device that also has integrated RFID technology. The automatic exchange of settings and other information via a proximity-based RFID data exchange allows a media player to quickly establish a secure communication link with another device via a commonly supported wireless protocol such as Ultra Wideband (UWB) or Bluetooth. Another aspect of the media player system pertains to a method of using the captured media capability of the connecting device to customize certain menu options and software parameters in the media player.

Ex-1004, Dua, Abstract.

51. Dua teaches that the wireless media player contains “both an RFID tag and an RFID reader” (for example, an RFID Tag-Reader Module) that establishes wireless connections with other external devices to enable functions and to exchange data. Ex-1004, Dua, [0014]-[0015], [0070]. In Dua, the wireless media players may be “cellular phones.” Ex-1004, Dua, [0004], [0057].

52. Dua further teaches integrating into cellular phones, as shown in Figure 6 below, an “RFID Tag-Reader Module” to allow the device to “rapidly exchange information with an electronic device that is in close proximity.” Ex-1004, Dua, [0070].

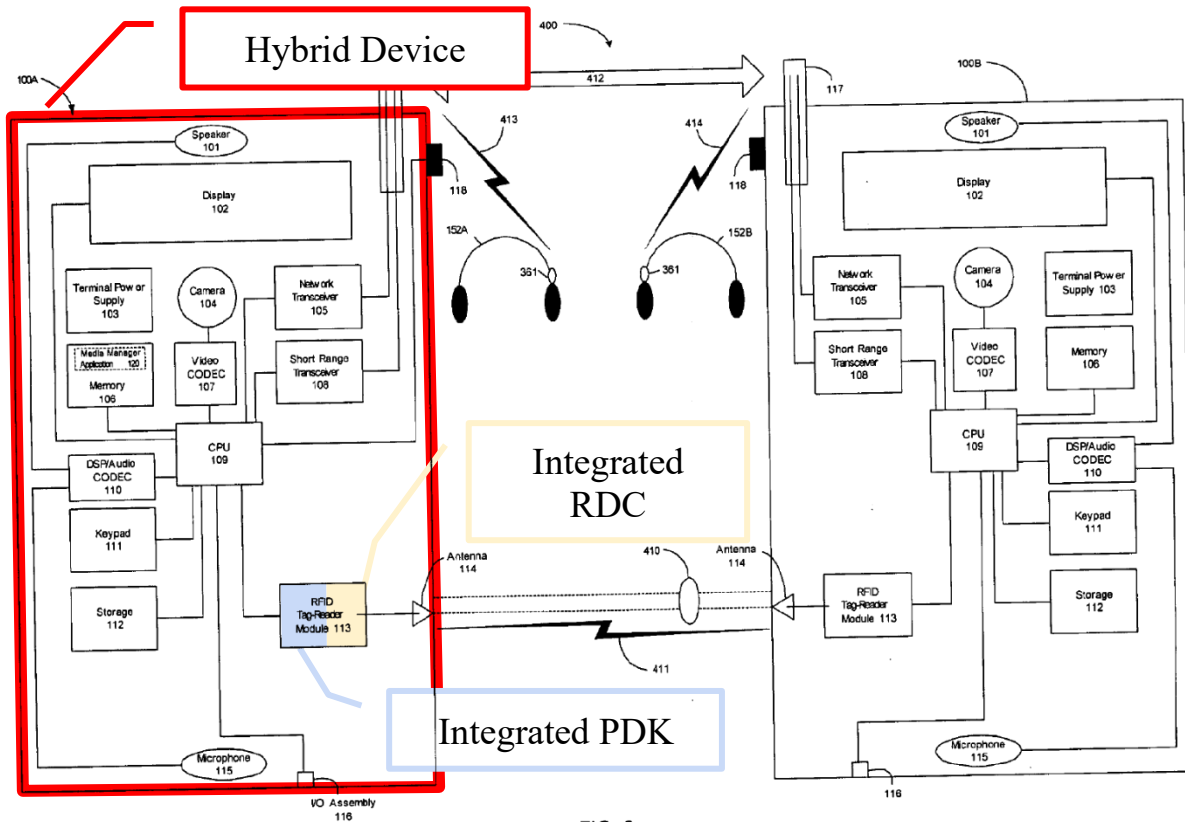


FIG. 6

Ex-1004, Dua, Fig. 6 (annotated).

53. As shown in Figure 4B below, the RFID Tag-Reader Module includes specific circuit components for “RFID tag functionality” and circuit components for “RFID reader functionality.” Ex-1004, Dua, [0106].

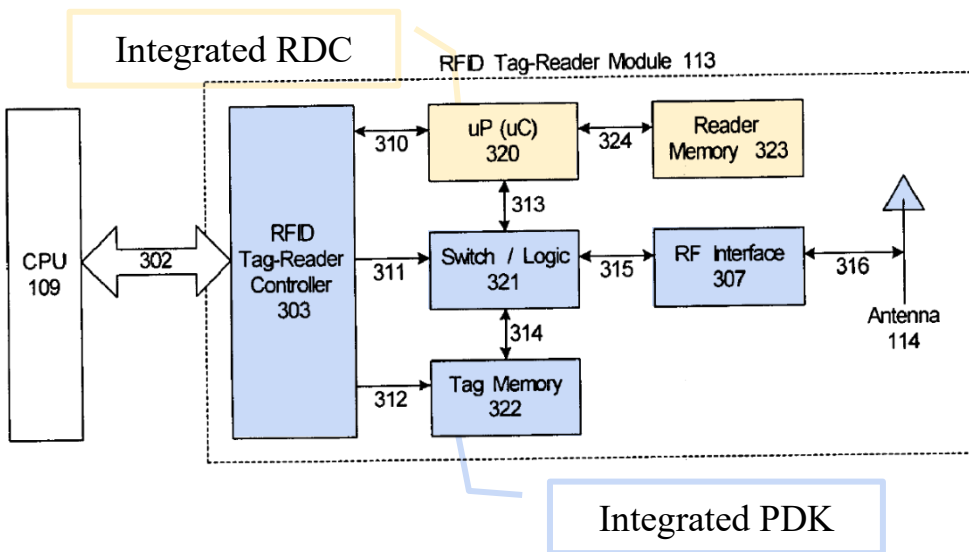


FIG. 4B

Ex-1004, Dua, Fig. 4B (annotated).

54. In Dua, the circuit components for “RFID tag functionality” (blue in Figure 4B) store both confidential information and encryption keys in a “tamper resistant” internal tag memory for gaining access to an external device. Ex-1004, Dua, [0108]-[0109]. According to Dua, this stored information may be encrypted. Ex-1004, Dua, [0109], [0152].

55. Dua discloses transmitting the stored information to an external reader, which reads the information transmitted by the tag to establish a secure connection. Ex-1004, Dua, [0092], [0100]-[0101], [0139].

56. In Dua, the circuit components for “RFID reader functionality” (yellow in Figure 4B) are capable of communicating with external RFID tags. Ex-1004, Dua, [0071].

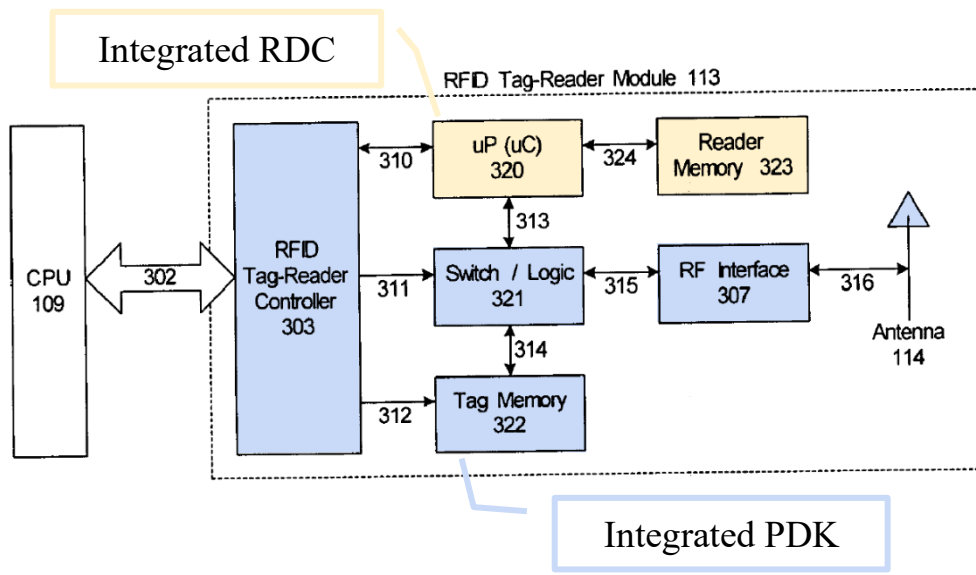


FIG. 4B

Ex-1004, Dua, Fig. 4B (annotated).

57. According to Dua, when operating with enhanced security, encryption keys are used to enhance security. Ex-1004, Dua, [0152].

58. In my opinion, a POSITA would have understood that in Dua, the RFID reader would receive encrypted data and decode the encrypted data using one of the stored encryption keys.

59. Lastly, Dua is not limited to enabling services such as “transmission of media assets to other devices in proximity via short-range RF,” but allows other additional functionalities such as “transacting at a point-of-sale location using a digital wallet application and the RFID capability.” Ex-1004, Dua, [0058], [0070], [0089].

B. Buer

60. European Patent Application Publication No. EP 1536306 (“Buer”) is titled “Proximity authentication system.” Ex-1005, Buer, Cover.

61. Buer’s Abstract states:

Access to secured services may be controlled based on the proximity of a wireless token to a computing device through which access to the secured services is obtained. An authorized user may be provided access to a service only when a wireless token assigned to the user is in the proximity of the computing device. A user’s credential may be stored on an RFID token and an RFID reader may be implemented within a security boundary on the computing device. Thus, the credential may be passed to the security boundary without passing through the computing device via software messages or applications. The security boundary may be provided, in part, by incorporating the RFID reader onto the same chip as a cryptographic processing component. Once the information is received by the RFID reader it may be encrypted within the chip. As a result, the information may never be presented in the clear outside of the chip. The cryptographic processing component may cryptographically encrypt/sign the credential received from the token so that assurance may be provided to a service provider that the credentials came from a token that was proximate to the computing device. An RFID reader, cryptographic processing

components and a wireless network controller may be implemented on a single chip in a mobile device.

Ex-1005, Buer, Abstract.

62. According to Buer, the computing device (or access device) may be implemented also as a mobile device, such as a cellular phone. Ex-1005, Buer, [0163], [0195].

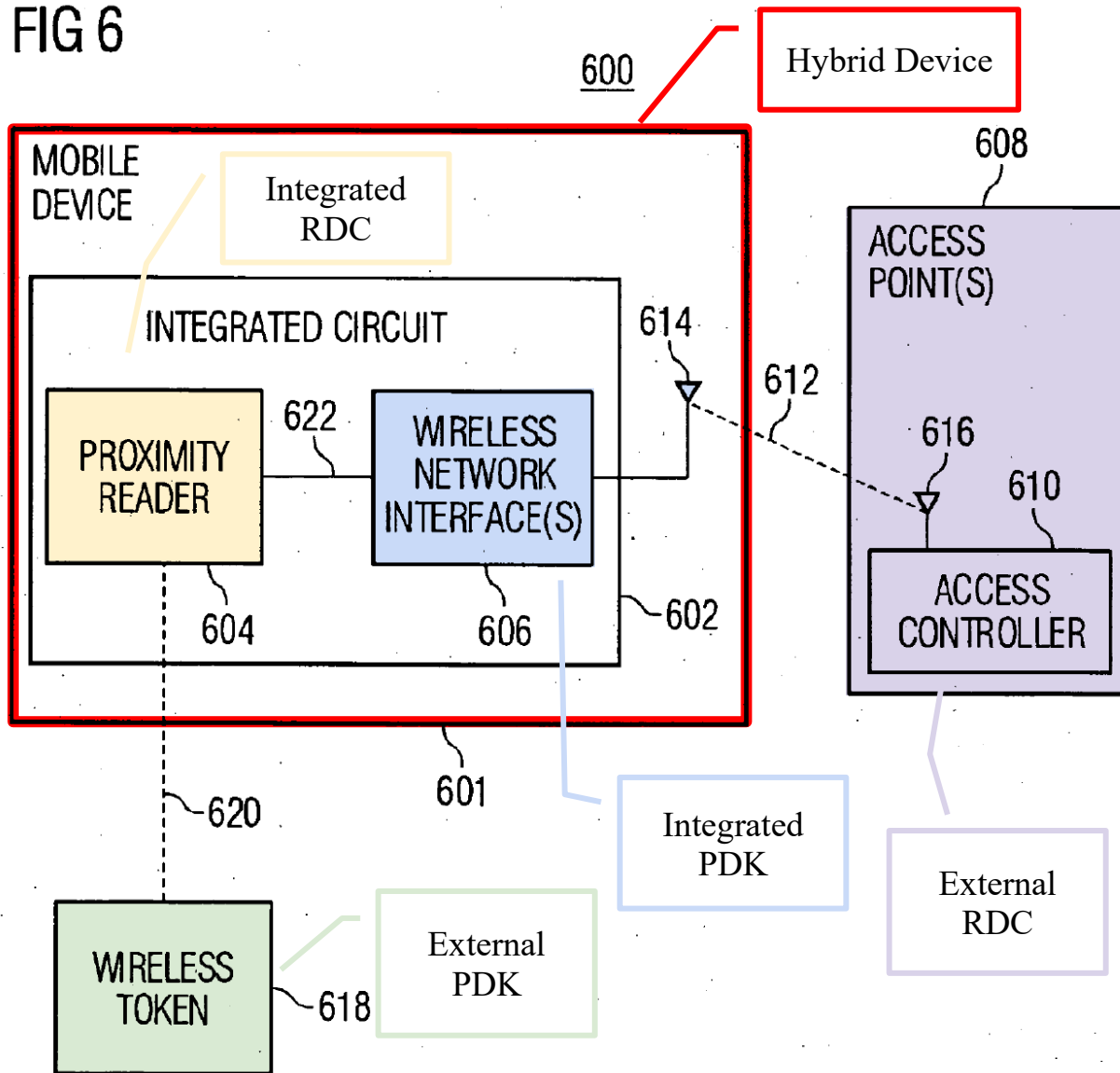
63. As Buer explains, when Buer's access device is implemented as a mobile device, the access device, in my opinion, could be used to enable various applications, functions, or services, including the following two embodiments:

- (1) “embodiments of a wireless proximity and authentication system that controls access to one or more data networks” as disclosed in Figures 5-7 and
- (2) “embodiments of security processing systems (i.e., key management systems) that include wireless proximity and authentication” as disclosed in Figures 8-11.

Ex-1005, Buer, [0155], [0176].

64. In the first embodiment, the mobile device (**red** in Figure 6 as shown below) may be enabled “to access one or more wireless networks (e.g., a cellular network, an 802.11 network, a Bluetooth network, etc.).” Ex-1005, Buer, [0163].

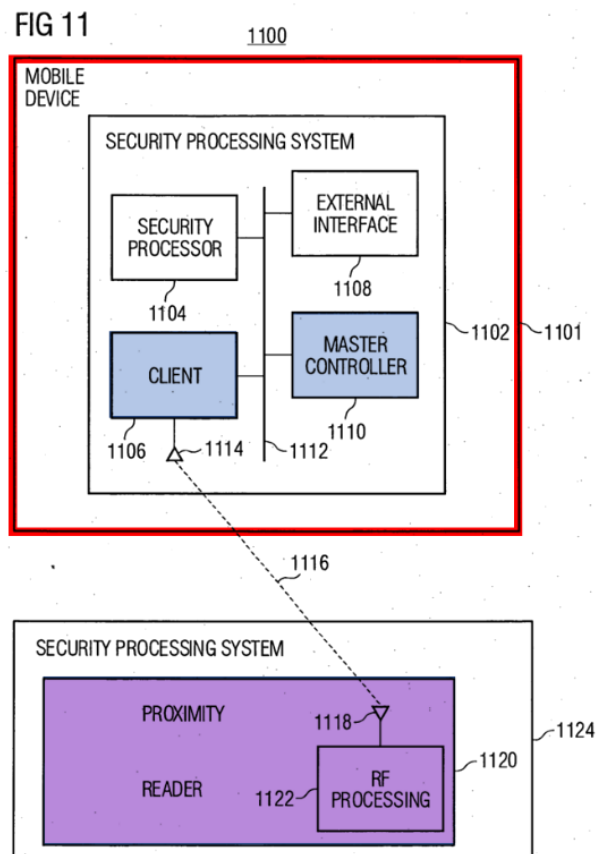
FIG 6



Ex-1005, Buer, Fig. 6 (annotated).

65. In Figure 6, the mobile device 601 (**red** in Figure 6) receives authentication information from the wireless token 618 via RF signals 620 and next communicates with the access points 608 wirelessly via RF signals 612. Ex-1005, Buer, [0164]-[0165].

66. In the second embodiment, the mobile device 1101 (red in Figure 11 as shown below) is “used to authenticate a user to another processing system,” such as an external proximity reader 1120, such as a computer that includes “point-of-sale components” (not shown) to “perform a sales transaction” (for example, “credit card transactions”).



Ex-1005, Buer, Fig. 11 (annotated), [0193]-[0196].

C. Giobbi '157

67. U.S. Patent Application Publication No. 2007/0245157 (“Giobbi '157”) is titled, “Two-Level Authentication for Secure Transactions.” Ex-1006, Giobbi '157, Cover.

68. Giobbi '157's Abstract states:

A system and method provide efficient, secure, and highly reliable authentication for transaction processing and/or access control applications. A Personal Digital Key stores one or more profiles (e.g., a biometric profile) in a tamperproof memory that is acquired in a secure trusted process. Biometric profiles comprise a representation of physical or behavioral characteristics that are uniquely associated with an individual that owns and carries the PDK. The PDK wirelessly transmits the biometric profile over a secure wireless transaction to a Reader for use in a biometric authentication process. The Reader compares the received biometric profile to a biometric input acquired at the point of transaction in order to determine if the transaction should be authorized.

Ex-1006, Giobbi '157, Abstract.

69. 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.” Ex-1006, Giobbi '157, Abstract.

70. Giobbi '157 further teaches that the PDK may be integrated into a hybrid device, “such as a cell phone,” as shown in Figure 3 below. Ex-1006, Giobbi '157, [0035], [0011].

