IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION

Petitioner,

v.

PROXENSE, LLC

Patent Owner

IPR2024-00407

U.S. Patent No. 9,679,289 B1

PATENT OWNER RESPONSE

TABLE OF CONTENTS

I. INTRODUCTION 1

II. RELATED MATTERS 1

III. OVERVIEW OF THE 289 PATENT 2

IV. CLAIM CONSTRUCTION 4

A. CLAIMS 1 AND 14 INVOKE 35 U.S.C. § 112, PARAGRAPH 6 4

B. APPLICABLE LAW 4

C. CLAIMS 1 AND 14 FAIL TO RECITE SUFFICIENTLY DEFINITE STRUCTURE FOR ENABLING ONE OR MORE OF AN APPLICATION, A FUNCTION AND A SERVICE 7

1. Local, Secured Information Stored by the Integrated, Secure Memory 8

2. Integrated RDC Communicating Wirelessly with the at Least One External Device within the Proximity Zone 19

3. Enablement Signal 22

D. PRIOR CONSTRUCTION BY THE DISTRICT COURT 27

V. RESPONSE TO GROUNDS FOR INVALIDITY RAISED 29

A. [GROUND 1A/1B] – CLAIMS 1-20 ARE NOT RENDERED OBVIOUS BY GIOBBI-157 AND GIOBBI-139 [1A] NOR BY GIOBBI-157, GIOBBI-139, AND DUA [1B] 29

B. [GROUND 2A] – CLAIMS 1-8, 10, 11, AND 14-19 ARE NOT RENDERED OBVIOUS BY BROADCOM 32

C. [GROUND 2B] – CLAIMS 1-20 ARE NOT RENDERED OBVIOUS BY BROADCOM AND GIOBBI-157 34

VI. CONCLUSION 35

TABLE OF AUTHORITIES

Page(s)

Cases

Computing v. Samsung Electronics America,
989 F.3d 1002 (Fed. Cir. 2021) ..... *passim*

Ergo Licensing, LLC v. CareFusion 303, Inc.,
673 F. 3d 1361 (Fed. Cir. 2012) 7, 9, 23

HTC Corp. v. IPCom GmbH & Co., KG,
667 F.3d 1270 (Fed. Cir. 2012) 21, 25, 26

In re Katz Interactive Call Processing Patent,
639 F. 3d 1303 (Fed. Cir. 2011)..... 7

Media Rights Technologies v. Capital One Financial,
800 F. 3d 1366 (Fed. Cir. 2015) 5

MTD Products Inc. v. Iancu,
933 F. 3d 1336 (Fed. Cir. 2019) 5

WMS Gaming, Inc. v. Int'l Game,
184 F.3d 1339 (Fed. Cir. 1999) 6

Williamson v. Citrix, LLC,
792 F.3d 1339 (Fed. Cir. 2015) 5, 6

Statutes

35 U.S.C. § 112..... *passim*

35 U.S.C. § 316 1

Regulations

C.F.R. § 42.120..... 1

EXHIBIT LIST

No.	Exhibit Description
2001	Claim Construction Order in *Proxense, LLC v. Samsung Electronics, Co., Ltd. et al.,* No. 6.21-CV-00210-ADA
2002	Memo In Support of Claim Construction Order in *Proxense, LLC v. Samsung Electronics, Co., Ltd. et al.*
2003	Markman Transcript from *Proxense, LLC v. Samsung Electronics, Co., Ltd. et al.*
2004	Claim Construction Order in *Proxense, LLC v., Google LLC,* No. 6:23-cv-00320-ADA
2005	Opening Claim Construction Brief in *Proxense, LLC v. Microsoft Corporation,* No. 6:23-cv-00319-ADA
2006	Responsive Claim Construction Brief in *Proxense, LLC v. Microsoft Corporation*
2007	Reply Claim Construction Brief in *Proxense, LLC v. Microsoft Corporation*
2008	Sur-reply Claim Construction Brief in *Proxense, LLC v. Microsoft Corporation*
2009	Opening Claim Construction Brief in *Proxense, LLC v. Samsung Electronics, Co., Ltd. et al.*
2010	Reply Claim Construction Brief in *Proxense, LLC v. Samsung Electronics, Co., Ltd. et al.*
2011	Joint Claim Construction Statement
2012	Plaintiff's Preliminary Claim Construction in *Proxense, LLC v. Apple, Inc*., No. 6:24-cv-00143-ADA
2013	Defendant's Preliminary Claim Construction in *Proxense, LLC v. Apple, Inc*., No. 6:24-cv-00143-ADA
2014	Declaration of Markus Jakobsson
2015	Claim Construction Order - *Proxense v. Microsoft Corporation*, No. 6:23-cv-319

I. INTRODUCTION

Pursuant to 35 U.S.C. § 316 and C.F.R. § 42.120, the Patent Owner, Proxense LLC ("Proxense"), submits this Patent Owner Response in response to the Petition for *Inter Partes* Review of claims 1-20 of U.S. Patent No. 9,679,289 B1 (the "289 Patent") filed by Petitioner, Microsoft Corporation ("Microsoft").

Proxense respectfully submits claims 1-20 are patentable over the instituted grounds, as each of the grounds relies on combinations of references failing to show *all* elements of the claimed invention. Specifically, the asserted references, either alone or in combination, fail to show the algorithm disclosed in the specification allowing any of "local, secured information stored by the integrated, secure memory," an "integrated RDC communicating wirelessly with [] at least one external device within the proximity zone," and an "enablement signal" to perform the function "enabling one or more of an application, a function and a service" as recited independent claims 1 and 14. Claims 1 and 14 each invoke 35 U.S.C. § 112, ¶ 6, by reciting the function of "enabling one or more of an application, a function and a service" is performed by general purpose computers, such that the disclosed structure for performing the function is the special purpose computer programmed to perform the algorithm disclosed in the specification. The Petition has not demonstrated claims 1-20 are unpatentable because none of the grounds demonstrate this algorithm in any of the asserted references.

II. RELATED MATTERS

The 289 Patent is currently being asserted against Petitioner in *Proxense v. Microsoft Corporation*, No. 6:23-cv-00319-ADA (W.D. Tex. May 2, 2023). The District Court issued a Claim Construction Order on May 24, 2024, a copy of which is attached as Exhibit 2011.

The 289 Patent is also currently being asserted against Co-Petitioner, Apple Inc (hereafter "Apple"), in *Proxense, LLC, v. Apple, Inc.,* No. 6:24-cv-00143 (W.D. Tex. March 18, 2024). The

parties have provided their Preliminary Claim Constructions, copies of which are attached as Exhibits 2012 and 2013.

The 289 Patent is also being asserted in *Proxense, LLC v. Google LLC*, No. 6:23-cv-00320 (W.D. Tex. May 2, 2023). The District Court issued a Claim Construction, a copy of which was previously submitted as Exhibit 2004.

The validity of the 289 Patent has also been challenged in the following proceedings before the Office: IPR2024-00783 and IPR2024-01319.

III. OVERVIEW OF THE 289 PATENT

The 289 Patent discloses and claims a technical improvement to solve the technical problem of being unable to expand proximity systems to new and third-party applications, by providing a novel control logic allowing memory to be used as local, secured storage for external applications. As noted in the Background section, most proximity system "typically do not have the capabilities to run different applications or to even interact with different applications" and lack "easy expandability to other situations or third party applications." 289 Patent, 2:15-21. To solve this problem, the patent discloses a novel control logic controlling "service blocks" within device memory that permits isolated storage and selection of different information for different applications. In operation, the control logic allows external applications to "gain access to a specific service block 112 by proving the corresponding access key 118." 289 Patent, 6:58-60. In addition to disclosing the control logic, the 289 Patent provides various examples of how the logic may be utilized in various general-purpose computers, such as cell phones, servers, personal computers, and credit card terminals. For example, with reference to Fig. 6 (reproduced below), the 289 Patent details simultaneous use of the control logic by different applications as a user accesses the website of his credit card provider:

[T]he first application 120Y1 might be the auto login/logoff, where a user logs in to a personal computer via a service block 112C that provides a username and password. 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. 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.

