Trials@uspto.gov
Tel: 571-272-7822

Paper 12
Entered: November 18, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

PROXENSE, LLC,
Patent Owner.

IPR2024-00784
Patent 10,073,960 B1

Before THU A. DANG, DAVID C. McKONE, and
NORMAN H. BEAMER, *Administrative Patent Judges.*

DANG, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background

Google LLC ("Petitioner") filed a Petition requesting an *inter partes* review of claims 1–20 (the "challenged claims") of U.S. Patent No. 10,073,960 B1 (Ex. 1001, "the '960 patent"). Paper 1 ("Pet."). Proxense, LLC ("Patent Owner") filed a Preliminary Response. Paper 5 ("Prelim. Resp."). With our authorization (Paper 8), Petitioner filed a Preliminary Reply to address Patent Owner's "means-plus-function" arguments in the Preliminary Response (Paper 9 ("Prelim. Reply")), and Patent Owner filed a Preliminary Sur-reply (Paper 11 ("Prelim. Sur-reply")).

Under 37 C.F.R. § 42.4(a), the Board has authority to determine whether to institute an *inter partes* review. Applying the standard set forth in 35 U.S.C. § 314(a), which requires demonstration of a reasonable likelihood that Petitioner would prevail with respect to at least one challenged claim, we grant Petitioner's request and institute an *inter partes* review of all challenged claims.

B. Related Proceedings

Petitioner identifies the '960 patent as the subject of *Proxense, LLC v. Microsoft Corp.*, No. 6.23-cv-00319 (W.D. Tex.) and *Proxense, LLC v. Google LLC*, No. 6:23-cv-00320 (W.D. Tex.) ("the parallel district court litigation"). Pet. 81–82. The claims of the '960 patent are also challenged in the *inter partes* review of *Microsoft Corp. v. Proxense, LLC*, IPR2024-00405. *Id.* at 82; Paper 6, 1.

C. The '960 Patent

The '960 patent, titled "Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use," issued on September 11, 2018, from Application No. 15/595,739, with a filing date of May 15, 2017. Ex. 1001, codes (54), (45), (21), (22). The '960 patent provides a hybrid device including a personal digital key (PDK) and a receiver-decoder circuit (RDC) that are coupled for communication with each other. *Id.* at code (57).

An illustration of the embodiment of the '960 patent's hybrid device as part of a cell phone is depicted in Figure 12, reproduced below:

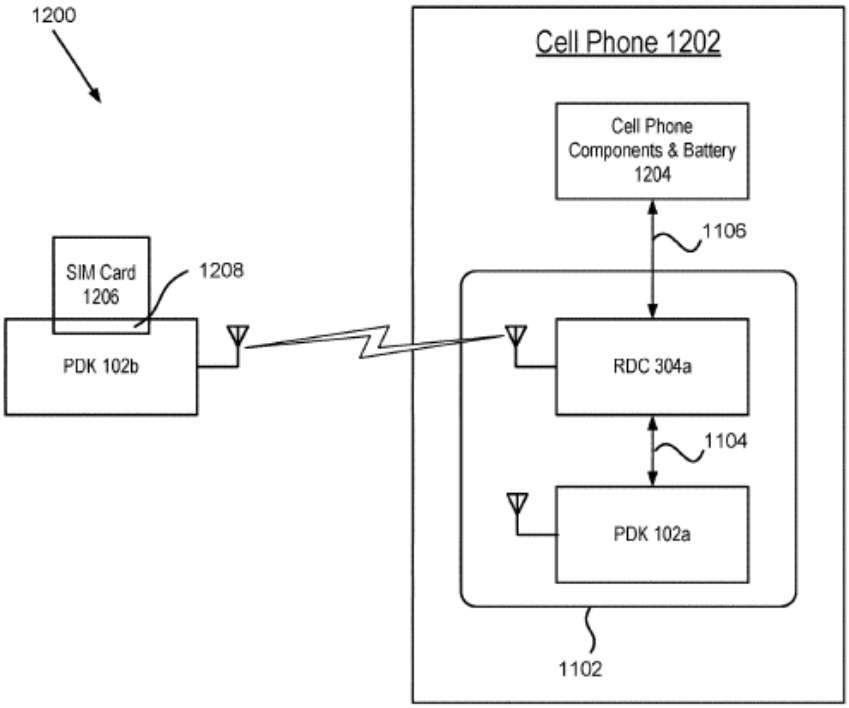


FIG. 12

Figure 12 shows system 1200 comprising PDK 102b and cell phone 1202. *Id.* at 14:55–56. As shown in Figure 12, cell phone 1202 further comprises cell phone components and battery 1204, and hybrid device 1102, wherein

hybrid device 1102 includes PDK 102a and RDC 304a coupled for communication with each other via signal line 1104. *Id.* at 14:56–61. Cell phone components and battery 1204 are coupled to RDC 304a by signal line 1106, allowing RDC 304a to use the communication capabilities of cell phone 1202 to communicate with other networks and devices. *Id.* at 14:61–67.

In one embodiment, system 1200 does not include PDK 102b, but instead, the functionality provided by PDK 102b is provided by PDK 102a that is part of hybrid device 1102. *Id.* at 16:6–8. The conventional SIM card is replaced with hybrid device 1102, which provides authorization control as well as a storage area for storing information specific to the user. *Id.* at 15:18–23. In such embodiment, hybrid device 1102 is coupled to cell phone 1202, in particular cell phone components and battery 1204, via internal integration or an access port. *Id.* at 16:24–26. Thus, PDK function becomes part of cell phone 1202 using battery power from cell phone 1202. *Id.* at 16:27–30.

D. The Challenged Claims

Of the challenged claims, claims 1 and 14 are independent. Independent claim 1 is illustrative of the challenged claims, and is reproduced below:

> 1. A device comprising:
>
> a battery;
>
> an integrated, secure memory storing local, secured information; and
>
> an integrated, wireless communication interface for communicating wirelessly with at least one external device

> within a proximity zone, the integrated, wireless communication interface communicatively coupled to the integrated, secure memory and coupled to draw power from the battery,
>
> 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.

Ex. 1001, 22:43–60.

E. Asserted Grounds of Unpatentability

Petitioner challenges the patentability of claims 1–20 of the '960 patent on the following grounds (Pet. 1):

Claim(s) Challenged	35 U.S.C. §[1]	Reference(s)/Basis
1–6, 8–11, 14–19	103	Dua[2], Giobbi '157[3]
1–7, 10, 11, 14–19	103	Buer[4]
4, 8–10, 12, 13, 17, 20	103	Buer, Giobbi '157

[1] The Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. §§ 102, 103, effective March 16, 2013. Because the application from which the '960 patent issued was a continuation of applications filed before this date, the pre-AIA versions of §§ 102, 103 apply.

[2] U.S. Patent Publication No. 2006/0258289 A1, published November 16, 2006, filed May 12, 2005 (Ex. 1004, "Dua").

[3] U.S. Patent Publication No. 2007/0245157 A1, published October 18, 2007, filed May 5, 2007 (Ex. 1006, "Giobbi '157").

[4] European Patent Application No. EP 1,536,306 A1, published June 1, 2005, filed September 30, 2004 (Ex. 1005, "Buer").

Claim(s) Challenged	35 U.S.C. §[1]	Reference(s)/Basis
4	103	Buer, Nishikawa[5]

Petitioner relies on the Declaration of Andrew Wolfe, Ph.D. (Ex. 1003) in support of its unpatentability contentions.

II. ANALYSIS

A. Claim Construction

We construe each claim "in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent." 37 C.F.R. § 42.100(b) (2023). Under this standard, claim terms are generally given their plain and ordinary meaning as would have been understood by a person of ordinary skill in the art (POSITA) at the time of the invention and in the context of the entire patent disclosure. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc).

Only those terms in controversy need to be construed, and only to the extent necessary to resolve the controversy. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Matal*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

We find that it is necessary to construe "local, secured information," and "enabling one or more of an application, a function and a service," but only to the extent necessary to resolve the disputed issues before us.

[5] European Patent Application No. EP 1,600,885 A1, published November 30, 2005, filed February 25, 2004 (Ex. 1014, "Nishikawa").

1. "local, secured information"

Claim 1 recites "an integrated, secure memory storing *local, secured information.*" Ex. 1001, 22:45−46 (emphasis added). Claim 14 similarly recites this limitation. *Id.* at 24:10–11.

Patent Owner asserts that "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." Prelim. Resp. 21. Patent Owner cites to the Specification:

> 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***.

Prelim. Resp. 21 (quoting Ex. 1001, 3:50–57). According to Patent Owner, "[t]his is the only instance in the specification where the term 'local secured information' appears," which "clearly defines 'which information is used as ***local secured information***.'" *Id.* at 22. Patent Owner contends that "'[l]ocal, 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." *Id.* at 23.

Petitioner does not propose a claim construction for "local, secured information" but relies on Dua's and Buer's "integrated, tamper-resistant memory" for storing "local, encrypted information." Pet. 28, 56 (citing Ex. 1004 ¶¶ 105, 109, 152; Ex. 1005 ¶¶ 13, 134–137; Ex. 1003 ¶¶ 133–134, 197–198).

The plain meaning of "an integrated, secure memory storing local, secured information," as claimed, suggests an integrated, secure memory for storing information locally, wherein the information is secured. *See* Pet. 28, 59; *see* also Prelim. Resp. 19–21. Further, nothing in the Specification clearly limits or redefines "local, secured information" to "information stored within a service block of a PDK and unlocked with a corresponding access key provided to the PDK," as Patent Owner proposes. Prelim. Resp. 23.

