

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS AMERICA, INC.,
Petitioner,

v.

PROXENSE, LLC
Patent Owner

Case No. IPR2021-01438
U.S. Patent No. 9,049,188 B1

**DECLARATION OF CHARLES ELDERING, Ph.D.
EXHIBIT 2009**

TABLE OF CONTENTS

I.	INTRODUCTION	- 1 -
II.	PROFESSIONAL BACKGROUND AND EXPERIENCE.....	- 1 -
III.	SCOPE OF ENGAGEMENT	- 3 -
IV.	SUMMARY OF OPINIONS.....	- 5 -
V.	LEGAL STANDARDS	- 6 -
A.	Burden of Proof.....	- 6 -
B.	Claim Construction	- 7 -
C.	Person of Ordinary Skill in the Art	- 7 -
VI.	LEVEL OF ORDINARY SKILL IN THE ART	- 8 -
VII.	TECHNOLOGY BACKGROUND.....	- 9 -
VIII.	OVERVIEW OF THE ‘188 AND ’700 PATENTS	- 10 -
IX.	CLAIMS AT ISSUE.....	- 13 -
A.	Claim Construction	- 17 -

I. INTRODUCTION

1. My name is Charles Eldering. I am over the age of 18, of sound mind, and am not otherwise disqualified from making this Declaration. I have personal knowledge of the facts contained in this Declaration and am competent to testify on the matters set forth below.

2. I have been retained by Patent Owner Proxense, LLC (“Proxense” or “Patent Owner”) and have been asked to provide my opinions on certain issues relating to the validity of U.S. Patent Nos. 9,049,188 and (“the ‘188 Patent) and 9,235,700 (“the ‘700 Patent”) and Petitioner Samsung Electronics America Inc.’s (“Samsung” or “Petitioner”) Petition for Inter Partes Review of that patent in IPR2021-01438 and IPR2021-01439.

II. PROFESSIONAL BACKGROUND AND EXPERIENCE

3. My qualifications are stated more fully in my *curriculum vitae*, a copy of which is provided at Exhibit 2010.

4. I have been working in the field of electrical engineering since at least 1989 when I received my Ph.D. in electrical engineering from the University of California at Davis. Prior to that I worked in the field of microelectronics as a physicist in the U.S. Air Force, working at the Rome Air Development Center (RADC) in the area of microelectronics reliability.

5. Subsequent to receiving my Ph.D. I worked in the telecommunications

field for Alcatel and then General Instrument corporation and Next Level Communications (which was acquired by General Instrument). At General Instrument I was involved in the use of the DigiCipher 2 (DCII) encryption technology which was used by the company to protect digital content on satellite and Community Access Television (CATV) networks.

6. Subsequent to my work in telecommunications I founded two companies, Expanse Networks, and Technology, Patents, and Licensing, Inc. (“TPL”). Expanse Networks was involved with the development of targeted advertising solutions for television networks, and TPL provided patent portfolio management services for a variety of clients ranging from startups to Fortune 500 companies, as well as performing research in a select number of areas. The targeted television assets of Expanse Networks were purchased in 2004, and TPL was retained to manage and expand the Expanse Networks patent portfolio. Some of the subsequent inventions are related to Digital Rights Management (“DRM”).

7. At TPL I frequently worked on patents related to DRM, watermarking, encryption and decryption, digital signatures, and Radio Frequency Identification (“RFID”). This work included analysis of the patents, as well as review of product literature and product to determine if the claimed technology was in use. When required, we acquired representative products and performed teardowns.

8. While at TPL I also conducted a research program in RFID systems. As a result of this work TPL filed a number of patents on inventions in the RFID field. These patents were successfully monetized through a portfolio sale in 2011.

9. As an entrepreneur I have founded and managed a number of technology and intellectual property companies, successfully monetizing the assets of three of those entities. As an inventor I have over 150 issued US patents. As a technologist and patent specialist I am a published author in the fields of telecommunications, microelectronics, patents, and public policy.

III. SCOPE OF ENGAGEMENT

10. I have been retained by Patent Owner to provide an analysis and opinions regarding the '188 and '700 Patents.

11. I understand that Dr. Wolfe has been retained by Petitioner to offer an opinion related to the validity of certain of the claims of the '188 and '700 Patents. *See* Wolfe Declaration ¶ 1. I have been asked to consider the opinions of Dr. Wolfe and provide my opinions on the teachings of the references cited by Dr. Wolfe and Petitioner, as well as the meaning of terms used in the claims and defined in the specifications of '188 and '700 Patents as they would be understood by those of ordinary skill in the art. I provide this testimony below.

12. The opinions expressed herein are my own opinions. They are based on my own education, experience, knowledge, and the documents I have reviewed

in advance of and while preparing this Declaration. These citations are meant to be exemplary, and not exhaustive. My conclusions or opinions are supported not only by the cited sources.

13. As of the date of this Declaration I have reviewed at least the following materials:

Exhibit No.	Material
Ex. 1001	‘700 patent
Ex. 1002	‘700 patent file history
Ex. 1003	Declaration of Dr. Wolfe (‘700) patent
Ex. 1004	Gobbi ‘157 Patent
Ex. 1005	Gobbi ‘139 Publication
Ex. 1006	Dua
Ex. 1007	Broadcom
Ex. 1001 – IPR 2021-1438	‘188 patent
Ex. 1002 – IPR 2021-1438	‘188 patent file history
Ex. 1003 – IPR 2021-1438	Declaration of Dr. Wolfe (‘188 patent)
Paper 2 – IPR 2021-1439	‘700 petition
Paper 1 – IPR 2021-1438	‘188 petition
Paper 9 – IPR 2021-1439	Patent Owner Preliminary Response (‘700 patent)
Paper 10 – IPR 2021-1438	Patent Owner Preliminary Response (‘188 patent)

Ex. 2010	Eldering C.V.
Ex. 2008	Markman Ruling (US District Court WDTX)
Ex. 2007	Markman Transcript (US District Court WDTX)

14. In addition, I have reviewed any other materials cited or relied on herein even if not listed in the above table. In reaching my opinions, I have also relied on my personal knowledge and experience in telecommunications, microelectronics, encryption and security, and RFID and the ‘188 and ‘700 Patents’ relevant fields of invention.

15. I am being compensated for my time spent in this matter at a rate of \$475.00 per hour plus reasonable expenses incurred in connection with my testimony. This compensation is not dependent on the opinions I provide or the outcome of this proceeding and is not otherwise contingent in any way on the issues involved in this matter. I have no financial interest in the case.

IV. SUMMARY OF OPINIONS

16. As expressed herein and described further below, it is my opinion that the combined teachings of the references cited by Dr. Wolfe and Petitioner fail to show all elements of the claims 1-20 of the ‘188 Patent and claims 1-20 of the ‘700 Patent.

17. It is also my opinion that “local secured information” as used in the

claims of the ‘188 and ‘700 Patents is explicitly defined in the specifications of the ‘188 and ‘700 Patents to as a “service block accessed by an access key provided to a PDK containing the service block.”

18. It is also my opinion that “enabling one or more of an application, a function, and a service” as used in the claims of the ‘188 and ‘700 Patents is explicitly defined in the specifications of the ‘188 and ‘700 Patents to mean “a memory controller of a PDK permitting access to service block of the PDK based on the PDK being provided an access key corresponding to the service block to be accessed.”

V. LEGAL STANDARDS

19. In this section, I address my understanding of various legal principles regarding validity of a United States patent. I am not an attorney, and my understanding of the legal principles are based on my experience as an expert as well as explanations from counsel.