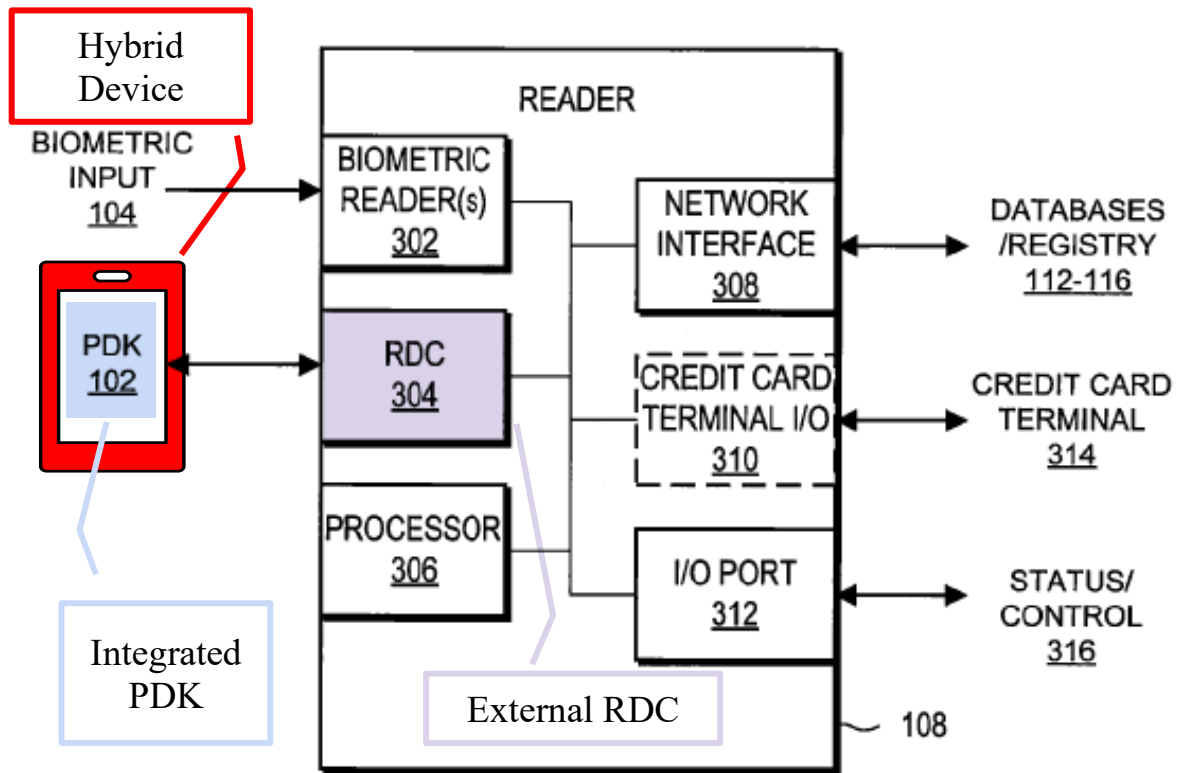


FIG. 3

Ex-1006, Giobbi '157, Fig. 3 (annotated).

71. In Giobbi '157, the integrated PDK wirelessly communicates with an external receiver-decoder circuit (RDC), such that information stored on the integrated PDK is transmitted to the external RDC located on a “Reader 108.” Ex-1006, Giobbi '157, [0012].

72. Further, the external RDC is communicatively coupled to an external database that is used for enabling an application, function, or 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-1006, Giobbi '157, [0053].

73. Giobbi '157 teaches that its hybrid device, which contains the PDK, enables an application, function, or service to take place by, for example, enabling a financial transaction, such as an ATM withdrawal:

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-1006, Giobbi '157, [0011], [0065].

D. Lee

74. PCT Application Publication No. WO 90/06633 (“Lee”) is titled, “Micro Powered RF Data Modules.” Ex-1008, Lee, Cover.

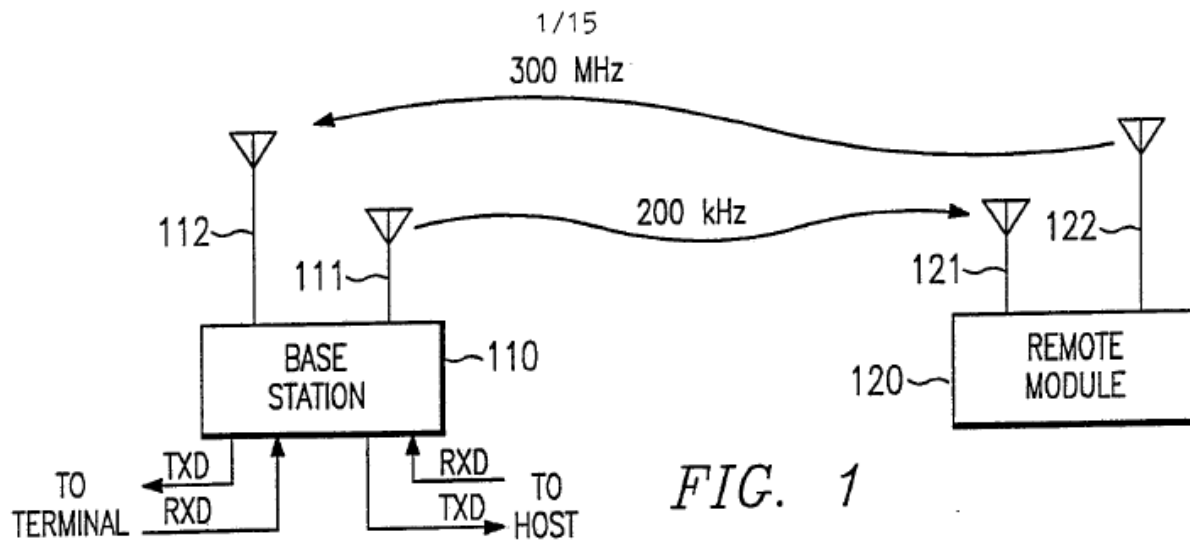
75. Lee’s Abstract states:

A low-power wireless data communication system, in which base stations (110) can automatically interface to batter[y]-powered portable data modules (210) as they are brought within

range. In the data modules (210), each receive antenna (121) is directly connected to a gain-controlled comparator (420A, 420B). Bandpass filtering (448) is accomplished economically by use of simple digital circuits. The two-level digital output from the comparator (420A, 420B) is fed (through an intersymbol detector, a counter, and a ripple-through magnitude comparator) to a state machine (552), which decodes the resulting digital waveform to a conventional serial-bus format. The internal data bus (701D) provides an interface to memory chips (262) and (optionally) to other chips, such as an electronic key. The decoder chip (220) also provides a secondary power supply to the other chips (230), and modulates the power supply (250) to assist detection of transitions on the reset-bar line of the serial bus (206). The modules (230) use widely different frequencies for read and write operations. (Transmissions by the base station (110) use a pulse-width modulation scheme where the most commonly used signals correspond to the shortest pulse. A "read" command is encoded as the same pulse width as one of the two write commands). In addition, a pair of touch contacts (270) can be used to override the RF link. Error-checking (Fig. 7E) is performed on incoming commands before memory access (260) is permitted. "Freshness seal 11 logic (510) prevents any battery drain until the module is initially turned on (by placing it in a strong field).

Ex-1008, Lee, Abstract.

76. As shown in Figure 1, a RF communication is established between a base station and one or more portable data modules.



Ex-1008, Lee, Fig. 1.

77. According to Lee, its portable data module is extremely compact and powered by a small battery. Ex-1008, Lee, 26:26-31. As Lee explains, its portable module can “store extensive identification parameters for the person to whom it is assigned.” The identification parameters include biometric information (for example, “fingerprints, faces, or retinas”), for access control of applications. Ex-1008, Lee, 31:30-32:2.

78. In Lee, the portable module further includes an access control chip that “act[s], in effect, as an electronic key.” Ex-1008, Lee, 78:16-24.

Lee further teaches that “multiple access control chips 230” can reside on “a common bus.” Ex-1008, Lee, 80:20-26.

E. Nishikawa

79. European Patent Application Publication No. EP 1600885 (“Nishikawa”) is titled “SIM Reader/Writer and Mobile Phone.” Ex-1014, Nishikawa, Cover.

80. Nishikawa’s Abstract states:

A SIM reader/writer 1 can be removably loaded with a SIM 2. The SIM reader/writer 1 has a case 1a, a controlling IC chip 3 placed in the case 1a, a USB/ISO7816 conversion IC chip 10, and an coil antenna 11a for noncontact communication placed in the case 1a. The case 1a is provided with a liquid crystal display 4, a fingerprint sensor 5 and a short-distance communication means 11b.

Ex-1014, Nishikawa, Abstract.

81. Nishikawa “relates to a SIM reader/writer provided with a detachable SIM having contact and noncontact interfaces and capable of displaying data held by the SIM on a display, and to a cellular phone.” Ex-1014, Nishikawa, [0001], [0017].

82. Nishikawa discloses an improved “e-token” (for example, “key holder type ID module”) that acts as “a SIM reader/writer ... having contact and noncontact interfaces.” Ex-1014, Nishikawa, [0001], [0006], [0017].

83. Specifically, Nishikawa teaches “ways to improve the convenience of the key holder type ID module by combining the IC chip of the SIM with contact and noncontact interfaces to provide the key holder type ID module with noncontact communication function, and by combining a coil antenna and a display with a reader/writer to be used in combination with the SIM to provide the reader/writer with a short-distance communication function and a fingerprint sensing function.” Ex-1014, Nishikawa, [0017].

84. In Nishikawa, the SIM card is “loaded with multiple applications, such as electronic money, an electronic ticket, a fingerprint template, a fingerprint collating engine and a personnel ID card.” Ex-1014, Nishikawa [0111].

85. Nishikawa further provides the keyholder type ID module with a “noncontact communication function and the short-distance communication means” for use “as an electronic ticket and as electronic money for various noncontact transactions” and with a “fingerprint sensor” for authentication “on the basis of biometric data.” Ex-1014, Nishikawa, [0113]-[0114].

VIII. Overview of the '289 Patent

A. Overview

86. As I explained previously, the '289 patent generally relates to keys and readers, such as RFID tags and RFID readers that interact with the RFID tags. Ex-1001, '289 patent, 1:45-2:10.

87. The '289 patent is directed to a “hybrid device” (**red**) that includes both an integrated personal digital key (PDK) (**blue**) and an integrated receiver-decoder circuit (RDC) (**yellow**) that communicate with each other via a signal line. Ex-1001, '289 patent, 2:25-29.

88. Like the prior art, the hybrid device in the '289 patent may be part of a cell phone.

89. As shown in Figure 12 below, the cell phone 1202 includes both an integrated PDK 102a and integrated RDC 304a that is coupled to one another via a signal line 1104.

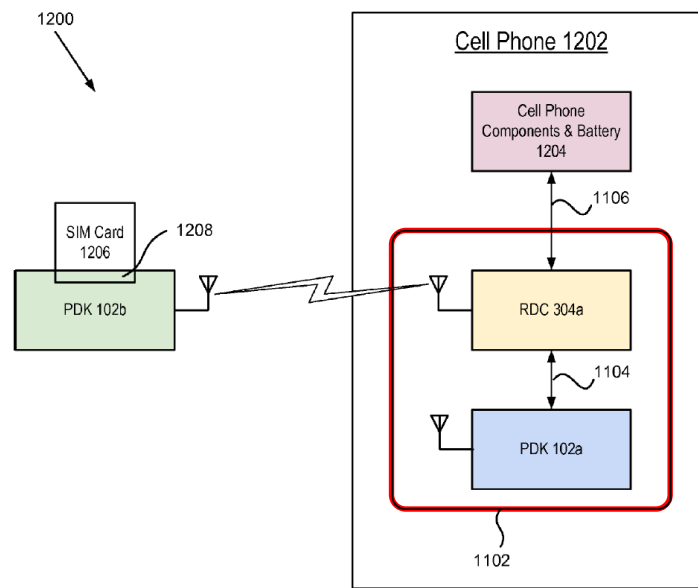


FIG. 12

Ex-1001, '289 patent, Fig. 12 (annotated).

90. According to the '289 patent, additional cell phone components and battery 1204 (**pink**) may be coupled to the integrated RDC 304a by a signal line

1106. Ex-1001, '289 patent, 14:45-64. The integrated RDC 304a may further communicate wirelessly with an external PDK 102b. Ex-1001, '289 patent, 14:59-61.

91. Additionally, the hybrid device, as shown in Figure 13 below, may interconnect with other external devices, such as an external RDC 304b (purple in Figure 13), so that the integrated PDK 102a (blue in Figure 13) communicates wirelessly with the external RDC 304b (purple), and the integrated RDC 304a (yellow in Figure 13) communicates wirelessly with at least one external PDK 102b (green in Figure 13) within its proximity zone.

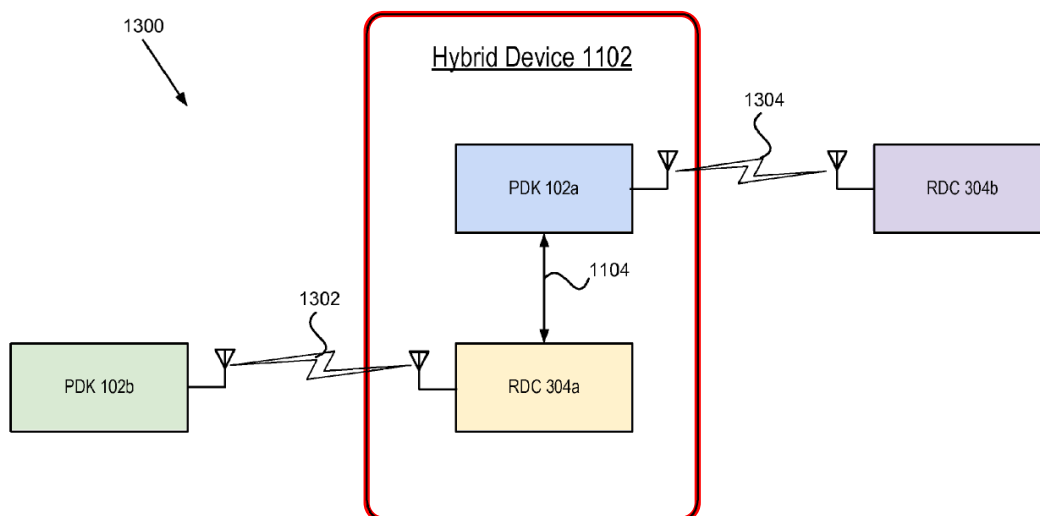


FIG. 13

Ex-1001, '289 patent, Fig. 13 (annotated), 16:47-63, 22:36-49.

92. The purpose of the integrated PDK and RDC in the '289 patent is to enable various applications, functions, or services, either on an external device or on the hybrid device using information stored on the integrated or external PDKs. According to the '289 patent, the information could be (1) financial information (for example, bank information, credit/debit card information, and account information, etc.); (2) biometric information (for example, fingerprint, palm print, retinal scan, etc.); or (3) personal identification information (for example, name, address, phone number, etc.). Ex-1001, '289 patent, 4:37-47, 7:7-18, 16:64-17:4.

93. As one example, the hybrid device may be used to access or enable a Wi-Fi service. According to the '289 patent, an external PDK 102b “provides ... information to the [integrated] RDC 304a of the hybrid device,” and the hybrid device “then communicates with the [external] RDC 304b to access the Wi-Fi service.” Ex-1001, '289 patent, 20:5-28. In this example, the hybrid device and the external PDK may belong to different users, and the hybrid device may thus use another user's information stored on the external PDK. Ex-1001, '289 patent, 20:5-28.

94. The '289 patent also provides another example where the hybrid device may use the credit card information stored on the integrated PDK to provide authorization to the external RDC to make a purchase using the cell phone, and in

this way, “to enable a service associated with the ... [external] RDC.” Ex-1001, ’289 patent, 16:64-17:4.

95. In this example, the purchase authorization, however, may depend on the presence of an external PDK being in proximity to the hybrid device. Ex-1001, ’289 patent, 17:4-11, 17:18-43. The external PDK first “authorizes the hybrid device,” which “in turn authorizes” the external RDC, such that a user can only make a purchase when the external PDK is in proximity to the hybrid device. Ex-1001, ’289 patent, 17:4-11, 17:18-21. In other words, the external PDK may be “used to enable specific features in the hybrid device.” Ex-1001, ’289 patent, 17:11-12.

B. Claim Construction

96. I understand that the district court in the Western District of Texas construed the following terms in a prior litigation ((*Proxense, LLC v. Samsung Elecs. Co., Ltd.*, No. 6:21-cv-00210-ADA (W.D. Tex.)):

- “hybrid device” means “A device comprising an integrated personal digital key (PDK) and an integrated receiver-decoder circuit.”
- “personal digital key” means “An operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for storing information particular to a user.”
- “biometric information” has “plain and ordinary meaning.”

- “financial information” has “plain and ordinary meaning.”
- “receiver-decoder circuit” means “A component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing.”
- “inheritance information” means “Information passed from a first device to a second device for use by the second device.”
- “enablement signal” requires no construction.

Ex-1009, Claim Construction Order, 3-4; see generally, Ex-1010, Memorandum. I understand that in the pending district court litigation, captioned *Proxense, LLC v. Google LLC*, No. 6:23-cv-00320 (W.D. Tex.), the court has adopted its prior constructions for “personal digital key” and “receiver-decoder circuit.” Ex-1020.

97. Counsel for Google has informed me that, in the pending district court litigation (*Proxense, LLC v. Google LLC*, No. 6:23-cv-00320 (W.D. Tex.)), Proxense has contended that no other terms “beyond what the Court had previously construed in the Samsung case” need to be construed, Ex-1016, 1. Thus, it is my understanding that Proxense has not contended they need any other constructions in district court.

98. Counsel for Google has further informed me that, in the pending district court litigation, Google has proposed to construe “personal digital key” to mean “a

collection of circuit components that includes an antenna, a transceiver, and a controller and memory for storing information particular to a user.” Ex-1015, 1.

99. It is also my understanding that Google has proposed to construe “receiver-decoder circuit” to mean “a collection of circuit components capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing.” Ex-1015, 1.

100. I understand that Google, as the petitioner to this *inter partes* review, submits that express interpretations of the challenged claims are not required to resolve this petition. Because no constructions are necessary to resolve this petition, I currently see no reason to disagree with this position; however, I reserve the right to modify my opinions in light of any claim constructions established by the Board or any Court in the future.

IX. Grounds 1 and 2: Claims 1-6, 8-11, And 14-19 Would Have Been Obvious Over Dua In View Of Giobbi ’157 or Dua In View of Giobbi ’157 and Kotola

A. Independent Claims

101. Dua alone or in view of Giobbi ’157 renders obvious each of independent claims 1 and 14.

1. Independent Claim 14

102. Independent claim 14 is the broadest independent claim of the ’289 patent.

103. I understand independent claim 14 is asserted in the pending district court litigation.

104. It is my opinion that Dua alone, or in view of Giobbi '157 renders obvious asserted independent claim 14.

a. [14pre] “A method comprising:”

105. I understand that the preamble for claim 14 is not limiting, but to the extent the preamble for claim 14 is limiting, it is my opinion that Dua discloses the preamble because Dua discloses a method to automatically set up and establish a wireless connection between two devices based on the proximity of the devices. Ex-1004, Dua, [0013].

b. [14a] “creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external device,”

106. In my opinion, Dua discloses limitation [14a] (“creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external device”).

107. In my opinion, Dua discloses the hybrid device in limitation [14a] because it discloses a media player (for example, cellular phone), as shown in Figure 6 below, that includes an RFID Tag-Reader Module that is integrated into the device. Ex-1004, Dua, [0057], [0070].