We are unpersuaded by Patent Owner's contention that the Specification "clearly defines 'which information is used as ***local secured information***.'" Prelim. Resp. 22. Although Patent Owner points to an "instance" in the Specification that it alleges is such a "clear[] defin[ition]" (*id.*), this portion of the Specification merely shows an exemplary embodiment and *not* a definition. *See* Ex. 1001, 3:50–57. In particular, the language Patent Owner points to in the Specification provides that "[i]n *this example*, the sensor 108 contains three of the service block access keys 118A, D, F," wherein "[t]he 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." *See id.* (emphasis added). That is, although the referenced portion of the Specification indicates that, in an example, information stored in a "service block" can be used as "local, secured information," nothing in the Specification limits "local, secured information" to "information stored within service block of a PDK and unlocked with a corresponding access key provided to the PDK,"

as Patent Owner contends.[6] Prelim. Resp. 23. Any special definition for "local, secured information" limiting it to "information stored within a service block of a PDK and unlocked with a corresponding access key provided to the PDK" must be set forth in the Specification with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). We do not discern such clarity, deliberateness, and precision to be present here.

In view of the plain language of the claims and the Specification, we determine that the term "local, secured information" encompasses information stored locally on an integrated, secure memory, wherein the information is secured, and is not limited to information stored within a service block of a PDK and unlocked with a corresponding access key provided to the PDK.

2. "enabl[ing] one or more of an application, a function, and a service"

Claim 1 recites "one or more of (a) the integrated, wireless communication interface. . . *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*." Ex. 1001, 22:53−60 (emphasis added). Claim 14

[6] We are unpersuaded by Patent Owner's contention that "the permissive language 'in this example' does not expand the definition 'local secure information'" because "it applies to the sensors." Prelim. Resp. 22. The Specification is clear that, in this example, "the" same service access keys 118 contained by the sensor allow the sensor to unlock information "used as local secured information." *See* Ex. 1001, 3:50–57.

similarly recites an enablement signal "enabling one or more of an application, a function and a service." *Id.* at 24:18–19.

a) Claim construction in District Court

Patent Owner asserts that "[i]n response to arguments asserted in *Proxense v. Samsung* [("the Samsung case")] that the term 'hybrid device' was indefinite, the District Court found it necessary to construe the term 'enabled.'" Prelim. Resp. 4. Patent Owner cites to the District Court's Memorandum in Support of Claim Construction Order:

> An application, function, or service is 'enabled' by a PDK when it receives information from a PDK in exchange for an access key.

Prelim. Resp. 4 (quoting Ex. 2002, 26). Patent Owner contends that Petitioner has not challenged this construction, and thus, "[u]nless compelled otherwise, this Board must 'presume . . . that the same claim term in the same patent or related patents carries the same construed meaning." *Id.* at 4–5 (citing *Omega Engineering, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1334 (Fed. Cir. 2003)).

We are unpersuaded by Patent Owner's contention that "the District Court found it necessary to construe the term 'enabled.'" Prelim. Resp. 4. In particular, we disagree that the District Court in the Samsung case provided any construction for the term "enabled." *Id.* Although Patent Owner points to the District Court's Memorandum in Support of Claim Construction Order (*id.* (citing Ex. 2002, 26)) to support its contention that the District Court construed the term "enabled," this portion of the District Court's Memorandum merely discusses that "hybrid device" is not indefinite, and discusses exemplary operations of the "hybrid device" from

which a POSITA "could reasonably ascertain the scope of the claim." *See* Ex. 2002, 26.[7] That is, a determination of whether a term is indefinite is not the same thing as construing a claim term. Thus, the District Court's determination that "hybrid device" is not indefinite did not constitute a construction of that term, much less provide a construction of "enabled" recited elsewhere in the claim. In any case, even if assuming *arguendo* that the referenced portion of the district court's Memorandum indicates that a POSITA could reasonably ascertain the scope of the claim (*id.*), nothing in the Memorandum provides a definition of "enabled" as being limited to when an application, function, or service "receives information from a PDK in exchange for an access key," as Patent Owner contends. Prelim. Resp. 8.

b) Means-plus function analysis

Patent Owner further contends that the term "enabling" "may further be defined by way of a means-plus-function analysis." Prelim. Resp. 8. According to Patent Owner, "§ 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.'" *Id.* (citing *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1349 (Fed. Cir. 2015)). Patent Owner contends that because none of "the 'local secured information', 'wireless communication interface' [and] 'enablement signal' provide sufficiently definite structure," the term

[7] Even if the Court's explanation that "[a]n application, function, or service is 'enabled' by a PDK when it receives information from a PDK in exchange for an access key" is an express construction, the Board is not required to adopt that construction. *See Power Integrations, Inc. v. Lee*, 797 F.3d 1318, 1326 (Fed. Cir. 2015) ("There is no dispute that the board is not generally bound by a prior judicial construction of a claim term.").

"enabling" "must be construed consistent with the only algorithm disclosed in the specification." *Id.* at 10. Patent Owner then contends that "[c]ontrol logic 250 is thus an algorithm for accessing a service block (i.e., memory) of a 'PDK' by providing the corresponding 'access key,'" and thus, the '960 patent states that "applications are 'enabled' from a service block by providing the corresponding access key." *Id.*

In reply, Petitioner points out that "none of the claims of the '960 patent recite the disputed limitation in 'means-plus-function' or 'step-plus-function' format." Prelim. Reply 2. Thus, Petitioner contends that, "[b]ecause the disputed claim limitations do not employ 'means for' or 'step for,' the presumption is that the terms local secured information, wireless communication interface, and enablement signal each convey[s] sufficiently definite structure or act and, thus, [is] not subject to § 112, ¶ 6." *Id.* (citing *Dyfan, LLC v. Target Corp.*, 28 F.4th 1360, 1367 (Fed. Cir. 2022)). According to Petitioner, "the terms 'local secured information,' 'wireless communication interface,' and 'enablement signal,' provide sufficiently definite structure or an act," because they are "not used as 'generic terms or black box recitations of structure or abstractions.'" *Id.* at 3 (citing *Dyfan*, 28 F.4th at 1368). Petitioner contends that "when a 'structure-connoting term . . . is coupled with a description of the [term's] operation' § 112 ¶ 6 does not apply." *Id.*

Patent Owner then responds that, although the claims do not recite the word "means," "the failure of the claims to recite a recognized 'nonce' word is not determinative." Prelim. Sur-reply 1. According to Patent Owner, claim terms "wireless communication interface," "local secured information," and "enablement signal" at issue "could not be understood by

person of ordinary skill in the art to have a sufficiently definite meaning as the name for structure for the claimed functions." *Id.*

We are unpersuaded by Patent Owner's contentions. In particular, we are unpersuaded that "enabling" may be defined by way of means-plus-function analysis. Prelim. Resp. 8. As Petitioner points out, "none of the claims of the '960 patent recite the disputed limitation in 'means-plus-function' or 'step-plus-function' format." Prelim. Reply 2. As Petitioner contends, when a disputed claim limitation does not employ "means for" language, the presumption is that each of the terms conveys sufficiently definite structure or act and, thus, is not subject to § 112 ¶ 6. *Id.*; *see also Dyfan*, 28 F.4th at 1367.

Although this presumption is rebuttable and can be overcome if the challenger demonstrates that the claim term fails to recite sufficiently definite structure (*see Raining Computing v. Samsung Electronics America*, 998 F.3d 1002, 1005 (Fed. Cir. 2021)), we are unpersuaded that Patent Owner has demonstrated that claim terms "wireless communication interface," "local secured information," and "enablement signal" fail to recite sufficiently definite structure. That is, Patent Owner has not sufficiently demonstrated that the terms could not be understood by person of ordinary skill in the art "to have a sufficiently definite meaning as the name for structure for the claimed functions." Prelim. Sur-reply 1. We agree with Petitioner that the terms are "not used as 'generic terms or black box recitations of structure or abstractions.'" Prelim. Reply 3; *see Dyfan*, 28 F.4th at 1368. As Petitioner points out, "when a 'structure-connoting term . . . is coupled with a description of the 'term's' operation' § 112 ¶ 6 does not

apply." *Id.*; *accord Linear Tech. Corp. v. Impala Linear Corp.*, 379 F.3d 1311, 1320 (Fed. Cir. 2004); *Dyfan*, 28 F.4th at 1368.

c) Claim construction using the *Phillips* standard

According to Patent Owner, under *Phillips*, "[t]he claims . . . do not stand alone," but rather, "they are part of a fully integrated written instrument, consisting principally of a specification that concludes with the claims." Prelim. Resp. 10 (citing *Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005) (*en banc*)). Patent Owner then contends that the '960 patent "implicitly define[s] that 'an application, function, or service is "enabled" by a PDK when it receives information from a PDK in exchange for an access key." *Id.* at 12 (citing Ex. 2002, 26). Patent Owner references several examples in the Specification. *Id.* at 12–19 (citing Ex. 1001, 3:58–4:2, 8:62–9:5, 9:6–19, 9:48–10:03, Figs. 1, 4, 5, 6). In particular, Patent Owner makes reference to Figure 6 of the '960 patent:

> 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 auto[ ]login/logoff, where a user logs into a personal computer via a service block 112C that provides a username and password.

Prelim. Resp. 12–13 (quoting Ex. 1001, 9:48–57) (emphasis omitted). Patent Owner contends that, as shown in Figure 6, "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." *Id.* at 15.

Patent Owner contends that other "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."

Prelim. Resp. 15. Patent Owner also references Figure 1 of the '960 patent:

> 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.

Prelim. Resp. 15–16 (citing Ex. 1001, 3:58–4:2) (emphasis omitted).

"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," Patent Owner then references Figure 4 of the '960 patent:

> 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 [s]ensor 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.

Prelim. Resp. 17 (quoting Ex. 1001, 8:62–9:5).

With "others," Patent Owner references Figure 5 of the '960 Patent:

> An example of a remote application (FIG.5) is a credit card transaction. The sensor 108 in this case could be a credit card

> terminal. When the PDK 102 is brought in close proximity, the credit card terminal 108 attaches to the PDK 102 (using service block[ ]112A). The terminal 108 then sends the PDK[ ]ID 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 PDK[ ]102 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.

Prelim. Resp. 17–18 (quoting Ex. 1001, 9:6–19).

Petitioner does not propose an express claim construction for "enabl[ing] one or more of an application, a function, and a service" but relies on Dua's and Buer's "local, encrypted information" stored in an "integrated, tamper-resistant memory." Pet. 28, 56 (citing Ex. 1004 ¶¶ 105, 109, 152; Ex. 1005 ¶¶ 13, 134–137; Ex. 1003 ¶¶ 133–134, 197–198).