289 Patent, 9:43-63.

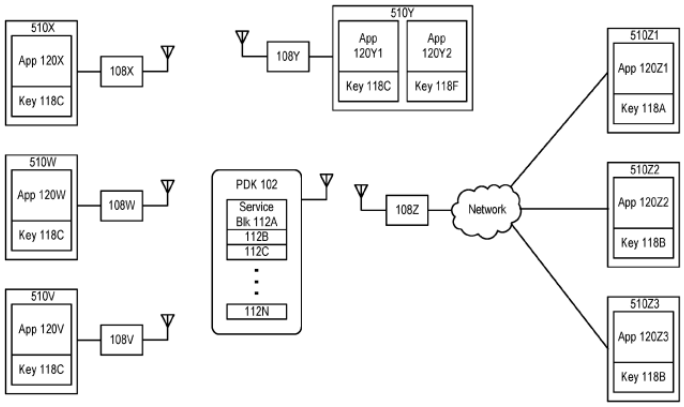


FIG. 6

As the above illustrates, when implemented, the control logic generates an enablement signal enabling one or more of an application, a function and a service by having the application, function or service to be enabled authenticate by exchanging an access key for the ability to store, retrieve and/or modify data in a service block of local secured memory.

IV. CLAIM CONSTRUCTION

Determining whether the Petition raises sufficient grounds of invalidity requires construing independent claims 1 and 14. Independent claim 1 recites that function of "enabling one or more of an application, a function and a service" is performed by "local, secured information stored by the integrated, secure memory" and/or an "integrated RDC communicating wirelessly with the at least one external device within the proximity zone." Independent claim 14 recites the function is performed by an "enablement signal." These terms must be construed to determine the corresponding structures performing the recited function. Only then can it be determined whether the Petition includes all elements of claims 1 and 14 in the asserted references.

A. Claims 1 and 14 Invoke 35 U.S.C. § 112, Paragraph 6

Independent claims each recite the function of "enabling one or more of an application, a function and a service." Accordingly, it must be determined if each of claims 1 and 14 recite a sufficiently definite structure for performing that function, other than a general-purpose computer. Here, the claims do not recite a sufficiently definite structure for performing the function, but rather a general-purpose computer. Therefore, the claims invoke 35 U.S.C. § 112, ¶ 6, and the claims must be construed to cover only the structure, material, or acts described in the specification as corresponding to the claimed structure. With respect to claims 1 and 14, the structure is the algorithm the general-purpose computer is programmed to perform.

B. Applicable Law

> To determine whether § 112 ¶ 6 applies to a claim limitation, we must inquire whether the words of the claim are understood by persons of ordinary skill in the art to have a ***sufficiently definite meaning as the name for structure. If those words lack a sufficiently definite meaning, § 112 ¶ 6 applies***. If the limitation uses the word 'means,' there is a rebuttable presumption that § 112 ¶ 6 applies. If not, there is a rebuttable presumption that the provision does not apply. But that

> presumption can be overcome and § 112 para. 6 will apply if the challenger demonstrates that ***the claim term fails to recite sufficiently definite structure*** or else recites function without reciting sufficient structure for performing that function.

Raining Computing v. Samsung Electronics America, 989 F.3d 1002, 1005 (Fed. Cir. 2021) (citing *Williamson v. Citrix, LLC,* 792 1139 (Fed. Cir. 2015) (internal quotations, brackets, and citations omitted and emphasis added).

The above is often misstated as requiring the term "means" be replaced by a recognized "nonce" word. But that is just *one way* to demonstrate that a claim limitation fails to recite a sufficiently definite structure:

> One way to demonstrate that a claim limitation fails to recite sufficiently definite structure is to show that, although not employing the word 'means,' the claim limitation uses a similar 'nonce' word that can operate as a substitute for `means' in the context of § 112, para. 6… In each case, ***a critical question*** is whether the claim term is used in common parlance or by persons of skill in the pertinent art ***to designate structure***, including either a particular structure or a class of structures.

MTD Products Inc. v. Iancu, 933 F. 3d 1336, 1341 (Fed. Cir. 2019) (emphasis added). Accordingly, the failure of the claims to recite a recognized "nonce" word is *not* determinative. Rather, the critical question is whether claim, when read in light of the specification, designates a structure. *Media Rights Technologies v. Capital One Financial*, 800 F. 3d 1366, 1372 (Fed. Cir. 2015) ("In undertaking this analysis, we ask if the claim language, read in light of the specification, recites sufficiently definite structure to avoid § 112, ¶ 6.").

Once it has been determined that § 112, ¶ 6, is invoked, the construction of the claim term attributed for performing the function must be determined, which occurs in two steps.

> The first step in construing a means-plus function claim is to 'identify the claimed function. After identifying the function, we then determine what structure, if any,

> disclosed in the specification corresponds to the claimed function. Under this second step, structure disclosed in the specification is corresponding structure only if the specification or prosecution history clearly links or associates that structure to the function recited in the claim.

Raining Computing, 989 F.3d at 1007 (citing *Williamson v. Citrix, LLC,* 792 1139 (Fed. Cir. 2015) (internal quotations and citations omitted).

When the structure disclosed for performing the function is a general-purpose computer, as here, the second step requires identifying an algorithm disclosed in the specification for accomplishing the function.

> If the function is performed by a general-purpose computer or microprocessor, then the second step generally further requires that the specification disclose the algorithm that the computer performs to accomplish that function… For means-plus-function claims in which the disclosed structure is a computer, or microprocessor, programmed to carry out an algorithm, we have held that "the disclosed structure is not the general purpose computer, but rather the special purpose computer programmed to perform the disclosed algorithm.

Raining Computing, 989 F.3d at 1007 (citing *WMS Gaming, Inc. v. Int'l Game Tech.,* 184 F.3d 1339 (Fed. Cir. 1999) (internal quotations and citations omitted). There is, however, a narrow exception to the rule that an algorithm must be disclosed for a general-purpose computer to satisfy the disclosure requirement. In instances where the recited function is merely, "processing," "storing," and "receiving," a general-purpose computer is sufficient:

> [W]e held that absent a possible narrower construction of the terms 'processing,' 'receiving,' and 'storing,' the disclosure of a general-purpose computer was sufficient. We explained that in substance, claiming 'means for processing,' 'receiving,' and 'storing' may simply claim a general-purpose computer, although in means-plus-function terms.

Ergo Licensing, LLC v. CareFusion 303, Inc., 673 F. 3d 1361, 1365 (Fed. Cir. 2012) (citing *In re Katz Interactive Call Processing Patent*, 639 F. 3d 1303 (Fed. Cir. 2011) (internal quotations and citations omitted). Accordingly, when the function recited in the claims requires more than storing, receiving, or processing, an algorithm must be disclosed in the specification.

Should an adequate structure not be found within the specification, then the claim is indefinite. *Raining Computing*, 989 F.3d at 1007 ("And finally, if the patentee fails to disclose adequate corresponding structure, the claim is indefinite.").

C. Claims 1 and 14 Fail to Recite Sufficiently Definite Structure for Enabling One or More of An Application, a Function and a Service

Claims 1 and 14 each recite the function of "enabling one or more of an application, a function and a service" without reciting a sufficiently definite structure for performing that function. Claim 1 attributes to the function to "local, secured information stored by the integrated, secure memory" or an "integrated RDC communicating wirelessly with the at least one external device within the proximity zone." Claim 14 attributes the function to an "enablement signal." But none of these structures are recognized by those skilled in the art as sufficiently *definite* structures for performing the function. Jakobsson Decl.[1], ¶ 36 ("[T]he structures recited for performing the function of "enabling one or more of an application, a function and a service" recited in claims 1 and 14 of the 289 Patent are not used in common parlance or by persons of skill in the pertinent art to designate structure or a class of structures recognized for performing the function."). The claims themselves and the specification further inform that the recited structures for performing the function are nothing more than the generic abilities of general-purpose computers or meaningless nonce words. Jakobsson Decl., ¶ 18 ("The terms, rather, connote the general and generic abilities of general purposes computers or are a completely meaningless nonce

[1] The Declaration of Markus Jakobsson ("Jakobsson Decl.") is attached hereto as Exhibit 2014.

defined only by the intended action to be performed."). Consequently, the structure for performing the function of "enabling one or more of an application, a function, and service" must be an algorithm disclosed in the specification. *Raining Computing*, 989 F.3d at 1007 ("For means-plus-function claims in which the disclosed structure is a computer, or microprocessor, programmed to carry out an algorithm, we have held that "the disclosed structure is not the general purpose computer, but rather the special purpose computer programmed to perform the disclosed algorithm."). Absent such an algorithm within the specification, the claims would be indefinite. *Raining Computing*, 989 F.3d at 1007 ("And finally, if the patentee fails to disclose adequate corresponding structure, the claim is indefinite."). But here the specification "discloses a control logic that can be used by an 'RDC,' 'wireless communication interface,' and 'local, secured information' to 'enable one or more of an application, a function and service." Jakobsson Decl., ¶ 18. Furthermore, "the same control logic generates 'an enablement signal enabling one or more of an application, a function and a service. Jakobsson Decl., ¶ 18. Accordingly, the control logic disclosed in the specification is the structure for "enabling one or more of an application, a function, and service."