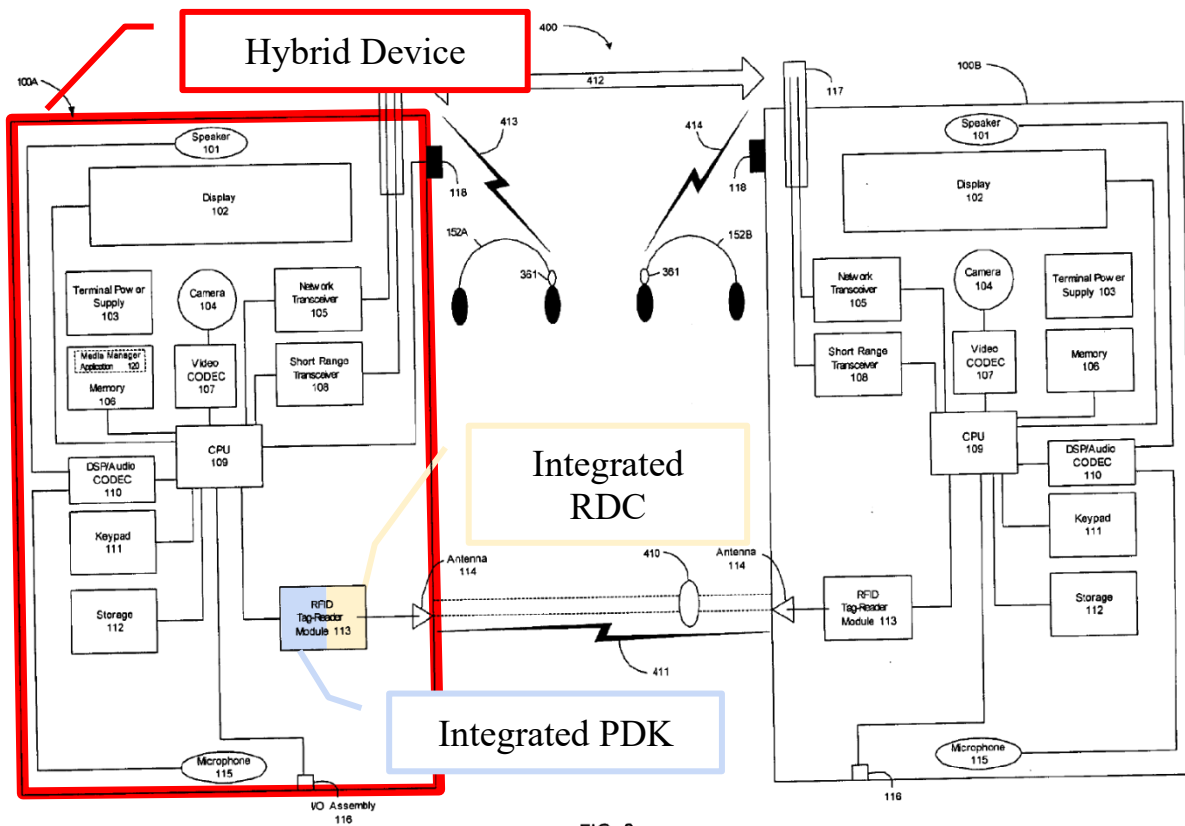


FIG. 6

Ex-1004, Dua, Fig. 6 (annotated).

108. Dua's media player ("hybrid device," **red** in Figure 6) includes an RFID Tag-Reader Module 113 (which in my opinion is an "integrated PDK," **blue**; "integrated RDC," **yellow**) that enables the device to "rapidly exchange information with an electronic device that is in close proximity and which also has integrated RFID technology." Ex-1004, Dua, [0057], [0070], Figs. 1, 6.

109. Further, Dua's RFID Tag-Reader Module, as shown in Figure 4B below, includes "both an RFID tag [(the claimed "integrated PDK," **blue**)] and an RFID reader [(the claimed "integrated RDC," **yellow**)]." Ex-1004, Dua, [0089].

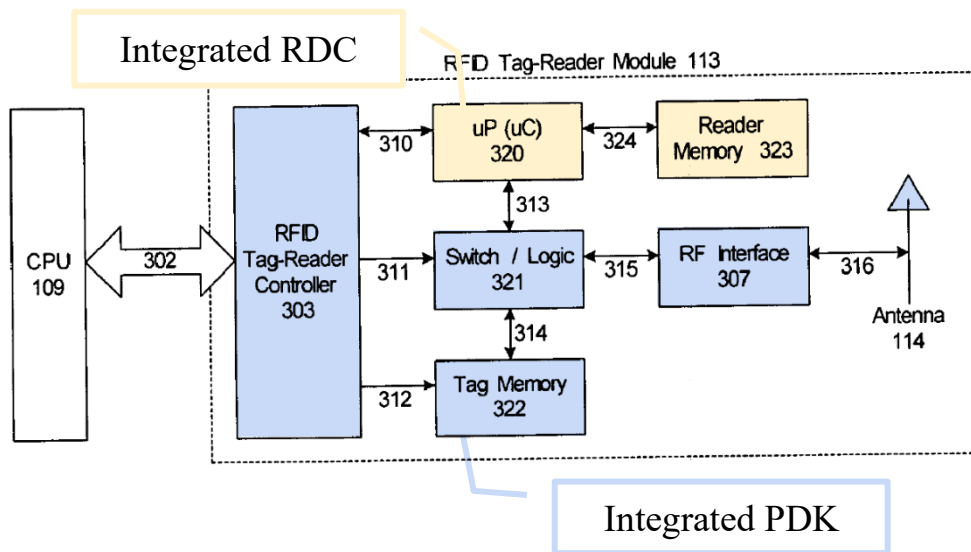


FIG. 4B

Ex-1004, Dua, Fig. 4B (annotated).

110. In my opinion, Dua's Tag-Reader Module (**blue**) includes a collection of circuit components that makes up a "personal digital key" under either the district court's construction or Google's proposed construction:

- District Court's Construction: "personal digital key" means "an operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for storing information particular to a user."
- Google's Proposed Construction: "personal digital key" to mean "a collection of circuit components that includes an antenna, a transceiver, and a controller and memory for storing information particular to a user."

111. For example, Dua's operably connected collection of components includes an antenna 114 and an RF Interface 307 (a transceiver) capable of modulating and demodulating RF signals for communications with an external tag reader (an RDC). Ex-1004, Dua, [0101], [0104], [0106]. Dua's RFID Tag-Reader Module (**blue**) further includes "an integrated RFID Tag-Reader Controller 303 that manages all communication between CPU 109 and the functional components of RFID Tag-Reader Module 113," and "tag logic" 321. Ex-1004, Dua, [0106], [0108].

112. "Correspondingly, the tag memory 322 is connected to the switch/logic component 321" and "to the RFID Tag-Reader Controller 303 in order to receive configuration data." Ex-1004, Dua, [0108]. The Tag Memory 322 for storing tag data may be a "configurable tag memory," such as a "non-volatile configurable memory," and may be "tamper resistant as to prevent hackers from retrieving confidential information and encryption keys" stored therein. Ex-1004, Dua, [0105], [0109].

113. In Dua, the stored information may include a "user identifier" or "other attributes (e.g., a complete calling card containing the contact information for the device owner such as f[u]ll name, title, company, mailing address, E.164 number, e-mail address, etc.)." Ex-1004, Dua, [0133], Fig. 7. The RFID tag component may also store information to enable services with an external device, including "electronic payments at the point-of-sale and secure key access to buildings, cars,

etc.” Ex-1004, Dua, [0070], [0089]. It is my opinion that the tag-Reader Controller 303 and Tag Memory 322 thus store information particular to a user.

114. In my opinion, Dua’s Tag-Reader Module (**yellow**), as shown, includes a collection of circuit components that makes up a “receiver-decoder circuit” under either the district court’s construction or Google’s proposed construction:

- District Court’s Construction: “receiver-decoder circuit” means “a component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing.”
- Google’s Proposed Construction: “receiver-decoder circuit” to mean “a collection of circuit components capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing.”

115. For example, Dua’s operably connected components include a reader logic 320 that is implemented as a microcontroller (μ C) and a microprocessor (μ P). Ex-1004, Dua, [0106]. “The reader logic operates the interface and protocol framework for communicating with RFID tags (passive communication mode) and in particular, when supporting active communication mode, for communicating with RFID tag reader devices.” Ex-1004, Dua, [0106].

116. The RFID “reader component” is used for “transmitting interrogation signals via its antenna to an external electronic device’s RFID tag when in close

proximity, and receiving a response signal from the external device's RFID tag." Ex-1004, Dua, [0071], [0100]. In Dua, the response signal includes "RFID transmission data." Ex-1004, Dua, [0130]-[0143]. A reader memory 323 may also be used as a buffer storage for communication with media player 100, as well as with an RFID tag or another RFID tag reader device. Ex-1004, Dua, [0107].

117. In Dua, when "enhanced security is desired" for RFID transmission, encryption keys are used and shared between the external device and the hybrid device to facilitate the sharing of "sensitive" information between the devices. Ex-1004, Dua, [0152].

118. In my opinion, a POSITA reading Dua would have understood that the encryption keys provide "enhanced security" by enabling the devices to store encrypted, "sensitive" information. Ex-1004, Dua, [0152]. For example, it would have been obvious to store encrypted "confidential information" in the external device's tag memory and transfer encrypted information to enhance security during the data transfer to the hybrid device. Ex-1004, Dua, [0109].

119. In my opinion, a POSITA would have been motivated to use an encryption key to improve RFID security so that "hackers" could not access the encrypted, confidential information during any data transfer from the external device to the hybrid device, as Dua suggests. Ex-1004, Dua, [0109], [0152]; *see also* Ex-1006, Giobbi '157, [0047] ("[T]he data can be encrypted by the transceiver ...

and transmitted over a secure link.”), [0050] (“Encrypting data transmitted between the PDK 102 and Reader 108 minimizes the possibility of eavesdropping or other fraudulent activity.”)

120. In my opinion, a POSITA would further have had a reasonable expectation of success in encrypting the RFID transmissions because Dua explains that the encryption key is stored in the external tag memory (external PDK), and the external tag could transfer the encryption key to an RFID reader (integrated RDC) for decrypting the encrypted data. Ex-1004, Dua, [0108]-[0109], [0152]. In my opinion, the RFID reader (integrated RDC) thus would receive any confidential data in an encrypted format and decode the encrypted data using the encryption key.

121. Further, to the extent that Proxense contends the claimed RDC requires separate wireless communication components (for example, RF interface and antenna) different from the claimed PDK, in my opinion, it would have been obvious to include a separate RF interface and antenna, instead of common RF interface and antenna. Ex-1017, [0058] (the mobile terminal including a separate terminal RFID reader module 220 that communicates wirelessly using a separate antenna 219 in addition to the RFID tag 215); [0056]-[0057] (RFID tag 215 is connected to antenna 220), Fig. 4.

122. In my opinion, a POSITA would have been motivated to use multiple antennas because doing so provides antenna diversity for mitigating fading and

improving signal reception and enables simultaneous transmission and reception of signals. Adding an additional RF interface and antenna to Dua's RFID Tag-Reader Module would have been no more than duplicating prior art elements according to known methods to yield predictable results because Dua's device already uses multiple antennas and transceivers for sending and receiving different signals. Ex-1004, [0062], [0084]. Moreover, Dua itself fully incorporated by reference details concerning such "other RFID Tag-Reader Module designs." Ex-1004, [0114] (citing Ex-1017); Ex-1017, Fig. 4, [0056]-[0058]. Thus, in my opinion, a POSITA would further have had a reasonable expectation of success in duplicating the RF interface and antenna to include separate wireless communication components for the RFID tag and RFID reader.

123. It would have been obvious to use separate antennas, as Kotola teaches, because Dua's citation to Kotola "provide[s] a justification for combining the references for obviousness purposes." *Commonwealth Sci. & Indus. Rsch. Org. v. Buffalo Tech. (USA), Inc.*, 542 F.3d 1363, 1372 (Fed. Cir. 2008).

124. Moreover, it is my opinion that a POSITA would have been motivated to use multiple antennas because doing so provides antenna diversity for mitigating fading and improving signal reception and enables simultaneous transmission and reception of signals.

125. A POSITA, in my opinion, would further have had a reasonable expectation of success in using additional wireless communication components for RFID reader.

126. Accordingly, in my opinion, Dua discloses a hybrid device, as claimed.

127. Dua discloses creating a first wireless link during an RFID discovery process as in limitation [14a] because the RFID reader component generates and transmits interrogation signals to create an RFID link between the integrated RFID reader (integrated RDC) in the hybrid device and an external RFID tag in an external device, as shown in Figure 6 below. Ex-1004, Dua, [0122].

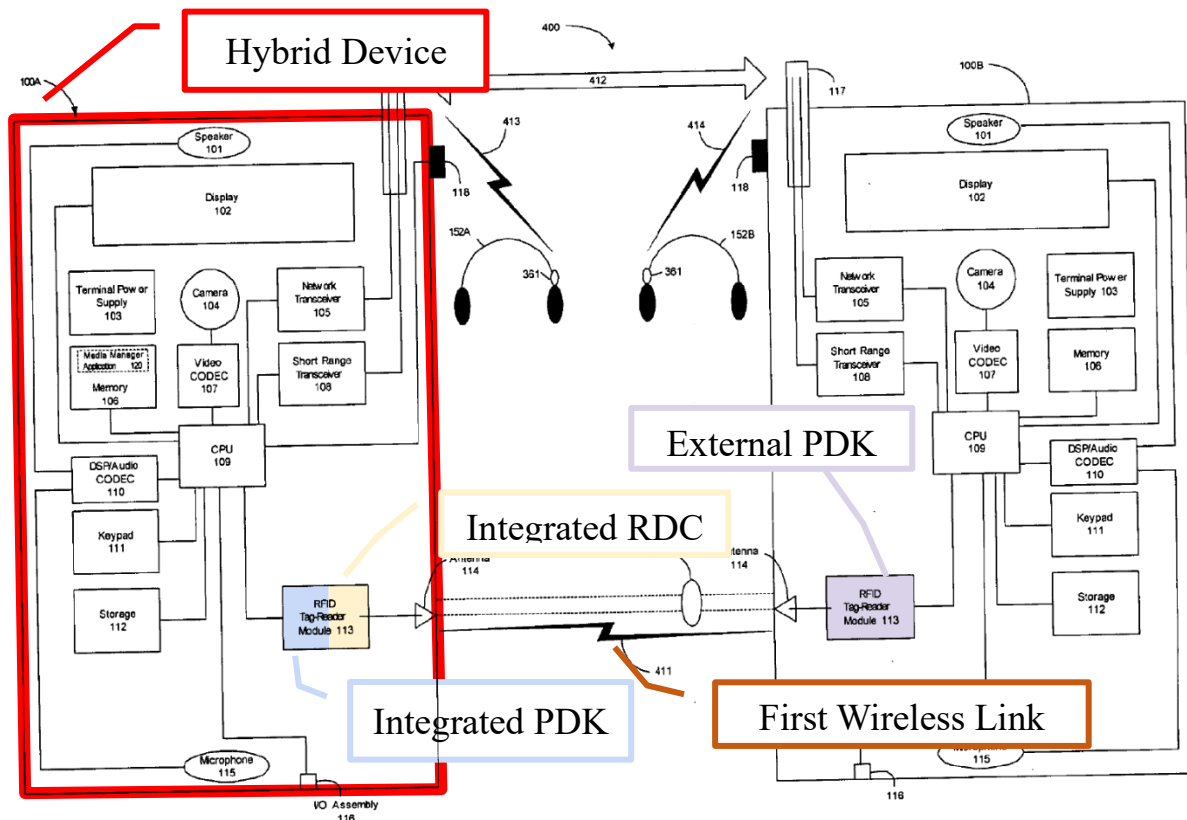


FIG. 6

Ex-1004, Dua, Fig. 6 (annotated).

128. Because in the hybrid device and in the external device, both components are labeled as “RFID Tag-Reader Module 113,” they both include the circuit components required for the claimed “PDK” and “RDC,” as addressed above.

129. The “reader component” of the “RFID Tag-Reader Module 113” in device 100A (integrated RDC) then communicates with the “tag component” of the “RFID Tag-Reader Module 113” in device 100B (external PDK). Ex-1004, Dua, [0071]-[0072], [0127]-[0128]. The “tag components” of the “RFID Tag-Reader Module 113” in device 100A (integrated PDK) also communicates with the “reader component” of the “RFID Tag-Reader Module 113” in device 100B (external RDC).

130. Further, as Dua explains, the “reader component” is used for transmitting interrogation signals to an external electronic device’s RFID tag when in close proximity. Ex-1004, Dua, [0071]-[0072], [0127].

c. [14b] “the hybrid device including an integrated, secure memory and the integrated RDC, wherein the integrated, secure memory stores local, secured information;”

131. In my opinion, Dua discloses limitation [14b] (“the hybrid device including an integrated, secure memory and the integrated RDC, wherein the integrated, secure memory stores local, secured information”).

132. As I discussed in Section IX.A.1.b, Dua’s hybrid device includes an integrated PDK and an integrated RDC.

133. In my opinion, Dua's integrated PDK includes an integrated, secure memory. As Dua explains, Dua's RFID Tag-Reader Module (**blue**) includes a Tag Memory 322 such as a "non-volatile configurable memory" that may be "tamper resistant as to prevent hackers from retrieving confidential information and encryption keys" stored therein. Ex-1004, Dua, [0105], [0109]. Accordingly, it is my opinion that the integrated tag memory securely stores information therein.

134. Moreover, as I have explained, in Dua, when "enhanced security is desired," encryption keys are used and shared between the hybrid device and external device to facilitate the sharing of "sensitive" information between the devices. Ex-1004, Dua, [0152].

135. In my opinion, a POSITA reading Dua would have understood that the encryption keys provide "enhanced security" by encrypting "sensitive" information using those keys. Ex-1004, Dua, [0152]. For example, in my opinion, it would have been obvious to encrypt the "confidential information" stored in the hybrid device's tag memory to enhance security. Ex-1004, Dua, [0109].

136. In my opinion, a POSITA would have been motivated to use an encryption key to improve RFID security so that "hackers" could not access the encrypted, confidential information during any data transfer from the hybrid device to the external device, as Dua suggests. Ex-1004, Dua, [0109], [0152].

137. In my opinion, a POSITA would further have had a reasonable expectation of success in using encryption to enhance security because Dua explains that the encryption key is stored in the integrated tag memory (integrated PDK), and the tag could transfer the encryption key to an external RFID reader for decrypting the encrypted data. Ex-1004, Dua, [0109], [0152].

138. Accordingly, in my opinion, Dua's integrated tag memory (integrated PDK) thus would store local, encrypted "confidential information" in an integrated, tamper-resistant memory.

d. [14c] "receiving a first signal, at the integrated RDC, via the first wireless link, from the external device; and"

139. In my opinion, Dua discloses limitation [14c] ("receiving a first signal, at the integrated RDC, via the first wireless link, from the external device").

140. In my opinion, Dua discloses limitation [14c] because it discloses receiving "RFID transmission data" (a first signal) at the hybrid device's reader component (the integrated RDC) via the first wireless link from the external RFID tag (the external PDK). Ex-1004, Dua, [0127].

141. For example, as Dua explains, during the RFID discovery process, after the external device's RFID tag received the interrogation signals, the external device's RFID tag transmits RFID transmission data to the hybrid device. Ex-1004, Dua, [0127]-[0144]. In Dua, the transmitted RFID transmission data (first signal)

includes information such as “communication settings, media processing capabilities, and other parameters” for establishing a wireless connection with the external device. Ex-1004, Dua, [0128].

e. [14d] “generating an enablement signal enabling one or more of an application, a function and a service.”

142. I have been informed that limitation [14d] is recited as allowing “mixed operations” involving several alternatives: what is being enabled (for example, application, function, or service). Ex-1001, ’289 patent, Abstract, 16:39-46. I have further been informed that because limitation [14d] recites alternative events,² “the entire element is disclosed by the prior art if one alternative ... is in the prior art.” *Fresenius USA, Inc. v. Baxter Int’l, Inc.*, 582 F.3d 1288, 1298 (Fed. Cir. 2009).

143. In my opinion, Dua discloses limitation [14d] (“generating an enablement signal enabling one or more of an application, a function and a service”).

144. In my opinion, Dua discloses [14d] because it discloses that, after receiving the RFID transmission data from an external device with an RFID tag-reader module, the hybrid device automatically generates “a Bluetooth paging

² This is consistent with Proxense purported construction of “one or more of an application, a function and a service” limitation as requiring only “application, function, or service.” Ex-1018, 10 (Ex. E, Preliminary Infringement Contentions).

message” (an enablement signal) to enable an application, function, or service. Ex-1004, Dua, [0123], [0128].

145. In my opinion, because Dua discloses enabling an application, function, or service on either device with an RFID tag-reader module, Dua discloses this claim limitation.