A. Burden of Proof

20. I understand that an issued United States Patent is presumed valid by statute and that the party challenging the validity of an issued United States Patent bears the burden of proof to demonstrate that such patent is invalid. I understand that in the context of an *Inter Partes* Review, a petitioner bears the burden to prove invalidity by a preponderance of the evidence. I understand this is a different legal

standard than a District Court litigation, where the challenger of a patent's validity is required to prove its case by clear and convincing evidence. I have applied the preponderance of the evidence standard to my opinions as expressed in this Declaration.

B. Claim Construction

21. I understand that terms within a patent claim should be given their plain and ordinary meaning to a POSITA at the time of the invention. I understand that the plain and ordinary meaning is determined from the language of the claims, the written description, and the prosecution history of the patent at issue. I understand that an inventor can act as his or her own lexicographer, ascribing a specific meaning to claim terms.

22. Counsel has also advised me that a claim construction order has been issued in a parallel district court proceeding (US District Court WDTX, 6:21-CV-00210-ADA). I have considered and incorporated that claim construction in my analysis.

C. Person of Ordinary Skill in the Art

23. I understand that an important consideration when evaluating a patent's validity is the level of ordinary skill in the relevant art. For example, in determining how much technical information is taught by a particular reference, that reference's disclosure should be considered from the perspective of a

POSITA. Similarly, when evaluating the disclosure of the patent at issue, the understanding of a POSITA is taken into account.

24. I understand that several factors are considered in determining the level of ordinary skill in the art, including the educational level of active workers in the field, the types of problems encountered in the art, the nature of prior art solutions to those problems, prior art patents and printed publications, the activities of others, the sophistication of the technology involved, and the rapidity of innovations in the field.

VI. LEVEL OF ORDINARY SKILL IN THE ART

25. I understand that Petitioner and Dr. Wolfe contend that a person of ordinary skill in the art (“POSITA”) at the time of the invention of the ‘700 Patent “would have had a bachelor’s degree in electrical engineering (or an equivalent degree) with at least three years of experience in the field of encryption and security (or equivalent experience)” or “more education could compensate for less experience and vice versa.” Pet. 4-5 (citing Wolfe Decl. ¶ 23).

26. Dr. Wolfe maintains that a POSITA would have had a bachelor’s degree in computer or electrical engineering (or an equivalent degree) with at least three years’ experience in the field of encryption and security (or equivalent experience). I agree with the level of education proposed by Dr. Wolfe, but disagree with the field of experience, which I believe should be any of the fields

of microelectronics, RFID, or encryption and security.

27. I am at least a person of ordinary skill in the art with respect to this matter.

28. For the purposes of offering my opinions on the issues herein, I have applied this definition of a POSITA. I am familiar with the knowledge and capabilities of one of ordinary skill in this area based on my experience working with other engineers. In addition, I personally met this definition of a POSITA at the time of invention and the opinions offered herein are from the viewpoint of a POSITA.

VII. TECHNOLOGY BACKGROUND

29. I have reviewed the '188 Patent and '700 Patent and the descriptions of the '188 Patent and '700 Patent contained in the Petitions and Dr. Wolfe's declarations. To the extent I do not specifically opine on something raised in the Petitions or Dr. Wolfe's declarations, that does not mean I agree with the point or issue. While I disagree with aspects of Petitioner's and Dr. Wolfe's descriptions of the '188 and '700 Patents, those aspects are not germane to the issues I address in this Declaration, other than as specifically indicated in this Declaration.

30. Please note all citations made in this Declaration are with respect to the '700 Patent, which shares a common specification with the '188 Patent.

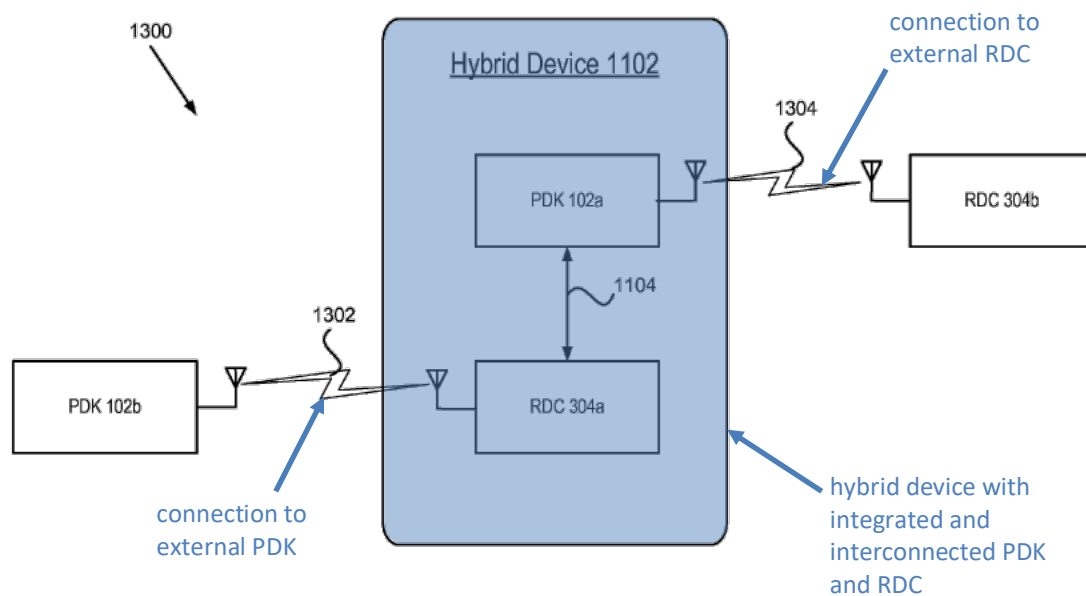
VIII. OVERVIEW OF THE ‘188 AND ‘700 PATENTS

31. The ‘700 Patent is titled “Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use” and issued from Application No. 14/677,893 (the 893 Application), which was filed on April 2, 2015. Through a series of continuation applications, it claims priority to U.S. Provisional Application No. 60/992,953 filed on Dec. 6, 2007.

32. The ‘188 Patent is titled “Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use” and issued from Application No. 14/171,705 (the 705 Application), which was filed on Feb. 3, 2014. Through a series of continuation applications, it claims priority to U.S. Provisional Application No. 60/992,953 filed on Dec. 6, 2007.

33. Claims 1-9 and 20 of the ‘188 Patent and claims 1-10 of the ‘700 Patent recite “hybrid” devices containing both a personal digital key (PDK) and receiver-decoder circuit (RDC) that are coupled for communication with each other. Similarly, claims 10-19 of the ‘188 Patent and claims 11-20 of the ‘700 Patent recite methods utilizing hybrid devices including an integrated PDK and an integrated RDC. The internal PDK of the hybrid devices can communicate with an external RDC, and the internal RDC can communicate with external PDKs. FIG. 13 of both the ‘188 Patent ‘700 Patent, reproduced below (with a box around the Hybrid Device and annotations regarding the various connections), illustrates

the structure of the hybrid device recited in claims 1-20 of the '188 Patent and claims 1-20 of the '700 Patent.



34. Because of the unique structure and nature of the hybrid device recited in claims 1-20 of the '188 Patent and claims 1-20 of the '700 Patent, the collectively claimed devices and methods enable applications, functions or services based on local, secured user information. As discussed below, the methods and devices presented in claims 1-20 of the '188 Patent and claims 1-20 of the '700 Patent utilize a control logic implemented by a controller the integrated PDK to select and permit access to service blocks based on access keys provided

to the PDK, thereby enabling independent authorizations from external PDKs in communication with the integrated RDC and/or to external RDCs in communication with the integrated PDK. ‘188 Patent, claim 1 (“one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service”); ‘700 Patent, claim 1 (“one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service”); ‘188 Patent, claim 10 (“generating an enablement signal enabling one or more of an application, a function, and a service”); and ‘700 Patent, claim 11 (“generating an enablement signal enabling one or more of an application, a function, and service”). Alternatively, the claimed methods and devices permit “daisy chained authorizations,” in which the integrated PDK and integrated RDC collectively enable an application, a function or a service, such as a parent authorizing a child to authorize a purchase an item. *Id.*

35. In summary, the hybrid devices recited in claims 1-20 of the ‘188 Patent and claims 1-20 of ‘700 Patent allow for enabling applications, functions, and services based on local, secured user information, through use of an integrated PDK in communication with an external RDC and/or an integrated RDC in communication with an external RDC.