The plain language in claim 1 of enabling an application, a function, or a service does not suggest a requirement that information be received from a PDK in exchange for an access key. Ex. 1001, 22:53–60. Nothing in the Specification clearly limits the integrated, secure memory "enabl[ing] one or more of an application, a function, and a service" to "receiv[ing] information from a PDK in exchange for an access key," as Patent Owner proposes. Prelim. Resp. 12–19. Thus, we determine that "enabl[ing] one or more of an application, a function, and a service" does not require receiving information from a PDK in exchange for an access key.

We are unpersuaded by Patent Owner's contention that the Specification implicitly defines "enabl[ing] one or more of an application, a function, and a service" as requiring receiving information from a PDK in

exchange for an access key. Prelim. Resp. 12–19. As Patent Owner acknowledged, "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." *Id.* at 11 (citing *Trustees of Columbia Univ. v. Symantec*, 811 F.3d 1359, 1363–64 (Fed. Cir. 2016) (emphasis added)). Here, Patent Owner points to no portions in the Specification that provide the requisite reasonable clarity, deliberateness, and precision to warrant interpreting the claim language at issue as requiring "receiving information from a PDK in exchange for an access key." *Id.* at 12–19.

Although Patent Owner points to Figures 1 and 4–6 of the Specification for such implicit definition, as Patent Owner acknowledges, Figures 1 and 4–6 of the Specification merely show various "examples" of "enabling an application, a function or a service" presented in the Specification. Prelim. Resp. 18. In particular, the language in the Specification that Patent Owner points to with respect to Figure 6 provides "*[i]n some cases*, the first application 120Y1 is *enabled* from a first service block 112C," wherein "*[f]or example*, the first application 120Y1 *might be* the *auto login/logoff*, where a user logs into a personal computer via a service block 112C that provides a username and password."[8] *See* Ex. 1001, 9:48–57 (emphases added). With respect to Figure 1, such teaching in the Specification shows that "*[i]n one example*, a biometric is required in order *to access* specific service blocks 112." *See id.* at 3:58–4:2 (emphases

[8] Although Patent Owner contends that the phrase "'[i]n some cases' [] references the ability of a device to have more than one application enabled by a service block" (Prelim. Resp. 14), this portion of the Specification is clear that, in some (not all) cases, a first application, for example, an auto login/logoff, is enabled from a first service block. *See* Ex. 1001, 9:48–57.

added). With respect to Figure 5, such teaching in the Specification shows that "*[a]n example* of a remote application [] is a credit card transaction," wherein "[t]he credit card issuer *may* then *send* a service block access key [] back to the sensor," and "[t]he contents of the service block [] *could* then *be sent back* to the credit card issuer." *Id.* at 9:6–19 (emphases added). With respect to Figure 4, such teaching in the Specification shows that "*[a]n example* of a local application (FIG. 4) is an *auto login/logoff* of a personal computer," wherein, "*[f]or example*, a standard *may specify* that particular service block 112B contains username and password." *See id.* at 8:62–9:5 (emphases added).

Although the referenced portions of the Specification discuss various examples wherein information may be received to "enable" various applications, functions, or services, nothing in these referenced portions of the Specification clearly requires the "enabl[ing] an application, a function, or a service" to only be by "receiv[ing] information from a PDK in exchange for an access key," as Patent Owner contends. Prelim. Resp. 12–19. That is, Patent Owner points to no special definition, implicit or explicit, for "enabl[ing] an application, a function or a service" limiting it to "receiv[ing] information from a PDK in exchange for an access key" that is set forth in the Specification with reasonable *clarity, deliberateness, and precision*. *In re Paulsen*, 30 F.3d at 1480.

In view of the plain language of the claims and the Specification, we determine that the term "enabl[ing] an application, a function, and a service" recited in claims 1 and 14 is not limited to receiving information from a PDK in exchange for an access key. We determine no further explicit

construction of this term is necessary to resolve the controversy. *See Vivid Techs.*, 200 F.3d at 803.

B. Principles of Law

A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, "would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of non-obviousness.[9] *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

C. Claims 1–6, 8–11, and 14–19 as Allegedly Obvious over Dua and Giobbi '157 (Ground 1)

According to Petitioner, the claims of the '960 patent are directed to a "hybrid device" that includes both "an integrated personal digital key (PDK) and "an integrated receiver-decoder circuit (RDC)." Pet. 2. Petitioner provides an annotated Figure 12 of the '960 patent, reproduced below, to illustrate its contentions.

[9] Neither party presents evidence or arguments regarding objective evidence of non-obviousness in the instant proceeding at this time.

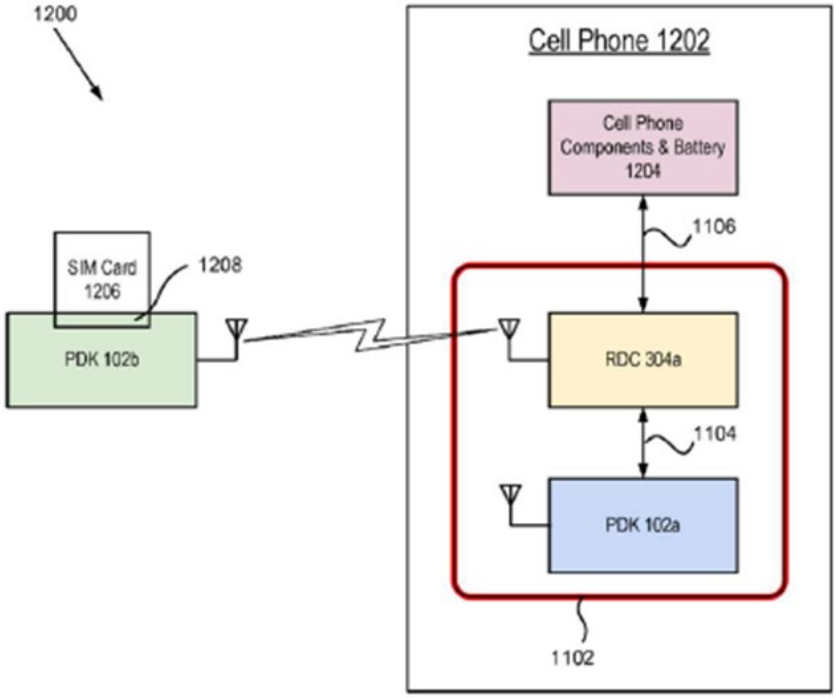


FIG. 12

The above annotated Figure 12 of the ’960 patent in the Petition shows device 1102 (red), i.e., “hybrid device,” that includes integrated PDK 102a (blue) and integrated RDC 304a (yellow) that communicate with each other via signal line 1104. Pet. 3; *see* also Ex. 1001, 2:32–37, Fig. 12. Petitioner contends that, as shown, battery 1204 (pink) may be coupled to integrated RDC 304a by signal line 1106, and integrated RDC 304a may also communicate wirelessly with external PDK 102b (green). Pet. 3; Ex. 1001, 14:53–15:5.

Petitioner further contends that the ’960 patent’s hybrid device may interconnect with other external devices. Pet. 3. Petitioner provides an annotated Figure 13 of the ’960 patent, reproduced below, to illustrate its contentions.

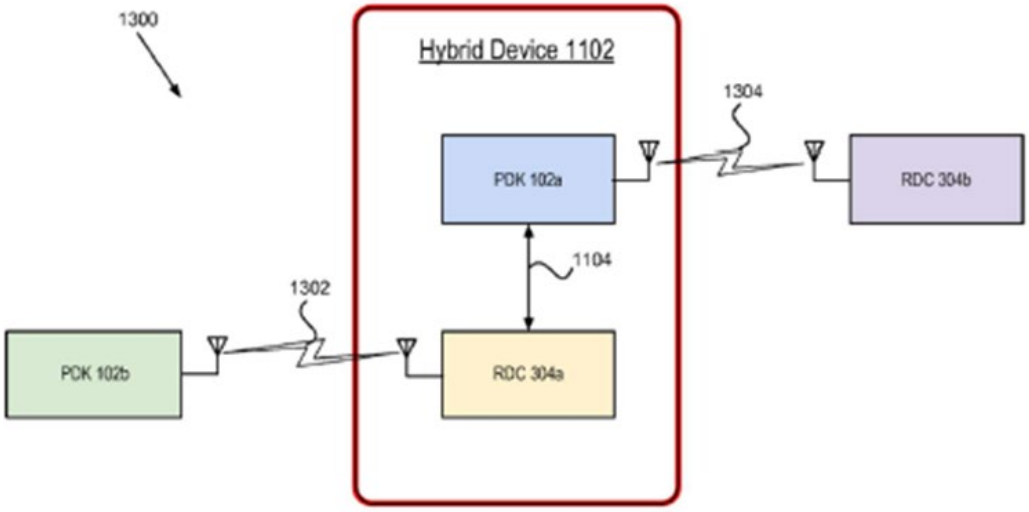


FIG. 13

The above annotated Figure 13 of the '960 patent in the Petition shows hybrid device 1102 (red) interconnected with other external devices so that integrated PDK 102a (blue) communicates wirelessly with external RDC 304b (purple), and integrated RDC 304a (yellow) communicates wirelessly with external PDK 102b (green) within its proximity zone. Pet. 3–4; *see* also Ex. 1001, 16:55–17:4, 22:43–60, Fig. 13. According to Petitioner, the purpose of '960 patent's integrated PDK and RDC is "to enable various applications, functions, or services either on an external device or on the hybrid device using information stored on the integrated or external PDKs." Pet. 4 (citing Ex. 1001, 4:44–54, 7:14–25, 17:5–12).

Petitioner then contends that claims 1–6, 8–11, and 14–19 of the '960 patent would have been obvious over by Dua and Giobbi '157. Pet. 15–39. In particular, Petitioner contends that, similar to the '960 patent, Dua teaches "a hybrid device ('cellular phone') containing 'both an RFID tag and an RFID reader' that establishes wireless connections with other devices to

enable functions and to exchange data," wherein the cellular phone uses "an 'RFID Tag-Reader Module,' to 'rapidly exchange information with an electronic device that is in close proximity.'" *Id.* at 7–8 (citing Ex. 1004 ¶¶ 15, 70).