146. To the extent that the enablement signal must be generated by the integrated RFID reader, it is my opinion that Dua discloses this.

147. For example, according to Dua, the digital media may be playing on a hybrid device, and the user of the hybrid device may decide to transmit the digital media to an external device. Ex-1004, Dua, [0126]. In Dua, by bringing the external device into proximity with the hybrid device, the hybrid device’s integrated RFID reader (RDC) wirelessly communicates interrogation signals to the external device’s RFID tag, which in turn wirelessly communicates RFID transmission data to the integrated RFID reader (RDC). Ex-1004, Dua, [0127]-[0142].

148. This RFID discovery/paging process in Dua causes the hybrid device to generate a Bluetooth paging message (enablement signal) to enable a service (for example, wireless connection and transmission of media) on the external device.

149. According to Dua, the Bluetooth paging message causes the external device to perform a wireless connection set up, and upon completion, the hybrid device “automatically transmits” media content to the external device. Ex-1004,

Dua, [0128], [0123]. A POSITA would have recognized this as consistent with the Bluetooth specification including the service discovery profile, the cordless telephony profile, and the headset profile³

150. Moreover, during the transmission of the media content, the media could be “automatically convert[ed] ... into a format that is supported by” the external device. Ex-1004, Dua, [0161], [0172].

151. Thus, in my opinion, Dua’s Bluetooth paging message may be used to enable wireless transmission of media that would not have otherwise been supported by the external device. Ex-1004, Dua, [0161], [0172].

152. Additionally, and alternatively, in my opinion, Dua’s Bluetooth paging message is generated to enable a function (for example, wireless connection) between the hybrid device and external device. Ex-1004, Dua, [0144]. For example, as Dua explains, the hybrid device and target device may “conserve power by not always having their wireless interface turned on.” Ex-1004, Dua, [0144], [0137]. Dua’s RFID transmission data then helps “facilitate the automatic activation of a radio transceiver with an appropriate communications protocol,” such as exchanging Bluetooth paging messages, to enable wireless connectivity functions in the two devices. Ex-1004, Dua, [0144].

³ See *e.g.* BLUETOOTH SPECIFICATION Version 1.0 B Volume 2 at pp. 90, 133, and 202.

153. To the extent that the enablement signal must be generated by the integrated RFID tag (integrated, secure memory), it is my opinion that Dua also discloses this.

154. For example, Dua's integrated RFID tag could establish "wireless communication between a diverse set of [external] devices" for various purposes, including "for electronic payments" at point-of-sale or to "secure key access to buildings." Ex-1004, Dua, [0052], [0070].

155. In Dua, "a credit card profile or other payment information" may be stored on the hybrid device. Ex-1004, Dua, [0224]. During electronic payments using RFID technology, Dua's integrated RFID tag (integrated, secure memory) would generate RFID signal (enablement signal) to exchange financial information with the external point-of-sale device that is in close proximity to enable electronic payments. Ex-1004, Dua, [0070].

156. While Dua does not expressly disclose where the credit card profile or other payment information is stored, in my opinion, a POSITA would have been motivated to securely store the financial information in its tamper-resistant tag memory "to prevent hackers from retrieving confidential information." Ex-1004, Dua, [0105], [0109].

157. Indeed, as Giobbi '157 teaches, "credit/debit card information" used to complete financial transactions (for example, "charging a credit card for a

purchase”) would be stored in a “profile memory field 232” in the “physical access secured and tamperproof” memory. Ex-1006, Giobbi ’157, [0036], [0042], [0063].

158. In my opinion, a POSITA would have been motivated and capable of storing the “credit card profile or other payment information” in Dua’s tag memory because storing the “credit card profile or other payment information” in tag memory would require minimal modification without undue experimentation. Such a combination, in my opinion, would have been no more than combining prior art elements according to known methods to yield predictable results. A POSITA would further have had a reasonable expectation of success in storing “credit card profile or other payment information” in Dua’s tamper-resistant tag memory.

2. Independent Claim 1

159. It is my opinion that Dua alone, or in view of Giobbi ’157 renders obvious asserted independent claim 1.

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

160. To the extent the preamble is limiting, Dua discloses the hybrid device because it discloses a media player (for example, cellular phone) that includes an RFID Tag-Reader Module. Ex-1004, Dua, [0057], [0070]. Section IX.A.1.b.

b. [1a] “an integrated, secure memory storing local, secured information; and”

161. In my opinion, Dua discloses limitation [1a] (“an integrated, secure memory storing local, secured information”).

162. For example, Dua's hybrid device renders obvious an integrated, tamper-resistant memory storing local, encrypted information. Ex-1004, Dua, [0105], [0109], [0152]. Section IX.A.1.c.

c. [1b] “an integrated reader-decoder circuit (RDC) for communicating wirelessly with at least one external device within a proximity zone,”

163. In my opinion, Dua discloses limitation [1b] (“an integrated reader-decoder circuit (RDC) for communicating wirelessly with at least one external device within a proximity zone”).

164. For example, Dua discloses that its RFID reader component (RDC) communicates wirelessly with at least one external RFID tag when within a proximity zone. Ex-1004, Dua, [0071]-[0072], [0122], [0127]. Section IX.A.1.b.

d. [1c] “the integrated RDC communicatively coupled to the integrated, secure memory for communication with the integrated, secure memory,”

165. In my opinion, Dua discloses limitation [1c] (“the integrated RDC communicatively coupled to the integrated, secure memory for communication with the integrated, secure memory”).

166. For example, Dua's RFID reader component (RDC) is communicatively coupled to the integrated, secure tag memory for communication with the integrated, secure tag memory (PDK), as shown in Figure 4B below.

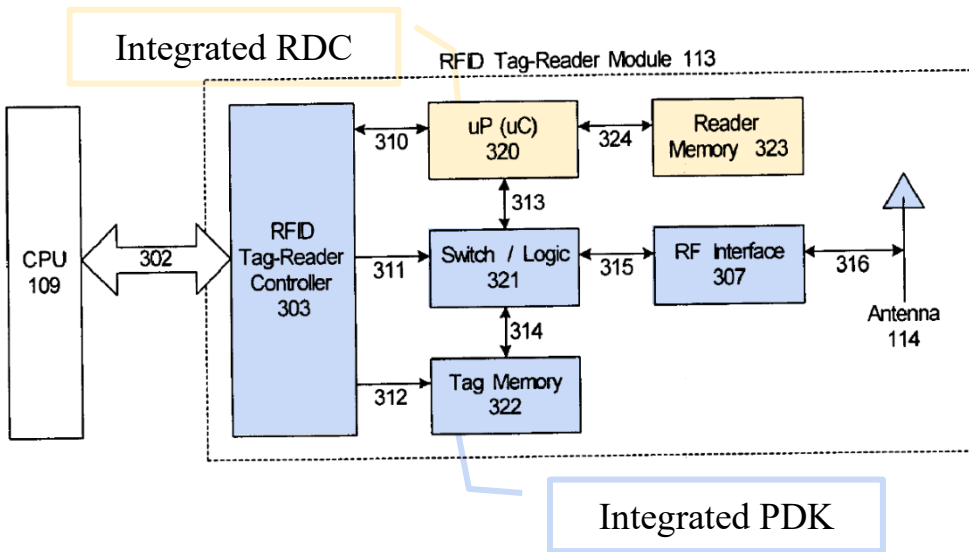


FIG. 4B

Ex-1004, Fig. 4B (annotated).

167. In Dua, the RFID Tag-Reader Module includes “an integrated RFID Tag-Reader Controller 303 that manages all communication between CPU 109 and the functional components of RFID Tag-Reader Module 113,” and “tag logic” (or switch/logic component 321). Ex-1004, Dua, [0106], [0108].

168. Dua further explains that during cross-discovery, an RFID tag can be written with data received by an RFID reader. Ex-1004, Dua, [0152]. Thus, in my opinion, the integrated RDC is communicatively coupled to the integrated, secure memory to update the information stored in the RFID tag memory. Ex-1004, Dua, [0151]-[0154].

- e. **[1d] “wherein one or more of (a) the integrated RDC communicating wirelessly with the at least one external device within the proximity zone and (b) the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and a service.”**

169. In my opinion, Dua discloses limitation [1d] (“wherein one or more of (a) the integrated RDC communicating wirelessly with the at least one external device within the proximity zone and (b) the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and a service”).

170. For example, in my opinion, Dua discloses that either the integrated RDC or the local, secured information stored by the integrated, secure memory (PDK) enables an application, function, or service. Section IX.A.1.e.

171. For example, Dua discloses that, when an external device is within a proximity zone of its integrated RFID reader (RDC), the integrated RFID reader (RDC) communicates wirelessly with the external device’s RFID tag. Section IX.A.1.e. In this example, data received by the RFID reader is sent to the hybrid device’s CPU for use by applications operating on the hybrid device to generate a Bluetooth paging message to enable a wireless connection and transmission of media to the external device, as in limitation [1d](a). Ex-1004, Dua, [0103], [0123], [0128], [0161], [0172].

172. As another example, Dua teaches that the local, encrypted financial information stored in the integrated, tamper-resistant memory enables “electronic payments” at point-of-sale, as in limitation [1d](b). Ex-1004, Dua, [0052], [0070], [0109]. Section X.A.1.e.

B. Dependent Claims

- 1. 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 is enabled, at least in part, on the hybrid device.”**

173. In my opinion, Dua discloses that “at least one of the one or more of the application, the function, and the service is enabled, at least in part, on the hybrid device,” as recited in claim 2.

174. In my opinion, Dua discloses its application, service, or function that is enabled runs *on the hybrid device itself*. See limitation [14d]. For example, in Dua, the hybrid device may “conserve power by not always having their wireless interface turned on.” Ex-1004, Dua, [0144], [0137]. Dua’s hybrid device uses the RFID discovery/paging process to help “facilitate the automatic activation of a radio transceiver” in the hybrid device. Ex-1004, Dua, [0144].

- 2. 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 is enabled, at least in part, external to the hybrid device using an external RDC, the hybrid device communicatively coupled to wirelessly communicate with the external RDC.”**

175. In my opinion, Dua discloses that “at least one of the one or more of the application, the function, and the service is enabled, at least in part, external to the hybrid device using an external RDC, the hybrid device communicatively coupled to wirelessly communicate with the external RDC,” as recited in claim 3.

176. In my opinion, Dua discloses an application, function, or service that is enabled runs *externally to the hybrid device using an external RDC*. See limitations [1d], [14d]. For example, Dua’s integrated RFID tag could establish “wireless communication between a diverse set of [external] devices” for various purposes, including “for electronic payments” at point-of-sale or to “secure key access to buildings.” Ex-1004, Dua, [0052], [0070]. Dua’s hybrid device uses RFID to wirelessly communicate with the external RF 13.56 MHz readers. Ex-1004, Dua, [0089]. Credit card information stored in the hybrid device is sent via the integrated RFID Tag-Reader Module to the external RFID reader at the point-of-sale device for enabling electronic payments. Ex-1004, Dua, [0070], [0224].

177. In my opinion, a POSITA reading Dua would have desired to stored encrypted credit card information in the hybrid device to provide enhanced security. Ex-1004, Dua, [0152].

178. A POSITA, in my opinion, would have been motivated to improve RFID security so that the credit card information that is transferred between a tag and a reader could be encrypted so that “hackers” could not access the sensitive information, as Dua suggests. Ex-1004, [0109], [0152]; *see also* Ex-1006, [0047] (“[T]he data can be encrypted by the transceiver ... and transmitted over a secure link.”), [0050] (“Encrypting data transmitted between the PDK 102 and Reader 108 minimizes the possibility of eavesdropping or other fraudulent activity”).

179. In my opinion, a POSITA would further have had a reasonable expectation of success in using encryption to enhance security because Dua explains that the encryption key is stored in the tag memory, and the tag could transfer the encryption key to an RFID reader for decrypting the encrypted data. Ex-1004, [0108]-[0109], [0152]. The reader thus would receive the credit card information in an encrypted format and decode the encrypted credit card information using the encryption key. Thus, in my opinion, the external RFID reader would be an external RPC because the external RFID reader would decrypt the encrypted credit card information.

3. Claim 4: “The hybrid device of claim 1, wherein the local, secured information includes biometric information for authenticating a user.”

180. In my opinion, Dua in view of Giobbi ’157 renders obvious that “the local, secured information includes biometric information for authenticating a user,” as recited in claim 4.

181. In my opinion, Dua in view of Giobbi ’157 renders obvious that the information stored locally on its integrated tag is secured biometric information for authenticating a user.

182. For example, Dua discloses that its hybrid device may include “an integrated biometric fingerprint reader [to] provide[] enhanced security for protecting ... against unauthorized use.” Ex-1004, Dua, [0058]. Giobbi ’157 further teaches storing “biometric profile” in a local, secured memory, so that a user would use “a matching biometric input” obtained from the hybrid device to “unlock” the tag memory. Ex-1006, Giobbi ’157, [0043]. Giobbi ’157 further teaches that the biometric input would be used to compare “stored biometric information” to authenticate the user (for example, fingerprint authentication). Ex-1006, Giobbi ’157, [0028], [0037]-[0038], [0048].

183. In my opinion, a POSITA would have been motivated to include biometric information for authenticating a user in Dua’s local, tamper-resistant tag

memory because doing so would promote Dua's purpose of "enhanc[ing] security for protecting ... against unauthorized use." Ex-1004, Dua, [0058].

184. In my opinion, a POSITA would have been capable of storing "biometric information for authenticating a user" in Dua's tag memory, as Giobbi '157 teaches, because Dua's hybrid device has an integrated biometric fingerprint reader, Ex-1004, [0058], and it would have required minimal modification without undue experimentation to store the "biometric fingerprint" information in Dua's tag memory. Such a combination, in my opinion, would have been no more than combining prior art elements according to known methods to yield predictable results.. A POSITA would further have had a reasonable expectation of success in storing "biometric information for authenticating a user" in Dua's tamper-resistant tag memory.

4. Claim 5: "The hybrid device of claim 1, wherein the local, secured information includes biometric information based on a biometric scan of a finger, the biometric information for authenticating a user."

185. In my opinion, Dua discloses that "the local, secured information includes biometric information based on a biometric scan of a finger, the biometric information for authenticating a user," as recited in claim 5.

186. In my opinion, Dua in view of Giobbi '157 renders obvious that the biometric information is based on a biometric scan of a finger. Ex-1006, Giobbi '157, [0037]; Section IX.B.3.

187. For example, Giobbi '157 explains that in the “case of fingerprint authentication,” “the biometric profile sample may represent only [a] small portion area of the full fingerprint image,” “the fingerprint profile sample ... [may] describe[] an arc of one or more lines of the fingerprint,” or “the fingerprint profile sample can be data representing color information of the fingerprint.” Ex-1006, [0038].

5. Claim 6: “The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information.”

188. In my opinion, Dua discloses that “the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information,” as recited in claim 6.

189. In my opinion, Dua in view of Giobbi '157 renders obvious that the local, secure information may be “credit card profile or other payment information” used to complete financial transactions (for example, “electronic payments” at point-of-sale). Ex-1004, Dua, [0052], [0070], [0224]; Section IX.A.1.e.

190. Further in my opinion, to the extent that Dua does not expressly discloses where the credit card profile or other payment information is stored, but Dua in view of Giobbi '157 renders obvious that the credit card profile or other payment information would have been stored in its tamper-resistant tag memory. Ex-1004, Dua, [0105], [0109]; Section IX.A.1.e.

- 6. Claim 8: “The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on an authorization of the financial information using an external authentication database, the financial information transmitted to the external authentication database.”**

191. In my opinion, Dua discloses that “the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on an authorization of the financial information using an external authentication database, the financial information transmitted to the external authentication database,” as recited in claim 8.

192. For example, Giobbi '157 discloses that its external reader is communicatively coupled “to receive and/or transmit information to remote databases for remote authentication.” Ex-1006, Giobbi '157, [0031], [0053]. Giobbi '157's remote databases include a “validation database ... for authorizing a transaction to be processed.” Ex-1006, Giobbi '157, [0033]. Giobbi '157's “process

involves transmitting credit card (or other purchasing information) to a validation database 112 to authorize the purchase and receive the status of the card.” Ex-1006, Giobbi ’157, [0074].

193. In my opinion, a POSITA would have been motivated to use an external validation database, as Giobbi ’157 teaches, because the validation database would provide protection to ensure that “the card is active and not reported lost or stolen and that sufficient funds are present to execute the purchase,” Ex-1006, Giobbi ’157, [0074], when Dua’s RFID Tag-Reader Module is used for “electronic payments at the point-of-sale.” Ex-1004, Dua, [0070].

194. A POSITA would have been motivated to use an external validation database, as Giobbi ’157 teaches, because doing so would require minimal modification without undue experimentation. Such a combination, in my opinion, would have been no more than combining prior art elements according to known methods to yield predictable results. A POSITA would further have had a reasonable expectation of success in using a validation database to complement the financial transaction.

7. Claim 9: “The hybrid device of claim 8, wherein the external authentication database is separate from a merchant providing a sale in the financial transaction.”

195. In my opinion, Dua discloses that “the external authentication database is separate from a merchant providing a sale in the financial transaction,” as recited in claim 9.

196. For example, as I discussed with respect to claim 8, Giobbi ’157 discloses an external validation database. Giobbi ’157 further discloses that “in purchase transactions, the validation database 112 is a credit card validation database that is separate from the merchant providing the sale.” Ex-1006, Giobbi ’157, [0033].

8. Claim 10: “The hybrid device of claim 1, wherein the one or more of the application, the function and the service enabled based on the local, secured information stored by the integrated, secure memory includes a first application, function or service based on a first subsets of local, secured information stored by the integrated, secure memory and a second application, function or service based on a second subset of local, secured information, the first and second subset of local, secured information having different accessibility.”

197. In my opinion, Dua discloses that “the one or more of the application, the function and the service enabled based on the local, secured information stored by the integrated, secure memory includes a first application, function or service based on a first subsets of local, secured information stored by the integrated, secure memory and a second application, function or service based on a second subset of

local, secured information, the first and second subset of local, secured information having different accessibility,” as recited in claim 10.

198. For example, as the '289 patent explains, a device may have two applications, each of which can access a different local, secured information stored on an integrated, secure memory. Ex-1001, '289 patent, 9:41-47. A first application (for example, “auto login/logoff”) may be “enabled” based on a first local, secured information (for example, “username and password”). Ex-1001, '289 patent, 9:47-50. A second application (for example, “credit card transaction”) may use a second local, secured information (for example, “biometric information” or “credit card information,” etc.). Ex-1001, '289 patent, 9:50-55, 9:13-19.

199. Similarly, Dua discloses its integrated RFID tag could establish “wireless communication between a diverse set of devices,” including “for electronic payments” at point-of-sale or to “secure key access to buildings.” Ex-1004, Dua, [0052], [0070]. In my opinion, it would have been obvious that the information for “electronic payments” is different from information for “secure key access to buildings.” For example, Giobbi '157 discloses storing multiple user profiles, such as biometric profile, PIN profile, picture profile, registry profile, credit cards, and personal information, in its secured and tamperproof memories. Ex-1006, Giobbi '157, [0037]-[0042], [0058]. Each of Giobbi '157's profiles provides a different accessibility to certain application, function, or service, such that, one

profile may be used to enable “access to secure physical or digital assets,” and another may be used for completing a purchase transaction. Ex-1006, Giobbi ’157, [0063].

200. In my opinion, a POSITA would have been motivated to store multiple subsets of local, secured information, as Giobbi ’157 teaches, so the hybrid device can access different applications, functions, or services. In my opinion, a POSITA would have been motivated to store a credit card information in one subset of local, secured information for credit card processing, and a biometric profile or PIN profile in another subset of local, secured information for accessing physical assets, such as gaining access to buildings.