1. Local, Secured Information Stored by the Integrated, Secure Memory

Claim 1 attributes the function of the "enabling one or more of an application, a function and service" to "local, secured information stored by the integrated, secure memory." "§ 112 para. 6 will apply if the challenger demonstrates that ***the claim term fails to recite sufficiently definite structure*** or else recites function without reciting sufficient structure for performing that function." *Raining Computing*, 989 F.3d at 1005 (emphasis added). The term "local, secured information stored by the integrated, secure memory" is not a structure recognized by those of ordinary skill in the art to provide a sufficiently definite structure for performing the function of "enabling on or

more of an application, a function and a service". Jakobsson Decl., ¶¶ 18 and 36. Accordingly, claim 1 invokes § 112, ¶ 6.

Since claim 1 invokes § 112, ¶ 6 by failing to recite a sufficiently definite structure for the performing the recited function, the claim must be construed. "The first step in construing a means-plus function claim is to 'identify the claimed function." *Raining Computing*, 989 F.3d at 1007. With respect to claim 1, the recited function is "enabling one or more of an application, a function and service." "After identifying the function, we then determine what structure, if any, disclosed in the specification corresponds to the claimed function." *Raining Computing*, 989 F.3d at 1007. Claim 1 recites the function is performed by "local, secured information stored by the integrated, secure memory." On its face, the recited structure is nothing more than the ability of general-purpose computer to utilize a computer readable media store data within tamper proof memory. Jakobsson Decl., ¶ 37. The PTAB itself recognized such in its Institution Decision by determining "the term 'local, secured information' as claimed encompasses information stored locally on an integrated, secure memory, wherein the information is secured…" Paper 8 at 11-12. Thus, both the Board and Dr. Jakobsson agree that "local, secured information stored by the integrated, secure memory" is nothing more than the storing of data by a computer-readable media. However, "computer-readable media or storage devices amount to nothing more than a general-purpose computer." *Rain Computing,* 989 F.3d at 1007 (Fed. Cir. 2021). Furthermore, "controlling access to one or more software application packages to which the user has a subscription requires more than merely plugging in a general purpose computer." *Id.* (citing *Ergo Licensing, LLC v. CareFusion 303, Inc.*, 673 F.3d 1361 (Fed. Cir. 2012) (internal quotations and brackets omitted).

"If the function is performed by a general-purpose computer or microprocessor, then the second step generally further requires that the specification disclose the algorithm that the

computer performs to accomplish that function." *Rain Computing,* 989 F.3d at 1007 (Fed. Cir. 2021). The algorithm is provided twice in the patent. The first instance of the algorithm is provided to define "local, secured information."

> 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***.

289 Patent, 3:45-50 (emphasis added).

The Board, regrettably, has not recognized the above passage as explicitly defining "local, secured information" with respect to an algorithm. In support of disregarding this explicit definition, the Board cites the preceding sentence. Paper 8, at 10-11. But the full passage from the specification, which ought to be considered, reads:

> 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."

289 Patent, 3:43-50.

The passage starts out by stating "a PDK contains multiple services block 112A-N," clearly indicating the paragraph topic is service blocks. Then, paragraph goes onto to state "each service block 112 is accessed using a corresponding service block access key." This statement defines how a service block is accessed – *i.e*. by using the "corresponding service block access key." Only then does the paragraph states, "***In this example, the sensor 108 contains three of the service block access keys 118A, D, F***." As an initial matter, the subject of this sentence is sensor 108--*not*

service blocks (which is the subject of the paragraph as whole). Accordingly, the statement does not describe service blocks or how they are accessed. Rather, the sentence is merely making a statement about *sensor 108*. Particularly, it states the number of access keys held by sensor 108. But the number of access keys held by sensor 108 has *nothing do with* the operation of service blocks, or the "local secured information" locked within a service block. Thus, it is improper to limit statements made in the paragraph regarding service blocks and the operation "the local secured information" they hold based on a single sentence stating the number of keys held by something that is not even the topic of the paragraph. The paragraph concludes by stating: "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." This final sentence provides an algorithm defining "local, secured information" – *i.e*. unlocking stored information in exchange for an access key. Jakobsson Decl., ¶¶ 38-39. That sensor 108 may have three, or even one, access key is irrelevant to the operation of the "local secured information" stated in the passage. It only relates to the amount of "local secured information" which sensor 108 – *i.e*. limited by the number of access keys possessed. Based on the foregoing and the Declaration of Dr. Jakobsson, Patent Owner respectfully requests the Board reconsider its position.

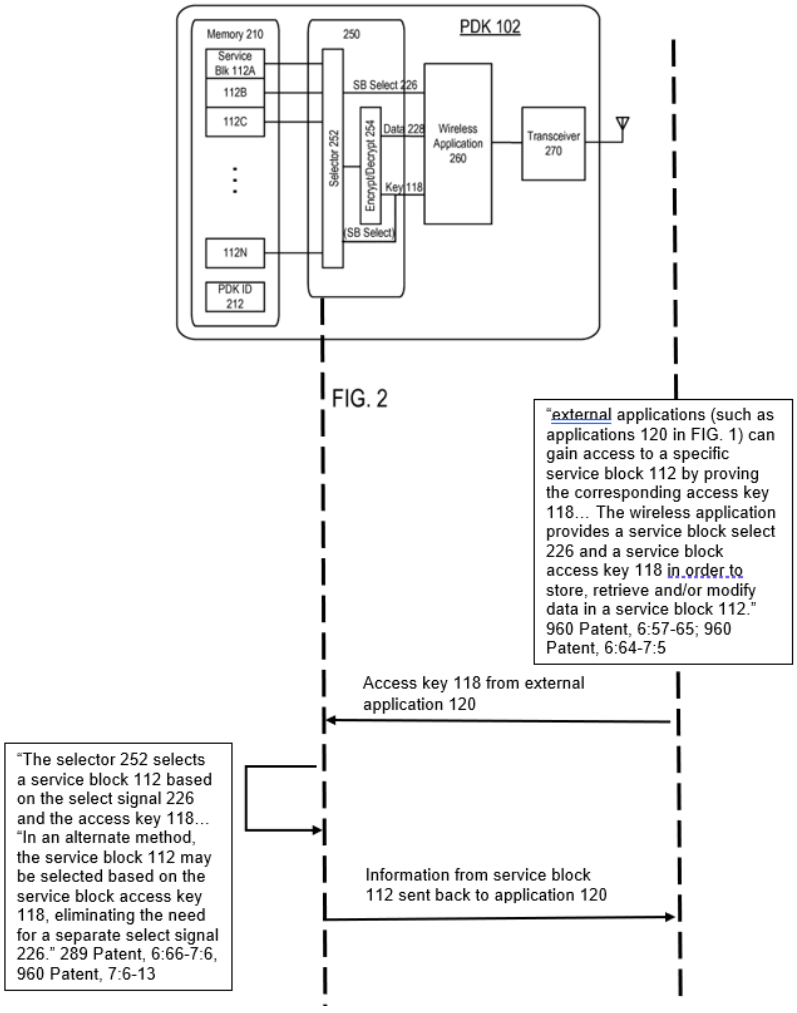
Regardless, the algorithm is presented a *second time* with reference to "control logic 250." Jakobsson Decl., ¶¶ 40-41.

> 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.

289 Patent, 6:57-7:6 (emphasis added).

Dr. Jakobsson graphically presents the above algorithm as follows:



Jakobsson Decl., ¶ 41.

The passage begins by summarizing the operation of the algorithm of control logic 250 as one in which "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***." Accordingly, when executed, the algorithm of control logic 250 exchanges an "access key" provided by an application for the information held within "service block," consistent with the recognized function of an access key. Jakobsson Decl., ¶ 42. Thus, the specification provides an algorithm.

For the algorithm to be the structure corresponding to the recited function "enabling one or more of an application, a function and service" it must be clearly linked to the function. *Raining Computing*, 989 F.3d at 1007 ("Under this second step, structure disclosed in the specification is corresponding structure only if the specification or prosecution history clearly links or associates that structure to the function recited in the claim.") The specification does just that with reference to Figures 1 and 4-6. Jakobsson Decl., ¶¶ 43-54.