IX. CLAIMS AT ISSUE

36. I understand Petitioner is challenging the validity of claims 1-20 of the '188 Patent. Claims 1 and 10 are independent claims and are reprinted below.

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

6	The hybrid device of claim 1, wherein the integrated PDK stores local, secured financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information.
7.	The hybrid device of claim 1, wherein the hybrid device is a cell phone.
8.	The hybrid device of claim 1, wherein the external PDK is included in jewelry.
9.	The hybrid device of claim 1, comprising a storage for inheritance information.
10pre	A method comprising:
10A	creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external personal digital key (PDK),
10B	the hybrid device including an integrated PDK and the integrated RDC,
10C	wherein the integrated PDK stores local, secured biometric information for authenticating a user,

10D	receiving a first signal at the integrated RDC via the first wireless link from the external PDK;
10E	generating an enablement signal enabling one or more of an application, a function and a service.

37. I understand Petitioner is also challenging the validity of claims 1-20 of the '700 Patent. Claims 1 and 11 are independent claims and are reprinted below.

Claim	U.S. Patent No. 9,235,700
1pre	A hybrid device comprising:
1A	an integrated personal digital key (PDK) for storing local, secured financial information a user and capable of communicating wirelessly with an external receiver-decoder circuit (RDC); and
1B	an integrated RDC for communicating wirelessly with at least one external PDK within a proximity zone,
1C	the integrated RDC coupled to the integrated PDK by a first signal line for communication,
1D	the integrated RDC coupled to at least one other component of the hybrid device by a second signal line,
1E	one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service.
2	The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on the hybrid device.

3	The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on a device external to the hybrid device and communicatively coupled to the external RDC.
4	The hybrid device of claim 1, wherein the integrated PDK includes local, secured biometric information for authenticating a user, the biometric information based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a photograph, a signature, a voice sample, DNA and RNA.
5	The hybrid device of claim 1, wherein the external PDK stores local, secured financial information.
6	The hybrid device of claim 1, wherein the integrated PDK stores local, secured financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information.
7.	The hybrid device of claim 1, wherein the hybrid device is a cell phone.
8.	The hybrid device of claim 1, wherein the external PDK is included in jewelry.
9.	The hybrid device of claim 1, comprising a storage for inheritance information.
10	The hybrid device of claim 1, wherein the external PDK is included in a watch
11pre	A method comprising:
11A	creating a first wireless link between an integrated receiver- decoder circuit (RDC) of a hybrid device and an external personal digital key (PDK),

11B	the hybrid device including an integrated PDK and the integrated RDC,
11C	wherein the integrated PDK stores local, secured financial information,
11D	receiving a first signal at the integrated RDC via the first wireless link from the external PDK;
11E	generating an enablement signal enabling one or more of an application, a function and a service.

38. I understand that the ‘188 Patent has the same specification and is in the same patent family as the ‘700 Patent. I understand that Samsung has petitioned for an *Inter Partes* Review of the ‘188 and ‘700 Patents, which were instituted. I have submitted a copy of this declaration in connection with both IPRs.

A. Claim Construction

39. I understand that Dr. Wolfe saw “no reason to disagree” with Samsung’s position that “no constructions are necessary to resolve this petition.” Wolfe Decl., Para. 27. I disagree. Claims 1 and 10 of the ‘188 Patent and claims 1 and 10 of the ‘700 Patent each recite “local secured memory” and “enabling one or more of an application, a function, and a service.” The shared specification of the ‘188 and ‘700 Patents explicitly defines these terms. These terms, therefore, must be construed at least to the extent of interpreting them consistent with the

definitions provided in the shared specification.

40. Furthermore, the Hon. Alan Albright, in the Western District of Texas, construed the terms as follows, in Proxense’s favor, following briefing and a *Markman* hearing:

Term	Court’s Construction
“hybrid device” (Claims 1-12, 15, 20)	A device comprising an integrated personal digital key (PDK) and an integrated receiver-decoder circuit.
“Personal digital key” (Claims 1, 10).	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” (Claims 1, 4, 10, 13).	No construction necessary, plain and ordinary meaning.
“financial information” (Claims 5, 6, 14, 17).	No construction necessary, plain and ordinary meaning.
“receiver-decoder circuit” (Claims 1, 10).	A component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing.
“inheritance information” (Claims 9, 18).	Information passed from a first device to a second device for use by the second device.
“enablement signal” (Claims 10-12, 17)	No construction needed.

41. As I discuss below, Dr. Wolfe consistently takes liberties with the term “hybrid” and labels prior art as containing “hybrid” structures simply because they have an integrated PDK or RDC, disregarding elements recited in the claims

defining an integrated PDK of a hybrid device. As indicated above, the Court in the Western District of Texas has defined the term “hybrid device” as a “device comprising an integrated personal digital key (PDK) an integrated receiver-decoder circuit [(RDC)].” Such a construction flows naturally from claim 1 of the ‘188 Patent and claim 1 of the ‘700, each of which recite “a hybrid device comprising: an integrated personal digital key (PDK)... and an integrated RDC.” The construction is also necessitated by claim 10 of the ‘188 Patent and claim 11 of the ‘700 each reciting “the hybrid device including the integrated PDK and the integrated RDC.” Claims 1 and 10 of the ‘188 Patent and claims 1 and 11 of the ‘700 Patent go onto further define the integrated PDK. Dr. Wolfe fails to establish that what he identifies as “hybrid devices” contain all the elements of an integrated PDK recited claims 1 and 10 of the ‘188 Patent and claims 1 and 11 of the ‘700 Patent.

42. For instance, Dr. Wolfe suggests that the information stored in the PDKs of the prior art is equivalent to the “local, secured financial information” recited in claims 1 and 11 of the ‘700 Patent and the “local, secured biometric information” recited in claims 1 and 10 of the ‘188 Patent. The shared specification of the ‘188 and ‘700 Patents explicitly defines “local secured information” three times as information stored within **service blocks of the integrated PDK accessed by corresponding service block access keys**. *See* ‘700 Patent, 3:34-41

(“The PDK 102 includes multiple service blocks 112A-N as described in more detail in FIG. 2. Each service block 112 is accessed using a corresponding service block access key 118. In this example, the sensor 108 contains three of the service block access keys 118A, D, F. The service block access keys 118 allow the sensor 108 to unlock information stored in the corresponding service blocks 112, *which information is used as local secured information.*” (Emphasis added.)); 5:46-54 (“The service blocks 112 can be used for purposes other than user authentication. For example, information used or produced by an application 120 can be transferred back and forth to the corresponding service block 112. That is, each service block 112 can be used as *a local secure memory for the corresponding application 120.* Thus, a service 120B may store certain sensitive information in service block 112B, and a separate service 120C will not be able to access that information without the corresponding access key 118B.” (Emphasis added.)); and 8:64-9:3 (“These two examples illustrate basic concepts of the capabilities of the service blocks and how an application (service) may use them. Since service blocks preferably are both readable and writable, services may use them as they see fit (i.e. debit, username/password, credit card information, etc.). In some sense, *the service block acts as a secure local memory on the PDK.*” (Emphasis added.)).