In response, Patent Owner contends that these references "cannot render the challenged claims invalid and unpatentable." Prelim. Resp. 23–26. In particular, Patent Owner contends that the Petition fails to demonstrate that the combination of references "discloses (a) 'local, secured information' or (b) 'enabling one or more of an application, a function, and a service.'" *Id.* at 23.

We briefly summarize Dua and Giobbi '157 below.

1. Dua

Dua, titled "Wireless Media System and Player and Method of Operation," discloses a wireless media system "for the automatic establishment of wireless connectivity with other electronic devices" using an integrated Radio Frequency Identification (RFID) to exchange communication settings, media capability, and other parameters with an external device that also has integrated RFID technology. Ex. 1004, codes (54), (57). Exchange of settings and other information is automatic by using a proximity-based RFID data exchange that allows a media player to quickly establish a secure communication link with another device. *Id.*

In particular, Dua discloses a media player with an RFID Tag-Reader Module. *Id.* ¶ 24, Fig. 1. The RFID tag-reader module is capable of functioning as both an RFID tag and an RFID reader, and allows interoperability with readers and tags compatible with existing international

standards. *Id.* ¶ 15. A functional diagram of Dua's RFID tag-reader module is shown in Figure 4B, reproduced below.

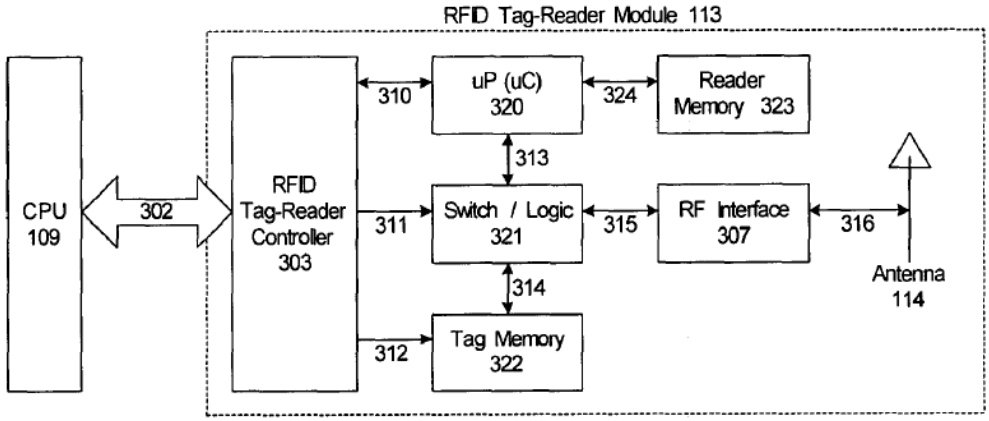


FIG. 4B

Figure 4B is block diagram of RFID Tag-Reader Module 113 including integrated RFID Tag-Reader Controller 303 that manages all communication between CPU 109 and the functional components of RFID Tag-Reader Module 113. *Id.* ¶ 106. Hardware and software interface 302 between CPU 109 and RFID Tag-Reader Controller 303 allows an application operating a media player to control functions of RFID Tag-Reader Module 113 and to exchange data with it. *Id.* RF interface 307 and antenna 114 "are used by the RFID reader functionality and RFID tag functionality." *Id.* Reader logic 320 provides a data communication interface to the media player 100 and the application executed thereon and "operates the interface and protocol framework for communicating with RFID tags . . . and in particular, when supporting active communication mode, for communicating with RFID tag reader devices." *Id.*

The reader component of RFID Tag-Reader Module 113 is "used for transmitting interrogation signals via its antenna to an external electronic device's RFID tag when in close proximity, and receiving a response signal from the external device's RFID tag." *Id.* ¶ 71. Reader memory 323 is used

as a buffer storage for communication with the media player as well as with an RFID tag or another RFID tag reader device. *Id.* ¶ 107. Switch/logic component 321 interposed between RF interface 307 and reader logic 320 allows switching between RFID reader functionality and RFID tag functionality. *Id.* ¶ 108. Tag memory 322 is used to receive configuration data from applications operating on the media player. *Id.* "[M]emory components in RFID Tag-Reader Module 113 may be tamper resistant as to prevent hackers from retrieving confidential information and encryption keys." *Id.* ¶ 109. In one embodiment, enhanced security is provided as "both devices can share each other's encryption keys via the RFID exchange." *Id.* ¶ 152.

2. Giobbi '157

Giobbi '157, titled "Two-Level Authentication for Secure Transaction," discloses a PDK that stores biometric profiles in "a tamper-proof memory that is acquired in a secure trusted process," wherein the biometric profiles comprise a "representation of physical or behavioral characteristics that are uniquely associated with an individual that owns and carries the PDK." Ex. 1006, codes (54), (57). An illustration of Giobbi '157's system for securely authenticating an individual for transaction processing and/or access control applications is depicted in Figure 1, reproduced below.

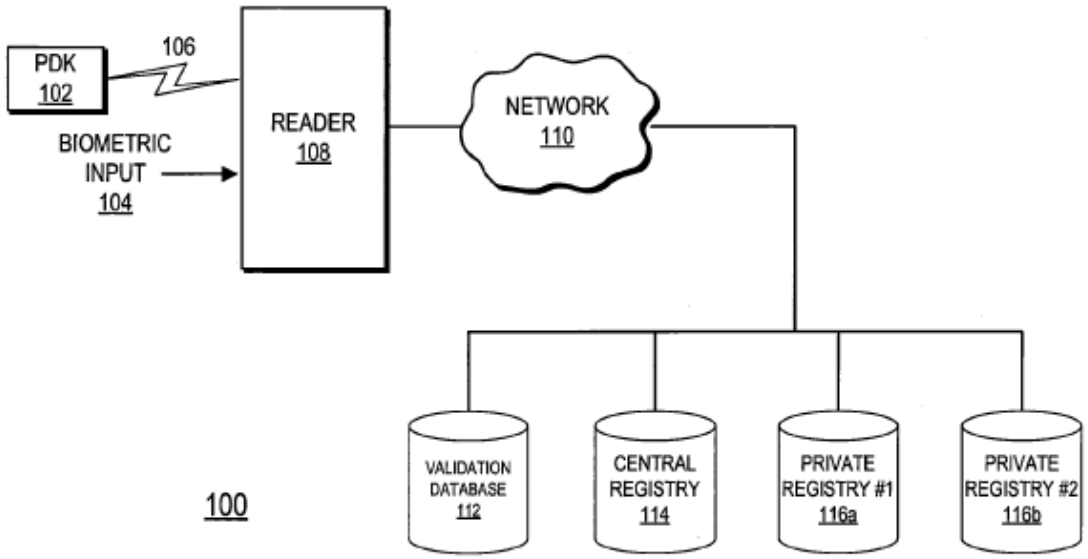


FIG. 1

Figure 1 is a block diagram of system 100 for secure electronic authentication comprising PDK 102, reader 108, network 110, and one or more external databases including validation database 112. *Id.* ¶ 26. As shown in Figure 1, reader 108 is coupled to PDK 102 by wireless link 106 and coupled to network 110 by either a wired or wireless link. *Id.* Reader 108 is also adapted to receive biometric input 104 from a user. Network 110 couples validation database 112, central registry 114, and two private registries 116 to reader 108. *Id.*

Reader 108 is depicted in Figure 3, reproduced below.