First, with reference to Figure 1, the specification details the use of the algorithm to enable the function of biometric authentication, such that biometric authentication by sensor 108 is enabled by the sensor exchanging an access key to unlock and retrieve a biometric held within a service block. Jakobsson Decl., ¶¶ 43-45.

> 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 per mitted 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)."

289 Patent, 3:51-4:6.

Dr. Jakobsson graphically presents the flow of the above process as follows:

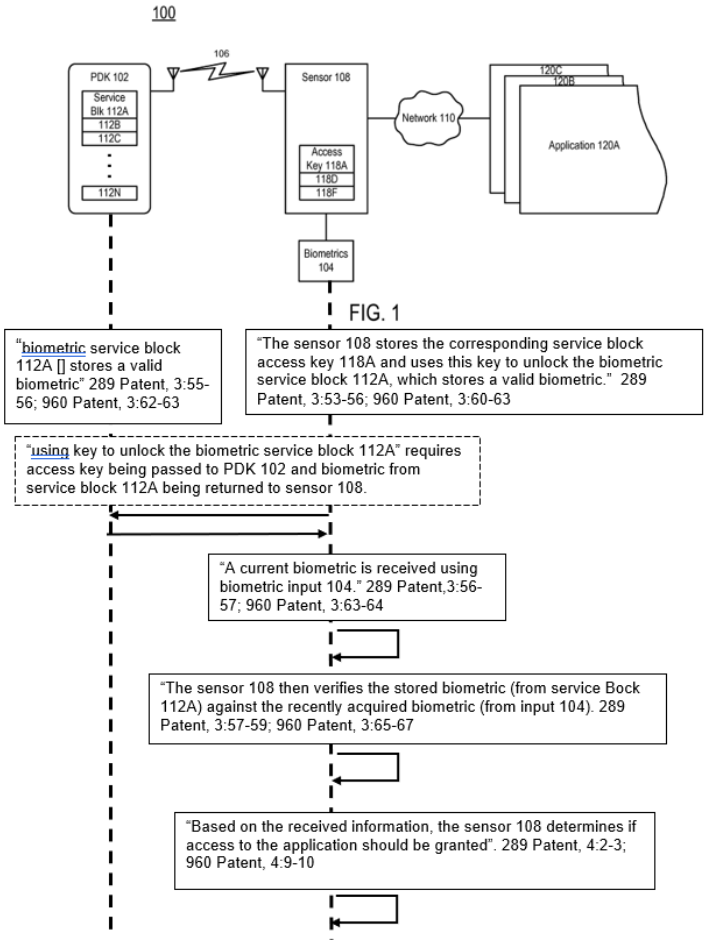


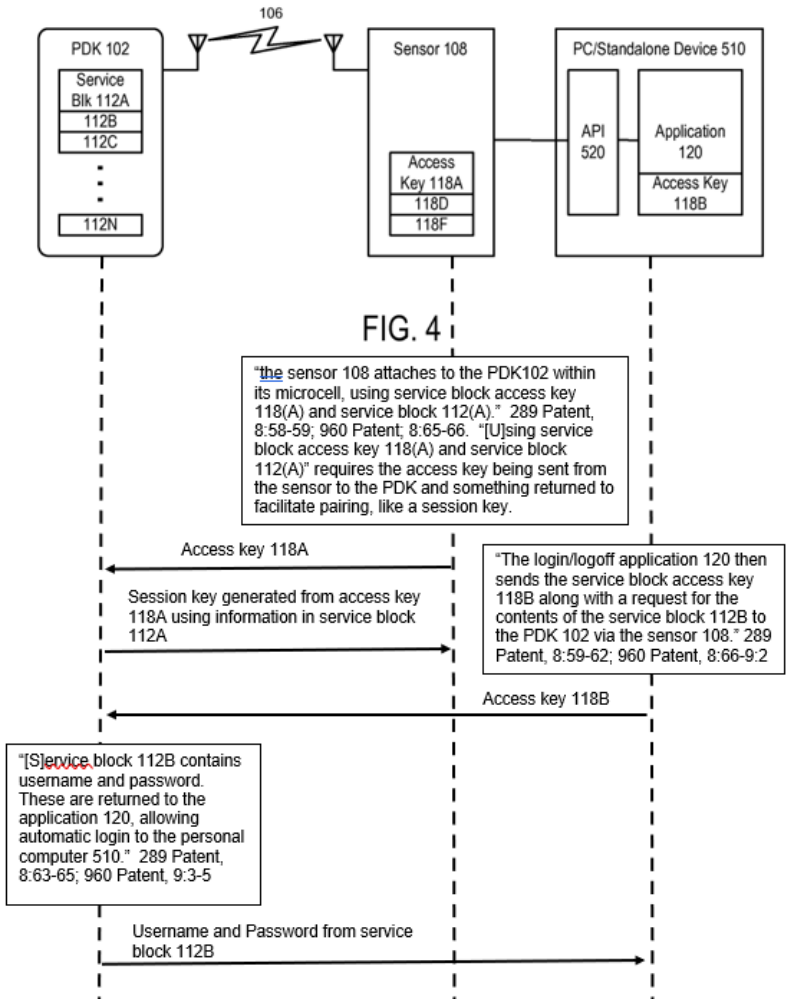
FIG. 1

With reference to Figure 4, the shared specification details how the algorithm of exchanging an access to retrieve information held within service block enables an auto login/logoff application. Jakobsson Decl., ¶¶ 46-48.

> 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 block112A). 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.

289 Patent, 8:55-65.

Dr. Jakobsson graphically presents the flow as follows:



Jakobsson Decl., ¶ 47.

As shown above, the flow begins with the creation of a wireless link facilitating wireless communication between the sensor 108 and the PDK 102. Jakobsson Decl., ¶ 48. However, despite the presence of the wireless link, application 120 is not enabled until it exchanges an access key 118(B) to unlock and retrieve a username and password held within service block 112(B). Jakobsson Decl., ¶ 48. Accordingly, the wireless link is not sufficient to enable application 120.

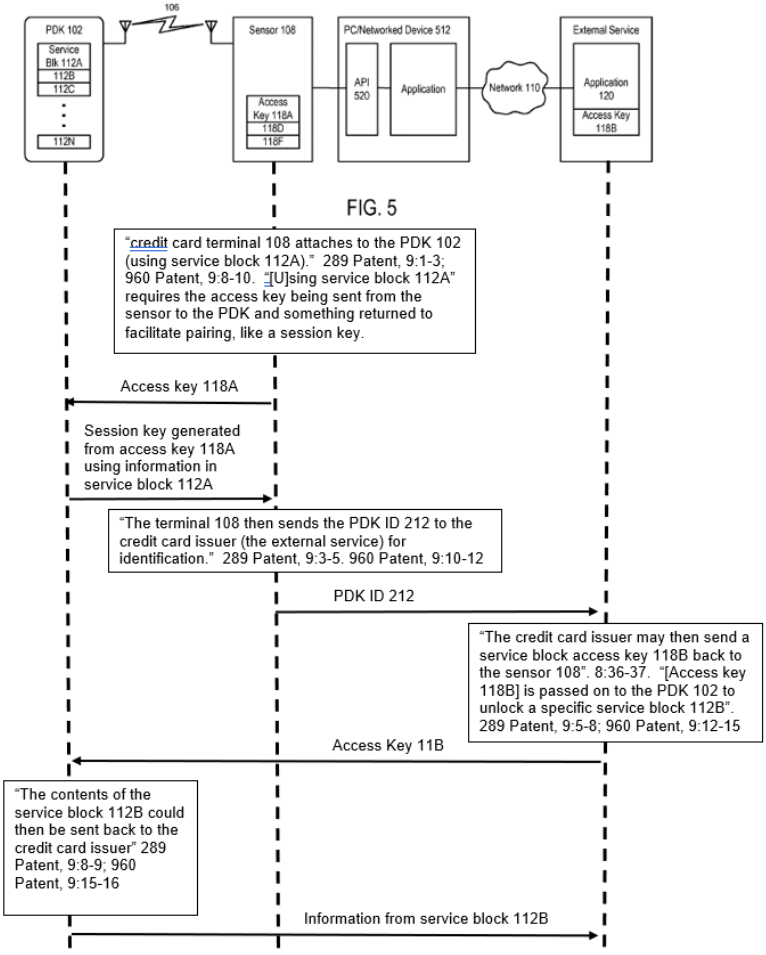
With reference to Figure 5, the specification details how the algorithm of control logic 250 can be used to enable the service of using a credit card. Jakobsson Decl., ¶¶ 49-52.

