**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

---

**BEFORE THE PATENT TRIAL AND APPEAL BOARD**

---

MICROSOFT CORPORATION,
Petitioner,

v.

PROXENSE, LLC
Patent Owner

---

U.S. Patent No. 10,073,960 B1
IPR Case No.: 2024-00405

# PROXENSE, LLC'S PRELIMINARY RESPONSE TO PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 10,073,960 B1

## TABLE OF CONTENTS


I. Introduction ..... 1

II. Claim Construction ..... 1

A. 37 C.F.R. § 42.100(b) Statement ..... 1

B. Previously Construed Terms: Enabling One or More of an Application, a Function, and a Service ..... 2

C. Term to be Construed on First Instance: Local Secured Information ..... 20

III. Response to Grounds for Invalidity Raised ..... 23

A. [GROUND 1A/1B] – Claims 1-20 Are Not Rendered Obvious by Giobbi-157 and Giobii-139 [1A] nor by Giobbi-157, Giobbi-139, and Dua [1B] ..... 23

1. Local, Secured Information ..... 24

2. Enabling One or More of an Application, a Function, and a Service ..... 26

B. [GROUND 2A] – Claims 1-8, 10, 11, and 14-19 Are not Rendered Obvious by Broadcom ..... 29

1. Local, Secured Information ..... 29

2. Enabling One or More of an Application, a Function, and a Service ..... 31

C. [GROUND 2B] – Claims 1-20 Are Not Rendered Obvious by Broadcom and Giobbi-157 ..... 33

IV. Conclusion ..... 34

**EXHIBIT LIST**

| No. | Exhibit Description |
|---|---|
| 2001 | Claim Construction Order in *Proxense v. Samsung Electronics, Co., Ltd. et al.,* No. 6.21-CV-00210-ADA |
| 2002 | Memo In Support of Claim Construction Order in *Proxense v. Samsung Electronics, Co., Ltd. et al.* |
| 2003 | Markman Transcript from *Proxense v. Samsung Electronics, Co., Ltd. et al.* |
| 2004 | Claim Construction Order in *Proxense v., Google LLC,* No. 6:23-cv-00320-ADA |
| 2005 | Opening Claim Construction Brief in *Proxense v. Microsoft Corporation,* No. 6:23-cv-00319-ADA |
| 2006 | Responsive Claim Construction Brief in *Proxense v. Microsoft Corporation* |
| 2007 | Reply Claim Construction Brief in *Proxense v. Microsoft Corporation* |
| 2008 | Sur-reply Claim Construction Brief in *Proxense v. Microsoft Corporation* |
| 2009 | Opening Claim Construction Brief in *Proxense v. Samsung Electronics, Co., Ltd. et al.* |
| 2010 | Reply Claim Construction Brief in *Proxense v. Samsung Electronics, Co., Ltd. et al.* |

# I. INTRODUCTION

Pursuant to 35 U.S.C. § 313 and 37 C.F.R. § 42.107, Patent Owner, Proxense LLC ("Proxense") submits the following Preliminary Response to the Petition for Inter Partes Review of claims 1-20 of U.S. Patent No. 10,073,960 B1 ("the 960 Patent") filed by Petitioner Microsoft Corporation ("Petitioner" or "Microsoft").

The patent at issue is currently being asserted against Petitioner in *Proxense v. Microsoft Corporation,* No. 6:23-cv-00319-ADA (W.D. Tex. May 2, 2023). Petitioner and Patent Owner have exchanged Markman briefs. Pursuant to Rule 42.100(b), when the District Court issues its claim construction, Patent Owner will file a request asking the Board to consider and adopt the District Court's construction. In other proceedings involving the 960 Patent family members, the same District Court has construed the challenged claims contrary to the specific grounds asserted in the Petition. Accordingly, it is unlikely that Petitioner could credibly pursue the specific grounds asserted in the Petition. *Inter partes* review, consequently, should not be instituted.

# II. CLAIM CONSTRUCTION

## A. 37 C.F.R. § 42.100(b) Statement

Terms appearing within the claims of the 960 Patent have twice been construed by a district court in *Proxense, LLC v. Samsung Electronics, Co., Ltd. et al.,* No. 6.21-CV-00210 (W.D. Tex. March 5, 2021) ("Proxense v. Samsung") and *Proxens, LLCe v., Google LLC,* No. 6:23-cv-00320-ADA (W.D. Tex. May 2, 2023) ("Proxense v. Google"). The Claim Construction Order and Memorandum in Support of Claim Construction Order issued in *Proxense v. Samsung,* along with a Transcript of the *Markman* hearing, are provided herewith as Exhibits 2001, 2002, and 2003, respectively. Likewise, the Claim Construction Order issued in *Proxense v. Google* is provided herewith as Exhibit 2004.

A *Markman* hearing regarding the challenged claims is currently pending in *Proxense v. Microsoft Corporation,* No. 6:23-cv-00319-ADA (W.D. Tex. May 2, 2023) ("Proxense v. Microsoft"). Petitioner filed is opening claim construction brief on November 6, 2023, a copy of which is attached as Exhibit 2005. Patent Owner filed its responsive claim construction brief on November 27, 2023, a copy of which is attached as Exhibit 2006. The Petitioner then filed a reply claim construction brief on December 11, 2023, a copy of which is attached as Exhibit 2007. Finally, Patent Owner filed a sur-reply claim construction brief on December 27, 2023, a copy of which is attached as Exhibit 2008. When the District Court issues its claim construction, Patent Owner will file a request asking the Board to consider the District Court's construction.

### B. Previously Construed Terms: Enabling One or More of an Application, a Function, and a Service

Pursuant to Rule 42.100(b), Patent Owner requests the Board to consider and adopt the relevant constructions previously given the following terms in both *Proxense v. Samsung* and *Proxense v. Google*. Though the former deals with different patents, the 960 Patent is part of the same family and is thus a related patent. This Board must "presume, unless otherwise compelled, that the same claim term in the same patent or related patents carries the same construed meaning." *Omega Engineering, Inc. v. Raytek Corp*., 334 F.3d 1314, 1334 (Fed. Cir. 2003).