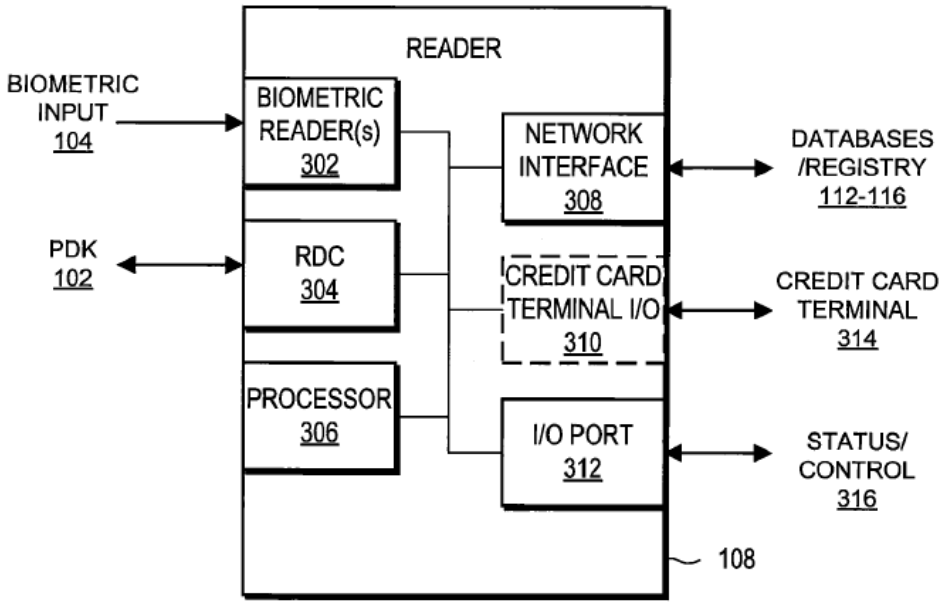


FIG. 3

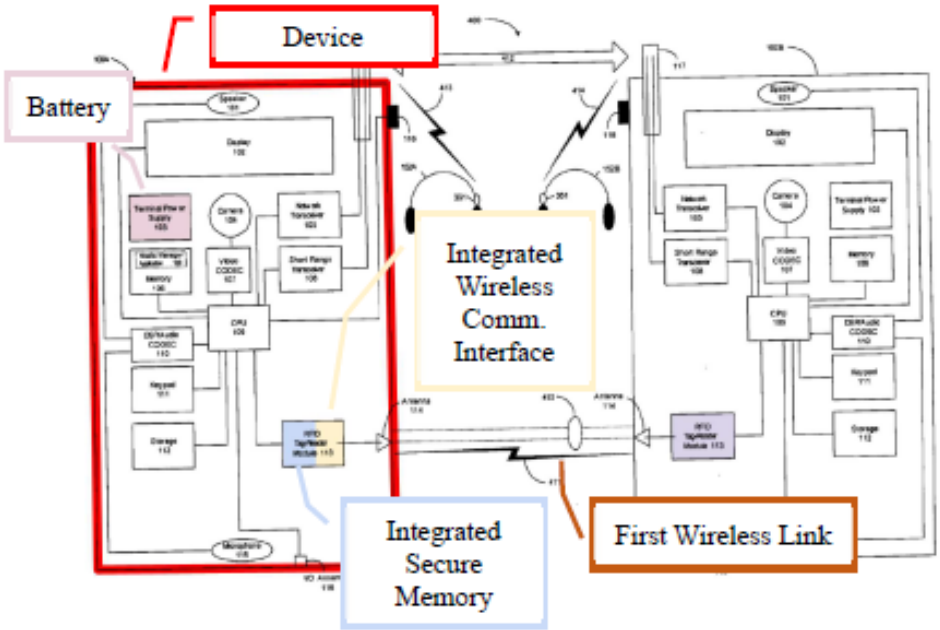
Figure 3 is a block diagram of reader 108 that includes one or more biometric readers 302, receiver-decoder circuit (RDC) 304, processor 306, network interface 308, I/O port 312, and optionally credit card terminal I/O 310. *Id.* ¶ 49. As shown in Figure 3, RDC 304 provides wireless interface to PDK 102, wherein RDC 304 wireless receives data from PDK 102 in an encrypted format and decodes the encrypted data for processing by processor 306. *Id.* ¶ 50. Generally, processor 306 processes data received by reader 108 or data to be transmitted by reader 108, wherein biometric input 104 received by biometric reader 302 can be processed and compared to biometric profile 220 received from PDK 102 in order to determine if a transaction should be authorized. *Id.* ¶ 52.

3. Analysis of Claims 1–6, 8–11, 14–19 as Allegedly Obvious over Dua and Giobbi '157 (Ground 1)

We begin by addressing in detail Petitioner's contentions and Patent Owner's arguments with respect to the limitations of representative claim 1.

i. Preamble, "A device"

Petitioner contends that, "[t]o the extent that the preamble is limiting, Dua discloses the device because it discloses a media player (e.g., cellular phone) with an RFID Tag-Reader Module." Pet. 28 (citing Ex. 1004 ¶¶ 57, 70; Ex. 1003 ¶ 131). Petitioner provides an annotated Figure 6 of Dua, shown below, to illustrate its contentions.



The above annotated Figure 6 of Dua, according to Petitioner, illustrates "Dua's media player ('device,' red)" which includes "a battery (pink)," "RFID Tag-Reader Module 113 (e.g., 'integrated, secure memory,' blue; 'integrated wireless communication interface,' yellow)" that "enables the device to 'rapidly exchange information with an electronic device [with

RFID] that is in close proximity.'" Pet. 17 (citing Ex. 1004, Figs. 1, 6, ¶¶ 57, 70).

At this stage of the proceeding, Patent Owner does not present arguments in the Preliminary Response addressing the specific merits of Petitioner's contentions with respect to the preamble. *See generally* Prelim. Resp. 23–26.[10]

Having reviewed all of Petitioner's assertions regarding this claim limitation, as well as the supporting evidence, we determine on this record that Petitioner has made a sufficient showing that the combination of Dua and Giobbi '157 teaches a "device."

ii. "a battery," "an integrated, secure memory storing local, secured information"

Petitioner contends that Dua's device includes "a battery, such as 'a rechargeable power supply 103 (e.g., rechargeable lithium polymer battery).'" Pet. 28 (citing Ex. 1004 ¶ 59; Ex. 1003 ¶ 132). At this stage of the proceeding, Patent Owner does not present arguments in the Preliminary Response addressing the specific merits of Petitioner's contentions with respect to this limitation. *See* generally Prelim. Resp. 23–26.

Having reviewed all of Petitioner's assertions regarding this claim limitation, as well as the supporting evidence, we determine on this record that Petitioner has made a sufficient showing that the combination of Dua and Giobbi '157 teaches a "battery."

---

[10] Because there is no dispute between the parties that Dua in view of Giobbi '157 teaches a device, as recited in the preamble, for purposes of institution, we need not decide whether the preamble is limiting. *See Nidec*, 868 F.3d at 1017 (noting that "we need only construe terms 'that are in controversy'" (quoting *Vivid*, 200 F.3d at 803)).

Petitioner then contends that, Dua's RFID Tag-Reader Module includes "Tag Memory 322 for storing tag data," that "may be a 'non-volatile configurable memory' and 'tamper resistant' to prevent hackers from retrieving 'confidential information and encryption keys.'" Pet. 18 (citing Ex. 1004 ¶¶ 105, 109). According to Petitioner, Dua "renders obvious an integrated, tamper-resistant memory storing local, encrypted information." *Id.* at 28 (citing Ex. 1004 ¶¶ 105, 109, 152; Ex. 1003 ¶¶ 133–134).

Patent Owner argues that the claimed "local, secured information" is 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." Prelim. Resp. 23. Although Patent Owner acknowledges that Dua's "Tag Memory 322" may be a non-volatile configurable memory that is tamper resistant (*id.* at 24), Patent Owner contends that neither the Petition nor the declaration of its expert, Dr. Wolfe, establishes that Dua discloses "local, secured information" in the manner disclosed by the '960 patent. *Id.* In particular, Patent Owner contends that "Dua fails to disclose that [the] 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." *Id.* (citing Ex. 1003 ¶¶ 109–117).

Patent Owner also contends that 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." Prelim. Resp. 24 (citing Ex. 1006 ¶¶ 11, 36). According to Patent Owner, Giobbi '157 also 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." *Id.*

We find Petitioner's arguments persuasive on this point. In particular, as Petitioner contends, and Patent Owner acknowledges, Dua discloses an "RFID Tag-Reader Module" which includes "Tag Memory 322" that may be tamper resistant. Pet. 18; *see* Ex. 1004 ¶¶ 105, 109. Thus, we find persuasive Petitioner's reliance on Dua's Tag Memory 322, which locally stores information in a tamper-resistant manner, for teaching an integrated, secure memory for storing information locally, wherein the information is secured. *Id.*

In our claim construction section above, we gave "an integrated, secure memory storing local, secured information" its ordinary and customary meaning as an integrated, secure memory for storing information locally, wherein the information is secured. In particular, we determine that an interpretation of "local, secured information" encompasses information stored locally on an integrated, secure memory, but is not limited to "confidential information or encryption keys" stored "within a service block of a RFID tag and unlocked with a corresponding access key provided to the RFID tag," as Patent Owner contends. Prelim. Resp. 24.

On this preliminary record, we are persuaded that Petitioner also has made a sufficient showing that the combination of Dua and Giobbi '157 teaches "an integrated, secure memory storing local, secured information."

iii. "an integrated, wireless communication interface for communicating wirelessly with at least one external device within a proximity zone"

Petitioner contends that Dua's "RFID reader component (integrated, wireless communication interface) communicates wirelessly with at least one external RFID tag when within a proximity zone." Pet. 28–29 (citing Ex. 1004 ¶¶ 71–72, 122, 127; Ex. 1003 ¶¶ 135–136). At this stage of the proceeding, Patent Owner does not present arguments in the Preliminary Response addressing the specific merits of Petitioner's contentions with respect to this claim limitation. *See generally* Prelim. Resp. 23–26.

Having reviewed all of Petitioner's assertions regarding this claim limitation, as well as the supporting evidence, we determine on this record that Petitioner has made a sufficient showing that the combination of Dua and Giobbi '157 teaches "an integrated, wireless communication interface for communicating wirelessly with at least one external device within a proximity zone."

iv. "the integrated, wireless communication interface communicatively coupled to the integrated, secure memory and coupled to draw power from the battery"

Petitioner contends that Dua's "RFID reader component (integrated, wireless communication interface) is communicatively coupled to the integrated, secure tag memory for communication with the integrated, secure tag memory." Pet. 29 (citing Ex. 1003 ¶ 137). Petitioner provides an annotated Figure 4B of Dua, shown below, to illustrate its contentions.

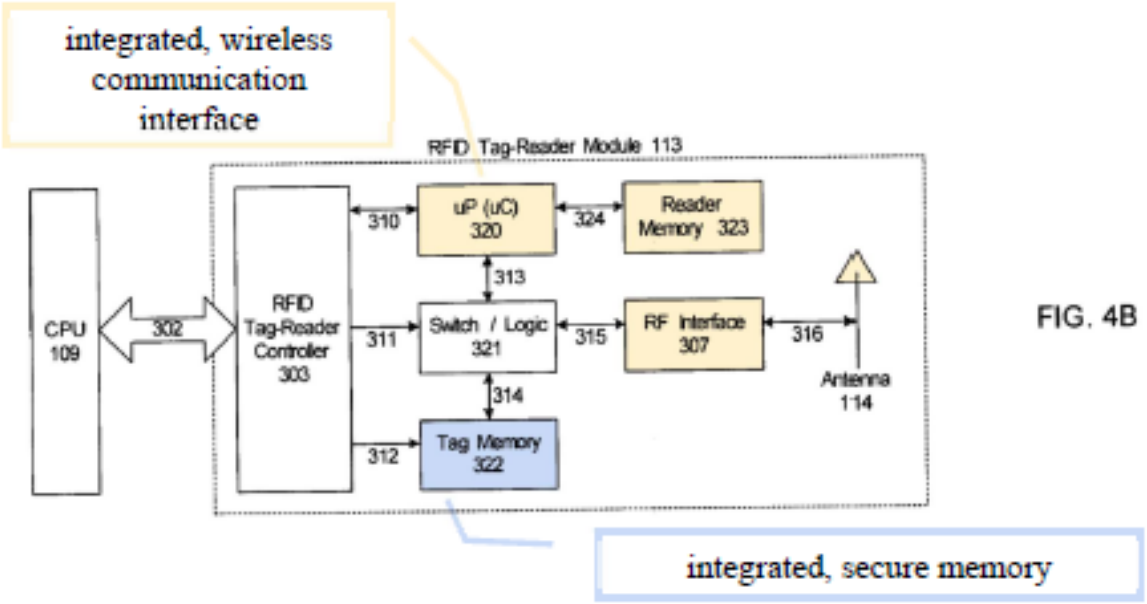


FIG. 4B

The above annotated Figure 4B of Dua, according to Petitioner, illustrates RFID Tag-Reader Module 113 that includes integrated RFID Tag-Reader controller 303 for managing all communications between CPU 109 and the functional components of RFID Tag-Reader Module 113, and "'tag logic' (e.g., switch/logic component 321)." Pet. 29 (citing Ex. 1004 ¶¶ 106, 108). According to Petitioner, "[d]uring cross-discovery, an RFID tag can be written with data received by an RFID reader," wherein "the integrated, wireless communication interface is communicatively coupled to the integrated, secure memory to update the information stored in the RFID tag memory." *Id.* at 29–30 (citing Ex. 1004 ¶¶ 151–154). Further, Petitioner contends that "Dua's RFID reader component is communicatively coupled to draw power from the battery to transmit interrogation signals." *Id.* at 30 (citing Ex. 1004 ¶¶ 71, 94; Ex. 1003 ¶ 138).

