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

Paper 11
Entered: August 13, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION,
Petitioner,

v.

PROXENSE, LLC,
Patent Owner.

IPR2024-00573
Patent 8,646,042 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

Microsoft Corporation ("Petitioner") filed a Petition requesting an *inter partes* review of claims 1, 5, 6, 8–11, 13, and 14 (the "challenged claims") of U.S. Patent No. 8,646,042 B1 (Ex. 1001, "the '042 patent"). Paper 2 ("Pet."). Proxense, LLC ("Patent Owner") filed a Preliminary Response. Paper 7 ("Prelim. Resp.").

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 '042 patent as the subject of *Proxense, LLC v. Microsoft Corporation*, No. 6.23-cv-00319 (W.D. Tex.) and *Proxense, LLC v. Google LLC et al.*, No. 6.23-cv-00320 (W.D. Tex.) ("the parallel district court litigations"). Pet. 89. Other patents in the family of the '042 patent are challenged by a different petitioner in *Samsung Electronics America, Inc. v. Proxense, LLC*, IPR2021-01438, Paper 1; and *Samsung Electronics America, Inc. v. Proxense, LLC*, IPR2021-01439, Paper 2. *Id.* at 89–90.

C. The '042 Patent

The '042 patent, titled "Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use," issued on February 4, 2014, from Application No. 13/445,825, with a filing date of April 12, 2012.

Ex. 1001, codes (54), (45), (21), (22). The ’042 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 ’042 patent’s hybrid device is depicted in Figure 1, reproduced below:

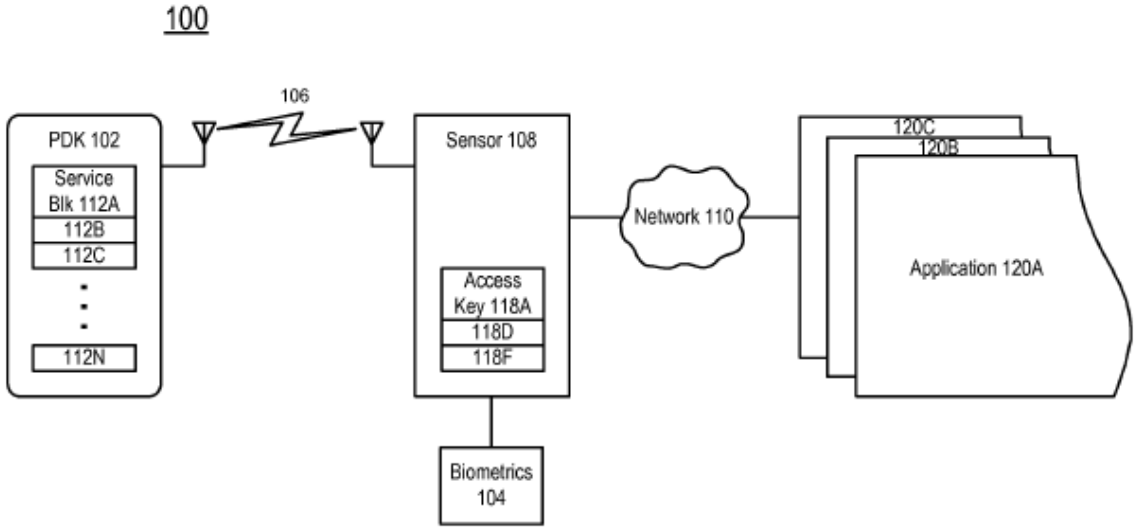


FIG. 1

Figure 1 is a block diagram of system 100 comprising PDK 102, sensor 108, network 110, and one or more applications 120 (including services). *Id.* at 2:64–3:1. In Figure 1, sensor 108 is coupled to PDK 102 by wireless link 106 and coupled to network 110 by a wired or wireless link. *Id.* at 3:1–3. In the exemplary embodiment shown in Figure 1, applications 120 are accessed over network 110, with sensor 108 being adapted to receive biometric input 104 from a user and displaying status to a user. *Id.* at 3:3–6.

In the example shown in Figure 1, sensor 108 contains three service block access keys 118A, 118D, 118F, wherein service block access keys 118 allow sensor 108 to unlock information stored in corresponding service

blocks 112, which information is used as local secured information. *Id.* at 3:13–20. In one example in which a biometric input is required in order to access specific service blocks in PDK 102, service block 112A is used for verification of the biometric input and sensor 108 uses stored corresponding service block access key 118A to unlock biometric service 112A. *Id.* at 3:21–26. A current biometric information is received using biometric input 104, and sensor 108 verifies the stored biometric input (from service block 112A) against the recently acquired biometric information (from input 104). *Id.* at 3:26–29.