The term "enabling one or more of an application, a function, and a service" appears in claims 1-3, 6-8, 10 and 14-16 of the 960 Patent.

Claim 1, in pertinent part, recites:

> "wherein one or more of (a) the integrated, wireless communication interface communicating wirelessly with the at least one external device within the proximity zone enables one or more of an application, a function, and a service and (b) the

local, secured information stored by the integrated, secure memory ***enables one or more of an application, a function, and a service***."

Claim 2 recites:

"wherein at least one of the ***one or more of the application, the function, and the service is enabled***, at least in part, on the device."

Claim 3 recites:

"wherein at least one of the ***one or more of the application, the function, and the service is enabled***, at least in part, external to the device using an external, wireless communication interface, the device communicatively coupled to wirelessly communicate with the external, wireless communication interface."

Claim 6 recites:

"wherein the local, secure information includes financial information and at least one of the ***one or more of the application, the function, and the service enabled*** completes a financial transaction based on the financial information."

Claim 7 recites:

"wherein the local, secure information includes financial information and at least one of the ***one or more of the application, the function, and the service enabled*** completes a financial transaction based on a signal received from the at least one external device by the by the integrated, wireless communication interface."

Claim 8 recites:

"wherein the local, secure information includes financial information and at least ***one of the one or more of the application, the function, and the service enabled*** completes a financial transaction based on an authorization of the financial

information using an external authentication database, the financial information transmitted to the external authentication database."

Claim 10 recites:

"wherein the ***one or more of the application, the function and the service enabled*** based on the local, secured information stored by the integrated, secure memory includes a first application, function or service based on a first subsets of local, secured information stored by the integrated, secure memory and a second application, function or service based on a second Subset of local, secured information, the first and second Subset of local, secured information having different accessibility."

Claim 14, in pertinent part, recites:

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

Claim 15 recites:

"wherein at least one of the ***one or more of the application, the function, and the service is enabled*** at least in part on the device."

Claim 16 recites:

"sending the enablement signal, wherein at ***least one of the one or more of the application, the function, and the service is enabled*** at least in part on a device external to the hybrid device and communicatively coupled to an external, wireless communication interface."

In response to arguments asserted in *Proxense v. Samsung* that the term "hybrid device" was indefinite, the District Court found it necessary to construe the term "enabled" such that:

> 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 'enable[es] one or more of an application, a function, and a service' when it forwards such a message to the application, function, or service. The claimed 'hybrid device' carries out these functions.

Exhibit 2002 at 26.

Petitioner ***has not challenged*** this construction in *Proxense v. Microsoft*. Unless compelled otherwise, this Board must "presume … that the same claim term in the same patent or related patents carries the same construed meaning." *Omega Engineering, Inc.*, 334 F.3d at 1334 (Fed. Cir. 2003). The construction of "enabled" provided by the District Court is consistent with the algorithm disclosed in the specification, and the implicit definition of "enabling" provided in the specification. Accordingly, there is no compelling reason for this Board not to presume the claim term carries the same meaning as previously construed by the District Court.

In the *Proxense v. Samsung* case, the District Court's consideration of Samsung's arguments and its resulting opinion and construction of "enables" are instructive. Samsung argued that the specifications, and claims 1-3 of the 188 Patent, and claims 1-3 of the 700 Patent shared internal inconsistencies, which allegedly made it impossible to determine "the precise boundaries of what is 'on the hybrid device' and what is 'external to the hybrid device". Exhibit 2010 at 12. Samsung further argued the specification was allegedly "unclear if the hybrid device needs to consist of both RDC and PDK, or can consist of only one of RDC and PDK". Exhibit 2009 at 16. But as noted above, the abstract of the 188 Patent, 700 Patent, and 960 Patent all begin by stating, "[a] hybrid device includes a personal digital key (PDK) and a receiver-decoder circuit (RDC)." Likewise, the Summary of each of the 188 Patent, 700 Patent, and 960 Patent describe that "various drawbacks of the prior art are overcome by providing a hybrid device including a personal digital

key (PDK) and a receiver-decoder circuit (RDC)." 188 Patent, 1:66-2:1; 700 Patent, 2:18-20; and 960 Patent, 2:32-34.

Samsung attempted to disregard these clear disclosures and asserted that the subsequent statement in the shared Abstract that "[t]he hybrid device operates in one of several modes including, PDK only, RDC only, or PDK and RDC" contradicted the beginning of the Abstract. Exhibit 2009 at 16. Samsung similarly argued that the statement in the specification of each patent that "for purposes of explanation below, each device is enabled with either or both RDC and PDK functionality" and that "[t]hose skilled in the art will recognize that in other embodiments, the hybrid device 1102 has multiple instances of PDK functionality or multiple instances of the RDC functionality or multiple instances of both" created ambiguity by "suggest[ing] just one of RDC or PDK functionality is sufficient". Exhibit 2009 at 16-17.

In subsequent briefing, Samsung argued that some alleged inconsistency from the specification extended into claims 1-3 of the 188 Patent and claims 1-3 of the 700 Patent. According to Samsung, the recitation in claim 2 in each of the 188 and 700 Patents that "one or more of the application, the function, and the service are enabled at least in part on the hybrid device" and the recitation in claim 3 in each of the 188 and 700 Patents that the same be enabled "external to the hybrid device" failed to provide certainty as what is "on the hybrid device" and what is "external to the hybrid device." Exhibit 2010 at 12-13. (Similar statements are found in claims 2 and 3 of the 700 Patent.)

During the *Markman* hearing, Samsung stated they "intend[ed] to spend most of [their] time talking about the 'hybrid device' term" because it represents "a critical issue in the case with respect to this family." Exhibit 2003 at 32:13-15. Regarding the Patent Owner's construction of "hybrid device," Samsung argued that the "construction of a hybrid device is inconsistent and

wrong, given the disclosure in the specification, because the hybrid device is described in the patent as having only RDC functionality." Exhibit 2003 at 39:19-22. Samsung alleged that this was "the rare case, Your Honor, that we submit where the patent itself provides the contradiction which the Federal Circuit says is a basis for invalidating these claims." Exhibit 2003 at 39:19-22.