201. Moreover, a POSITA would have been motivated to use multiple profiles, as Giobbi ’157 teaches, because doing so would require minimal modification without undue experimentation. Such a combination, in my opinion, would have been no more than combining prior art elements according to known methods to yield predictable results. A POSITA would further have had a reasonable expectation of success in using multiple profiles.

9. Claim 11: “The hybrid device of claim 1, wherein the hybrid device is a cell phone.”

202. In my opinion, Dua discloses that “the hybrid device is a cell phone,” as recited in claim 11.

203. For example, Dua discloses the hybrid device may be a portable electronic device such as a cell phone. Ex-1004, Dua, [0057], [0070]; claims 1, 14.

10. Claim 15: “The method of claim 14, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on the hybrid device.”

204. In my opinion, Dua discloses that “at least one of the one or more of the application, the function, and the service is enabled at least in part on the hybrid device,” as recited in claim 15. See claim 2.

11. Claim 16: “The method of claim 14 further comprising: sending the enablement signal, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on a device external to the hybrid device and communicatively coupled to an external RDC.”

205. In my opinion, Dua discloses “sending the enablement signal, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on a device external to the hybrid device and communicatively coupled to an external RDC,” as recited in claim 16. See claim 3.

12. Claim 17: “The method of claim 14, wherein the local, secured information includes biometric information for authenticating a user.”

206. In my opinion, Dua discloses that “the local, secured information includes biometric information for authenticating a user,” as recited in claim 17. See claim 4.

13. Claim 18: “The method of claim 14, wherein the local, secured information includes financial information and wherein the one or more of the application, the function and the service completes a financial transaction.”

207. In my opinion, Dua discloses that “the local, secured information includes financial information and wherein the one or more of the application, the function and the service completes a financial transaction,” as recited in claim 18. See claim 6.

14. Claim 19: “The method of claim 14, wherein the hybrid device is a cell phone.”

208. In my opinion, Dua discloses that “the hybrid device is a cell phone,” as recited in claim 19. See claim 11.

X. Ground 3: Claims 1-7, 11, and 14-19 Would Have Been Obvious Over Buer.

A. Independent Claims

209. In my opinion, Buer renders obvious each of independent claims 1 and 14. Independent claim 14 is representative.

1. Independent Claim 14

a. [14pre] “A method comprising:”

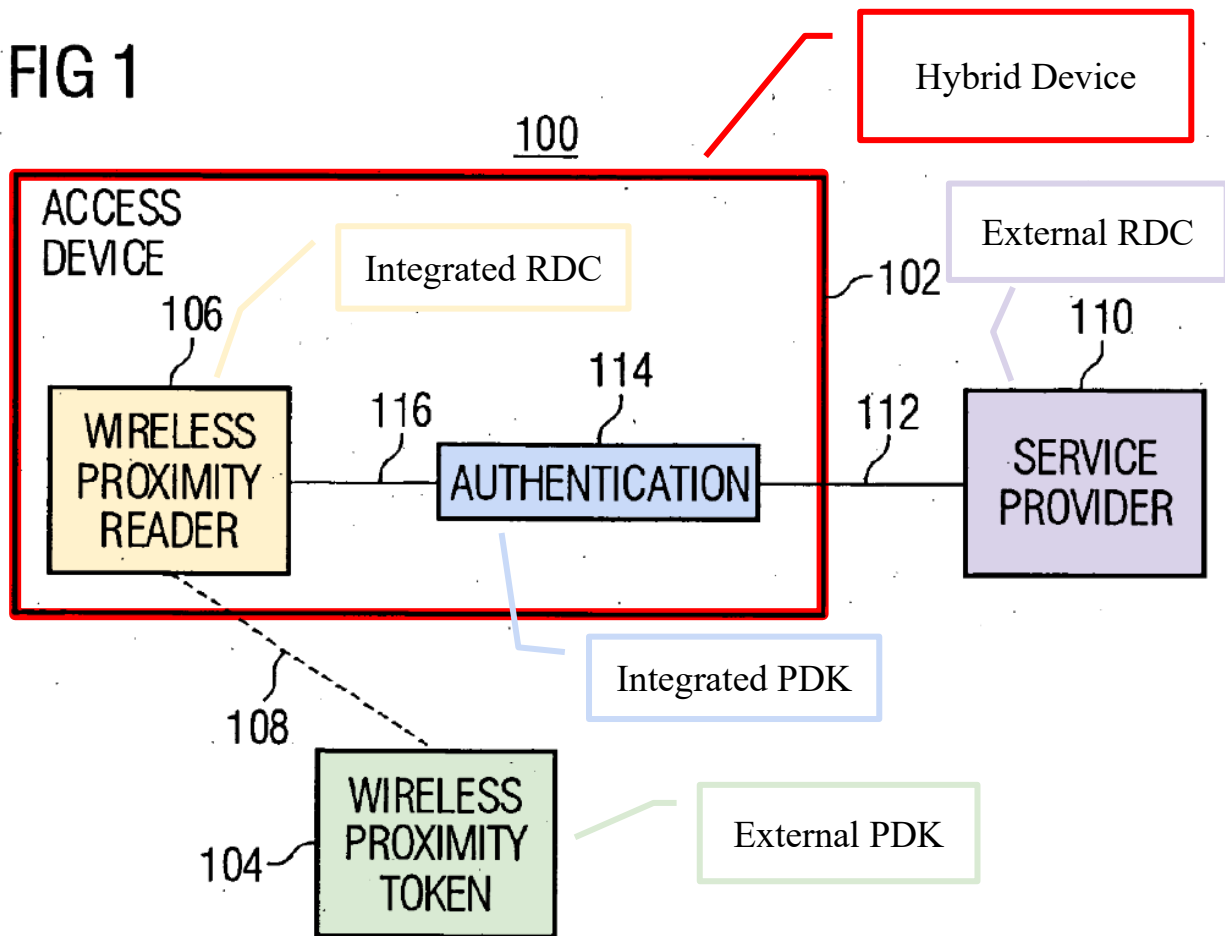
210. To the extent the preamble for claim 14 is limiting, it is my opinion that Buer discloses the preamble because it discloses a method for an access device to access a secured service.

b. [14a] “creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external device,”

211. In my opinion, Buer discloses limitation [14a] (“creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external device”).

212. Buer discloses the hybrid device in limitation [14a] because it discloses an access device, as shown in Figure 1 below, that combines an authentication circuitry (an integrated PDK) and a wireless proximity reader (an integrated RDC) to provide a hybrid device.

IPR2024-00783 Dr. Wolfe Declaration
U.S. Patent No. 9,679,289



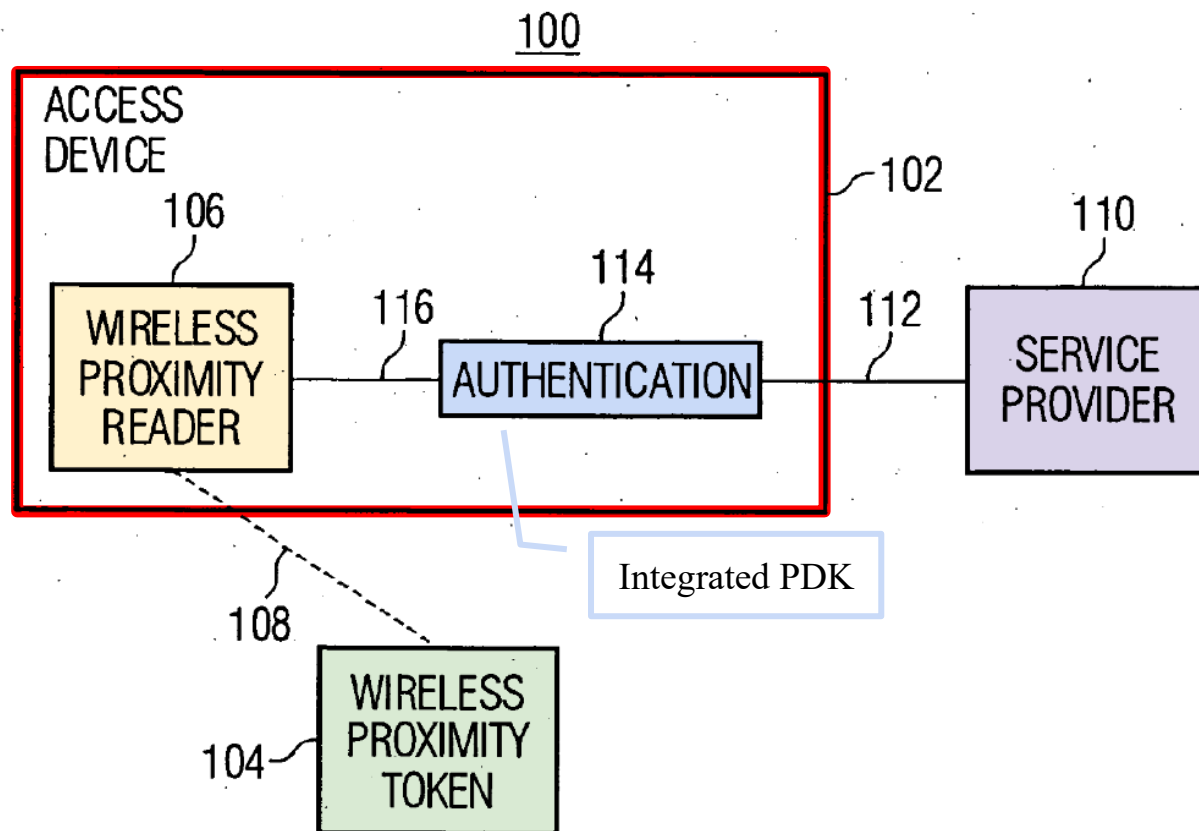
Ex-1005, Buer, Fig. 1 (annotated).

213. In Buer, the authentication system provides access to a secured service, where the access is controlled based on the proximity of a wireless token to an access device. For example, in Figure 1, Buer's access device 102 ("hybrid device," red) includes two components: an authentication component 114 ("integrated PDK," blue) and a wireless proximity reader 106 ("integrated RDC," yellow). Ex-1005, Buer, [0118], Fig. 1. The authentication component 114 is configured to process (for example, encrypt or sign) the information before sending it to the service provider

110 (purple). Ex-1005, Buer, [0118], Fig. 1. The wireless proximity reader 106 is configured to receive information from a wireless proximity token 104 (“external PDK,” green) when the token is proximate to the access device. Ex-1005, Buer, [0111]-[0112], Fig. 1.

214. In my opinion, in Buer’s access device, as shown in Figure 1 below, the authentication component discloses the integrated PDK.

FIG 1



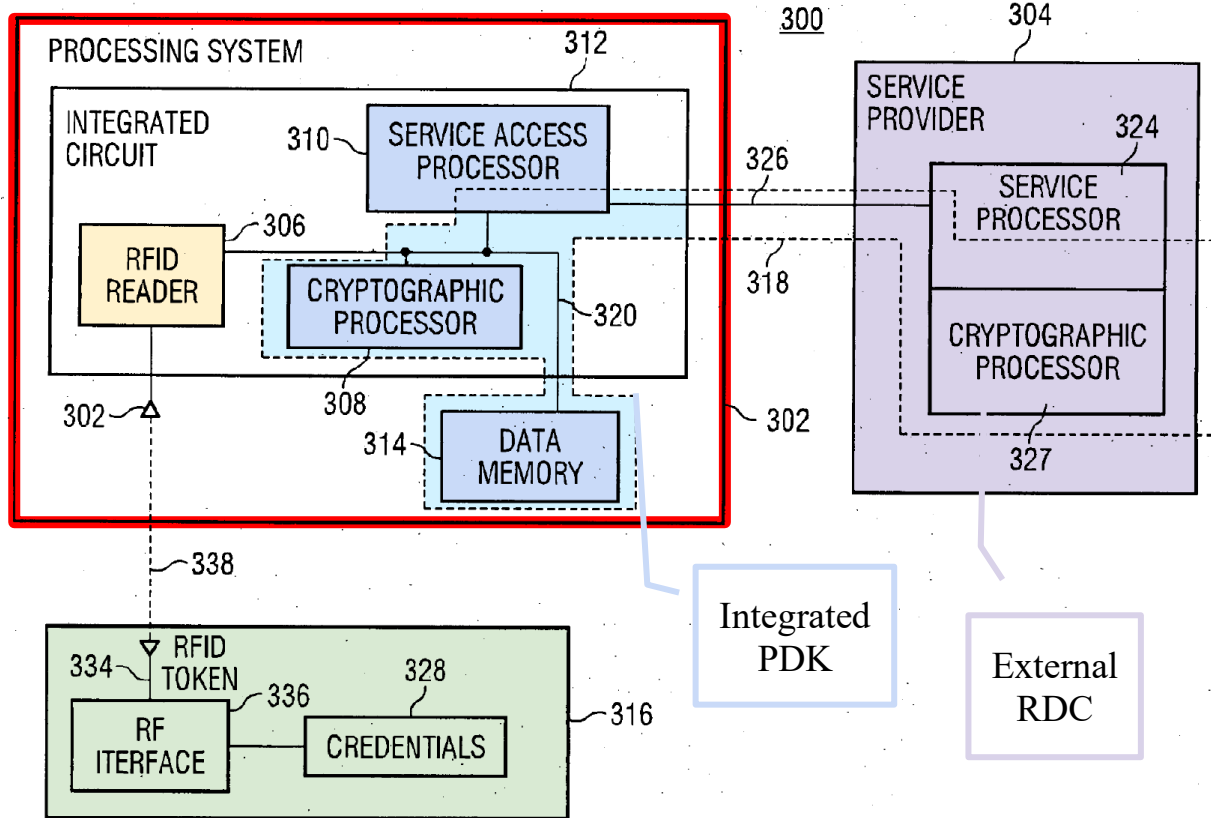
Ex-1005, Buer, Fig. 1 (annotated).

215. In Buer, the authentication component is implemented as a cryptographic processing system, Ex-1005, Buer, Figs. 3, 6, and, in my opinion, is a “personal digital key” under either the district court’s construction or Google’s proposed construction:

- District Court’s Construction: “personal digital key” means “an operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for storing information particular to a user.”
- Google’s Proposed Construction: “personal digital key” to mean “a collection of circuit components that includes an antenna, a transceiver, and a controller and memory for storing information particular to a user.”

216. The authentication component (for example, cryptographic processing system), as shown in Figure 3 below, is an operably connected collection of circuit components (**blue**) that include a service access processor for communicating with an external service provider (that is, it includes “an antenna and a transceiver for communicating with a[n] RDC”) and cryptographic processor and data memory (“controller and memory for storing information particular to a user”). Ex-1005, Buer, [0137].

FIG 3



Ex-1005, Buer, Fig. 3 (annotated).

217. Further, Buer's cryptographic processor 308 acts as a controller for encrypting any important information, such as a user's credentials ("information particular to a user"), received from the external token. Ex-1005, Buer, [0119], [0135]-[0137], [0141], [0150]. The encrypted information (and credentials) is stored in data memory 314 within the cryptographic boundary 318 (light blue). Ex-1005, Buer, [0135], [0137].

218. Buer's service access processor 310 then sends encrypted information via a communication link 326 to an external cryptographic processor 322, 327⁴ (purple) for decryption and/or authentication processing, as necessary. Ex-1005, Buer, [0138], [0152]-[0153].

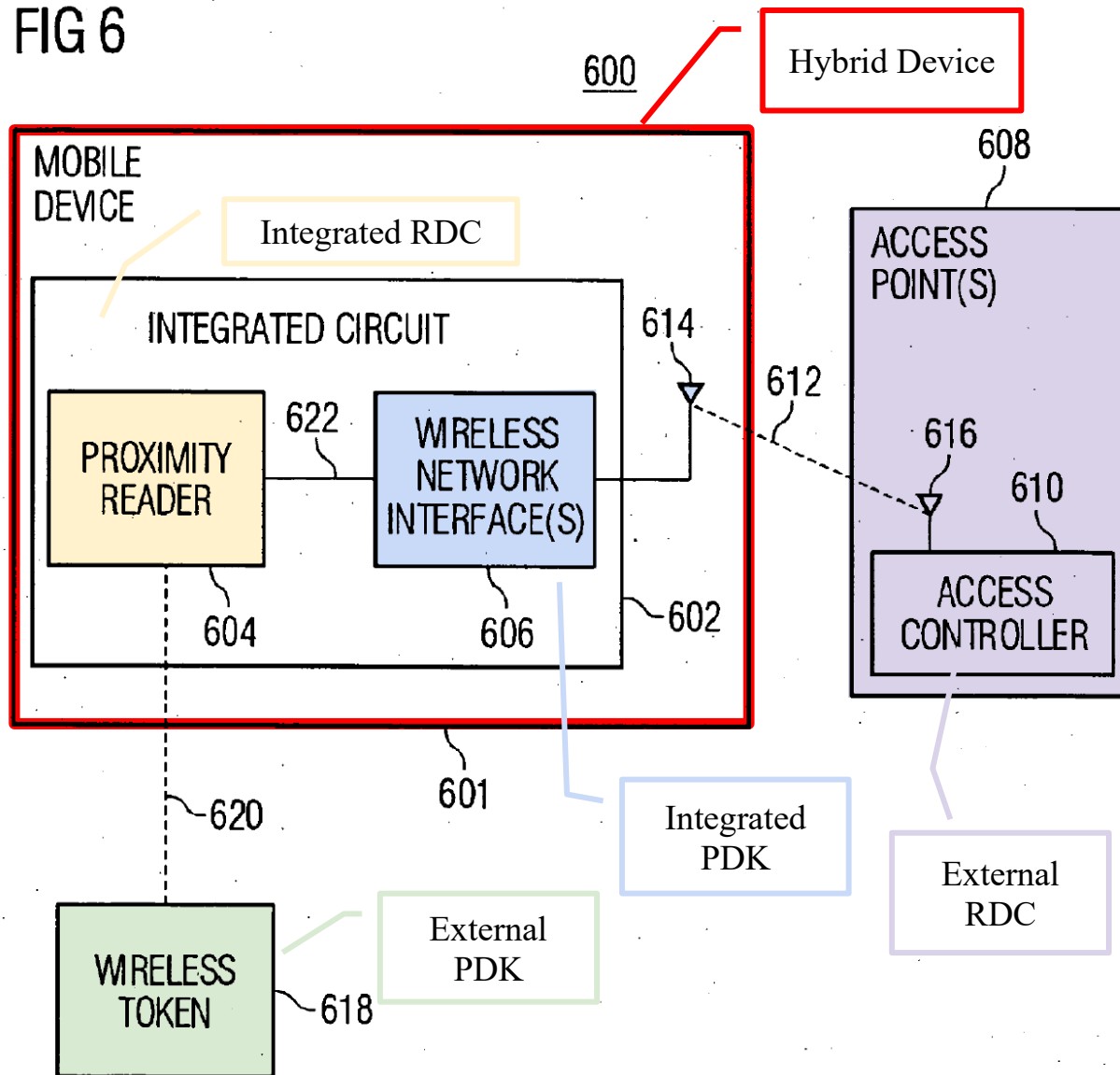
219. While Buer does not expressly disclose whether communication link 326 is a wireless communication link, in my opinion, a POSITA would have understood the disclosure of "lead lines in the drawings may comprise a data network, for example, a local network and/or a wide area network (e.g., the Internet)," Ex-1005, Buer, [0199]-[0201], to suggest that the encrypted information would be transmitted wirelessly via an antenna and a transceiver.