At this stage of the proceeding, Patent Owner does not present arguments in the Preliminary Response addressing the specific merits of

Petitioner's contentions with respect to this claim limitation. *See generally* Prelim. Resp. 23–26.

Having reviewed all of Petitioner's assertions regarding this claim limitation, as well as the supporting evidence, we determine on this record that Petitioner has made a sufficient showing that the combination of Dua and Giobbi '157 Dua teaches an "integrated, wireless communication interface communicatively coupled to the integrated, secure memory and coupled to draw power from the battery."

v. "wherein one or more of (a) the integrated, wireless communication interface . . . 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."

Petitioner contends that Dua discloses that "either the integrated, wireless communication interface or the local, secured information stored by the integrated, secure memory enables an application, function or service." Pet. 39 (citing Ex. 1003 ¶¶ 139–140). According to Petitioner, Dua discloses that, "when an external device is within a proximity zone of its integrated RFID reader (integrated, wireless communication interface), the integrated RFID reader (integrated, wireless communication interface) communicates wirelessly with the external device's RFID tag." *Id.* at 31 (citing Ex. 1003 ¶ 141). Petitioner contends that, in Dua, data received by the RFID reader is sent to the device's CPU for use by applications operating on the device to generate a Bluetooth paging message to enable a wireless connection and transmission of media to the external device. *Id.*

(citing Ex. 1004 ¶¶ 103, 123, 128, 161, 171; Ex. 1003 ¶ 142). Further, Petitioner contends that Dua teaches that "the local, encrypted financial information stored in the integrated, tamper-resistant memory enables 'electronic payments' at point-of-sale." *Id.* (citing Ex. 1004 ¶¶ 52, 70, 109; Ex. 1003 ¶ 143).

Patent Owner responds that "Dua does not contemplate that information is received in exchange for an access key provided to the PDK." Prelim. Resp. 25. Patent Owner acknowledges Dua discloses "the use of RFID technology to establish wireless communication between a media player and a diverse set of devices," wherein the media player "sends a 'Bluetooth paging message' to a headphone unit or target media player," and in response to the page, "the headphone unit/target media player performs a 'connection setup' with media player." *Id.* at 25–26 (citing Ex. 1004 ¶¶ 51–52, 123, 128). However, Patent Owner contends that "nowhere does Dua teach or describe that this 'connection setup' is accomplished by providing an access key in exchange for information held locally in the PDK's service blocks." *Id.* at 26.

We find Patent Owner's arguments unavailing. In particular, Patent Owner is relying on a claim construction of "enabling" requiring "providing an access key in exchange for information held locally in the PDK's service blocks" (Prelim. Resp. 25) that is not required by our construction discussed above. As discussed above, we determine that the term "enabl[ing] an application, a function, or a service" is not limited to "receiv[ing] information from a PDK in exchange for an access key."

Dua teaches that, when an external device is within a proximity zone of its integrated RFID reader, the integrated RFID reader communicates

wirelessly with the external device's RFID tag. *See* Ex. 1003 ¶ 141. We are persuaded by Petitioner's reliance on Dua for teaching that data received by the RFID reader sent to the device's CPU is used to generate a Bluetooth paging message "to enable a wireless connection and transmission of media to the external device." Pet. 31; *see* Ex. 1004 ¶¶ 103, 123, 128, 161, 171. We are also persuaded by Petitioner's contention that information stored in the integrated, tamper-resistant memory "enables 'electronic payments' at point-of-sale." *Id.*; *see also* Ex. 1004 ¶¶ 52, 70, 109.

On this preliminary record, we are persuaded that Petitioner has made a sufficient showing that the combination of Dua and Giobbi '157 teaches that "one or more of (a) wireless communication interface . . . 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."

vi. Claim 1 Conclusion

On the present record, we determine Petitioner has demonstrated a reasonable likelihood that it will prevail on its assertion that claim 1 would have been obvious over the combination of Dua and Giobbi '157.

vii. Claims 2–6, 8–11, and 14–19

Petitioner provides detailed explanations as to how the combination of Dua and Giobbi '157 allegedly renders obvious independent claim 14 reciting similar limitations as claim 1, and claims 2–6, 8–11, and 15–19 respectively depending from claims 1 and 14, citing Dr. Wolfe's testimony for support. Pet. 15–39 (citing Ex. 1004 ¶¶ 13, 47, 50, 52, 57–59, 70–72, 89, 94, 100, 103, 105, 106, 108, 109, 122, 123, 126–144, 152–154, 161, 172, 224, Figs. 1, 4, 4B, 6, 7; Ex. 1006 ¶¶ 28, 31, 33, 36–42, 43, 48, 53, 58, 63,

74; Ex. 1003 ¶¶ 105–142, 144–158, 161–169). At this stage in the proceeding, Patent Owner does not address separately these explanations and supporting evidence by Petitioner regarding claims 2–6, 8–11, and 14–19. *See generally* Prelim. Resp. 23–26.

Having reviewed Petitioner's arguments and supporting evidence in the present record, we determine Petitioner has demonstrated a reasonable likelihood that it will prevail on its assertion that claims 2–6, 8–11, and 14–19 would have been obvious over the combination of Dua and Giobbi '157.

D. Claims 1–7, 10, 11, and 14–19 as Allegedly Obvious over Buer (Ground 2), Claims 4, 8–10, 12, 13, 17, and 20 as Allegedly Obvious over Buer and Giobbi '157 (Ground 3), and Claim 4 as Allegedly Obvious over Buer and Nishikawa (Ground 4)

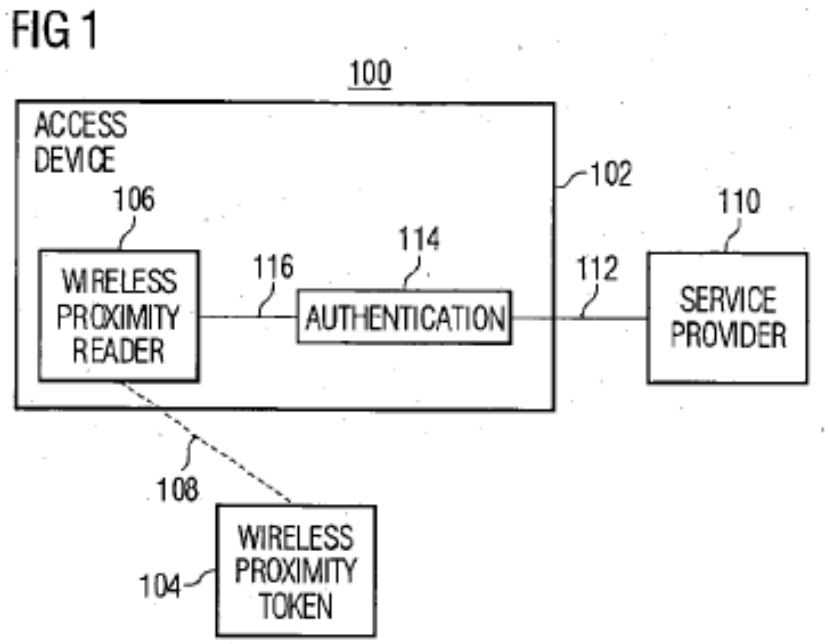
Alternatively, Petitioner contends that claims 1–7, 10, 11, and 14–19 of the '960 patent also would have been obvious over Buer (Pet. 39–76), that claims 4, 8–10, 12, 13, 17, and 20 of the '960 patent would have been obvious over Buer and Giobbi'157 (Pet. 63–76), and that claim 4 would have been obvious over Buer and Nishikawa (Pet. 76–78). In response, Patent Owner contends that Petitioner fails to demonstrate that Buer discloses or renders obvious the claim limitations. Prelim. Resp. 26–30.

We briefly summarize Buer and Nishikawa below.

1. Buer

Buer, titled "Proximity Authentication System," discloses controlling access to secured services based on the proximity of a wireless token to a computing device through which access to the secured services is obtained, wherein an authorized user is provided access to a service only when the wireless token assigned to the user is in the proximity of the computing device. Ex. 1005, codes (54), (57). A user's credential may be stored on the

token and a reader may be implemented within a security boundary on the computing device, and thus, the credential may be passed to the security boundary without passing through the computing device via software messages or applications. *Id.* An illustration of Buer's proximity-based authentication system is depicted in Figure 1, reproduced below.



Buer's Figure 1 is a block diagram of system 100 comprising access device 102 used to determine whether wireless token 104 assigned to a user or users is proximate to access device 102. *Id.* ¶¶ 110–111. As shown in Figure 1, wireless proximity reader 106 is configured to receive signals 108 from wireless proximity token 104, wherein signals 108 includes information that uniquely identifies wireless proximity token 104 and includes credentials (e.g., a password) that may be used to access a secured service provided by service provider 110. *Id.* ¶ 111.