Samsung's arguments failed, however, and the District Court found the term "hybrid device" to be definite and provided a construction for the term "enables" as used in claim 1 of the 188 and 700 Patents consistent with the entirety of the shared specification of the 188, 700, and 960 Patents. Claims are definite when "viewed in light of the specification and prosecution history, inform those skilled in the art about the scope of the invention with reasonable certainty." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S.Ct. 2120, 2129 (2014). "[A]n indefiniteness analysis under 35 U.S.C. § 112, ¶ 2 is inextricably intertwined with claim construction." *Cox Communications v. Sprint Communication Co. LP.*, 838 F.3d 1224, 1232 (Fed. Cir. 2016). "Accordingly, the common practice of training questions of indefiniteness on individual claim terms is a helpful tool. Indeed, if a person of ordinary skill in the art cannot discern the scope of a claim with reasonable certainty, it may be because one or several claim terms cannot be reliably construed." *Id.* The District Court, therefore, resolved the issue of indefiniteness by construing the claim term "enables."

"Enables" was the most logical claim term upon which to "train" the issue of indefiniteness. The thrust of Samsung's argument was that it is contradictory for a "hybrid device" to include both an integrated RDC and an integrated PDK – as the District Court construed the term – yet operate in one of (1) a PDK only mode, (2) an RDC only mode, or (3) PDK and RDC mode. Claim 1 of the 188 Patent and claim 1 of the 700 Patent themselves recite alternative modes of operations, with each reciting "one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service." The plain construction of this shared limitation is that

the RDC only "enabl[es] one or more of an application, a function, and a service," the PDK only "enabl[es] one or more of an application, a function, and a service," or both the RDC and PDK "enabl[e] one or more of an application, a function, and a service." Claims 2 and 3 of both the 188 and 700 Patents further limit one of the alternative modes of operation presented in claim 1. Accordingly, if "enables" could be construed then the claims are not indefinite. Samsung's effort attempting to establish otherwise has failed.

As the District Court construed the term, "[a]n application, function, or service is 'enabled' by a PDK when it receives information from a PDK in exchange for an access key." Exhibit 2002 at 26. That is, when the PDK only "enabl[es] one or more of an application, a function, and a service" it does so by providing information in exchange for an access key. This construction is consistent with the algorithm disclosed in the specification for "enabling" applications, functions, and/or services.

"[E]nabling," may further be defined by way of a means-plus-function analysis. The claims of the 188 and 700 Patents each recite the PDK "enabl[es] one or more of an application, a function, and a service." The PDK is thus defined in the claims as performing a function of "enabling." As such, 35 U.S.C. § 112, paragraph 6, may be considered. "When a claim term lacks the words 'means' … § 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 a sufficient structure for performing that function." *Williamson v. Citrix Online, LLC,* 792 F.3d 1339, 1349 (Fed. Cir. 2015) (citing *Watts v. XL Sys, Inc.,* 232 F.3d 877, 880 (Fed. Cir. 2000)).

Here, if a "PDK" is not a sufficiently definite structure, then § 112, ¶ 6 applies because it recites the function of "enabling." As detailed *supra*, the District Court construed a "PDK" as "including an antenna and a transceiver for communicating with a RDC and a controller and

memory for storing information particular to a user." Exhibit 2001 at 3-4; and Exhibit 2004 at 4. The District Court's construction finds supports in the specifications of the 188 Patent, 700 Patent, and 960 Patent, ***which all state*** that "[i]n 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 the user." 188 Patent, 13:46-49; 700 Patent, 14:4-7; and 960 Patent, 14:28-31. A "PDK" thus comprises two subassemblies. Under the relevant case law, neither assembly could suffice as the definite structure for "enabling one or more of an application, a function, and a service."

The first subassembly comprising "an antenna and a transceiver" would not be a definite structure for "enabling one or more of an application, a function, and a service." Even adding a "controller" (i.e., a processor), the requisite definite structure is not provided. *See HTC Corp. v. IPCom GmbH & Co., KG*, 667 F.3d 1270, 1280 (Fed. Cir. 2012) (citing *Aristocrat Techs. Austl. Pty LTD. v. Int'l Game Tech,* 521 F.3d 1328,1333 (Fed. Cir. 2008)) ("The processor and transceiver amount to nothing more than a general-purpose computer. We have 'consistently required that the structure disclosed in the specification be more than simply a general purpose computer or microprocessor.'"). What is required is "an algorithm that the [controller] and transceiver execute." *Id.* The first subassembly thus fails to disclose a sufficiently definite structure, absent an algorithm (which is provided in the specification).

The second subassembly comprising "a controller and memory" is similar. "[C]omputer-readable medial or storage devices amount to nothing more than a general-purpose computer." *Rain Computing v. Samsung Electronics America,* 989 F.3d 1002, 1007 (Fed. Cir. 2021). "Enabling one or more of an application, a function, and a service" requires more "than merely plugging in a general purpose computer." *Ergo Licensing, LLC v. CareFusion,* 303 F.3d 1361,1365 (Fed. Cir.

2012). "Rather, some special programming, i.e., an algorithm, would be required to [enable] the software application packages." *Rain Computing,* 989 F.3d at 1007. The second subassembly thus also fails to disclose a sufficiently definite structure, absent an algorithm (which is also provided in the specification).

Though the claims of the 960 Patent do not recite a "PDK" nor "hybrid device," they do recite the components of a "PDK." The District Court construed a "PDK" as "including an antenna and a transceiver for communicating with a RDC." Claims 1 and 14 each recite "an integrated, wireless communication interface." If "an antenna and a transceiver" is not a definite structure for "enabling one or more of an application, a function, and a service," then the wireless communication interface, which is necessary provided by an antenna and a transceiver, must also not be a sufficiently definite structure.

Claims 1 and 14 also recite "an integrated, secure memory storing local, secured information." The District Court construed a "PDK" as also including "a controller and memory for storing information particular to a user." Integrated, secure memory storing local, secured information is a type of memory. Consequently, if "a control and memory" is not a definite structure for "enabling one or more of an application, a function, and a service," then integrated, secure memory storing local, secured information must also not be a sufficiently definite structure.