43. The first time the shared specification defines the term “local secure information” as information stored within service blocks of the integrated PDK

accessed by corresponding service block access keys, it is done as the shared specification introduces a PDK utilizing FIG. 1 to assist the reader in understanding the PDK and its operable relationship with respect to other components. As noted with respect to FIG. 1, “in this example, the sensor 108 contains three of the service blocks access keys 118A, D, F.” ‘700 Patent, 3:37-38. True to this statement, sensor 108 in FIG. 1 is shown as having three keys. The sensor need not hold any service block access keys 118. For instance, FIG. 6 shows five sensors 108V, W, X, Y, Z each lacking a service block access key 118. Rather, the service block access keys 118 are held by applications 120V, W, X, Y1, Y2, Z1, Z2, Z3. A person of ordinary skill in the art, therefore, would understand “in this example” as referencing the number of access keys 118 held by sensor 108 -- *not* a general statement regarding “local secure memory” defined in the subsequent sentence.

44. The previously two sentences and subsequent sentences, however, would be understood by a person skilled in the art as making general statements regarding PDK. The statement “the PDK 102 includes multiple service blocks 112A-N as described in more detail in FIG. 2,” appearing at col. 3, lines 34-35, would be understood as defining the PDK as comprising at least one service block. Additionally, it would be understood that a more detailed description of the service blocks is provided subsequently in the shared specification.

45. From the following statement that “each service block 112 is accessed using a corresponding service block access key 118,” appearing at col. 3, lines 35-36, a person skilled in the art would understand that service blocks 112 are secured by access keys 118. Reinforcing this understanding, the final sentence of the paragraph begins by stating “the service blocks access keys 118 allow the sensor to unlock information stored in the corresponding service blocks.” ‘700 Patent, 3:38-40. The final clause of the sentence, “which information is used as local secured information,” appearing at col. 3, lines 40-41, would be understood by those of ordinary skill in the art as defining local secure memory as the information stored within service blocks of the integrated PDK accessed by corresponding service block access keys.

46. The second time the shared specification defines the term “local secure information” as information stored within service blocks of the integrated PDK accessed by corresponding service block access keys, it is immediately following examples in which the local secured information held within the service block is user authentication information. The statement made at col. 5, lines 46-47, that “the service blocks 112 can be used for purposes other than user authentication” would be understood as indicating service blocks 112 are capable of holding other types of information. The following sentence, appearing at col. 5, lines 47-49, confirms this understating by stating, “For example, information

used or produced by an application 120 can be transferred back and forth to the corresponding service block 112.” Given that the service blocks are previously detailed as being accessed using an access key, a person skilled in the art would understand that the information transferred to and/or from the service blocks by the application 120 would be local secured information. The subsequent sentence, at col. 5, lines 49-51, reiterates and confirms this understanding: “That is, each service block can be used as a *local secure memory* for the corresponding application 120.” As service blocks are accessed using the corresponding service blocks access keys, it would be understood that to access the local secure information stored in a particular service block an application would have to have the corresponding key. As to leave little doubt in the reader’s mind, the following sentence appearing at col. 5, lines 51-54, states, “Thus, a service 120B may store certain sensitive information in service block 112B, and a separate service 120C will not be able to access that information without the corresponding access key 118B.” The remainder of the paragraph further drives this point home. This redundancy would reinforce to those of ordinary skill in the art that local secure information is defined in the shared specification as information stored within service blocks of the integrated PDK accessed by corresponding service block access keys.

47. The third time the shared specification defines the term “local secure

information” as information stored within service blocks of the integrated PDK accessed by corresponding service block access keys follow the presentation of even more examples which “illustrate the basic concepts of the capabilities of the service blocks and how an application (service) may use them.” ‘700 Patent, 8:64-66. Here it is reiterated that service blocks may be readable and writeable and may hold diverse information. ‘700 Patent, 8:66-9:1. The definition of local secure information as information stored within service blocks of the integrated PDK accessed by corresponding service block access keys is then briefly reiterated when the shared specification states: “In some sense, the service block act as a secure local memory on the PDK”.

48. Given these repeated reiterations, which are not limited to embodiments but are global in scope, a person skilled in the art would understand “local secure information” as being defined in the shared specification as information stored within service blocks of the integrated PDK accessed by corresponding service block access keys.

49. In addition to the repeated reiterations, a person of ordinary skill in the art would understand the definition of “local secure information” as information stored within service blocks of the integrated PDK accessed by corresponding service block access keys to be consistent with the definition of PDK provided in the shared specification. At col. 14, lines 4-7, the shared

specification states: “In a minimal embodiment, the PDK102a includes an antenna and a transceiver for communicating with a RDC (not shown) and a controller and memory for storing information particular to a user.” Consistent with this statement, the Hon. Alan Albright in the case pending before him in the Western District of Texas construed a PDK as “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.” The term “controller”, however, was not construed, as I understand the parties did not raise this term for construction by the Court. It is my opinion, however, that a “controller” in the context of memory for storing information particular to a user would be understood by those skilled in the art as a digital circuit and associated software/firmware for managing the read and write operations through control logic.

50. The control logic implemented by the controller is detailed at col. 6, lines 43-59, with reference to FIG. 2 to assist the reader in understanding. There it is stated:

“Regardless of how created, once created, external applications (such as applications 120 in FIG. 1) can gain access to a specific service block 112 by proving the corresponding access key 118. In FIG. 2, this is shown conceptually by control logic 250. The wireless application 260 on the PDK 102 communicates to the sensor (not shown in FIG.

2) via transceiver 270. The wireless application provides a service block select 226 and a service block access key 118 in order to store, retrieve and/or modify data in a service block 112. The selector 252 selects a service block 112 based on the select signal 226 and the access key 118. The encryption engine 254 encrypts/decrypts data 228 flowing to/from the service block 112 based on the access key 118 (or some other key generated based on the access key, for example a session key). In an alternate method, the service block 112 may be selected based on the service block access key 118, eliminating the need for a separate select signal 226.”

51. The flow of the foregoing process is reflected in the figure below:

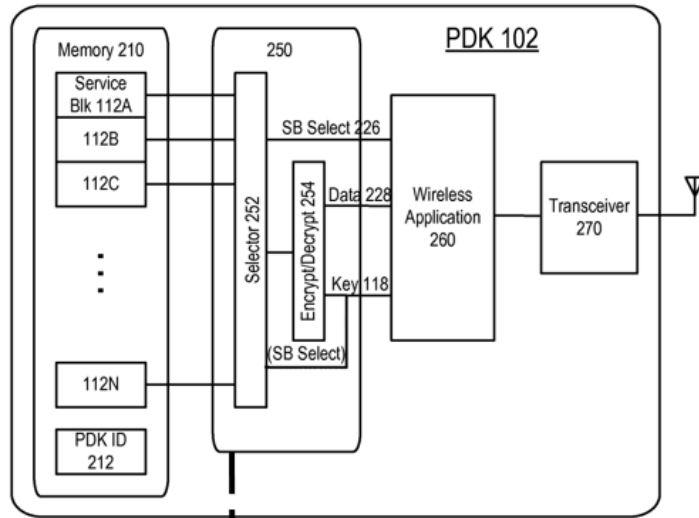
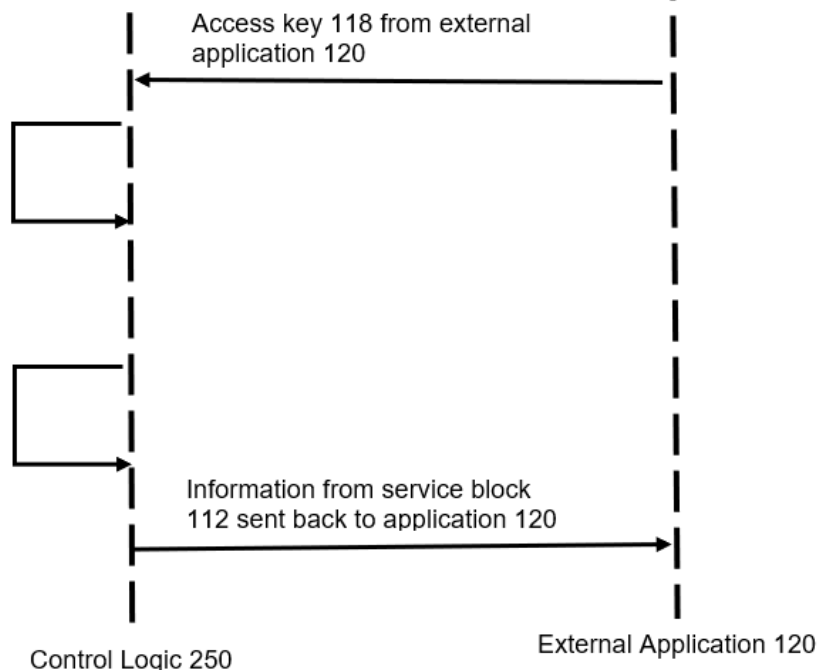