> 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 block112A). 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.

289 Patent, 8:66-9:12.

Dr. Jakobsson graphically presents the flow as follows:



Jakobsson Decl., ¶ 50.

As before, the flow begins with the creation of a wireless link facilitating wireless communication between the credit card terminal 108 and the PDK 102. Jakobsson Decl., ¶ 51. However, despite the presence of the wireless link, the service of charging a card is not enabled until the credit card issuer sends an access key 118B to unlock and retrieve the contents of service block 112B. Jakobsson Decl., ¶ 51. Accordingly, the wireless link is not sufficient to enable the service.

"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." 289 Patent, 9:20-22. The algorithm of control logic 250, however, can also be used with multiple applications, functions and services, as illustrated by Figure 6. Jakobsson Decl., ¶¶ 52-53.

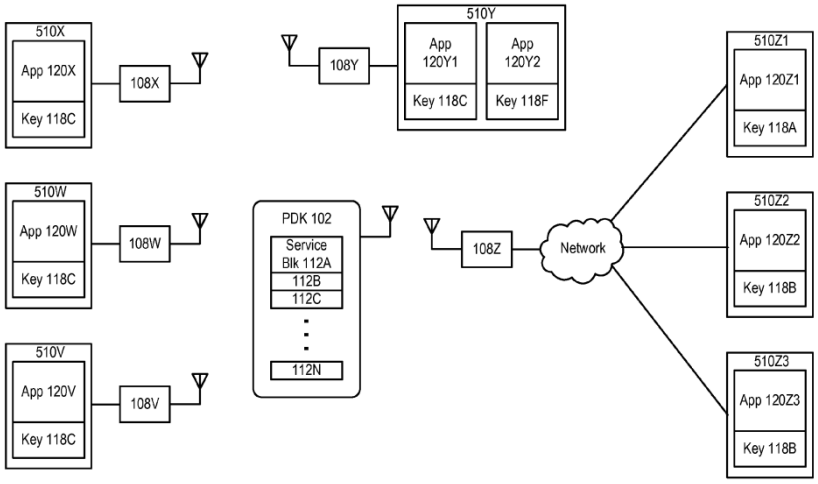


FIG. 6

Again, access to a service block is dependent on being able to exchange the right access key to unlock and retrieve the information held within the service block. Jakobsson Decl., ¶ 53. Thus, "applications 120W. 120X and 120Y1 can each access service block 112C since each application has access to service block access key 118C." 289 Patent, 29-32. The algorithm of control logic 250 allows multiple applications to use the same PDK simultaneously. Jakobsson

Decl., ¶ 51. For instance, "the first application 120Y1 might be the auto login/logoff, where a user logs in to a personal computer via a service block 112C that provides a username and password." 289 Patent, 9:47-50. As application 120Y1 has a copy of access key 118C, it can exchange access key 118C to unlock and retrieve the username and password in service block 112C. Jakobsson Decl., ¶ 51. After a user has logged onto the computer, the user may authenticate via biometric verification application 120Y2. Jakobsson Decl., ¶ 51. "Application 120Y2 compares this against a biometric stored in a second service block 112F on the PDK." 289 Patent, 9:55-56. Application 120Y2 can make the comparison because it has access key 118F, which can be exchanged to unlock and retrieve a biometric stored in service block 112F. Jakobsson Decl., ¶ 51. After biometric authentication, "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." 289 Patent, 9:59-62. Yet again, an application, function, or service is enabled by exchanging an access key to unlock and retrieve information held within the service block. Jakobsson Decl., ¶ 51.

The above examples from the specification unmistakenly link the algorithm of control logic 250 to the ability of "local, secured information stored by the integrated, secure memory" to perform the function of "enabling one or more of an application, a function and service." Therefore, claim 1 must be construed as including the algorithm of control logic 250. Absent such a construction, claim 1 would be indefinite. *Raining Computing*, 989 F.3d at 1007 ("And finally, if the patentee fails to disclose adequate corresponding structure, the claim is indefinite.").

2. Integrated RDC Communicating Wirelessly with the at Least One External Device within the Proximity Zone

Claim 1 also attributes the function of the "enabling one or more of an application, a function and service" to an "integrated RDC communicating wireless with the at least one external device within a proximity zone." "§ 112 para. 6 will apply if the challenger demonstrates that ***the***

claim term fails to recite sufficiently definite structure or else recites function without reciting sufficient structure for performing that function." *Raining Computing*, 989 F.3d at 1005 (emphasis added). The term "integrated RDC communicating wireless with the at least one external device within a proximity zone" is not a structure recognized by those of ordinary skill in the art to provide a sufficiently definite structure for performing the function of "enabling on or more of an application, a function and a service." Jakobsson Decl., ¶¶ 18 and 36. Accordingly, claim 1 invokes § 112, ¶ 6.

Since claim 1 invokes § 112, ¶ 6 by failing to recite a sufficiently definite structure for the performing the recited function, the claim must be construed. "The first step in construing a means-plus function claim is to 'identify the claimed function." *Raining Computing*, 989 F.3d at 1007. With respect to claim 1 the recited function is "enabling one or more of an application, a function and service." "After identifying the function, we then determine what structure, if any, disclosed in the specification corresponds to the claimed function." *Raining Computing*, 989 F.3d at 1007. Claim 1 recites the function is also performed by an "integrated RDC communicating wireless with the at least one external device within a proximity zone." On its face, the recited structure is nothing more than the ability to receive data via Bluetooth, Wi-Fi, and other wireless protocols. Jakobsson Decl., ¶¶ 55-57.

Furthermore, the specification does not provide any significant structure for the receiver decoder circuit. Jakobsson Decl., ¶¶ 56-57. The specification merely describes an RDC as follows:

> The RDC 304 provides the wireless interface to the PDK 102. Generally, the RDC 304 wirelessly receives data from the PDK 102 in an encrypted format and decodes the encrypted data for processing by the processor 306.

289 Patent, 7:45-48.

Dr. Jakobsson characterizes the RDC as "just a wireless interface that can decode or decrypt received data," as in Bluetooth, Wi-Fi and other wireless communication protocols. Jakobsson Decl., ¶ 57. Petitioner Microsoft, Co-Petitioner Apple, and Patent Owner are in full agreement with Dr. Jakobsson. Each has proposed a construction for RDC involving nothing more than a structure that receives data. Before the District Court, Microsoft asserted an RDC should be construed as "a circuit that ***wirelessly receives encrypted data*** from the PDK and decodes it". Exhibit 2005*, Microsoft Corporation Opening Claim Construction Brief,* at 17. Likewise, Apple proposed a construction of RDC as "a component or collection of components, capable of ***wirelessly receiving data*** in an encrypted format and decoding the encrypted data for processing." Exhibit 2013, *Defendant's Disclosure of Preliminary Claim Constructions,* at 4. Patent Owner has proposed the same construction as Co-Petitioner Apple. Exhibit 2006, *Plaintiff Proxense, LLC's Responsive Claim Construction Brief, Proxense v. Microsoft*, at 12. Accordingly, there is agreement that an RDC is nothing more than a receiver. But a "processor and transceiver amount to nothing more than a general-purpose computer." *HTC Corp. v. IPCom GmbH & Co., KG*, 667 F.3d 1270, 1280 (Fed. Cir. 2012). And, as noted above, creating a wireless link facilitating receipt of data does not enable an application, function, or service. Rather, enablement does not occur until an access key is exchanged to unlock and retrieve the contents of a service block, per control logic 250. Accordingly, an RDC alone is not a sufficiently definite structure.

"If the function is performed by a general-purpose computer or microprocessor, then the second step generally further requires that the specification disclose the algorithm that the computer performs to accomplish that function." *Rain Computing,* 989 F.3d at 1007 (Fed. Cir. 2021). As detailed above, an algorithm is provided in the specification as control logic 250, which when executed allow RDC to perform the function of "enabling one or more of an application, a

function and service." Claim 1, accordingly, must be construed as including the algorithm of control logic 250. Absent such a construction, claim 1 would be indefinite. *Raining Computing*, 989 F.3d at 1007 ("And finally, if the patentee fails to disclose adequate corresponding structure, the claim is indefinite.").