Because neither the first subassembly nor second subassembly of a "PDK" would provide a sufficiently definite structure, absent an algorithm, "enabling" must be construed consistent with the only algorithm disclosed in the specification. The 188, 700 and 960 Patents each disclose the same algorithm: control logic 250:

> "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."

188 Patent, 6:23-31; 700 Patent, 6:43-51; and 960 Patent, 6:64-7:5.

Prior to disclosing control logic 250, each of the 188, 700 and 960 Patents detail that memory 210 of a "PDK" "stores various service blocks 112A-N." 188 Patent, 6:8-9; 700 Patent, 6:28-29; and 960 Patent, 6:49-50. Control logic 250 is thus an algorithm for accessing a service block (i.e., memory) of a "PDK" by providing the corresponding "access key."

In addition to providing an algorithm for accessing a service block of a "PDK" by providing a corresponding "access key," the specification of each of the 188, 700 and 960 Patents states that applications are "enabled" from a service block by providing the corresponding access key. This would provide the sufficiently definite structure.

Claim construction during IPR follows the *Phillips* standard. Under *Phillips,* "[t]he claims … do not stand alone. Rather they are part of a fully integrated written instrument, consisting principally of a specification that concludes with the claims." *Phillips v. AWH Corp.,* 415 F.3d 1303, 1315 (Fed. Cir. 2005) (en banc). Thus, when applying the *Phillips* standard, "[t]he specification is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term." *Id.*

> A claim term may be redefined without any explicit definitional format. To the extent Petitioner cites *Thorner v. Sony Computer Entertainment America, LLC*, 669 F.3d 1362 (Fed. Cir. 2012) for the proposition that there is a heavy presumption that claim terms carry their accustomed meaning in the relevant community at the relevant time, which presumption can only be overcome in only two specific circumstances, this is a common misapplication of *Phillips*: "[Columbia] argues

> that "there is a heavy presumption that claim terms carry their accustomed meaning in the relevant community at the relevant time" which can only be "overcome in only two circumstances: the patentee has expressly defined a term or has expressly disavowed the full scope of the claim." Appellant's Br. 26 (emphasis added) (citation and quotation marks omitted). For this proposition, it cites to several recent cases including *Thorner v. Sony Computer Entertainment America LLC*, 669 F.3d 1362 (Fed.Cir.2012). … Our case law does not require explicit redefinition or disavowal. *See, e.g.*, *Aventis Pharma S.A. v. Hospira, Inc.*, 675 F.3d 1324, 1330 (Fed.Cir.2012) ("This clear expression need not be in haec verba but may be inferred from clear limiting descriptions of the invention in the specification or prosecution history."). Indeed, our en banc *Phillips* opinion rejected this very approach."

*Trustees of Columbia Univ. v. Symantec,* 811 F.3d 1359, 1363 (Fed. Cir. 2016).

Even when a claim term's meaning in the specification differs from its meaning in the relevant community at the relevant time, "*Phillips* made clear, a claim term may be clearly redefined without an explicit statement of redefinition and even when guidance is not provided in explicit definitional format, the specification may define claim terms by implication such that the meaning may be found in or ascertained by a reading of the patent documents." *Trustees of Columbia Univ.* 811 F.3d at 1363-64 (Fed. Cir. 2016).

One manner of defining a claim term by implication is by consistent usage in the specification. "[W]hen a patentee uses a claim term throughout the entire patent specification, in a manner consistent with only a single meaning, he has defined that term 'by implication.'" *Bell Atlantic Network Serv. v. Covad Communications,* 262 F.3d 1258, 1271 (Fed. Cir. 2001). Moreover, "[w]hether a claim must, in any particular case, be limited to the specific embodiment presented in the specification, depends in each case on the specificity of the description of the invention and on the prosecution history." *Liebel-Flarsheim Company v. Medrad, Inc.,* 358, F.3d

898, 907 (Fed. Cir. 2004). Accordingly, *Liebel-Flarsheim* forecloses construing a claim term consistent with its usage in all disclosed embodiments, when "[t]he prosecution history [] affirmatively preclude[s] a narrow reading of the claim language." *Irdeto Access, Inc. v. Echostar Satellite Corp.*, 383 F.3d 1295, 1302 (Fed. Cir. 2004). Absent such disclaimer, a consistent usage throughout the embodiments in the specification defines a claim term by implication.

When the specification does not contemplate an alternative, even permissive language does not negate an implied definition. *See Irdeto Access,* 383 F.3d at 1301 ("All examples in the specification, *Irdeto* argues, are permissive rather than mandatory, illustrative rather than exhaustive, and do not necessarily or explicitly exclude a group made up of all subscribers… Yet *Irdeto* cannot explain every example in the specification, all of which consistently point to an implicit definition of group as a subset of all subscribers in the system.).

Under these guiding principles of *Phillips*, the specification of the 188, 700 and 960 Patents implicitly define that "an application, function, or service is 'enabled' by a PDK when it receives information from a PDK in exchange for an access key." Exhibit 2002 at 26. With reference to common FIG. 6 (reproduced below), each Patent states:

> "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."