220. Indeed, the cryptographic processing system (while not shown), when implemented in Buer's mobile device (red), is used to "cryptographically encrypt/sign the information" before the mobile device "sends the signed information" via a wireless a network interface (blue) "to the network access provider (e.g., access point 608)" (purple). Ex-1005, Buer, [0165], [0170], [0174]. As shown in Figure 6, the mobile device (red) includes an antenna 614 and wireless network interface(s) 606 (blue) that are used to send the encrypted (or signed) information over a wireless network (for example, a cellular network, an 802.11

⁴ Figure 3 appears to include a typographical error.

network, a Bluetooth network, etc.) via RF signals 612 to the network access provider. Ex-1005, Buer, [0163], [0165], [0174].

FIG 6



Ex-1005, Buer, Fig. 6 (annotated).

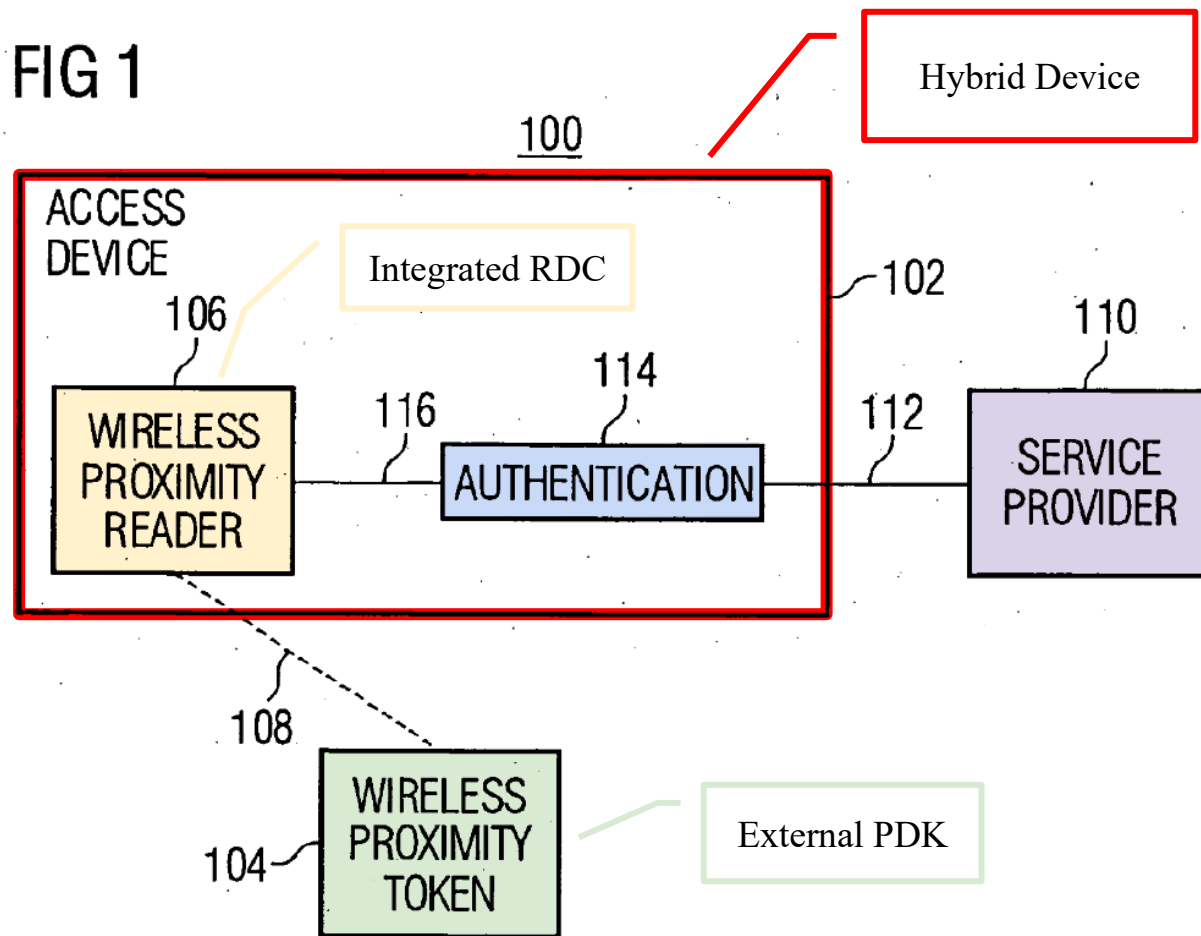
221. Thus, in my opinion, Buer's cryptographic processing system, including its cryptographic processor, service access processor, and data memory, is an integrated PDK.

222. Buer's wireless proximity reader discloses the integrated RDC in limitation [14a] and is a "receiver-decoder circuit" under either the district court's construction or Google's proposed construction:

- District Court's Construction: "receiver-decoder circuit" means "a component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing."
- Google's Proposed Construction: "receiver-decoder circuit" to mean "a collection of circuit components capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing."

223. For example, Buer's wireless proximity reader 106 ("integrated RDC," **yellow**), as shown in Figure 1 below, is a component that is "configured to receive signals 108 (e.g., RF signals)" from at least one wireless proximity token 104 ("external PDK," **green**) when the token 104 is "proximate to the access device 102." Ex-1005, Buer, [0111].

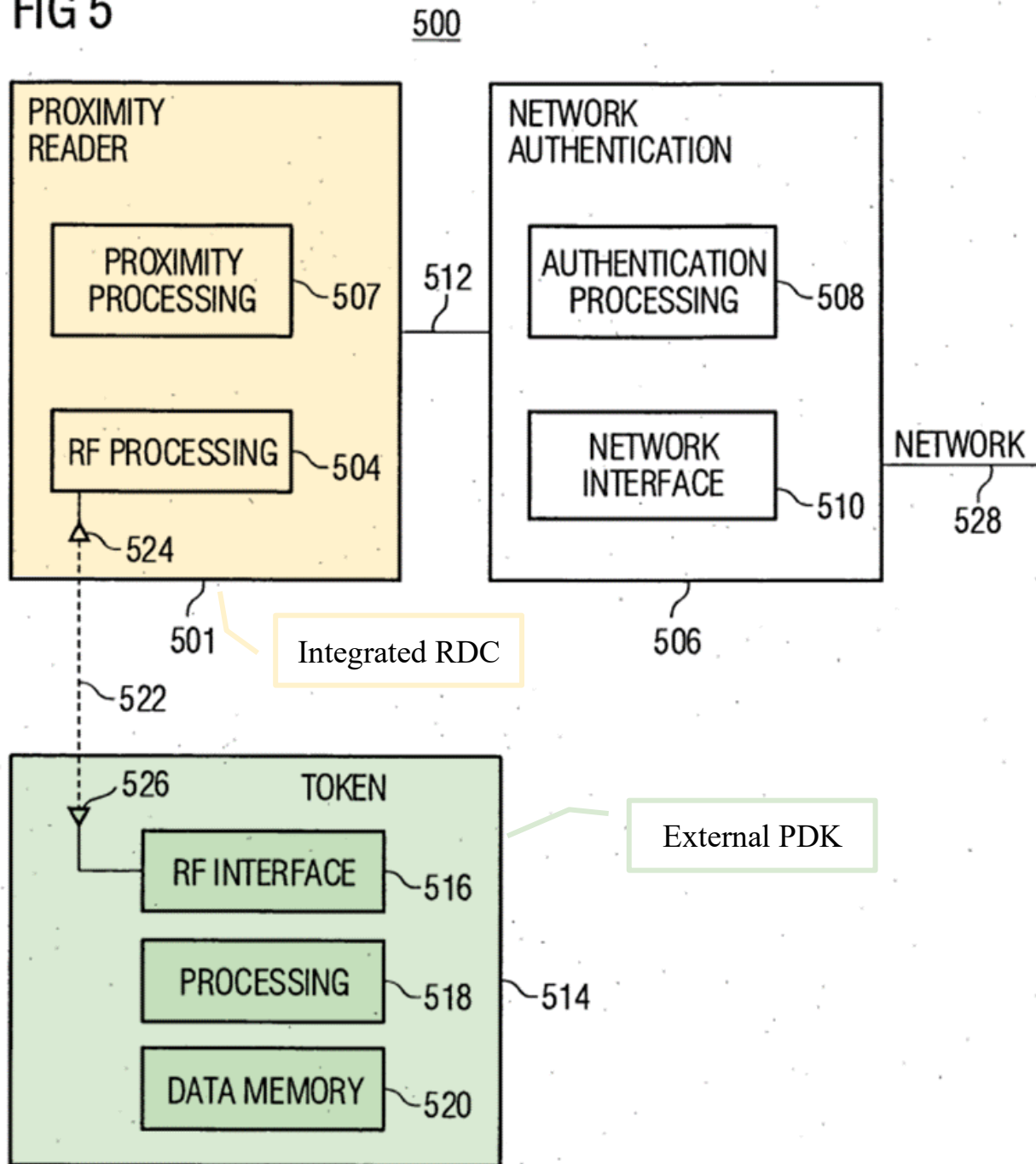
FIG 1



Ex-1005, Buer, Fig. 1 (annotated).

224. Buer's proximity reader 501 may include a collection of circuit components, including an antenna 524, an RF processing component 504, and a proximity processing component 502, 507, as shown in Figure 5 below. Ex-1005, Buer, [0157]. (In Figure 5, the proximity processing component should be labeled 502, not 507. See Ex-1005, Buer, [0157].)

FIG 5



Ex-1005, Buer, Fig. 5 (annotated).

225. Buer's "wireless proximity reader and token may be implemented using one or more of a wide variety of wireless proximity techniques." Ex-1005, Buer,

[0128]. Buer's proximity reader and the external token further communicate via RF signals when they are within proximity to one another. Ex-1005, Buer, [0112], [0146], [0157], [0173]. In particular, the token stores encrypted authentication information that is provided to the proximity reader. Ex-1005, Buer, [0130], [0158]. The reader receives the encrypted data and extracts any embedded information. Ex-1005, Buer, [0097], [0184]. Thus, in my opinion, the proximity reader necessary decodes the encrypted information for later processing (including for extracting the embedded information, as disclosed).

226. Because Buer's access device includes an integrated authentication component and a wireless reader, it is my opinion that Buer discloses a hybrid device that includes both an integrated PDK and an integrated RDC, as recited in limitation [14a].

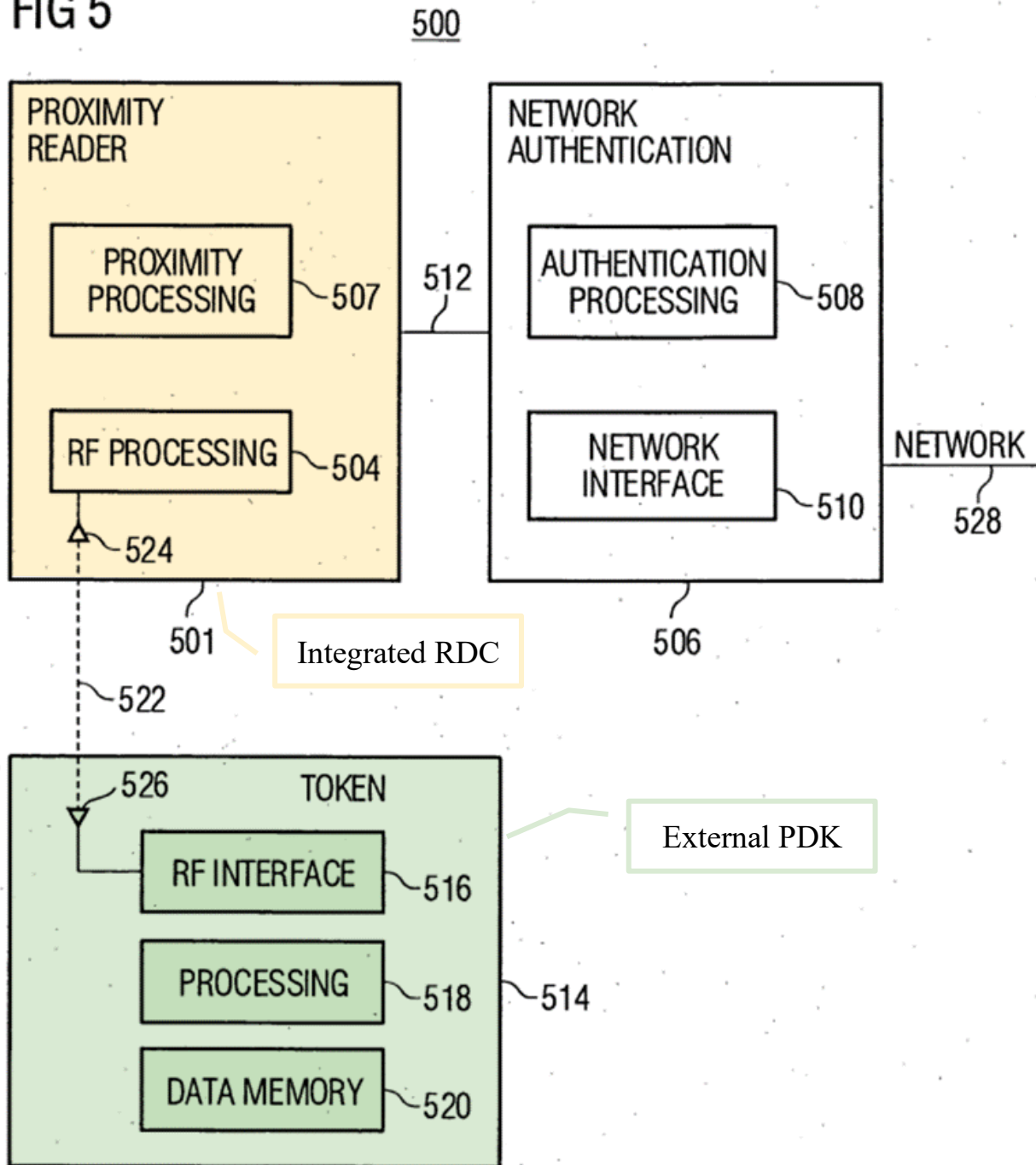
227. Additionally, in my opinion, Buer discloses creating a first wireless link between the wireless proximity reader (integrated RDC) and a wireless proximity token (external device) as in limitation [14a].

228. For example, as Buer explains, "an RFID signaling sequence" between the reader and the wireless token includes creating a first set of RF signals that are "used to power and activate the token" before the token can send its information to the reader. Ex-1005, Buer, [0146]–[0149]. In Buer, the wireless token is an "external PDK" that acts as a physical authentication/verification mechanism (for example,

“what the user possesses”). Ex-1005, Buer, [0114]. If the request was made without the token, access may be denied. Ex-1005, Buer, [0011]. However, if the token is in proximate of the reader, “after the system verifies that the user (e.g., the user’s token) is relatively close to the device,” access to various services, applications, or functions (for example, access to data networks, application, or financial transactions) may be enabled. Ex-1005, Buer, [0120]-[0122], [0155].

229. In my opinion, Buer’s external token discloses the external PDK, similar to Buer’s integrated PDK, because it is also an operably connected collection of circuit elements including antenna 526, an RF interface 516 (transceiver), processing component 518, and data memory 520 for storing user information, as shown in Figure 5. Ex-1005, Buer, [0157]-[0159].

FIG 5



Ex-1005, Buer, Fig. 5 (annotated).

230. Buer's RF interface 516 with antenna 526 (in Figure 5) is used to transmit/receive RF signals via line 522 to/from the proximity reader (integrated

RDC). Ex-1005, Buer, [0157]. Buer's processing component 518 acts as a controller for "control[ing] communication with the proximity reader 501," "enabl[ing] the token 514 to be programmed with the authentication information," "process[ing] RF signals received from the proximity reader 501," and "control[ing] the generation of appropriate signals to send the authentication information." v Ex-1005, Buer, [0159]. And Buer's processing component 518 and data memory 520 are used to store the "authentication information such as network authentication credentials, passwords and/or certificates" (for example, "information particular to a user"). Ex-1005, Buer, [0158]-[0159].

231. Accordingly in my opinion, Buer's external token discloses an external PDK, consistent with the court's and Google's constructions.

c. [14b] "the hybrid device including an integrated, secure memory and the integrated RDC, wherein the integrated, secure memory stores local, secured information;"

232. In my opinion, Buer discloses limitation [14b] ("the hybrid device including an integrated, secure memory and the integrated RDC, wherein the integrated, secure memory stores local, secured information").

233. For example, Buer's hybrid device includes an integrated PDK, which includes an integrated, secure memory and the wireless proximity reader (integrated RDC). Section X.A.1.b. As Buer explains, the integrated PDK may use "tamper resistant and/or tamper evident hardware." Ex-1005, Buer, [0013], [0134]. Further,

the information is encrypted when stored in data memory 314 within the cryptographic boundary. Ex-1005, Buer, [0135], [0137]. Thus, in my opinion, Buer discloses an integrated, tamper-resistant memory storing local, encrypted information.

d. [14c] “receiving a first signal, at the integrated RDC, via the first wireless link, from the external device; and”

234. In my opinion, Buer discloses limitation [14c] (“receiving a first signal, at the integrated RDC, via the first wireless link, from the external device”).

235. In my opinion, Buer discloses the integrated reader receives RFID signals, including proximity signaling and authentication information, during the RFID signaling from the external token. For example, during the initial RFID signaling sequence, Buer’s token may perform proximity signaling by sending RF signals to the proximity reader for the proximity reader to verify that a particular token is within range. Ex-1005, Buer, [0157]-[0158]. Buer’s token further generates additional RF signals to send the encrypted authentication information that is stored in the token to the proximity reader. Ex-1005, Buer, [0148]-[0150]; *see also* Ex-1005, Buer, [0097], [0130], [0158]-[0159], [0184].

236. Buer’s integrated reader receives the RFID signals that are broadcasted from the wireless token and extracts the encrypted authentication information (for

example, credentials) from the RFID signals. Ex-1005, Buer, [0148]-[0150], Fig. 4; *see also* Ex-1005, Buer, Figs. 7, 9.