3. Enablement Signal

Claim 14 attributes the function of the "enabling one or more of an application, a function and service" to an "enablement signal." "§ 112 para. 6 will apply if the challenger demonstrates that ***the claim term fails to recite sufficiently definite structure*** or else recites function without reciting sufficient structure for performing that function." *Raining Computing*, 989 F.3d at 1005 (emphasis added). The term "enablement signal" is not a structure recognized by those of ordinary skill in the art to provide a sufficiently definite structure for performing the function of "enabling on or more of an application, a function and a service", rather it is meaningless nonce merely reciting the function it performs. Jakobsson Decl., ¶ 58. Accordingly, claim 14 invokes § 112, ¶ 6.

Since claim 14 invokes § 112, ¶ 6 by failing to recite a sufficiently definite structure for the performing the recited function, the claim must be construed. "The first step in construing a means-plus function claim is to 'identify the claimed function." *Raining Computing*, 989 F.3d at 1007. With respect to claim 14 the recited function is "enabling one or more of an application, a function and service." "After identifying the function, we then determine what structure, if any, disclosed in the specification corresponds to the claimed function." *Raining Computing*, 989 F.3d at 1007. Claim 14 recites the function is performed by an "enablement signal."

On its face, the recited structure is nothing more than the ability to receive data. As defined by the American Heritage Dictionary, the term signal means "[t]he sound, image, or message transmitted or received by means of telecommunications." American Heritage Dictionary Entry:

signal (ahdictionary.com), https://ahdictionary.com/word/search.html?q=signal. Thus, an enablement signal is nothing more than the receipt of data by a computer. If the receipt of data were sufficient to enable the function of "enabling or more of an application, a function and service," then the "enablement signal" would be a sufficiently definite structure. *Ergo Licensing, LLC,* 673 F.3d at 1365 ("We explained that in substance, claiming 'means for processing,' 'receiving,' and 'storing' may simply claim a general-purpose computer, although in means-plus-function terms"). Claim 14, however, clearly says otherwise. The first element of claim 14 is "creating a first wireless link," which is followed by "receiving a first signal." But the link and the first signal don't "enable one or more of an application, a function and service." Claim 14, rather, recites "***generating*** an enablement signal enabling one or more of an application, a function and service." Accordingly, by the express langue of claim 14, the mere receipt of data via a wireless link is insufficient to perform the function of "enabling one or more of an application, a function and service."

The specification, thankfully, details an enablement signal and how it is generated, with reference to Figures 14 and 15 (reproduced below).

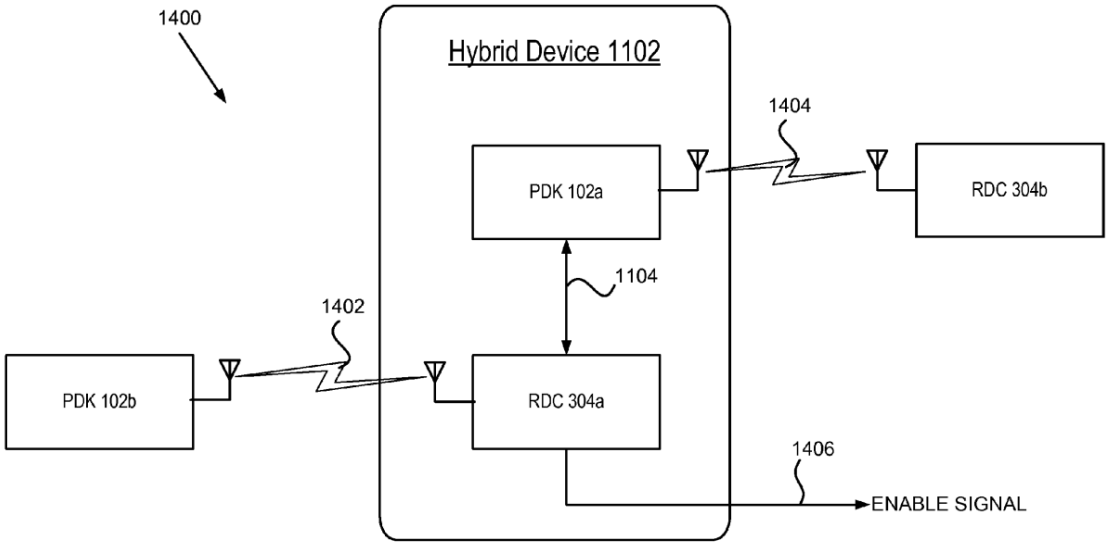

1400
Hybrid Device 1102
1404
PDK 102a
RDC 304b
1104
1402
PDK 102b
RDC 304a
1406
ENABLE SIGNAL

FIG. 14

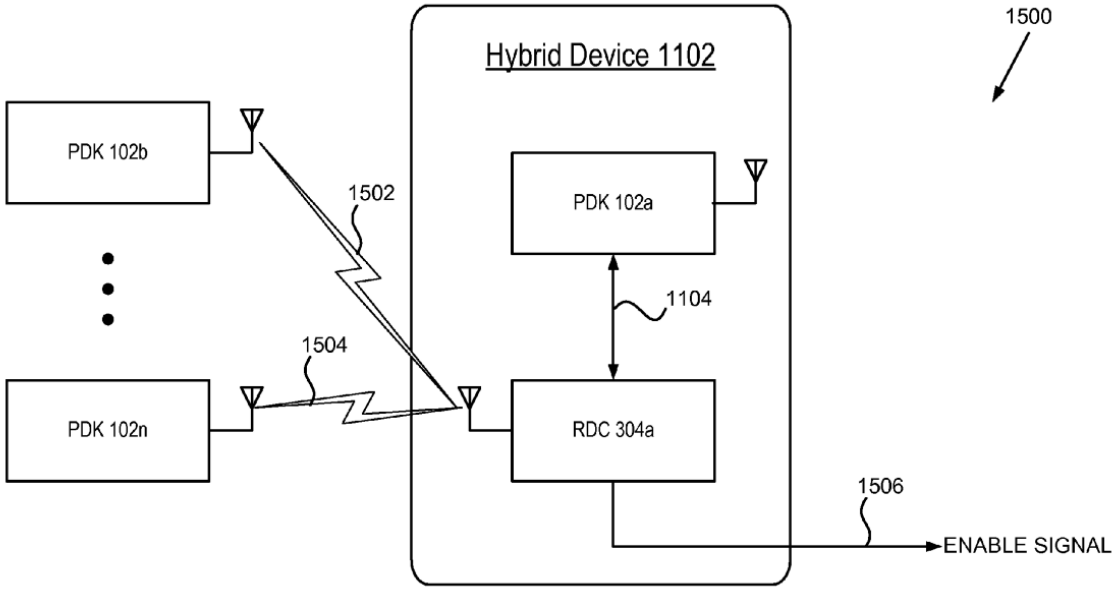

1500
Hybrid Device 1102
PDK 102b
1502
PDK 102a
1104
1504
PDK 102n
RDC 304a
1506
ENABLE SIGNAL

FIG. 15

The specification details that a link between an RDC and PDK is required to generate an enablement signal on a signal line between an RDC and a device. Referencing Figure 14, the specification states, "***only when the hybrid device 1102 has multiple links 1402, 1404*** will the hybrid device 1102 ***generate an authorization or enable signal*** on signal line 1406." 289 Patent, 17:47-50. Links 1402, 1404 are between PDKs 102b, 102a and RDCs 304a, 304b, respectively. "If either the RDC 304b or PDK102b is not present, the hybrid device 1102 does not allow operation of the personal computer." 289 Patent, 17:64-66. Another embodiment requiring the same is shown in Figure 15. "For the system 1500, only when multiple PDK links 1502,1504 to the hybrid device 1102 exist, will an authorization/enablement signal be generated on signal line 1506." 289 Patent, 18:4-6. Generating an enablement signal, therefore, depends upon the operation and interaction of a PDK and RDC. Jakobsson Decl., ¶ 60.

As noted above, Petitioner Microsoft, Co-Petitioner Apple, Patent Owner, and Dr. Jakobsson all agree that an RDC is nothing more than a receiver. But a "processor and transceiver amount to nothing more than a general-purpose computer." *HTC Corp.*, 667 F.3d at 1280. Accordingly, the RDC necessary to generate an "enablement signal" is a general purpose computer and thus cannot provide the sufficiently definite structure. *Rain Computing,* 989 F.3d at 1007 ("If the function is performed by a general-purpose computer or microprocessor, then the second step generally further requires that the specification disclose the algorithm that the computer performs to accomplish that function."). The same is true for a PDK.