188 Patent, 9:4-13; 700 Patent, 26-35; and 960 Patent, 9:48-57. (emphasis added.).

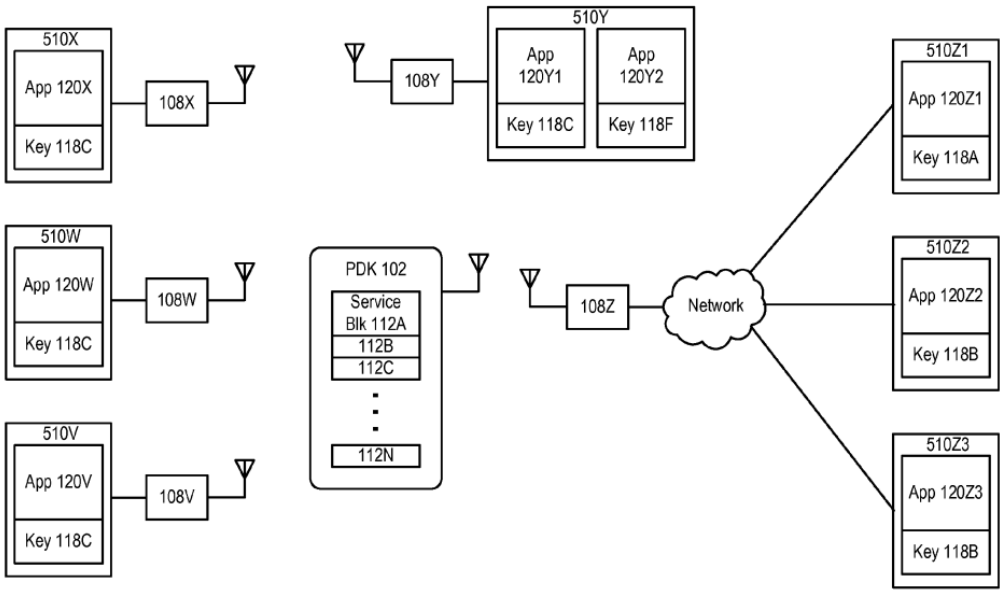


FIG. 6

As shown in FIG. 6., 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, Application 120Y1 is "enabled" from service block 112C when it receives the username and password held within service block 112C in exchange for access key 118C.

It would be erroneous under *Phillips* to disregard the above passage simply because it starts with the permissive language "in some cases". This language is not directed to the use of an access key to retrieve information from a service block to enable an application. Rather, it is directed to the number of applications on a device 510. As can be seen from FIG 6, device 510Y has two applications (App 120Y1 and App 120Y2), while the remaining six devices (510W, 510X, 510V, 510Z1, 510Z2, 510Z3) each only have a single application. Accordingly, device 510Y is a unique instance in FIG. 6 in which a device has two applications, each with unique access key, that are enabled from distinct service blocks. "In some cases," therefore, references the ability of a device to have more than one application enabled by a service block within the memory of a "PDK".

Furthermore, definition by implication is not negated by the inclusion of permissive language when the specification does not contemplate an alternative. *See Irdeto Access,* 383 F.3d at 1301 ("All examples in the specification, *Irdeto* argues, are permissive rather than mandatory, illustrative rather than exhaustive, and do not necessarily or explicitly exclude a group made up of all subscribers… Yet *Irdeto* cannot explain every example in the specification, all of which consistently point to an implicit definition of group as a subset of all subscribers in the system.). The remainder of the above passage consistently describes an application, a function, or a service being enabled by a PDK when it receives information from a service block of the PDK in exchange for an access key, as do the remaining examples presented in the specification.

After "application 120Y1 is ***enabled*** from a first service block 112C" to permit logging into a PC, the process continues by enabling a biometric verification application 120Y2 with biometrics stored in a second service block 112F.

> 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.

188 Patent, 9:13-21; 700 Patent, 35-44; and 960 Patent, 9:57-66.

As shown in FIG. 6, 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, biometric verification application 120Y2 is enabled by exchanging its access key 118F for the biometric held within service block 112F to compare against the live biometric information.

After enabling biometric verification application 120Y2 with the biometrics from service block 112F, a credit card service 120Z1 is enabled from service block 112A by providing access key 118A.

> "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."

188 Patent, 9:21-26; 700 Patent, 9:44-49; and 960 Patent, 9:66-10:3.

As shown in FIG. 6, 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, the credit card service 120Z1 is enabled by exchanging its access key 118A for the account data held within service block 112A to authorize a transaction.

The remaining examples of "enabling an application, a function, or a service" presented in the specification also detail receiving information from a PDK in exchange for an access key. The example presented in FIG. 1 details use of a biometric verification function being enabled by stored biometric received from a service block on a "PDK" in exchange for an access key.

> 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.

188 Patent, 3:22-33; 700 Patent, 3:42-53; and 960 Patent, 3:58-4:2.

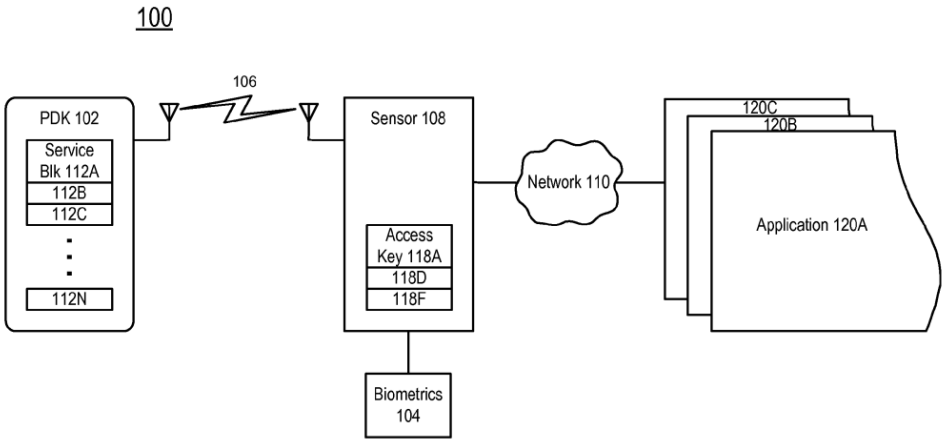


FIG. 1

Here again, an access key (118A) is provided to a "PDK" to obtain data held within a service block (118A) of the "PDK." The valid biometric obtained is compared against a current biometric as to enable biometric verification. Accordingly, a biometric verification function is enabled by exchanging its access key 118A for the biometric data held within service block 112A.

While the above may conclude with the statement that "[u]pon 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 specification makes clear that biometric verification alone is not sufficient. "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." 188 patent, 6:23-26; 700 Patent, 6:43-46; and 960 patent, 6:64-67 (emphasis added). Thus, biometric verification and exchanging an access key for information held within a service block may ***both*** be needed, but biometric verification alone will not be sufficient to enable applications 120.

Consistent with the requirement that an application, function, or service is "enabled" by a PDK when it receives information from a PDK in exchange for an access key, the specification presents another example referencing FIG. 4:

"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."