FIG. 2

"The selector 252 selects a service block 112 based on the select signal 226 and the access key 118." 6:52-53... "In an alternate method, the service block 112 may be selected based on the service block access key 118, eliminating the need for a separate select signal 226." 6:57-59.

"The encryption engine 254 encrypts/decrypts data 228 flowing to/from the service block 112 based on the access key 118 (or some other key generated based on the access key, for example a session key)." 6:54-57

"external applications (such as applications 120 in FIG. 1) can gain access to a specific service block 112 by providing the corresponding access key 118." 6:43-46... "The wireless application provides a service block select 226 and a service block access key 118 in order to store, retrieve and/or modify data in a service block 112." 6:49-51



Flow of Control Logic 250 Presented in Col. 6, Lines 43-59

52. As shown above and detailed in col. 6, lines 43-59, the control logic 250 implemented by a controller of the PDK provides access to store, retrieve, and/or modify data held within in a service block upon receipt of a corresponding access key.

53. Consistent with the minimal embodiment of a PDK noted above, the PDK 102 detailed in FIG. 2, “comprises a memory 210, control logic 250, wireless application 260 and a transceiver 270.” ‘700 Patent, 5:63-65. The minimal embodiment is detailed as containing “an antenna and a transceiver for communicating with a RDC,” which requires some instructions directing communications with the RDC via the transceiver. Such instructions are provided by wireless application 260. ‘700 Patent, 6:47-49 (“The wireless application 260 on the PDK 102 communicates to the sensor (not shown in FIG. 2) via transceiver 270.”). These instructions need not be a formal application. Furthermore, the encryption / decryption functionality may be omitted; especially if a secure communication between the PDK and RDC is utilized. Thus, “in other embodiments, the PDK 102a includes less functionality than that described above with reference to FIG. 2.” ‘700 Patent 14:2-4. Taking away wireless application 260 and encryption engine 254, antenna and transceiver 270 and control logic 250 are implemented by a controller and memory 210. The control logic 250, therefore, is a component of the minimal PDK detailed at col. 14, lines 4-8.

54. Aside from explicitly defining the term three times, the shared specification makes no other mention of “local secured information”. Accordingly, the shared specification only uses “local secured memory” to reference service blocks storing information which is accessed with a corresponding service block access key provided to the PDK. Additionally, the only description of a controller, necessary for a minimal embodiment of PDK, provided in the shared specification is that control logic 250 providing access to store, retrieve, and/or modify data held within in a service block upon receipt of a corresponding access key. Based on such explicit definitions, it is my opinion a person of ordinary skill in the art reading the claims in light of the specification would understand that the “local, secured financial information” recited in claims 1 and 11 of the ‘700 Patent and “local, secured biometric information” recited in claims 1 and 10 of the ‘188 Patent necessitates that the integrated PDK comprise a service block accessed with an access key provided to the integrated PDK. This is distinguished from simply storing information in a memory location. The prior art cited by Dr. Wolfe does not teach the elements of “local, secured financial information,” “local, secured biometric information,” or “local secured information” of any other kind, as these references simply demonstrate the storage of trusted information.

55. Both claim 1 of the ‘700 Patent and claim 1 of the ‘188 Patent recite

“one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service.” Similarly, claim 10 of the ‘188 Patent and claim 11 of the ‘700 Patent recite “generating an enablement signal enabling one or more of an application, a function and a service.” It is my opinion that the term “enabling one or more of an application, a function, and service” is explicitly defined in the specification as sending a message comprising information from a service block of a PDK unlocked, prior to transmission, with an access key provided to the PDK.

56. Referencing FIG. 6 to provide a visual conceptualization, the shared specification explicitly defines “enabling” as retrieving information from a service block of a PDK using an access key provided to the PDK using three different examples. As stated in col. 9, lines 4-35:

“FIGS. 4 and 5 illustrate a basic case where a single application accesses a single service block on a single PDK via a single sensor. The invention is not limited to this case. FIG. 6 illustrates a case with multiple applications, sensors, and service blocks. This illustrates the sharing of service blocks. As shown, service blocks may be limited to a single service or source or may be shared across multiple services and sources. A service block 112 is a protected memory element which allows an application 120 with the right credentials to access it. In this example, applications 120W, 120X and 120Y1 can each access service block 112C since each application has access to service block access key 118C. Similarly,

applications 120V, 120Z2 and 120Z3 can each access service block 112B... In some cases, the first application 120Y1 is enabled from a first service block 112C, thus allowing a second application 120Y2 to operate using a second service block 112F (although the two applications need not be on the same device 510). For example, the first application 120Y1 might be the autologin/logoff, where a user logs into a personal computer via a service block 112C that provides a username and password.”