An exemplary embodiment of sensor 108 is depicted in Figure 3, reproduced below:

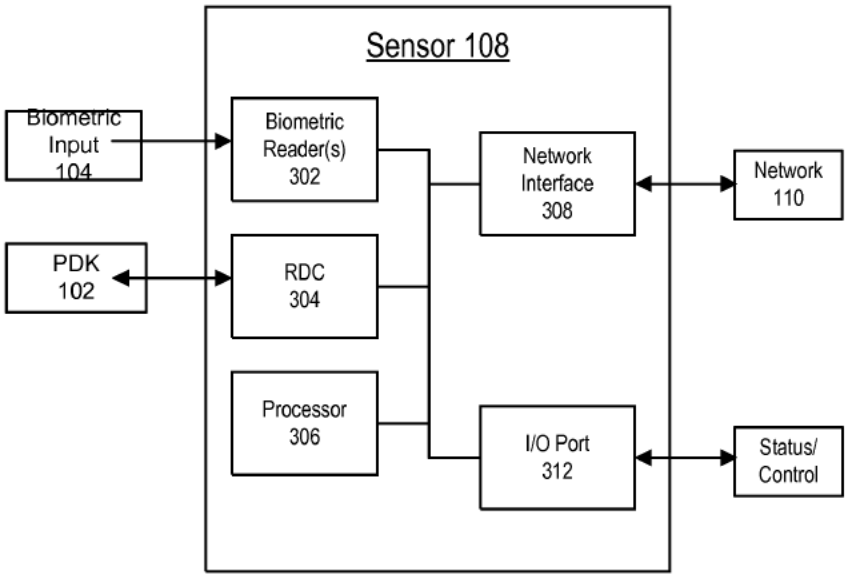


FIG. 3

Figure 3 is a block diagram of sensor 108 comprising one or more biometric readers 302, RDC 304, processor 306, network interface 308, and I/O

port 312. *Id.* at 7:4–7. As shown in Figure 3, RDC 304 provides the wireless interface to PDK 102. *Id.* at 7:10–11.

Biometric reader 302 receives and processes biometric input 104 from an individual. *Id.* at 7:23–7:30. I/O port 312 provides general input and output interface to sensor 108. *Id.* at 7:42–48.

D. The Challenged Claims

Of the challenged claims, claims 1 and 10 are independent. Independent claim 1 is illustrative of the challenged claims, and is reproduced below:

> 1. A hybrid device comprising:
>
> an integrated personal digital key (PDK) for storing information and capable of communicating wirelessly with at least one external receiver-decoder circuit (RDC); and
>
> an integrated RDC for communicating wirelessly with at least one external PDK within a proximity zone, the integrated RDC coupled to the integrated PDK by a first signal line for communication, the integrated RDC coupled to at least one other component of the hybrid device by a second signal line, one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service on one or more of the hybrid device and a device associated with the external RDC.

Ex. 1001, 21:52–65.

E. Asserted Grounds of Unpatentability

Petitioner challenges the patentability of claims 1, 5, 6, 8–11, 13, and 14 of the ’042 patent on the following grounds (Pet. 1–2):

Claim(s) Challenged	35 U.S.C. §[1]	Reference(s)/Basis
1, 5, 6, 8–11, 13, 14	103	Giobbi '157[2], Giobbi '139[3]
1, 5, 6, 8–11, 13, 14	103	Giobbi '157, Giobbi '139, Dua[4]
10, 11, 13, 14	103	Broadcom[5]

Petitioner relies on the Declaration of Dr. Patrick Traynor, 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) (2020). 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

[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 '042 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. 2007/0245157 A1, published October 18, 2007, filed May 5, 2007 (Ex. 1005, "Giobbi '157").

[3] U.S. Patent Publication No. 2004/0255139 A1, published December 16, 2004, filed May 17, 2004 (Ex. 1006, "Giobbi '139").

[4] U.S. Patent No. 9,042,819 B2, issued May 26, 2015, filed September 30, 2014 (Ex. 1007, "Dua").

[5] European Patent Application No. EP 1,536,306 A1 published June 1, 2005, filed September 30, 2004 (Ex. 1008, "Broadcom").

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)).