188 Patent, 8:19-29; 700 Patent, 8:40-50; and 960 Patent, 8:62-9:5.

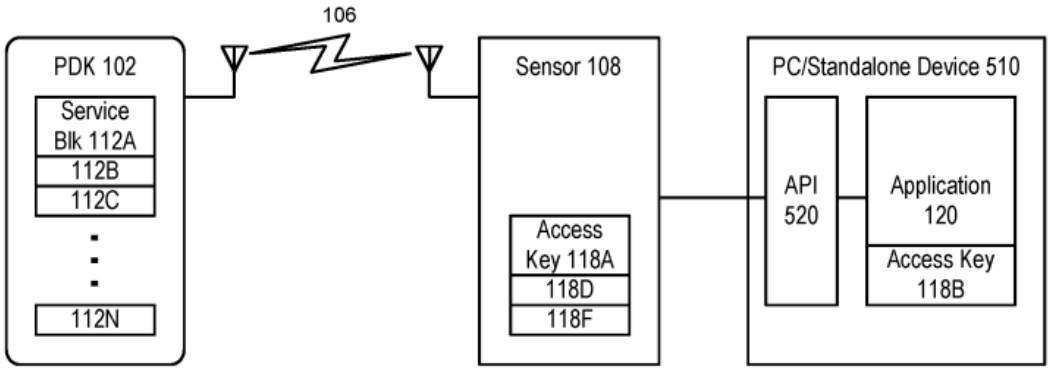


FIG. 4

As with the others, the login/logoff application 120 sends an access key (118B) to obtain the contents of a service block (112B) within a "PDK," which is returned to allow login. Accordingly, the login/logoff application 120 is enabled by exchanging its access key 118B for the username and password data held within service block 112B.

Again with reference to FIG. 5, the specification presents a final example of how an application, function, or service is "enabled" by a PDK when it receives information from a PDK in exchange for an access key:

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.

188 Patent, 8:30-42; 700 Patent, 8:51-63; and 960 Patent, 9:6-19.

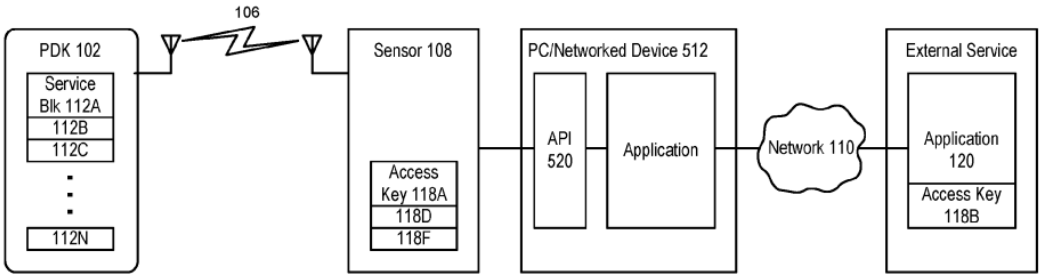


FIG. 5

Immediately following the above two example, the specification of each patent states that "[t]hese two examples illustrate basic concepts of the capabilities of the service blocks and how an application (service) may use them." 188 Patent, 8:43-45; 700 Patent, 8:64-66; and 960 Patent, 9:20-22. Illustrating the "basic concepts of the capabilities of service blocks," the referenced examples make a statement describing the invention as a whole with respect to the operation of service blocks to enable one or more of an application, a function, and a service. This further evidences that "enabling one or more of an application, function and service" is implicitly defined as exchanging an access key for information held within a service block of a PDK. *Modine Mfg. Co. v. US Intern. Trade Com'n,* 75 F.3d 1545, 1551 (Fed. Cir. 1996) ("[A]lthough Modine stresses the rule that the description of the preferred embodiment in the specification does not limit the

claims to that embodiment, when the preferred embodiment is described in the specification as the invention itself, the claims are not necessarily entitled to a scope broader than that embodiment.”).

By consistently describing “enabling one or more of an application, a function, and a service” as receiving information from a PDK in exchange for an access key, the specifications of the 188, 700, and 960 Patents implicitly define “enabled” as construed by the District Court. The construction of “enabled” provided by the District Court is thus not only consistent with the algorithm disclosed in the specification of each Patent, but also the implicit definition of “enabling” provided in the specification of each Patent. Accordingly, there is no compelling reason for this Board not to presume the claim term carries the same meaning as construed by the District Court.

**C. Term to be Construed on First Instance: Local Secured Information**

The term “local, secured information” appears in independent claims 1, 4-8, 10, 14, 17 and 18.

Claim 1, recites in pertinent part:

> “an integrated, secure memory storing ***local, secured information***;”
>
> “the ***local, secured information*** stored by the integrated, secure memory enables one or more of an application, a function, and a service.”

Claim 4 recites:

> “wherein the ***local, secured information*** includes biometric information for authenticating a user”

Claim 5 recites:

> “wherein the ***local, secured information*** includes biometric information based on a biometric scan of a finger, the biometric information for authenticating a user.”

Claim 6 recites:

"wherein the ***local, secure information*** includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information."

Claim 7 recites:

"wherein the ***local, secure information*** includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on a signal received from the at least one external device by the integrated, wireless communication interface."

Claim 8 recites:

"wherein the ***local, secure information*** includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on an authorization of the financial information using an external authentication database, the financial information trans mitted to the external authentication database."

Claim 10 recites:

"wherein the one or more of the application, the function and the service enabled based on the ***local, secured information*** stored by the integrated, secure memory includes a first application, function or service based on a first subsets of ***local, secured information*** stored by the integrated, secure memory and a second application, function or service based on a second subset of ***local, secured information***, the first and second subset of local, secured information having different accessibility."

Claim 14, in pertinent part, recites:

"the integrated, secure memory stores ***local, secured information***;"

Claim 17 recites:

"wherein the ***local, secured information*** includes biometric information for authenticating a user."

Claim 18 recites:

"wherein the ***local, secured information*** includes financial information and wherein the one or more of the application, the function and the service completes a financial transaction."

Claim construction during IPR follows the *Phillips* standard as described above. *Phillips,* 415 F.3d at 1315. The specification defines "local secured information" as information stored within a service block of a PDK and unlocked with a corresponding access key provided to the PDK. This definition is provided in the following passage:

> "The PDK102 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***." 960 Patent, 3:50-57 (emphasis added).