The specification states, that "[i]n a minimal embodiment, the PDK 102a 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." 289 Patent, 14:20-23. Consistent with this definition, Petitioner requested the District Court construe a PDK as "a device that includes ***an antenna, a***

transceiver for communicating with the RDC and ***a controller and memory*** for storing information particular to a user." Exhibit 2005, *Microsoft Corporation Opening Claim Construction Brief,* at 11 (emphasis added). Likewise, Apple proposed a construction of RDC 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." Exhibit 2013, *Defendant's Disclosure of Preliminary Claim Constructions,* at 4 (emphasis added). Patent Owner has proposed the same construction as Co-Petitioner Apple. Exhibit 2006, *Plaintiff Proxense, LLC's Responsive Claim Construction Brief, Proxense v. Microsoft*, at 10. Here again, a processor and transceiver amount to nothing more than a general purpose computer. *See HTC Corp.*, 667 F.3d at 1280 (Fed. Cir. 2012). Likewise, memory storing information particular to a user requires an algorithm. "[C]omputer-readable media or storage devices amount to nothing more than a general-purpose computer." *Rain Computing,* 989 F.3d at 1007 (Fed. Cir. 2021). A PDK thus amounts to nothing more than a general-purpose computer. "If the function is performed by a general-purpose computer or microprocessor, then the second step generally further requires that the specification disclose the algorithm that the computer performs to accomplish that function." *Id.* Accordingly, as both the PDK and RDC, which generate the "enablement signal enabling one or more of an application, a function and service," are general purpose computers, an algorithm is required.

As noted above, an algorithm executed by the controller of the PDK is detailed in the specification as "control logic 250." As noted previously detailed, the specification summarizes the operation of the algorithm as "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***." 289 Patent, 6:57-60. "If the function is performed by a general-purpose computer or microprocessor,

then the second step generally further requires that the specification disclose the algorithm that the computer performs to accomplish that function." *Rain Computing,* 989 F.3d at 1007. Claim 14, accordingly, must be construed as including the algorithm of control logic 250. Absent such a construction, claim 14 would be indefinite. *Raining Computing*, 989 F.3d at 1007 ("And finally, if the patentee fails to disclose adequate corresponding structure, the claim is indefinite.").

D. Prior Construction by the District Court

In instituting the presence proceedings, the Board determined that the District Court did not construe similar limitations in Claim 1 of related U.S. Patent No. 9,049,188 (hereafter "188 Patent") and Claim 1 of related U.S. Patent No. 9,235, 700 (hereafter "700 Patent") simply because the District Court's Memorandum in Support of Claim Construction Order (Ex. 2002) discusses the term "hybrid device". Paper 8, 11-12. Such a cursory analysis, however, ignores the entirety of the District Court proceedings.

The District Court was asked to construe the term "hybrid device", which Samsung alleged was indefinite. Consistent with Patent Owner's proposed claim construction, the District Court construed a "hybrid device" to be a "device comprising an integrated personal digital key (PDK) and an integrated receiver-decoder circuit [(RDC)]." Ex. 2002, at 25. The District Court then construed each of the terms PDK and RDC. A PDK was construed by the District Court to be 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." Ex. 2002, at 27. But as noted above, such a construction is nothing more than a general-purpose computer. The District Court also construed the term RDC as a "component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing." Ex. 2002, at 36. Such a construction, as also noted above, is also

nothing more than a general-purpose computer. Accordingly, the District Court effectively construed the term "hybrid device" to be a combination of two general-purpose computers.

Like the current claims at issue, claim 1 of the 188 Patent and claim 1 of the 700 Patent each recite "one or more of the ***integrated RDC*** and ***integrated PDK enabling one or more of an application, a function, and a service.***" Additionally, the claim 10 of the 188 Patent, claim 11 of the 700 Patent, and claim 14 of the 289, each recite "generating an enablement signal enabling one or more of an application, a function and a service." Thus, the claims at issue before the District Court recited the same functions at issue here (*i.e.*, "enabling one or more of an application, a function, and a service") performed by the what the District Court had construed to be general-purpose computers. "If the function is performed by a general-purpose computer or microprocessor, then the second step generally further requires that the specification disclose the algorithm that the computer performs to accomplish that function." *Rain Computing,* 989 F.3d at 1007. Should an adequate structure not be found within the specification, then the claim is indefinite. *Raining Computing*, 989 F.3d at 1007 ("And finally, if the patentee fails to disclose adequate corresponding structure, the claim is indefinite."). Accordingly, to the find the claims definite under § 112, the District Court had to find an algorithm in the specification allowing a PDK and/or RDC to "enable one or more of an application, a function, and service."

The District Court did so by paraphrasing the algorithm defining "local, secured information" that is implemented by "control logic 250" and demonstrated in all examples presented in the specification of "enabling one or more of an application, a function, and service." As such the District Court held:

> Claims 1 and 10 of the 188 Patent and claims 1 and 11 of the 700 Patent state, 'one or more of the ***integrated RDC*** and ***integrated PDK enabling one or more an application, a function and a service.***' An application, function, or service is

> 'enabled' by a PDK when it ***receives information from a PDK in exchange for an access key***. Similarly, ***an RDC 'enables*** one or more of an application, a function, and a service' ***when it forwards such a message to the application, function, or service***.

Ex. 2002, at 26.

Absent construing claims 1 and 10 the of the 188 Patent and claims 1 and 11 of the 700 Patent to include the algorithm defining local, secured information that is implement by control logic 250, or some other algorithm disclosed in the specification, the District Court would have been required to find claims indefinite. The District Court, therefore, construed the claims 188 and 700 Patents to include the algorithm implemented by control logic 250, which defines local, secured information. In view of the foregoing, Patent Owner respectfully requests the Board reconsider its characterizations of the District Court proceedings.

V. RESPONSE TO GROUNDS FOR INVALIDITY RAISED

A. [Ground 1A/1B] – Claims 1-20 Are Not Rendered Obvious by Giobbi-157 and Giobbi-139 [1A] nor by Giobbi-157, Giobbi-139, and Dua [1B]

The Petition fails to demonstrate that the combination of Giobbi 157 (U.S. Publication No. 2007/0245157), Giobbi 139 (U.S. Publication No. 2004/0255139), and Dua (U.S. Patent No. 9,042,819) discloses or renders obvious "enabling one or more of an application, a function, and a service." These references thus cannot render the challenged claims invalid and unpatentable.

Independent claims 1 and 14 each recite "enabling one or more of an application, a function, and a service." For the reasons stated above, claims 1 and 14 invoke 35 U.S.C. § 112, ¶ 6, such that the algorithm represented by control logic 250 and defining "local, secured information" performs the function of "enabling one or more of an application, a function and service. The Petition fails to establish Giobbi 157, Giobbi 139, or Dua, alone or in combination,

"enables an application, a function, and a service" using the algorithm. Consequently, the Petition fails to establish claims 1 and 14, and the claims dependent thereon, are invalid and unpatentable.

As noted *supra,* the algorithm of control logic 250, which defines "local, secured information," requires exchanging an access key to retrieve and unlock information held within a service block. The Petitioner alleges that this element can be found in the authentication process shown in Figure 4 of Giobbi 157. Petition, at 34-35, and 55-57. The process detailed in Figure 4 of Giobbi 157 includes sending various messages between a PDK and RDC. However, Giobbi 157 does not contemplate that the information is received in exchange for an access key.

At most, Giobbi 157 discloses starting an exchange with an unsecure connection. Giobbi 157 explains that the process shown in Figure 4 begins "[w]hen a PDK 102 comes within range of a Reader 108, communication is automatically established 402 between the RDC 304 and the PDK 102. . . . Generally, initial communication between the Reader 108 and the PDK 102 is not encrypted in order to provide faster and more power efficient communication." Giobbi 157, ¶ [0059]. After establishing unsecure communication, "[i]n step 404, a device authentication is performed. Here, the Reader 108 establishes if the PDK 102 is a valid device and the PDK 102 establishes if the Reader 108 is valid." Giobbi 157, ¶ [0060]. In performing device authentication,

> [t]he RDC 304 receives information and analyzes 502 information from the PDK 102; and the PDK 102 receives and analyzes 502 information received from RDC 304. Generally, this initial information is transmitted over a public communication channel in an unencrypted format. Based on this information, each device 102, 304 determines 504 if the other is valid . . . . If both the PDK 102 and the RDC 304 are determined by the other to be valid, the Reader 108 requests and receives 506 authentication type information from the PDK 102 indicating the different types of authentication the PDK 102 is capable of

> satisfying based on the types of profiles the PDK 102 stores . . . . If the PDK 102 does have one or more sufficient types of profiles, the devices are valid 510.