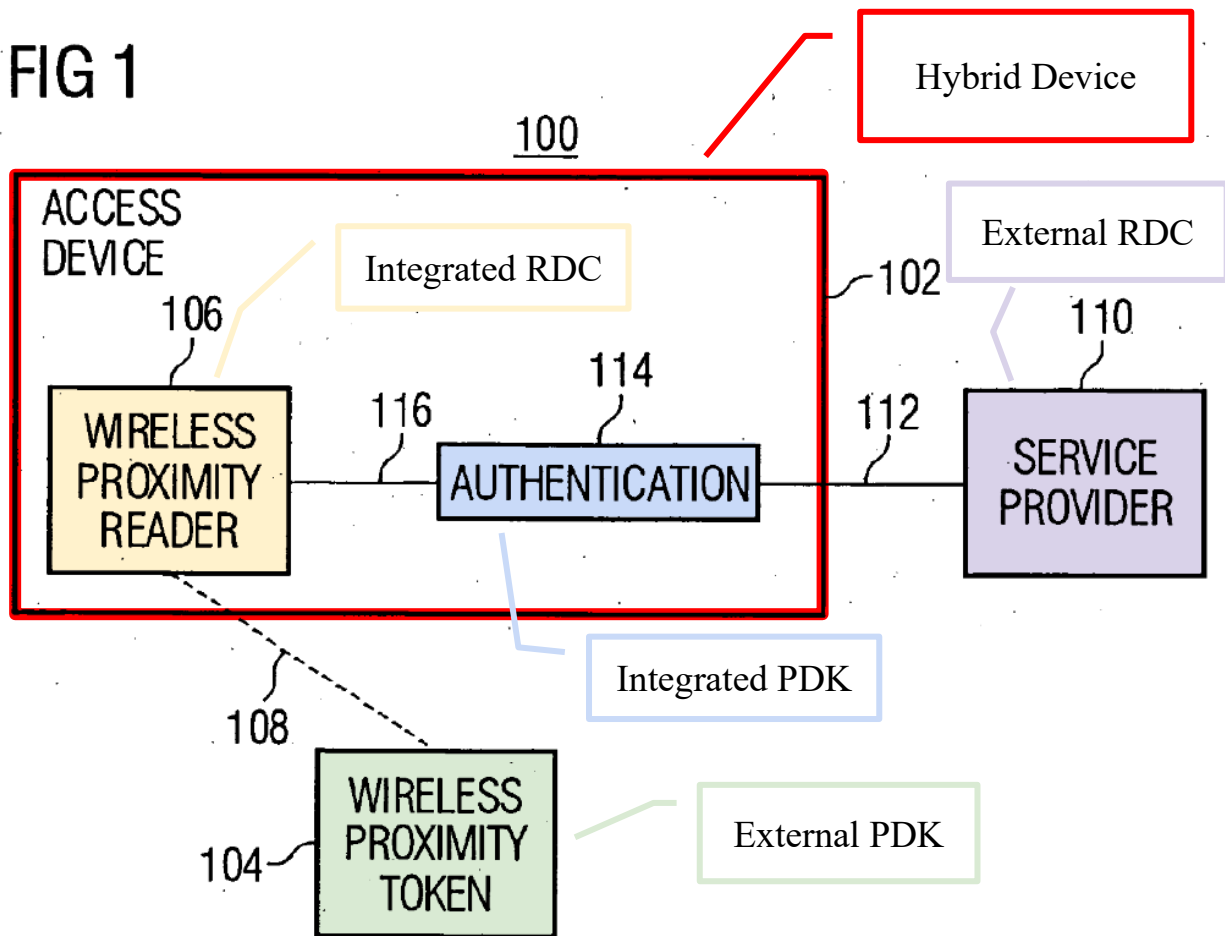
e. [14d] “generating an enablement signal enabling one or more of an application, a function and a service.”

237. I understand that Limitation [14d] is recited as allowing “mixed operations,” Ex-1001, ’289 patent, Abstract, 15:62-16:3216:39-462. Accordingly, it is my understanding that “the entire element is disclosed by the prior art if one alternative ... is in the prior art.” *Fresenius*, 582 F.3d at 1298.

238. In my opinion, Buer discloses limitation [14d] (“generating an enablement signal enabling one or more of an application, a function and a service”). In my opinion, Buer discloses the authentication component generating an enablement signal enabling a wide variety of applications, functions, or services, as in limitation [14d].

239. For example, Buer, as shown in Figure 1 below, provides encrypted or signed credentials to a service provider to enable access to secured services.

FIG 1



Ex-1005, Buer, Fig. 1 (annotated); *see also* Ex-1005, Buer, [0113] (“[T]he communication media 112 may comprise, for example, electric wires, optical cables or air.”).

240. In my opinion, Buer provides at least two examples: (1) proximity reader communicating wirelessly with an external token enables an application, function, or service or (2) the information stored by the integrated, secure memory enables an application, function, or service.

241. First, to the extent that the proximity reader communicating wirelessly with an external token enables an application, function, or service, Buer discloses that information received wirelessly by the integrated proximity reader from the external token enables the application, service, or function on the hybrid device itself.

242. For example, in Buer, after a proximity reader verifies a user (via an external token), the authentication component generates an enablement signal (for example, RF signal) providing the necessary authentication information (for example, signed information) via its cryptographic processing system to a service provider to enable a wide variety of applications, functions, or services on the hybrid device. Ex-1005, Buer, [0152], [0174].

243. Buer's service provide may enable access to the following requested service:

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

Ex-1005, Buer, [0120]; *see also, e.g.*, Ex-1005, Buer, [0122], [0155], [0162], [0195]-[0196]. As Buer explains, application access may include “invoking, interacting with or using the application or loading the application onto the access device.” Ex-1005, Buer, [0122]. Data network access may include “sending and/or receiving data over the network.” Ex-1005, Buer, [0122].

244. In my opinion, Buer, like the '289 patent, discloses enabling network access on a hybrid device. For example, Buer discloses that the network interface 606 performs “network authentication and connection processing” by “communicating with a respective access controller 610 in one or more access point(s) 608 via RF signals 612” transmitted via antennas 614. Ex-1005, Buer, [0165]. The RF signals generated by the wireless network interface are enablement signals that contain the encrypted or signed information that is sent to the “network access provider (e.g., access point 608).” Ex-1005, Buer, [0165], [0174].

246. Buer further discloses that information stored by the integrated, secure memory, such as credit card information, may “be used to authenticate a user to another processing system” (external device) associated with an external proximity reader 1120 (external RDC) that includes “point-of-sale components” to “perform a sales transaction,” such as “credit card transactions.” Ex-1005, Buer, [0193]-[0196]. For example, Buer’s mobile device may include a trusted platform module (TPM), which includes a proximity reader that is used to extract any user credential from a token. Ex-1005, Buer, [0184], [0190]-[0191], [0194]. The extracted credential would be stored in its integrated PDK via the local data memory 824. Ex-1005, Buer, [0185]. As Buer explains, the mobile device’s TPM may further include an RFID client, which generates an enablement signal (for example, RF signal containing credit card information) that is transmitted to another processing system, such as a computer with a point-of-sale device. Ex-1005, Buer, [0192]-[0195].

247. Thus, in my opinion, Buer discloses that, similar to the ’289 patent, “data services” may be enabled on the external security processing system. Ex-1005, Buer, [0195].

2. Independent Claim 1

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

248. In my opinion, Buer discloses the preamble because, as I discussed with respect to claim 14, Buer discloses the preamble because it discloses an access device that combines an authentication circuitry and a wireless proximity reader to provide a hybrid device. See claim 14; Section X.A.1.b.

b. [1a] “an integrated, secure memory storing local, secured information; and”

249. In my opinion, Buer discloses limitation [1a] (“an integrated, secure memory storing local, secured information”).

250. For example, Buer’s hybrid device includes an integrated PDK, which includes an integrated, tamper-resistant memory storing local, encrypted information. Ex-1005, Buer, [0013], [0134]-[0137]; Section X.A.1.c.

c. [1b] “an integrated reader-decoder circuit (RDC) for communicating wirelessly with at least one external device within a proximity zone,”

251. In my opinion, Buer discloses limitation [1b] (“an integrated reader-decoder circuit (RDC) for communicating wirelessly with at least one external device within a proximity zone”). In my opinion, Buer discloses the integrated wireless proximity reader (RDC) communicates “wirelessly with at least” an external token “within a proximity zone.” For example, Buer’s wireless proximity reader (RDC) is configured to receive RF signals when the token is “proximate to

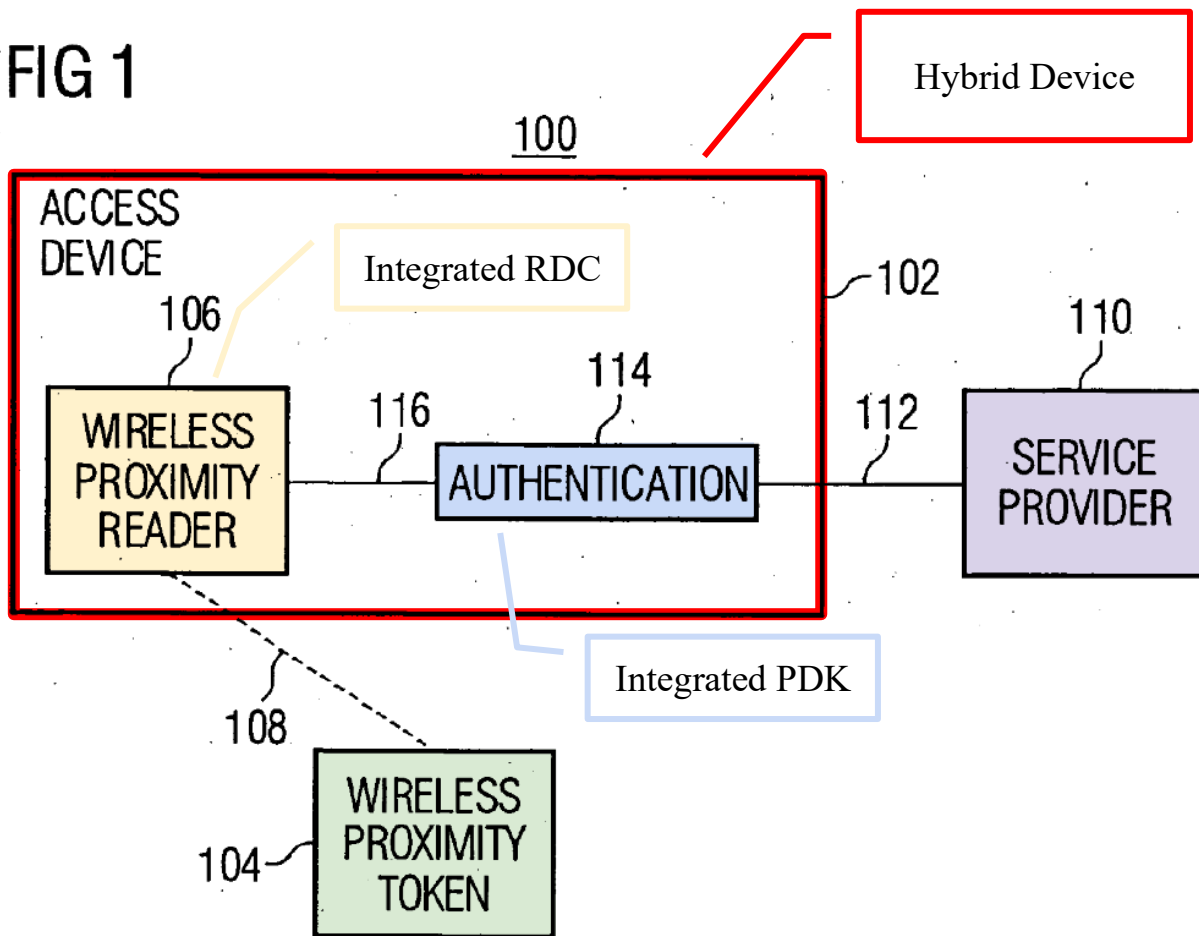
the access device,” such as “when they are within a predefined distance of each other.” Ex-1005, Buer, [0111], [0146]; Section X.A.1.b.

d. [1c] “the integrated RDC communicatively coupled to the integrated, secure memory for communication with the integrated, secure memory,”

252. In my opinion, Buer discloses limitation [1c] (“the integrated RDC communicatively coupled to the integrated, secure memory for communication with the integrated, secure memory”).

253. For example, Buer, as shown in Figure 1 below, discloses that the integrated “[wireless proximity] reader 106” is communicatively coupled to the integrated, secure memory in the “authentication component 114” “via a connection 116 within a common integrated circuit.” Ex-1005, Buer, [0116].

FIG 1



Ex-1005, Buer, Fig. 1 (annotated).

254. As I discussed above for limitation [1a], when Buer's authentication component is implemented as a cryptographic processing system, it is coupled to the reader via a first data bus 320 in Figure 3 or via a first internal lead 622 in Figure 6.

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

- e. **[1d] “wherein one or more of (a) the integrated RDC communicating wirelessly with the at least one external device within the proximity zone and (b) the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and a service.”**

255. I understand that limitation [1d] is recited as allowing “mixed operations” involving several alternatives: (1) what component is used to enable the application, function, or service (for example, “either or both RDC and PDK functionality”), (2) what is being enabled (for example, application, function, or service), and (3) which device is being enabled (for example, hybrid device or external RDC). Ex-1001, ’289 patent, Abstract, 16:39-46.

256. I further understand that because limitation [1d] recites alternative events, “the entire element is disclosed by the prior art if one alternative ... is in the prior art.” *Fresenius*, 582 F.3d at 1298.

257. In my opinion, Buer discloses limitation [1d] (“wherein one or more of (a) the integrated RDC communicating wirelessly with the at least one external device within the proximity zone and (b) the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and a service”).

258. As I discussed in Section X.A.1.e, Buer discloses the authentication component enabling a wide variety of applications, functions, or services. *See* limitation [14d].

259. With respect to (a) the integrated RDC communicating wirelessly with an external device within the proximity zone enables an application, function, or service, it is my opinion that Buer discloses this.

260. For example, Buer discloses that its integrated proximity reader (RDC), communicating wirelessly with an external token within a proximity zone, enables network access on a hybrid device. Ex-1005, Buer, [0120], [0122], [0165], [0174]-[0175], Figs. 6-7; Section X.A.1.e.

261. With respect to (b) the information stored by the integrated, secure memory enables an application, function, or service, it is my opinion that Buer also discloses this.

262. For example, Buer also discloses that the local, encrypted information stored by the integrated, tamper-resistant memory enables network access by sending encrypted or signed information to the “network access provider (e.g., access point 608).” Ex-1005, Buer, [0165], [0174], [0013], [0134]; Section X.A.1.e.

263. Alternatively, Buer discloses that credit card information stored in its trusted platform module (TPM) is used to enable another processing system, such as a computer with a point-of-sale device. Ex-1005, Buer, [0192]-[0195]. Thus, in my

opinion, “data services” may be enabled on the external security processing system of Buer, similar to the ’289 patent. Ex-1005, Buer, [0195].

B. Dependent Claims

- 1. 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 is enabled, at least in part, on the hybrid device.”**

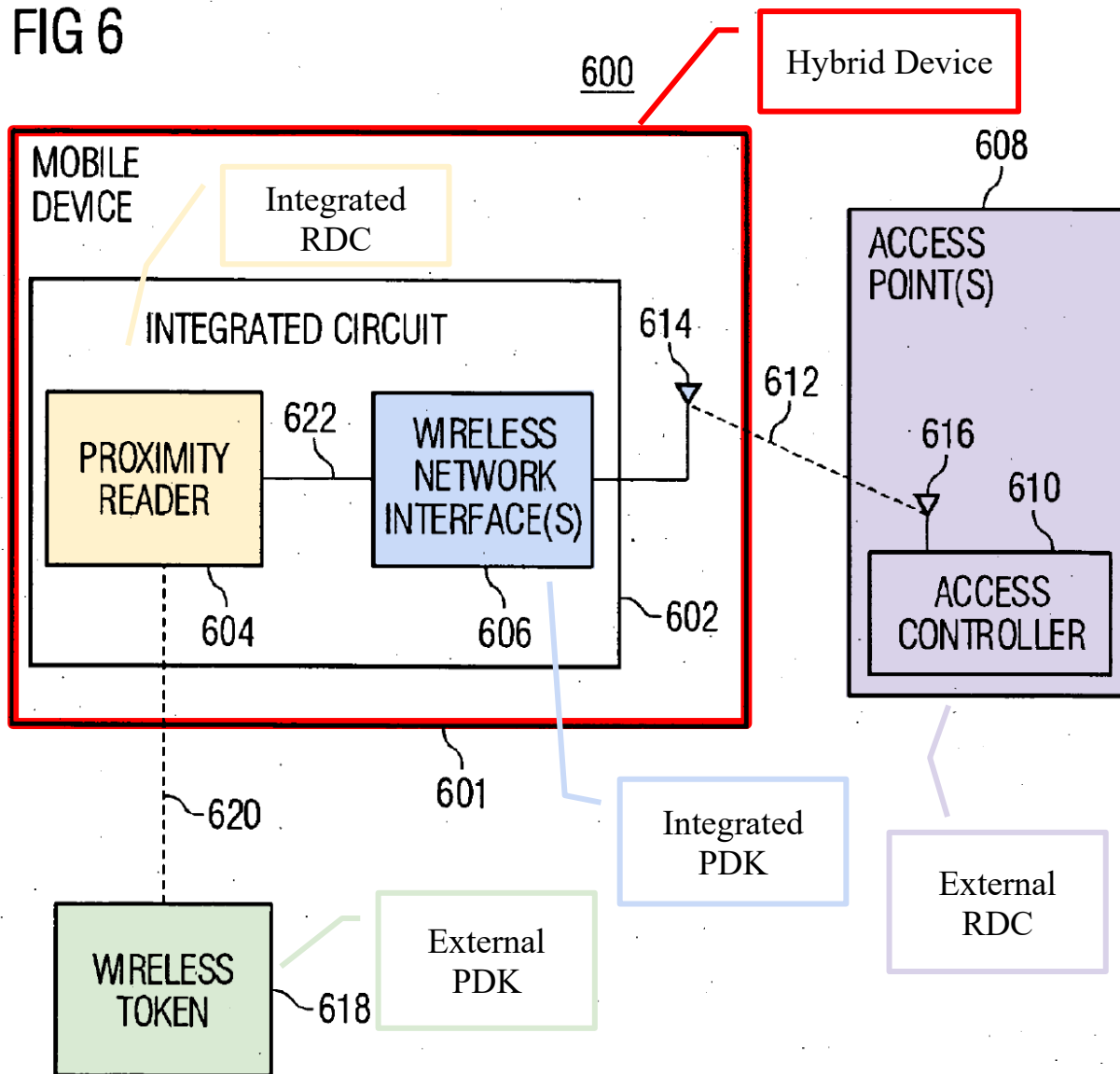
264. In my opinion, Buer discloses that “at least one of the one or more of the application, the function, and the service is enabled, at least in part, on the hybrid device,” as recited in claim 2. For example, Buer discloses a network access is enabled on the hybrid device. *See* limitation [1d](a).

- 2. 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 is enabled, at least in part, external to the hybrid device using an external RDC, the hybrid device communicatively coupled to wirelessly communicate with the external RDC.”**

265. In my opinion, Buer discloses that “at least one of the one or more of the application, the function, and the service is enabled, at least in part, external to the hybrid device using an external RDC, the hybrid device communicatively coupled to wirelessly communicate with the external RDC,” as recited in claim 3.

266. For example, as shown in Figure 6 below, Buer discloses that the encrypted information stored on the integrated, secure memory is wirelessly communicated to an external RDC to enable an application, function, or service,. *See* claim [1d](b).

FIG 6



Ex-1005, Buer, Fig. 6 (annotated).

267. Buer's service provider, as shown in Buer, Figs. 1, 3, 6, as a whole, or the internal cryptographic processor 322, 327, or access controller 610 individually, is an external "receiver-decoder circuit" because they are "capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for

processing,” under either the district court’s construction, or Google’s proposed construction:

- District Court’s Construction: “receiver-decoder circuit” means “a component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing.”
- Google’s Proposed Construction: “receiver-decoder circuit” to mean “a collection of circuit components capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing.”

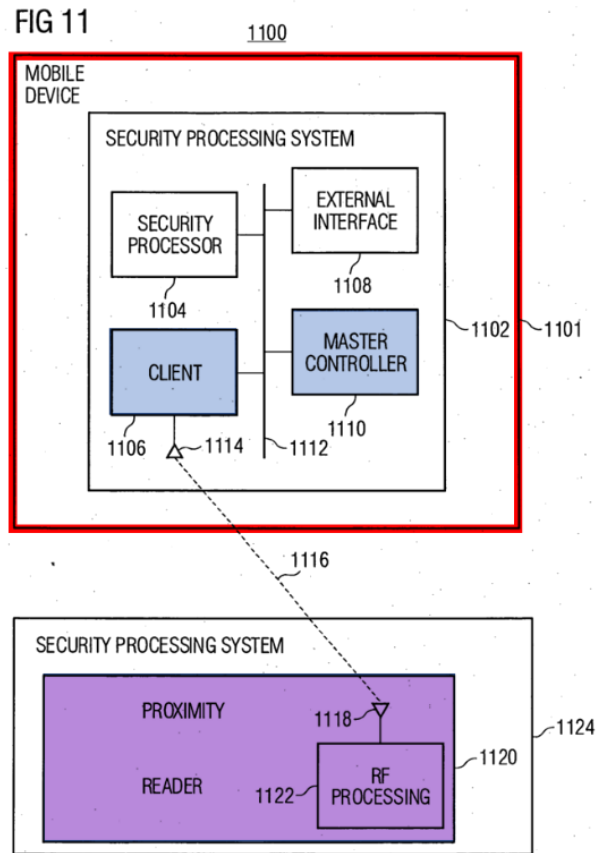
268. For example, Buer’s external cryptographic processor 322, 327 (**purple** in Figure 3) is capable of receiving encrypted information and “decrypti[ng] and/or authenticati[ng] operations necessary to ... receive the encrypted information and provide the information in the clear for internal processing.” Ex-1005, Buer, [0138]. In Figure 6, Buer’s access controller 610 is capable of wirelessly receiving data over a given wireless network. Ex-1005, Buer, [0165]. As Buer explains, the access controller 610 receives encrypted or “signed information.” Ex-1005, Buer, [0174]-[0175].