This is the only instance in the specification where the term "local secured memory" appears, and this only appearance is in the form of a definition that clearly defines "which information is used as ***local secured information.***" The implication of the above passage is that local secured information is that information stored within service block of a PDK and unlocked with a corresponding access key provided to the PDK. This is not merely secure memory nor is it

merely secured information. It is "local secured information," a concept defined by the specification.

Notably, the permissive language "in this example" does not expand the definition "local secure information," it applies to the sensors. The specification contains the following arguably permissive language: "In this example, the sensor 108 contains three of the service block access keys 118A, D, F." The inclusion of such language, however, does not negate the definition provided for "local secured information," especially when the specification does not contemplate an alternative for "local secured memory." *See Irdeto Access,* 383 F.3d at 1301. Indeed, replacing "local secure information" with just any "secure memory" would ignore a major aspect of the invention: the service block, access key pair system. No other examples are provided. As that definition of "local secure information" is the only instance in which the term appears, there is no alternative considered. Moreover, the above statement is made with reference to FIG. 1, which shows a sensor 108 containing three access keys 118A, D, F. The phrase "[i]n this example" is referencing the number of access keys held by the sensor 108 depicted in FIG. 1. In other examples, such as that shown in FIG. 6, sensors 108V, W, X, Y, and Z completely lack an access key 118. Accordingly, the statement is referencing the number of access keys a sensor 108 may have. Made with respect to the sensor 108, the statement has no bearing on components of the PDK nor the local secured information held within the service blocks of the PDK.

"Local, secured information" is thus defined in the specification as information stored within a service block of a PDK and unlocked with a corresponding access key provided to the PDK.

## III. 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 (a) "local, secured information," or (b) "enabling one or more of an application, a function, and a service." These references thus cannot render the challenged claims invalid and unpatentable.

**1. Local, Secured Information**

Independent claims 1 and 14 each recite "local, secured information." As noted supra, the specification defines "local, secured information" as information stored within a service block of a PDK and unlocked with a corresponding access key provided to the PDK. The Petition fails to establish such "local, secured information" is disclosed by Giobbi '157, Giobbi '139, or Dua, and thus fails to render claims 1 and 14, and the claims dependent thereon, invalid and unpatentable.

Petitioner asserts that Giobbi '157 discloses the "local, secured information" claimed by the challenged patent in its use of "a tamper-proof memory." Petition, 28-29. But Giobbi '157 does not go so far. Giobbi '157 only discloses a "portable device, referred to herein as a Personal Digital Key or 'PDK', stores one or more profiles . . . in a tamper-proof memory." Giobbi '157, ¶ [0011]. "The memory 210 can be read-only memory, a once-programmable memory, a read/write memory or any combination of memory types including physical access secured and tamper-proof memories." *Id.*, ¶ [0036]. Instead, Petitioner inserts the words "secured information" and "secure" in square brackets into the quote from Giobbi-157 where those words do not appear, and would make no sense, in the Giobbi-157. Additionally, Giobbi '157 notes, "The PDK 102 stores digital information in a tamper-proof format that uniquely associates the PDK 102 with an individual." *Id.*, ¶ [0028]. This tamper proof memory refers to the format of an overall memory of the PDK. Giobbi '157 does not disclose or suggest that tamper proof memory can include storing information within a service block of the PDK that is unlocked with a corresponding access key

provided to the PDK. Tamper-proof memory alone in Giobbi '157 provides no prior disclosure of a "local, secured information" in the specific format disclosed by the 960 Patent.

The Petitioner next asserts that Dua teaches an "RFID setup may act as an 'electronic key.'" Petition, at 29. But other than generically stating lofty goals, Dua provides no such disclosure. Dua merely discloses:

> In accordance with the invention, RFID Tag-Reader Module 113 allows interoperability with RF 13.56 MHZ readers and tags compatible with existing international standards, including ISO 14443 A/B, ISO 15693, FeliCa™, and NFC. Compatibility with these standards gives media player 100 the ability to not only establish a wireless connection with other electronic devices using RFID for setup as earlier described, but also allows media player 100 to function as an electronic key and wallet (for point-of-sale transactions).

Dua, 12:52-61. Dua, however, does not disclose, teach, or even suggest how these standards provide an "electronic key," let alone that such a key can be provided by storing information locally within a service block of the RFID tag, which information is unlocked with a corresponding access key provided to the RFID tag.

The Petitioner also cites to the passage within Dua that states: "In the case of RFID reader 304 functionality, the antenna 114 is adapted to transmit one or more interrogation signals and to receive one or more response signals for retrieving information from an RFID tag in an external electronic device". Dua, 14:53-57; Petition, at 31. But Dua does not disclose that the "interrogation signals" provide an access key to the RFID tag to unlock information stored within a service block of the RFID tag.

Likewise, the general statements that "[t]he information stored in RFID tag unit 306 that can be retrieved by an RFID reader device is stored in memory" and that "[a]ccess to the configurable tag memory may be limited to one or more specific applications executed on media

player 100 to ensure data integrity, which may be required and necessary depending on the kind of information stored" (Dua, 15:42-56) fail to suggest or disclose that such access control is accomplished by providing an access key to the RFID tag to unlock stored information.

Finally, though Dua notes that "memory components in RFID Tag-Reader Module 113 may be tamper resistant as to prevent hackers from retrieving confidential information and encryption keys" (Dua 16:31-34), this general statement fails to disclose that tamper proofing is accomplished by storing confidential information or encryption keys "locally," meaning within a service block of a RFID tag and unlocked with a corresponding access key provided to the RFID tag.

The repeated failures of Dua to disclose information stored locally within a service block of a PDK and unlocked with a corresponding access key provided to the PDK (i.e., "local, secured information") are not corrected by paragraph [61] of Dr. Traynor's Declaration, which amounts to nothing more than a mere recitation of the paragraph spanning pages 29 and 30 of the Petition and cites the very same passages refuted above. Consequently, neither the Petition nor the Declaration of Dr. Traynor establish that Dua discloses "local, secured information" in the manner disclosed by the 960 Patent.