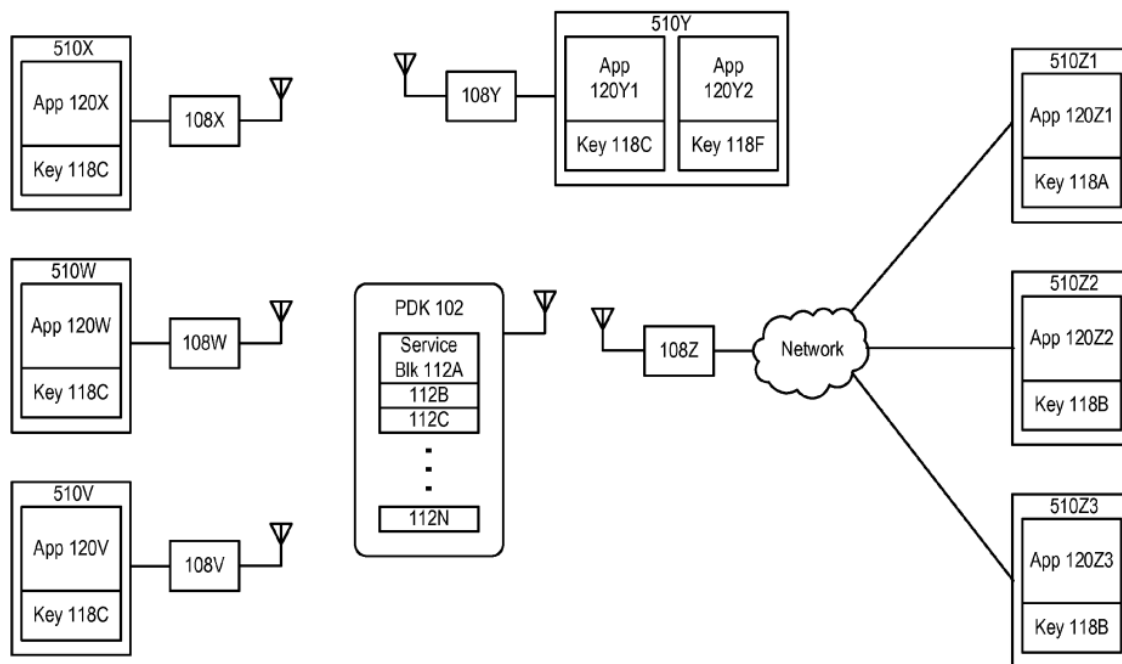


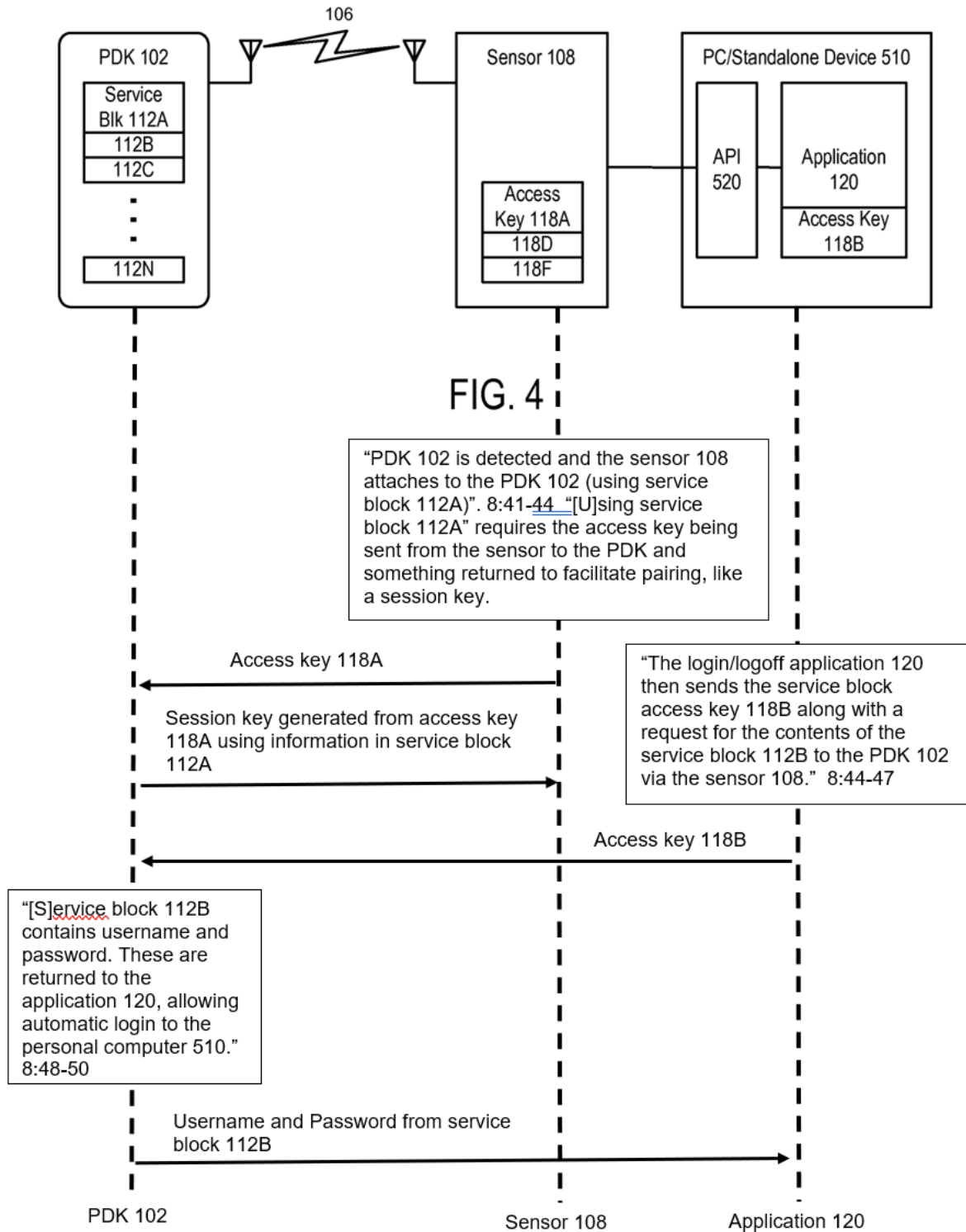
FIG. 6

57. As shown in FIG. 6 (reproduced above), service block 112C is part of PDK 102 and application 120Y1 has access key 118C permitting access to the username and password held within service block 112C. Accordingly, to access the username and password held within service block 112C, application 120Y1

must provide access key 112C to PDK 102 and receive back from PDK the username and password held within service block 112C. In fact, such a process is detailed with reference to FIG. 4 at col. 8, lines 40-50, which states:

“An example of a local application (FIG. 4) is an auto login/logoff of a personal computer. When a PDK 102 is within the proximity of the personal computer 510, the PDK 102 is detected and the Sensor 108 attaches to the PDK 102 (using service block 112A). The login/logoff application 120 then sends the service block access key 118B along with a request for the contents of the service block 112B to the PDK 102 via the sensor 108. For example, a standard may specify that particular service block 112B contains username and password. These are returned to the application 120, allowing automatic login to the personal computer 510.”

58. The flow of the foregoing process is reflected in the figure below:



Flow of Enabling Presented in Col. 8, Lines 40-50

59. As shown above and detailed in col. 8, lines 40-50, and col. 9, lines 4-35, enabling the auto login/logoff applications 120Y1 and 120 involves sending a message comprising information from a service block of a PDK unlocked, prior to transmission, with an access key provided to the PDK.

60. In addition to the auto login/logoff application 120Y1, with reference to FIG. 6, the shared specification provides a second example explicitly defining “enabling” of biometric verification application 120Y2. As stated in col. 9, lines 36-44:

“Now that the user is logged in, the user wishes to attach to his credit card company. The user types in the web address of the credit card provider, where the credit card provider requests the user's credentials. First, the user may have to provide some live biometric information. Application 120Y2 compares this against a biometric stored in a second service block 112F on the PDK. After the sensor 108Y verifies the correct biometrics, the sensor indicates to the PDK that external services may now access their service blocks.”

61. As shown in FIG. 6 (reproduced above), service block 112F is part of PDK 102 and application 120Y2 has access key 118F permitting access to the biometric held within service block 112F. Accordingly, to access the biometric held within service block 112F to compare against the live biometric information, application 120Y2 must provide access key 112F to PDK 102 and receive back

from PDK the biometric held within service block 112F. In fact, such a process is detailed with reference to FIG. 1 at col. 3, lines 42-64, which states:

“In one example, a biometric is required in order to access specific service blocks 112 in the PDK102. Verification of the biometric is achieved by using service block 112A. The sensor 108 stores the corresponding service block access key 118A and uses this key to unlock the biometric service block 112A, which stores a valid biometric. A current biometric is received using biometric input 104. The sensor 108 then verifies the stored biometric (from service block 112A) against the recently acquired biometric (from input 104). Upon proper Verification, various applications 120 are permitted to connect to the PDK102 via the sensor 108 and/or to gain access to other service blocks 112.