Giobbi 157, ¶ [0061]. But nowhere does Giobbi 157 teach or describe that this unsecure exchange of information is accomplished by providing an access key in exchange for information held locally in the PDK's service blocks, as required in the challenged claims.

The second exchange in Giobbi 157 similarly does not disclose providing an access key to retrieve and unlock information. After the initial exchange to validate the PDK and RDC:

> The method next determines 410 whether profile authentication is required based on the configuration of the Reader 108, the type of transaction desired or by request of a merchant or other administrator. If the Reader 108 configuration does not require a profile authentication in addition to the PDK authentication, then the Reader 108 proceeds to complete the transaction for the PDK 102 . . . . [C]ompleting 416 the transaction includes charging a credit card for a purchase. Alternatively, bank information, debit/check/ATM card information, coupon codes, or any other purchasing means information (typically stored in a profile memory field 232) can be transmitted by the PDK 102 in place of credit card information.

Giobbi 157, ¶ [0063]. Again, while the PDK may send a message containing various account information, Giobbi 157 fails to describe or otherwise teach unlocking such information from a service block in exchange for an access key, as required by the challenged claims.

Giobbi 157, therefore, fails to disclose "enabling one or more of an application, a function, and a service" as required by claims 1 and 14.

As an alternative to Giobbi '157, the Petition relies on Giobbi 139. Petition, at 37 and 58. Giobbi 139 merely teaches that when a "user's physical electronic key [is] within a short range

(e.g., few meters) of [a] playing device, the playing device reads [an] activation code carried in a secure radio frequency signal transmitted by the transceiver in the physical key to the transceiver in the [playing] device." Giobbi '139, ¶ [0036]. However, Giobbi 139 also fails to disclose that the "activation code" is provided in exchange for an access key provided by the playing device. Consequently, the playing of digital content as detailed by Giobbi 139 fails to "enabling one or more of an application, a function, and a service" as required by claims 1 and 14.

As neither Giobbi 157 nor Giobbi 139 disclose "enabling one or more of an application, a function, and a service" as required by claims 1 and 14, and given that the Petition fails to assert Dua discloses this element, the Petition fails to establish the combination of the combination of Giobbi '157, Giobbi '139, and Dua invalidates claims 1-20.

B. [GROUND 2A] – Claims 1-8, 10, 11, and 14-19 Are not Rendered Obvious by Broadcom

The Petition fails to demonstrate that Broadcom (EP 1 536 306) discloses or renders obvious "enabling one or more of an application, a function, and a service."

Independent claims 1 and 14 each recite "enabling one or more of an application, a function, and a service." For the reasons stated above, claims 1 and 14 invoke 35 U.S.C. § 112, ¶ 6, such that the algorithm represented by control logic 250 and defining "local, secured information" performs the function of "enabling one or more of an application, a function and service. The Petition fails to establish Broadcom "enables an application, a function, and a service" using the algorithm. Consequently, the Petition fails to establish claims 1 and 14, and the claims dependent thereon, are invalid and unpatentable.

As noted *supra,* the algorithm of control logic 250, which defines "local, secured information," requires exchanging an access key to retrieve and unlock information held within a service block. Broadcom, however, discloses accessing services by way of an RFID token freely

broadcasting credentials when activated by reader, which are subsequently passed onto a service provider for access. Accordingly, Broadcom at most teaches sending messages containing credential information from a token activated by proximity, which is distinct from the invention claimed in the Patent, as explained below.

"When a token 316 is relatively close to the RFID reader 306, an RF signal . . . may be received by an antenna 334 and processed by an RF interface 336 in the token 316." Broadcom, ¶ [0146]. "[T]he received RF signal may be used to power and activate the token 316." *Id*., ¶ [0147]. "[A]uthentication information such as network authentication credentials, passwords and/or certificates may be stored in a data memory . . . on the token 316." *Id*., ¶ [0148]. "When the token 316 is activated the RF interface may generate an RFID signal that is broadcasted by the antenna 334. Circuitry in the token 316 may be configured to modulate the RFID signal so that it includes some or all of the information stored on the token 316." I*d.*, ¶ [0149]. Broadcom's method of providing access to a service, accordingly, begins with a token sending a message containing authentication information. However, as the message is the result of the token being powered by an RF signal, the first message lacks information received from a token in exchange for an access key provided to the token.

Notably, no key is provided in exchange for the information. "[T]he RFID reader 306 that extracts the information from the RFID signal 330 may be located within an integrated circuit. . . [T]he integrated circuit 312 may include a cryptographic processor 308 that encrypts the information." *Id*., ¶ [0150]. "[A]fter the information is signed by a cryptographic processor 308, the service access processor 310 sends the signed information to the service processor 324." *Id.*, ¶ [0150]. "The service processor 324 then sends the received information to the cryptographic processor 322 for decryption. . . . The service processor then verifies that the received information

indicates that the user is authorized to access the requested service." *Id*., ¶ [0153]. "[T]he service processor 324 may then provide access to the requested service." *Id*., ¶ [0154]. After receiving the information, the reader encrypts it and forwards it along to a service provider. While decrypting the information may entail the use of a key, the service provider's key is used after the information has been received. Consequently, the information is not received in exchange for a key provided to the token, as required by the claims of the 289 Patent, but rather the key is used to read information that has already been received. Furthermore, the key is provided to the service provider to be enabled rather than by the service provider to be enabled. The message between the reader and the service provider, therefore, lacks information from the token received in exchange for an access key provided to the token by the application, function or service to be enabled, as required by the challenged claims. As a result, the Broadcom messages between token, the reader and the service provider are not "enabling one or more of an application, a function, and a service" as required by claims 1 and 14.

As Broadcom fails to disclose "enabling one or more of an application, a function, and a service" as required by claims 1 and 14, the Petition fails to establish that Broadcom invalidates claims 1-8, 10, 11, and 14-19.

C. [Ground 2B] – Claims 1-20 Are Not Rendered Obvious by Broadcom and Giobbi-157

As noted supra with respect to Ground 1A/1B, the Petition fails to establish that Giobbi 157 discloses all the elements of claims 1-20. Additionally, as noted supra with respect to Ground 2A, the Petition has not established Broadcom discloses all elements of the challenged independent claims 1 and 14. Accordingly, because elements of the independent claims are not met, the Petition fails to establish that Broadcom or Giobbi 157 or a combination thereof invalidate claims 1-20.

VI. CONCLUSION

The Petition fails to demonstrate that the combination of Giobbi 157, Giobbi 139, and Dua, and the combination of Broadcom and Giobbi 157 discloses "enabling one or more of an application, a function, and a service," as properly construed. The Petition, thus, fails to demonstrate the challenged claims invalid and unpatentable.

Dated: October 15, 2024

Respectfully submitted by,

By: */David L. Hecht/*
David L. Hecht (Reg. No. 61,618)
dhecht@hechtpartners.com
HECHT PARTNERS LLP
125 Park Avenue, 25th Floor
New York, NY 10017
P: (212) 851-6821

CERTIFICATE OF SERVICE (37 C.F.R. § 42.6(e))

Pursuant to 37 C.F.R. § 42.6(e), the undersigned hereby certifies that Patent Owner's Response was served on October 15, 2024 by e-mailing copies to the e-mail addresses as provided in Petitioner's Petition.

Dated: October 15, 2024

Respectfully submitted,

By: */David L. Hecht/*
David L Hecht Reg. No 61,618
Hecht Partners LLP
125 Park Avenue, 25th Floor
New York, NY 10017
Tel: 212-851-6821
E: dhecht@hechtpartners.com

Counsel for Patent Owner

CERTIFICATE OF WORD COUNT

Under the provisions of 37 C.F.R. § 42.24, the undersigned hereby certifies that word count for the foregoing Patent Owner Response (excluding the table of contents, certificate of service, word count, or listing of exhibits) total 10,261 words, which is less than the number of words allowed under 37 C.F.R. § 42.24(b)(1).

Dated: October 15, 2024

Respectfully submitted,

By: */David L. Hecht/*
David L Hecht Reg. No 61,618
Hecht Partners LLP
125 Park Avenue, 25th Floor
New York, NY 10017
Tel: 212-851-6821
E: dhecht@hechtpartners.com

Counsel for Patent Owner