269. In my opinion, a POSITA reading Buer would have understood that the access controller 610, or the service provider (for example, access point 608), would

decode the encrypted or signed information for further verification of the credentials, similar to the cryptographic processing disclosed in Figure 3.

270. Much like the '289 patent, Buer, in my opinion, discloses enabling network access by sending encrypted or signed information to the “network access provider (e.g., access point 608).” Ex-1005, Buer, [0165], [0174].

271. As a further example, and alternatively, Buer discloses that credit card information stored by the integrated, secure memory may “be used to authenticate a user to another processing system” (external device) associated with an external proximity reader 1120 (external RDC) that, as shown in Figure 11 below, includes “point-of-sale components” to “perform a sales transaction,” such as “credit card transactions.” Ex-1005, Buer, [0195]-[0196].



Ex-1005, Buer, Fig. 11 (annotated).

3. Claim 4: “The hybrid device of claim 1, wherein the local, secured information includes biometric information for authenticating a user.”

272. In my opinion, Buer discloses that “the local, secured information includes biometric information for authenticating a user,” as recited in claim 4.

273. Buer discloses that Buer’s various authorization data for authenticating a user includes “password” and biometric information. Ex-1005, Buer, [0181], [0114].

274. In my opinion, a POSITA reading Buer would have understood that when a token transfers its stored information (such as biometric information), Ex-1005, Buer, [0149], that information is encrypted using Buer's cryptographic processing and stored in the local, secured memory in the hybrid device. Ex-1005, Buer, [0135].

4. Claim 5: "The hybrid device of claim 1, wherein the local, secured information includes biometric information based on a biometric scan of a finger, the biometric information for authenticating a user."

275. In my opinion, Buer discloses that "the local, secured information includes biometric information based on a biometric scan of a finger, the biometric information for authenticating a user," as recited in claim 5.

276. Buer discloses that Buer's biometric information may be "a fingerprint" used to verify the authenticity of the user. Ex-1005, Buer, [0114], [0196], [0130].

5. Claim 6: "The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information."

277. In my opinion, Buer discloses that "the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information," as recited in claim 6. Buer discloses that the local, secure

information may be “credit card information,” and the information is used to “perform a sales transaction.” Ex-1005, Buer, [0195].

6. Claim 7: “The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on a signal received from the at least one external device by the integrated RDC.”

278. In my opinion, Buer discloses that “the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on a signal received from the at least one external device by the integrated RDC,” as recited in claim 7.

279. As I explained in Section X.B.2, Buer discloses that the integrated PDK sends financial information to the external RF processing component for use by the RF processing component. Ex-1005, Buer, [0194]-[0195]. Buer further explains that its external token may also be equipped “with smart card functionality” (for example, “credit cards”) so that a user’s “credit card information” may be provided to an integrated proximity reader in an access device. Ex-1005, Buer, [0129]-[0130], [0193], Fig. 8. It would have been obvious to implement Buer’s “key management functions” to “backup” or store the external token’s credit card information on the user’s cellular phone for point-of-sale transactions. Ex-1005, Buer, [0177], [0195].

280. In my opinion, a POSITA would have been motivated to use the token to transfer the credit card information in a secure manner to the cellular phone without the user having to directly enter the information into the device. Ex-1005, Buer, [0007]. Additionally, a POSITA would have been motivated to provide financial transactions “only when a wireless token assigned to the user is in the proximity of” the cellular phone to further protect against unauthorized use of the credit card information, Ex-1005, Buer, [0011], or to utilize the cellular phone’s “biometric reader to further verify the authenticity of the user,” Ex-1005, Buer, [0114].

7. **Claim 10: “The hybrid device of claim 1, wherein the one or more of the application, the function and the service enabled based on the local, secured information stored by the integrated, secure memory includes a first application, function or service based on a first subsets of local, secured information stored by the integrated, secure memory and a second application, function or service based on a second subset of local, secured information, the first and second subset of local, secured information having different accessibility.”**

281. Buer discloses that its access device can secure access to multiples applications, functions, or services. Ex-1005, Buer, [0120]-[122], [0193]-[0195]. For example, Buer provides different examples of services the access device may have access, including “data and/or a data processing service,” “a web page,” “processing application,” and “sales transactions.” Ex-1005, Buer, [0120]-[122], [0193]-[0195]. Buer further explains that “multiple sets of information (e.g.,

credentials) may be included on a single token to enable a user to access different services.” Ex-1005, Buer, [0127], [0177].

282. In my opinion, a POSITA would have found obvious that the different services would have had “different accessibility” based on the “key” or “credential” that may be “linked to a particular” service. In my opinion, a POSITA reading Buer would have understood that each of the keys or credentials stored in the access device would enable different applications, functions, or services, such that a first “key” or “credential” would be used to access, for example, data services, while a second “key” or “credential” would be used to access, for example, sales transactions.

8. Claim 11: “The hybrid device of claim 1, wherein the hybrid device is a cell phone.”

283. In my opinion, Buer discloses that “the hybrid device is a cell phone,” as recited in claim 11. For example, Buer discloses that the access device may be a mobile device, such as “a cellular phone.” Ex-1005, Buer, [0163].

9. Claim 15: “The method of claim 14, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on the hybrid device.”

284. In my opinion, Buer discloses that “at least one of the one or more of the application, the function, and the service is enabled at least in part on the hybrid device,” as recited in claim 15. See claim 2.

- 10. Claim 16: “The method of claim 14 further comprising: sending the enablement signal, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on a device external to the hybrid device and communicatively coupled to an external RDC.”**

285. In my opinion, Buer discloses “sending the enablement signal, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on a device external to the hybrid device and communicatively coupled to an external RDC,” as recited in claim 16. See claim 3.

- 11. Claim 17: “The method of claim 14, wherein the local, secured information includes biometric information for authenticating a user.”**

286. In my opinion, Buer discloses that “the local, secured information includes biometric information for authenticating a user,” as recited in claim 17. See claim 4.

- 12. Claim 18: “The method of claim 14, wherein the local, secured information includes financial information and wherein the one or more of the application, the function and the service completes a financial transaction.”**

287. In my opinion, Buer discloses that “the local, secured information includes financial information and wherein the one or more of the application, the function and the service completes a financial transaction,” as recited in claim 18. See claim 6.

13. Claim 19: “The method of claim 14, wherein the hybrid device is a cell phone.”

288. In my opinion, Buer discloses that “the hybrid device is a cell phone,” as recited in claim 19. *See* claim 11.

XI. Ground 4: Buer in view of Giobbi ’157 further renders obvious claims 4, 8-10, 12, 13, 17, and 20.

A. Claim 4: “The hybrid device of claim 1, wherein the local, secured information includes biometric information for authenticating a user.”

Claim 17: “The method of claim 14, wherein the local, secured information includes biometric information for authenticating a user.”

289. In my opinion, Buer and Giobbi ’157 renders obvious that “the local, secured information includes biometric information for authenticating a user,” as recited in claims 4 and 17.

290. Buer in view of Giobbi ’157 renders obvious claim 4 because the references discloses that the local, encrypted information is biometric information for authenticating a user. Buer, for example, discloses that its hybrid device may include “a biometric reader to further verify the authenticity of the user” using “biometric characteristic” such as “a fingerprint.” Ex-1005, [0114], [0181]. *See* Section X.B.3.

291. Giobbi ’157 further teaches storing “biometric profile” in a local, secured memory, so that a user would use “a matching biometric input” obtained from the hybrid device to “unlock” the tag memory. Ex-1006, Giobbi ’157, [0043].

As Giobbi '157 teaches, the biometric input would be used to compare “stored biometric information” to authenticate the user (e.g., fingerprint authentication). Ex-1006, Giobbi '157, [0028], [0037]-[0038], [0048].

292. In my opinion, a POSITA would have been motivated to include biometric information for authenticating a user in Buer’s local, tamper-resistant memory because doing so would promote Buer’s purpose of further restricting access to service until the user satisfies additional verification queries. Ex-1005, Buer, [0114], [0013], [0134].

293. In my opinion, a POSITA would have been capable of storing “biometric information for authenticating a user” in Buer’s memory, as Giobbi '157 teaches, because storing “biometric information for authenticating a user” in memory would require minimal modification without undue experimentation. Such a combination, in my opinion, would have been no more than combining prior art elements according to known methods to yield predictable results. A POSITA would further have had a reasonable expectation of success in storing “biometric information for authenticating a user” in Buer’s tamper-resistant memory.

B. Claim 8: “The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on an authorization of the financial information using an external authentication database, the financial information transmitted to the external authentication database.”

294. In my opinion, Buer and Giobbi ’157 renders obvious that “the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on an authorization of the financial information using an external authentication database, the financial information transmitted to the external authentication database,” as recited in claim 8.

295. Buer in view of Giobbi ’157 renders obvious claim 8, in my opinion, because Giobbi ’157 teaches that a financial transaction is completed based on an authorization of the financial information using an external authentication database. In Giobbi ’157, its external reader is communicatively coupled “to receive and/or transmit information to remote databases for remote authentication.” Ex-1006, Giobbi ’157, [0031], [0053]. According to Giobbi ’157, the remote databases include a “validation database ... for authorizing a transaction to be processed.” Ex-1006, Giobbi ’157, [0033]. For example, in Giobbi ’157, “the process involves transmitting credit card (or other purchasing information) to a validation database 112 to

authorize the purchase and receive the status of the card.” Ex-1006, Giobbi ’157, [0074].

296. In my opinion, a POSITA would have been motivated to implement Giobbi ’157’s validation database in Buer’s security processing system 1124 with the point-of-sale components because doing so would enhance Buer’s “credit card transactions,” Ex-1005, Buer, [0195]-[0196], to provide status information concerning whether “the card is active and not reported lost or stolen and that sufficient funds are present to execute the purchase,” Ex-1006, Giobbi ’157, [0074], which can only be verified using an external database. Accordingly, in my opinion, a POSITA would have been motivated to implement Buer’s external processing system with access to validation database to authorize the purchase and to “display[] status to a user.” Ex-1006, Giobbi ’157, [0026], [0074].

297. In my opinion, a POSITA would have been motivated to implement Buer’s external processing system with Giobbi ’157’s validation database, at least, because Buer and Giobbi ’157 are in the same field of endeavor—the field of incorporating RDC/PDK technology into hybrid devices to allow secure data sharing and services. Ex-1005, Abstract; Ex-1006, Giobbi ’157, [0026]. Likewise, a POSITA would recognize that Buer and Giobbi ’157 use similar techniques to solve the same problem.

298. In my opinion, a POSITA would have been capable of coupling one or more external databases to Buer's external processing system because Buer and Giobbi '157 use similar hardware, and the combination would require minimal modification without undue experimentation. Ex-1005, Buer, [0114], [0125], [0163]; Ex-1006, Giobbi '157, [0030], [0035]. Such a combination, in my opinion, would have been no more than combining prior art elements according to known methods to yield predictable results. A POSITA would further have had a reasonable expectation of success in integrating those components into Buer because Giobbi '157 explains how to do so via a network.

C. Claim 9: “The hybrid device of claim 8, wherein the external authentication database is separate from a merchant providing a sale in the financial transaction.”

299. In my opinion, Buer and Giobbi '157 renders obvious that “the external authentication database is separate from a merchant providing a sale in the financial transaction,” as recited in claim 9.

300. Buer in view of Giobbi '157 renders obvious claim 9, in my opinion, because Giobbi '157 discloses that “in purchase transactions, the validation database 112 is a credit card validation database that is separate from the merchant providing the sale.” Ex-1006, Giobbi '157, [0033].

D. Claim 10: “The hybrid device of claim 1, wherein the one or more of the application, the function and the service enabled based on the local, secured information stored by the integrated, secure memory includes a first application, function or service based on a first subsets of local, secured information stored by the integrated, secure memory and a second application, function or service based on a second subset of local, secured information, the first and second subset of local, secured information having different accessibility.”

301. In my opinion, Buer and Giobbi '157 renders obvious that “the one or more of the application, the function and the service enabled based on the local, secured information stored by the integrated, secure memory includes a first application, function or service based on a first subsets of local, secured information stored by the integrated, secure memory and a second application, function or service based on a second subset of local, secured information, the first and second subset of local, secured information having different accessibility,” as recited in claim 10.

302. In my opinion, Buer in view of Giobbi '157 renders obvious that a different application, function, or service is enabled based on different subsets of local, secured information. Buer, for example, teaches that the access device “may include a database (not shown) that matches a given token (or information from the token) with one or more default services,” and the access device may “automatically request the services” based on which token is within its proximity zone. Ex-1005, Buer, [0115], [0143]. According to Buer, a stored key on the access device “may be linked to a particular user, application, etc.” Ex-1005, Buer, [0177].

303. Giobbi '157 further teaches storing multiple user profiles, such as biometric profile, PIN profile, picture profile, registry profile, credit cards, and personal information, in its secured and tamperproof memories. Ex-1006, Giobbi '157, [0037]-[0042], [0058]. Each of the profiles in Giobbi '157 provides a different accessibility to certain application, function, or service. For instance, one profile in Giobbi '157 may be used to enable “access to secure physical or digital assets,” and another profile may be used for completing a purchase transaction. Ex-1006, Giobbi '157, [0063].

304. In my opinion, a POSITA would have been motivated to implement Buer's database to store multiple profiles, as Giobbi '157 teaches, because doing so would allow Buer to securely store information from multiple tokens to enable different accessibility of applications based on the linked tokens. Ex-1005, Buer, [0115], [0143]; Ex-1006, Giobbi '157, [0037]-[0042], [0058].

305. In my opinion, a POSITA would have been motivated to implement Buer's database to store multiple profiles, at least, because Buer and Giobbi '157 are in the same field of endeavor—the field of incorporating RDC/PDK technology into hybrid devices to allow secure data sharing and services. Ex-1005, Abstract; Ex-1006, Giobbi '157, [0026]. Likewise, a POSITA would recognize that Buer and Giobbi '157 use similar techniques to solve the same problem.

306. In my opinion, a POSITA would have been capable of storing multiple profiles in Buer's database because Buer and Giobbi '157 use similar hardware, and the combination would require minimal modification without undue experimentation. Such a combination, in my opinion, would have been no more than combining prior art elements according to known methods to yield predictable results. A POSITA would further have had a reasonable expectation of success in integrating those components into Buer because Giobbi '157 explains how to do so.

E. Claim 12: “The hybrid device of claim 1, wherein the at least one external device is included in jewelry.”

307. In my opinion, Buer and Giobbi '157 renders obvious that “the at least one external device is included in jewelry,” as recited in claim 12.

308. Buer teaches that its external token (PDK) 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-1005, Buer, [0130]. Giobbi '157 further teaches that a PDK “can be integrated into commonly carried items,” such as “jewelry items such as watches, rings, necklaces or bracelets.” Ex-1006, Giobbi '157, [0035]. In my opinion, it would have been obvious in view of Buer's disclosure of including a PDK in a wearable, such as a badge, to include the external PDK in other wearables, like jewelry, as Giobbi '157 teaches.

309. Further, in my opinion, a POSITA would also be motivated to combine these references at least because Giobbi '157 and Buer are in the same field of endeavor as the '289 patent (for example, the field of incorporating RDC/PDK technology into hybrid devices). Likewise, a POSITA would recognize that Giobbi '157 and Buer use similar techniques to solve the same problem as the '289 patent—as discussed throughout this Petition—and the Giobbi '157 and Buer references integrate PDKs and RDCs into hybrid devices in the same manner claimed by the '289 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 jewelries such as watches and necklaces, and Buer already contemplates including its PDK in a wearable.

F. Claim 13: “The hybrid device of claim 1, wherein the at least one external device is a watch.”

310. In my opinion, Buer and Giobbi '157 renders obvious that “the at least one external device is a watch,” as recited in claim 13. *See* claim 12.

G. Claim 20: “The method of claim 14, wherein the external PDK is included in a watch.”

311. In my opinion, Buer and Giobbi '157 renders obvious that “the external PDK is included in a watch,” as recited in claim 20. *See* claim 12.

XII. Ground 5: Claim 4 Would Have Been Obvious Over Buer And Nishikawa

A. Claim 4: “The hybrid device of claim 1, wherein the local, secured information includes biometric information for authenticating a user.”

312. In my opinion, Buer and Nishikawa renders obvious that “the local, secured information includes biometric information for authenticating a user,” as recited in claim 4.

313. In my opinion, Buer discloses a cellular phone storing local, secured information. *See* Section X.A.1.c. Nishikawa further discloses improving a “cellular phone” with capability of “be[ing] loaded with multiple applications, such as electronic money, an electronic ticket, a fingerprint template, a fingerprint collating engine and a personnel ID card.” Ex-1014, Nishikaway, [0111]. As Nishikawa explains, “[f]ingerprint data (biometric data) on the finger print of a special user ... is stored in the SIM [card]” of a cellular phone to authenticate the user “on the basis of biometric data.” Ex-1014, Nishikawa, [0073], [0114].

314. In my opinion, a POSITA would have been motivated to adapt Buer’s cellular phone to load multiple applications on a SIM card, as Nishikawa teaches, to improve the convenience of Buer’s cellular phone and to add additional capability, including the ability to store biometric information in addition to credit card information, and to use the standard size and shape of a conventional SIM card to

introduce additional features. Ex-1014, Nishikawa, [0111]; Ex-1013, Bella, 3:34-4:4, 11:15-27.

315. In my opinion, a POSITA would have also been motivated to improve authentication of the user of the cellular phone, which furthers Buer's express teaching on using a biometric to add an additional layer of authentication. Ex-1014, Nishikawa, [0111], [0073]; Ex-1005, Buer, [0114].

316. Further, in my opinion, a POSITA would have recognized that Buer and Nishikawa are in the same field of endeavor and use similar techniques to solve the same problem.

317. In my opinion, a POSITA would have been capable of adapting Buer's cellular phone to store biometric information on its SIM card, because Buer and Nishikawa use similar hardware, and the combination would require minimal modification without undue experimentation. Ex-1005, Buer [0114], [0125], [0163]; Ex-1014, Nishikawa, [0004]-[0013]. Such a combination, in my opinion, would have been no more than combining prior art elements according to known methods to yield predictable results. A POSITA would further have had a reasonable expectation of success in integrating those components into Buer because Nishikawa explains how to do so.

XIII. Conclusion

318. Based on my review and above analysis of the prior art, it is my opinion that claims 1-20 of the '289 patent are invalid.

319. I declare under penalty of perjury that the foregoing is true and correct. I declare that all statements made herein of my knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed this Friday, April 19, 2024.

/s  _____

APPENDIX A

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, [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 2nd 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, Quester 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.

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

Case	Venue	Case Number
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