2. Nishikawa

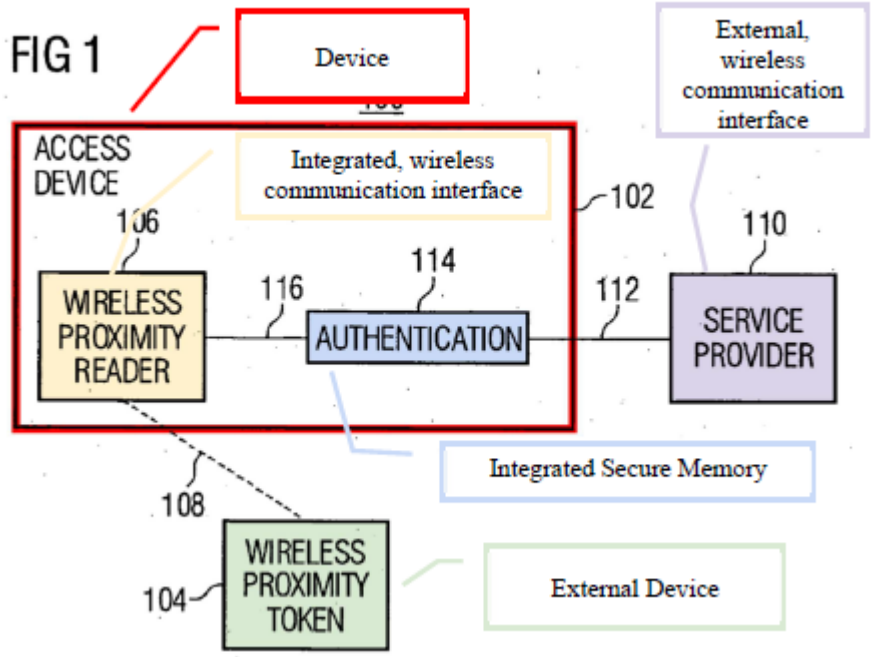
Nishikawa, titled "SIM Reader/Writer and Mobile Phone," discloses improving the convenience of a key holder type ID module by combining an IC chip of a SIM with contact and noncontact interfaces to provide the key holder type ID module with noncontact communication function. Ex. 1014, code (54), ¶ 17. Nishikawa also discloses combining a coil antenna and a display with a reader/writer to be used in combination with the SIM to provide the reader/writer with a short-distance communication function and a fingerprint sensing function. *Id.* ¶ 17.

3. Analysis of Claims 1–7, 10, 11, and 14–19 as Allegedly Obvious over Buer (Ground 2)

We begin by addressing in detail Petitioner's contentions and Patent Owner's arguments with respect to the limitations of representative claim 1.

i. Preamble, "A device"

Petitioner contends that, "[t]o the extent that the preamble is limiting, Buer discloses . . . an access device that combines an authentication circuitry and a wireless proximity reader to provide a device." Pet. 56 (citing Ex. 1003 ¶ 194). Petitioner provides an annotated Figure 1 of Buer, shown below, to illustrate its contentions.



The above annotated Figure 1 of Buer, according to Petitioner, illustrates "access device 102 ('device,' red)" that includes "two components: an authentication component 114 ('integrated, secure memory,' blue) and a wireless proximity reader 106 ('integrated, wireless communication interface,' yellow)." Pet. 41–42 (citing Ex. 1005, Fig. 1, ¶¶ 111–112, 118). Petitioner contends that, in Buer, "authentication component 114 is configured to process (e.g., encrypt or sign) the information before sending it to [] service provider 110 (purple)," and "wireless proximity reader 106 is configured to receive information from [] wireless proximity token 104 ('external, secure memory,' green) when the token is proximate to the access device." *Id.*

At this stage of the proceeding, Patent Owner does not present arguments in the Preliminary Response addressing the specific merits of

Petitioner's contentions with respect to the preamble. *See generally* Prelim. Resp. 26–30.[11]

Having reviewed all of Petitioner's assertions regarding this claim limitation, as well as the supporting evidence, we determine on this record that Petitioner has made a sufficient showing that Buer teaches a "device."

ii. "a battery," "an integrated, secure memory storing local, secured information"

Petitioner contends that Buer's access device includes "a battery when implemented as a mobile device, such as a cellular phone.'" Pet. 56 (citing Ex. 1005 ¶¶ 163, 195; Ex. 1003 ¶¶ 195–196). According to Petitioner, a POSITA "would have understood that the mobile device would include, although not shown, a battery to power its internal components." *Id.* at 47 (citing Ex. 1003 ¶ 179). At this stage of the proceeding, Patent Owner does not present arguments in the Preliminary Response addressing the specific merits of Petitioner's contentions with respect to this limitation. *See* generally Prelim. Resp. 26–30.

Having reviewed all of Petitioner's assertions regarding this claim limitation, as well as the supporting evidence, we determine on this record that Petitioner has made a sufficient showing that Buer teaches a "battery."

Petitioner then contends that "Buer's device includes an integrated, tamper-resistant memory storing local, encrypted information." Pet. 56 (citing Ex. 1005 ¶¶ 13, 134–137; Ex. 1003 ¶¶ 197–198). According to Petitioner, "Buer's cryptographic processor 308 acts as a controller for

[11] Because there is no dispute between the parties that Buer teaches a device, as recited in the preamble, for purposes of institution, we need not decide whether the preamble is limiting. *See Nidec*, 868 F.3d at 1017.

encrypting any important information, such as a user's credentials" received from an external token, and "the encrypted information (and credentials) is stored in data memory 314 within the crypted boundary 318," wherein "the memory may use 'tamper resistant and/or tamper evident hardware.'" *Id.* at 43–44 (citing Ex. 1005 ¶¶ 13, 119, 134–137, 141, 150; Ex. 1003 ¶ 175).

Patent Owner replies that Buer's "'data memory 314' is not unlocked by an access key provided by the service provider as required by the challenged claim(s)." Prelim. Resp. 26–27. In particular, Patent Owner repeats the argument that "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." *Id.* at 26. According to Patent Owner, Buer "only discloses the use of a key ***provided by a PDK*** to decrypt information received from data memory 314." *Id.* (citing Ex. 1005 ¶ 135).

We find Petitioner's arguments persuasive on this point. As Patent Owner acknowledges, Petitioner relies on Buer's "data memory 314" storing the claimed "local, secured information." Prelim. Resp. 26–27. In particular, Petitioner contends that data memory 314 stores information within the cryptographic boundary. Pet. 43–44. In fact, Patent Owner does not contest Petitioner's reliance on Buer's data memory 314 for teaching a tamper-resistant memory for storing encrypted information. Prelim. Resp. 26–27.

As discussed above, an interpretation of "local, secured information" as "information stored within a service block of a PDK and unlocked with a corresponding access key provided to the PDK," as Patent Owner asserts, (Prelim. Resp. 26) is not required.

We find persuasive Petitioner's reliance on Buer's data memory 314 storing "encrypted information (and credentials) . . . within the crypted boundary 318," wherein "the memory may use 'tamper resistant and/or tamper evident hardware,'" for teaching the claimed integrated, secure memory. Pet. 43–44; *see* Ex. 1005 ¶¶ 13, 134–135, 137.

On this preliminary record, we are also persuaded that Petitioner has made a sufficient showing that Buer teaches "an integrated, secure memory storing local, secured information."

iii. "an integrated, wireless communication interface for communicating wirelessly with at least one external device within a proximity zone"

Petitioner contends that Buer's "the integrated proximity reader (integrated, wireless communication interface) communicates 'wirelessly with at least' an external token 'within a proximity zone.'" Pet. 56–57 (citing Ex. 1003 ¶¶ 199–203). According to Petitioner, "Buer's wireless proximity reader (integrated, wireless communication interface) is configured to receive RF signals when the token is 'proximate to the access device,' such as 'when they are within a predefined distance of each other.'" *Id.* at 57 (citing Ex. 1005 ¶¶ 111, 146).

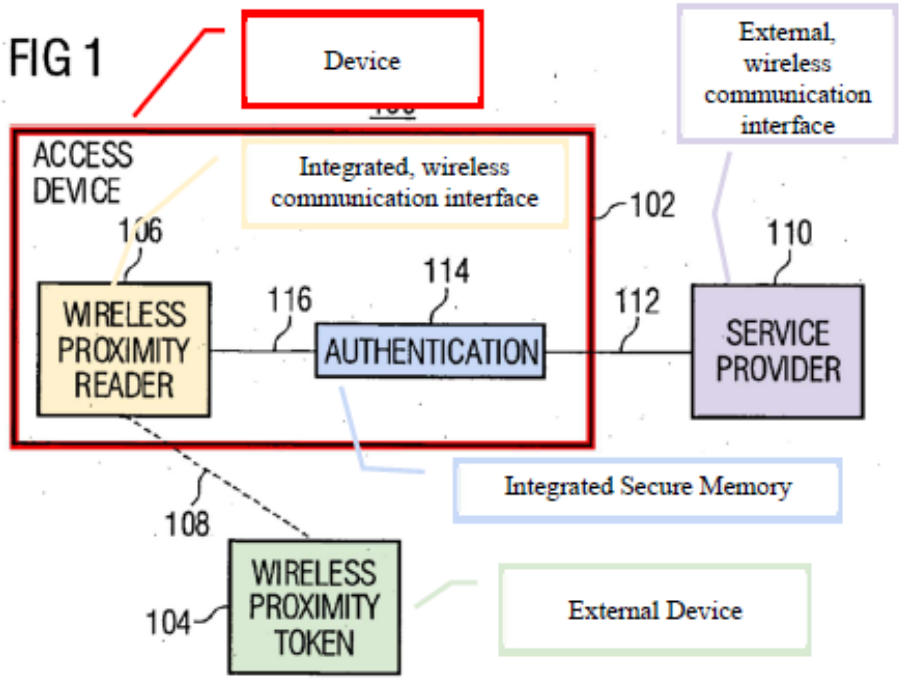
At this stage of the proceeding, Patent Owner does not present arguments in the Preliminary Response addressing the specific merits of Petitioner's contentions with respect to this limitation. *See generally* Prelim. Resp. 26–30.