As neither Giobbi '157 nor Dua disclose a "local, secured information", and given that the Petition fails to assert Giobbi '139 discloses this element, the Petition fails to establish the combination of Giobbi '157, Giobbi '139, and Dua can invalidate claims 1-20.

**2. 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." The Petition fails to establish Giobbi '157, Giobbi '139, or Dua "enables an application, a function, and a service" as that term has been construed by the District Court. Consequently, the Petition fails to establish claims 1 and 14, and the claims dependent thereon, are invalid and unpatentable.

As detailed *supra,* in response to arguments asserted in *Proxense v. Samsung* that the term "hybrid device" was indefinite, the District Court found it necessary to construe the term "enabled" such that:

> 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 'enable[es] one or more of an application, a function, and a service' when it forwards such a message to the application, function, or service. The claimed 'hybrid device' carries out these functions.

Exhibit 2002 at 26.

The Petitioner alleges that this element can be found in the authentication process shown in Figure 4 of Giobbi '157. Petition, at 33-36, and 55-56. 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 provided to the PDK.

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 can be accomplished by providing an access key in exchange for information held locally in the PDK's service blocks as required by the challenged claims.

The second exchange in Giobbi '157 similarly does not disclose providing an access key. After the initial exchange to validate the PDK and RDC, "[t]he 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 does not describe or otherwise teach that the message contains information obtained from the PDK in exchange for an access key provided to the PDK. 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 construed by District Court and required by claims 1 and 14.

As an alternative to Giobbi '157, the Petition relies on Giobbi '139. Petition, at 36 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 fails to disclose that the "activation code" is provided in exchange for an access key provided by the playing device. Additionally, as an "activation code is carried in a secure radio frequency signal," the signal is a message providing information, *i.e.*, the activation code. Consequently, the playing of digital content as detailed by Giobbi '139 fails to disclose the claim limitation "enabling one or more of an application, a function, and a service".

As neither Giobbi '157 nor Giobbi '139 disclose "enabling one or more of an application, a function, and a service" as the term has been construed by the District Court and given that the Petition fails to assert Dua discloses this element, the Petition fails to establish 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 the claim limitations (a) "local, secured information," or (b) "enabling one or more of an application, a function, and a service,"

#### 1. Local, Secured Information

Independent claims 1 and 14 each recite "local, secured information." As noted *supra*, the specification defines "local, secured information" as information stored within a service block of

a PDK and unlocked with a corresponding access key provided to the PDK. The Petition fails to establish such "local, secured information" is disclosed by Broadcom, and thus fails to establish claims 1 and 14, and the claims dependent thereon, are invalid and unpatentable.

The Petition asserts such memory is Broadcom's "data memory 314". But "data memory 314" is not unlocked by an access key provided by the service provider as required by the challenged claim(s). Rather, data memory 314 is decrypted with a key provided by the processing system to which it belongs.

Broadcom fails to disclose data memory 314 stores information within a service block unlocked with a corresponding access key provided to a PDK—it only discloses the use of a key ***provided by a PDK*** to decrypt information received from data memory 314. Broadcom teaches "in the event keys need to be sent out of the integrated circuit 312 (e.g., to be stored in data memory 314), the key may be first encrypted." Broadcom, ¶ [0135]. The encrypted information held within data memory 314 "may be sent between the integrated circuit 312 and a cryptographic processor 322 and a service processor 324 in the service provider 304 via a communication link 326. In this case, the cryptographic processors 308 and 322 may perform key exchange and encryption, decryption . . . to send and receive the encrypted information and provide the information in the clear for internal processing." *Id*., ¶ [0138]. Broadcom thus teaches a cryptographic processor 308 that provides a key to the service provider. After the encrypted information from data memory 314 is received by the service provider, "the service processor 324 then sends the received information to the cryptographic processor 322 for decryption." *Id*., ¶ [0153]. Accordingly, the service provider uses a key provided by cryptographic processor 308 to decrypt the information transmitted from data memory 314. To the extent cryptographic processor 308 is part of a PDK, Broadcom discloses information within data memory 314 is decrypted with a key ***provided by the***

***PDK***. Consequently, Broadcom does not disclose data memory 314 is holding local, secured information. Broadcom, therefore, fails to invalidate claims 1-8, 10, 11, and 14-19.

**2. 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." The Petition fails to establish Broadcom "enables an application, a function, and a service" as that term has been construed by the District Court. Consequently, the Petition fails to establish claims 1 and 14, and the claims dependent thereon, are invalid and unpatentable.

As detailed *supra,* in response to arguments asserted in *Proxense v. Samsung* that the term "hybrid device" was indefinite, the District Court found it necessary to construe the term "enabled" such that:

> 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 'enable[es] one or more of an application, a function, and a service' when it forwards such a message to the application, function, or service. The claimed 'hybrid device' carries out these functions.

Exhibit 2002 at 26.

Broadcom discloses accessing services by way of an RFID token freely broadcasting credentials when activated by a reader, which are subsequently passed onto a service provider for access. Accordingly, Broadcom teaches sending messages containing credential information from a token activated by proximity, which is distinct from the invention claimed in the 960 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." *Id.*, ¶ [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 960 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 and reader and reader and service provider are not "enabling one or more of an application, a function, and a service" as construed by the District Court.

As Broadcom fails to disclose "enabling one or more of an application, a function, and a service" as the term has been construed by the District Court, 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.

## IV. CONCLUSION

The Petition fails to demonstrate a reasonable likelihood that the Petitioner will prevail as to any of the challenged claims. *Inter partes* review of the 960 Patent should therefore be denied.

Dated: April 29, 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 SERVICE (37 C.F.R. § 42.6(e))**

Pursuant to 37 C.F.R. § 42.6(e), the undersigned hereby certifies that Patent Owner Proxense, LLC's Preliminary Response was served on April 29, 2024 by e-mailing copies to the following e-mail addresses as provided in Petitioner's Petition:

ipr42342-0133ip1@fr.com and ptabinbound@fr.com

Dated: April 29, 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 COMPLIANCE(37 C.F.R. § 42.24)

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 9,836 words, which is less than the 14,000 words allowed under 37 C.F.R. § 42.24(b)(1).

Dated: April 29, 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*