The system 100 can be used to address applications 120 where it is important to authenticate an individual for use. Generally, the sensor 108 wirelessly receives information stored in the PDK 102 that uniquely identifies the PDK 102 and the individual carrying the PDK102. The sensor 108 can also receive a biometric input 104 from the individual. Based on the received information, the sensor 108 determines if access to the application 120 should be granted. In this example, the system 100 provides authentication without the need for PINs or passwords (although PINs and passwords may be used in other implementations).”

62. The flow of this process is reflected in the figure below.

100

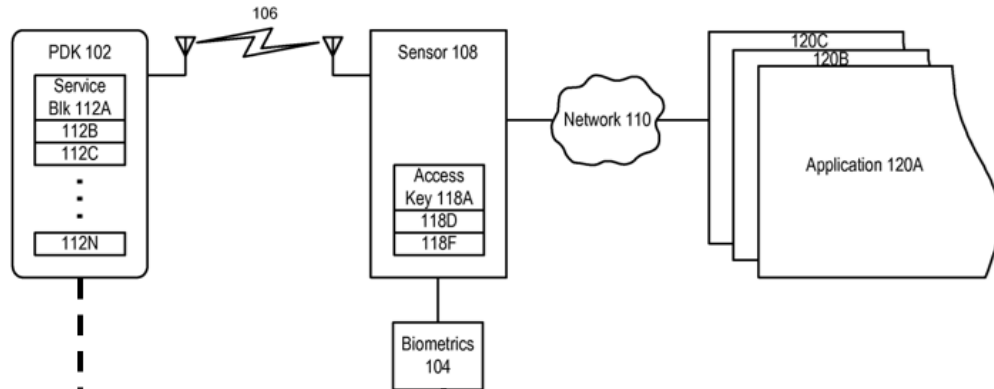
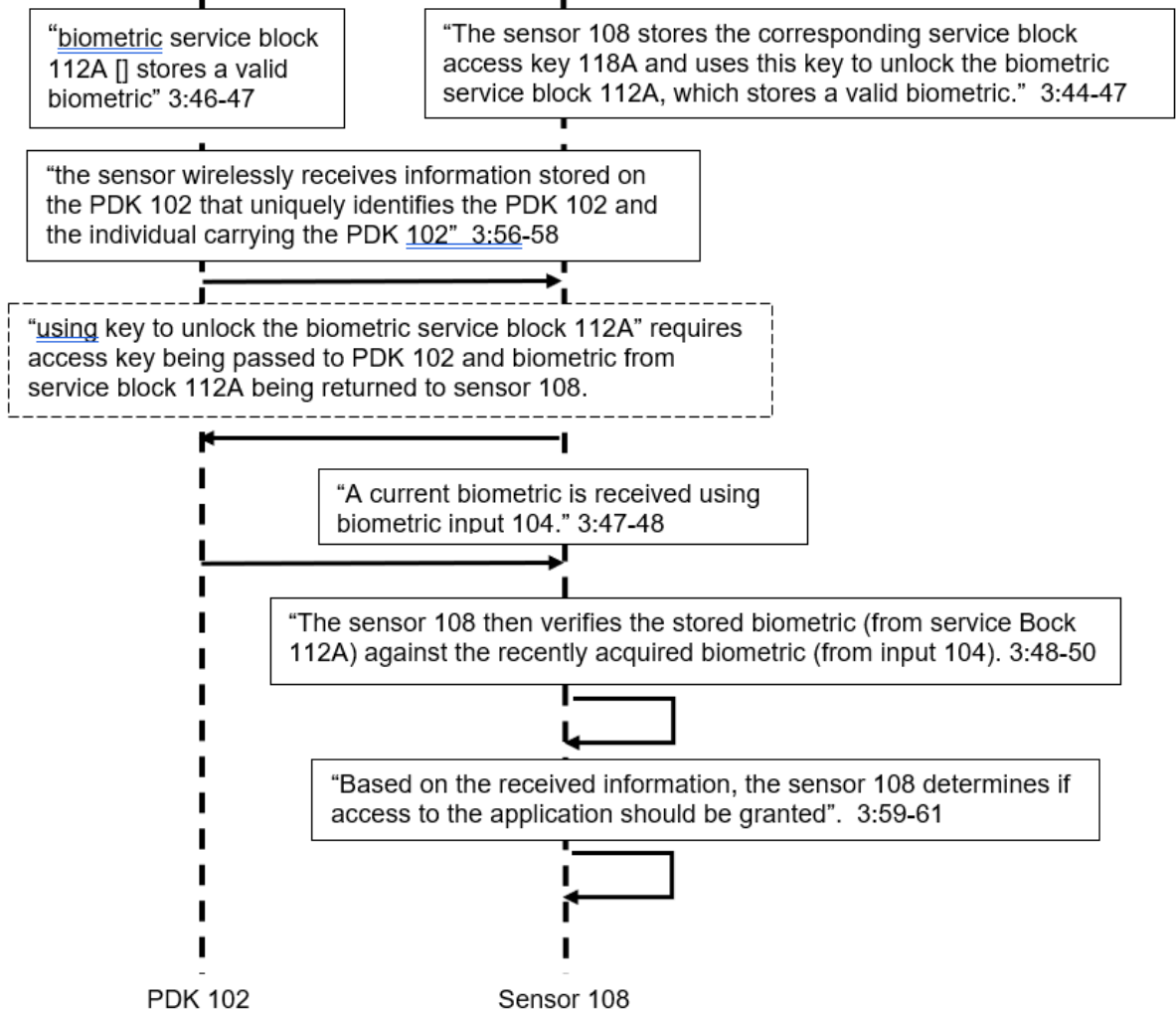


FIG. 1



Flow of Enabling Presented in Col. 3, Lines 42-64

63. As shown above and detailed in col. 3, lines 42-64, and col. 9, lines 36-44, enabling the biometric verification application 120Y2 and that on sensor 108 comprises sending a message comprising information from a service block of a PDK unlocked, prior to transmission, with an access key provided to the PDK.

64. In addition to the auto login/logoff application 120Y1 and the biometric verification application 120Y2, the shared specification provides a third example explicitly defining “enabling” of the services of credit card provide 120Z1. As stated in col. 9, lines 44-49, with reference to FIG. 6:

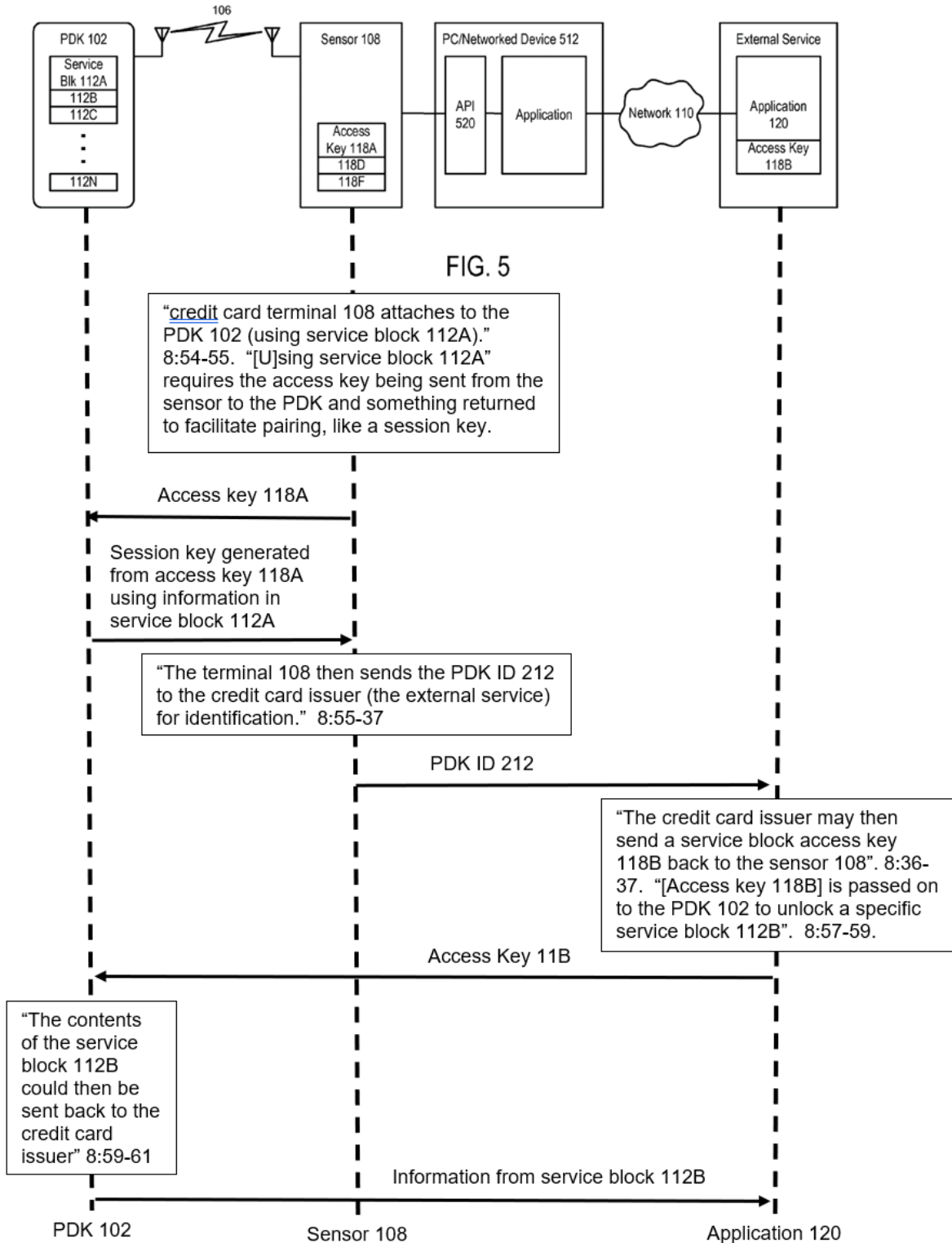
“The credit card provider 120Z1 then sends its service block access key 118A to the PDK where this third service block 112A is retrieved and sent back to the credit card issuer. The credit card issuer then verifies the data and authorizes the user's transaction.”

65. As shown in FIG. 6 (reproduced above), service block 112A is part of PDK 102 and credit card provider 120Z1 has access key 118A permitting access to the data held within service block 112A. Accordingly, in order to access and verify the data held within service block 112A, credit card provider 120Z1 must provide access key 112A to PDK 102 and receive back from PDK the data held within service block 112A. In fact, such a process is detailed with reference to FIG. 5 at col. 8, lines 51-63, which states:

“An example of a remote application (FIG.5) is a credit card transaction. The sensor 108 in this case could be a credit card terminal. When the PDK 102 is brought in close proximity, the

credit card terminal 108 attaches to the PDK 102 (using service block 112A). The terminal 108 then sends the PDKID 212 to the credit card issuer (the external service) for identification. The credit card issuer may then send a service block access key 118B back to the sensor 108, where it is passed on to the PDK102 to unlock a specific service block 112B. The contents of the service block 112B could then be sent back to the credit card issuer where further decryption could occur and the credit cardholder could be verified. Once verified, the credit card terminal displays that the transaction is approved.”

66. The flow of this process is reflected in the figure below.



Flow of Enabling Presented in Col. 8, Lines 51-63

67. As shown above and detailed in col. 8, lines 51-63, and col. 9, lines 44-49, enabling the service of credit card provider 120Z1 comprises sending a message comprising information from a service block of a PDK unlocked, prior to transmission, with an access key provided to the PDK.

68. Subsequent examples presented in the shared specification of a PDK “enabling one or more of an application, a function, and a service” likewise reference sending a message comprising information from a service block of the PDK. ‘700 Patent, 16:4-7 (“PDK 102a can provide access control password etc. for any type of functions enabled by the phone such as but not limited to gaming, personal computer access, e-commerce etc.”); 16:48-50 (“The hybrid device 1102 carries credentials (credit card, account information, etc.) that are used to enable a service associated with the second RDC 304b.”); 16:57-61 (“In other words, the second PDK 102b is used to enable specific features in the hybrid device 1102. The second PDK102b carries the user's cellular service account information that is used to enable specific cellular services.”); *id.* 17:41-43 (“A user carrying a PDK102b with the correct privileges must also be present to gain access to the computer.”).

69. Accordingly, the specification explicitly defines an integrated PDK “enabling one or more of an application, a function, and service” as the integrated PDK sending a message comprising information from a service block of the PDK

unlocked, prior to transmission, with an access key provided to the PDK.

70. The shared specification also explicitly defines the integrated RDC “enabling one or more of an application, a function, and service” as receipt by the integrated RDC of a message comprising information from a service block of a PDK unlocked, prior to transmission, with an access key provided to the PDK. ’700 Patent, 9:50-54 (“Furthermore, although the above scenarios focus mostly on service blocks in the PDK, applications may also use the basic authentication function that allows the PDK and sensor to verify each other. In this scenario, once the sensor and PDK finish their verification the application is signaled.”). While this definition is provided with respect to sensor 108, the shared specification states at col. 7, lines 31-32, that the RDC 304 of sensor 108 “provides the wireless interface PDK 102.”

71. Accordingly, those skilled in the art would understand all messages from the PDK are received via the RDC, and authentication would occur via the RDC and PDK. The shared specification further explicitly defines authentication, or attachment to a PDK, as entailing the use of a service block access key and a service block of the PDK. ’700 Patent, 8:9-11 (“In FIG.4, the sensor 108 attaches to the PDK102 within its microcell, using service block access key 118(A) and service block 112(A).”); 8:20-23 (“[T]he sensor 108 attaches to the PDK 102 in the same manner as FIG. 4, using service block access key 118A and service block

112A.”); 8:41-44 (“When a PDK 102 is within the proximity of the personal computer 510, the PDK 102 is detected and the Sensor 108 attaches to the PDK 102 (using service block112A).”); 8-53-55 (“When the PDK 102 is brought in close proximity, the credit card terminal 108 attaches to the PDK 102 (using service block112A).”).

72. Since service blocks are protected memory elements requiring the proper credentials for access, the use of a service block access key and service block to accomplish authentication requires the access key being sent from the sensor to the PDK and something being returned to the RDC facilitating pairing, like a session key. Accordingly, authentication between an RDC and PDK is explicitly defined as comprising sending a message from the PDK comprising information from a service block of a PDK unlocked, prior to transmission, with an access key provided to the PDK by the RDC.

73. In addition to explicitly defining enabling as the result of an authentication between an RDC and a PDK, the shared specification explicitly defines the integrated RDC “enabling one or more of an application, a function, and a service” as receipt by the integrated RDC of a message comprising information from a service block of a PDK unlocked, prior to transmission, with an access key provided to the PDK

74. While claim 1 of the ‘188 Patent and claim 1 of the ‘700 Patent recite

“one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and service”, claim 10 of the ‘188 Patent and claim 11 of the ‘700 Patent each recite “generating an enablement signal enabling one or more of an application, a function and a service”. Since “enabling one or more of an application, a function, and service” by a PDK is explicitly defined as the PDK sending a message and “enabling one or more of an application, a function, and service” by a RDC is defined as receiving a message, a person of ordinary skill in the art would understand the enablement signal is generated by a PDK after receipt of an access key by the PDK.

I declare under penalty of perjury that the foregoing is true and correct.

Date: May 23, 2022


Charles Eldering, Ph.D