Having reviewed all of Petitioner's assertions regarding this claim limitation, as well as the supporting evidence, we determine on this record that Petitioner has made a sufficient showing that Buer teaches "an

integrated, wireless communication interface for communicating wirelessly with at least one external device within a proximity zone."

iv. "the integrated, wireless communication interface communicatively coupled to the integrated, secure memory and coupled to draw power from the battery"

Petitioner contends that Buer's integrated, wireless proximity reader 106 is "communicatively coupled to the integrated, secure memory in the 'authentication component 114' 'via a connection 116 within a common integrated circuit.'" Pet. 57 (citing Ex. 1005 ¶ 116, Fig. 1; Ex. 1003 ¶ 201). Petitioner provides an annotated Figure 1 of Buer, shown below, to illustrate its contentions.



The above annotated Figure 1 of Buer, according to Petitioner, illustrates authentication component 114 as an operably connected collection of circuit components (blue), including a cryptographic processor and data memory.

Pet. 42–43, 57 (citing Ex. 1005 ¶¶ 116, 137, Figs. 1, 3, 6). Further, Petitioner contends that "[a]lthough Buer does not expressly disclose that the integrated wireless communication interface is powered by the battery, a POSITA would have understood that the integrated wireless proximity reader draws its energy from the battery." *Id.* at 48 (citing Ex. 1003 ¶ 181). Petitioner points to Patent Owner's acknowledgement that "mobile devices 'necessary [sic] require energy to power their operations, which, unless received from a wall plug or a PC, will be provided by a batter.'" *Id.* at 48, n.6 (quoting Ex. 1018 (Ex. F, Preliminary Infringement Contentions)), 3.

At this stage of the proceeding, Patent Owner does not present arguments in the Preliminary Response addressing the specific merits of Petitioner's contentions with respect to this claim limitation. *See generally* Prelim. Resp. 26–30.

Having reviewed all of Petitioner's assertions regarding this claim limitation, as well as the supporting evidence, we determine on this record that Petitioner has made a sufficient showing that Buer teaches an "integrated, wireless communication interface communicatively coupled to the integrated, secure memory and coupled to draw power from the battery."

v. "wherein one or more of (a) the integrated, wireless communication interface . . . 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."

Petitioner contends that Buer's "authentication component enabl[es] a wide variety of applications, functions, or services." Pet. 58 (citing Ex. 1003

¶¶ 204–205). According to Petitioner, Buer's "integrated proximity reader (integrated, wireless communication interface), communicat[es] wirelessly with an external token within a proximity zone, enabl[ing] network access on a device." *Id.* at 59 (citing Ex. 1005 ¶¶ 120, 122, 165, 174–175, Figs. 6–7; Ex. 1003 ¶¶ 206–208). Further, Petitioner contends that, also in Buer, "local, encrypted information stored by the integrated, tamper-resistant memory enables network access by sending encrypted or signed information to the 'network access provider (e.g., access point 608).'" *Id.* (citing Ex. 1005 ¶¶ 13, 134, 165, 174; Ex. 1003 ¶ 209). Alternatively, Petitioner contends that "Buer discloses that credit card information stored in its trusted platform module (TPM) is used to enable another processing system, such as a computer with a point-of-sale device." *Id.* (citing Ex. 1005 ¶¶ 192–195).

Patent Owner responds that "Buer teaches sending messages containing credential information from a token activated by proximity," which, according to Patent Owner, is "distinct from the invention claimed in the [']960 [p]atent." Prelim. Resp. 28. According to Patent Owner, Buer's method of providing access to a service "begins with a token sending a message containing authentication information," but the message "lacks information received from a token in exchange for an access key provided to the token." *Id.* at 28–29 (citing Ex. 1005 ¶¶ 146–149). That is, according to Patent Owner, "no key is provided in exchange for the information." *Id.* at 29. Accordingly, Patent Owner contends that "the Buer messages between token and reader and reader and service provider are not 'enabling one or more of an application, a function, and a service." *Id.* at 30.

We find Patent Owner's arguments unavailing, because Patent Owner is again relying on a claim construction of "enabling," requiring receiving information "from a token in exchange for an access key provided to the token" (Prelim. Resp. 28–30) that is not required by our construction discussed above. Thus, we are unpersuaded by Patent Owner's contention that Buer fails to disclose the "enabling" limitation because Buer's message lacks information received form a token in exchange for an access key provided to the token. *Id.* at 29.

Here, we are persuaded by Petitioner's reliance on Buer's integrated proximity reader communicating with an external token within a proximity zone as "enabl[ing] network access on a device." Pet. 59; *see* Ex. 1005 ¶¶ 120, 122, 165, 174–175, Figs. 6–7. We also find persuasive Petitioner's reliance on Buer's "local, encrypted information stored by the integrated, tamper-resistant memory" for "enabl[ing] network access" by sending encrypted or signed information to access point 608. *Id.*; *see* Ex. 1005 ¶¶ 13, 134, 165, 174). Alternatively, we find persuasive Petitioner's reliance on Buer's use of credit card information stored in its TPM "to enable another processing system, such as a computer with a point-of-sale device." *Id.*; *see* Ex. 1005 ¶¶ 192–195.

On this preliminary record, we are persuaded that Petitioner has made a sufficient showing that Buer teaches "one or more of (a) the integrated, wireless communication interface . . . 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."

vi. Claim 1 Conclusion

On the present record, we determine Petitioner has demonstrated a reasonable likelihood that it will prevail on its assertion that claim 1 would have been obvious over Buer.

vii. Claims 2–7, 10, 11, and 14–19

Petitioner provides detailed explanations as to how Buer allegedly renders obvious independent claim 14, reciting similar limitations as claim 1, and claims 2–7, 10, 11, and 15–19, respectively depending from claims 1 and 14, citing Dr. Wolfe's testimony for support. Pet. 39–55, 60–76 (citing Ex. 1005 ¶¶ 7, 11, 13, 97, 111–112, 114–115, 118–122, 127–130, 134–138, 141, 143146–150, 152–153, 155, 157–159, 162–163, 165, 173–175, 177, 181, 184–185, 190–196, Figs. 1, 3, 5–7, 11; Ex. 1006 ¶¶ 23, 26, 28, 30–31, 33, 35, 37–43, 48, 53, 58, 63, 74; Ex. 1003 ¶¶ 170–172, 174–188, 193, 211–237, 239–266). At this stage in the proceeding, Patent Owner does not address separately these explanations and supporting evidence by Petitioner regarding claims 2–7, 10, 11, and 14–19. *See generally* Prelim. Resp. 26–30.

Having reviewed Petitioner's arguments and supporting evidence in the present record, we determine Petitioner has demonstrated a reasonable likelihood that it will prevail on its assertion that claims 2–7, 10, 11, and 14–19 would have been obvious over Buer.

4. Analysis of Claims 4, 8–10, 12, 13, 17, and 20 as Allegedly Obvious over Buer in further view of Giobbi '157 (Ground 3)

Petitioner contends that claims 4, 8–10, 12, 13, 17, and 20 of the '960 patent would also have been obvious over Buer in further view of Giobbi

'157, providing the same arguments discussed above for the obviousness ground over Buer. Pet. 63–76. Patent Owner responds with the same arguments discussed above for the obviousness ground based on Buer. Prelim. Resp. 26–30.

Having reviewed Petitioner's arguments and supporting evidence in the present record, and Patent Owner's response, we determine, for generally the same reasons given above, that Petitioner has demonstrated a reasonable likelihood that it will prevail on its assertion that claims 4, 8–10, 12, 13, 17, and 20 of the '960 patent would also have been obvious over Buer and Giobbi '157.

5. Analysis of Claim 4 as Allegedly Obvious over Buer and Nishikawa (Ground 4)

Petitioner provides detailed explanations as to how the combination of Buer in further view of Nishikawa renders obvious claim 4 of the '960 patent, citing Dr. Wolfe's testimony for support. Pet. 76–78 (citing Ex. 1005 ¶¶ 114, 125, 163; Ex. 1014 ¶¶ 1, 4–13, 36, 73, 111, 114; Ex. 1003 ¶¶ 267–272). At this stage in the proceeding, Patent Owner does not address separately these explanations and supporting evidence by Petitioner regarding claim 4 over Buer and Nishikawa. *See generally* Prelim. Resp. 26–30.

Having reviewed Petitioner's arguments and supporting evidence in the present record, we determine Petitioner has demonstrated a reasonable likelihood that it will prevail on its assertion that claim 4 would have been obvious over the combination of Buer and Nishikawa.

III. CONCLUSION

Because we determine that Petitioner has demonstrated a reasonable likelihood that it would prevail in showing at least one of the challenged claims is unpatentable, we institute *inter partes* review as to all challenged claims and grounds presented in the Petition. 37 C.F.R. § 42.108(a). At this stage of the proceeding, we have not made a final determination as to the patentability of any of these challenged claims.

IV. ORDER

For the reasons given, it is

ORDERED that pursuant to 35 U.S.C. § 314, an *inter partes* review is instituted as to claims 1–20 of the '960 patent to determine whether:

1) claims 1–6, 8–11, and 14–19 are unpatentable under 35 U.S.C. § 103 as obvious over Dua and Giobbi '157;
2) claims 1–7, 10, 11, and 14–19 are unpatentable under 35 U.S.C. § 103 as obvious over Buer;
3) claims 4, 8–10, 12, 13, 17, and 30 are unpatentable under 35 U.S.C. § 103 as obvious over Buer and Giobbi '157; and
4) claim 4 is unpatentable under 35 U.S.C. § 103 as obvious over Buer and Nishikawa.

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial, which commences on the entry date of this Decision.

For PETITIONER:

Erika Arner
Kara Specht
Cory Bell
Shawn Chang
Safiya Aguilar
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
erika.arner@finnegan.com
kara.specht@finnegan.com
cory.bell@finnegan.com
shawn.chang@finnegan.com
safiya.aguilar@finnegan.com

For PATENT OWNER:

David Hecht
James Zak
HECHT PARTNERS LLP
dhecht@hechtpartners.com
zakx0017@umn.edu