1. "*hybrid device*"

Patent Owner proposes construing "hybrid device" recited in the challenged claims as "a device comprising an integrated personal digital key (PDK) and an integrated receiver decoder circuit," as construed by the District Court in a case filed by Patent Owner against Samsung, *Proxense, LLC v. Samsung Electronics Co.*, 6:21-cv-00210-ADA (W.D. Tex.) ("the Samsung case"). Prelim. Resp. 4–5 (citing Ex. 2001, 3 (construing claims of patents related to the '042 patent, but not claims of the '042 patent)). Petitioner contends that, "[f]or purposes of this proceeding, Petitioner adopts this construction [adopted in the District Court]." Pet. 4. We determine no explicit construction of "hybrid device" is necessary to resolve the parties' issues in controversy. *See Vivid Techs.*, 200 F.3d at 803.

2. "*receiver-decoder circuit (RDC)*"

Patent Owner proposes construing "receiver-decoder circuit" recited in the challenged claims as "a component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing" as construed by the District Court in the Samsung case. Prelim. Resp. 8–9 (citing Ex. 2001, 4; Ex. 2004, 4). Petitioner contends that, "[f]or purposes of this proceeding, Petitioner adopts

this construction [adopted in the District Court]." Pet. 5. We determine no explicit construction of "receiver-decoder circuit" is necessary to resolve the parties' issues in controversy. *See Vivid Techs.*, 200 F.3d at 803.

3. "*personal digital key (PDK)*"

Patent Owner proposes construing "personal digital key (PDK)" recited in the challenged claims as "a component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing" as construed by the District Court in the Samsung case. Prelim. Resp. 12–13 (citing Ex. 2001, 3–4; Ex. 2004, 4). Petitioner contends that, "[f]or purposes of this proceeding, Petitioner adopts this construction [adopted in the District Court]." Pet. 4. We determine no explicit construction of "personal digital key (PDK)" is necessary to resolve the parties' issues in controversy. *See Vivid Techs.*, 200 F.3d at 803.

4. "*enabling one or more of an application, a function, and a service*" (claims 1, 10)

Claim 1 recites a "one or more of the integrated RDC and integrated PDK *enabling one or more of an application, a function, and a service* on one or more of the hybrid device and a device associated with the external RDC." Ex. 1001, 21:61−65 (emphasis added). Claim 10 similarly recites "enabling one or more of an application, a function and a service on one or more of the hybrid device and a device associated with an external RDC." *Id.* at 22:37–40.

Patent Owner asserts that "[i]n 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.'" Prelim.

Resp. 13. In particular, 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. 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.

Prelim. Resp. 13–14 (citing Ex. 2002, 26). Patent Owner contends that Petitioner has not challenged this construction, and thus, "[t]his Board must 'presume . . . that the same claim term in the same patent or related patents carries the same construed meaning.'" *Id.* at 14 (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. 13. In particular, we disagree that the District Court in the Samsung case provided any construction for the term "enabled." *Id.* at 13–14. 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. That is, a determination of whether a term is indefinite is not the same thing as construing a claim term. Thus, the District Court, by determining that "hybrid device" is not indefinite, did not construe the term "enabled." Accordingly, although 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" limited to "exchanging an access key for information held within a service block of a PDK," as Patent Owner contends. Prelim. Resp. 27.

Patent Owner then contends that the '042 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.'" Prelim. Resp. 21. Patent Owner references several examples in the Specification. *Id.* at 21–28 (citing Ex. 1001, 3:21–32, 8:19–29, 9:6–13, Figs. 1, 4–6). In particular, Patent Owner makes reference to Figure 6 of the '042 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. 21–22 (quoting Ex. 1001, 9:6–13) (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 24.

Patent Owner then 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. 24. Patent Owner also references Figure 1 of the '042 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. 24 (citing Ex. 1001, 3:21–32) (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 '042 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. 25–26 (quoting Ex. 1001, 8:19–29).

With "others," Patent Owner references Figure 5 of the '042 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. 26–27 (quoting Ex. 1001, 8:30–42).

Petitioner does not propose a claim construction for "enabl[ing] one or more of an application, a function, and a service" but, in applying the prior art to the claims, relies on, for example, Giobbi '157's "transaction" which "includes enabling access to secure physical or digital assets (e.g., unlocking a door, opening a vault, providing access to a secured hard drive, etc.)." Pet. 37–39 (citing Ex. 1005, code (57), ¶¶ 11, 59–63, 65, Fig. 4; Ex. 1003 ¶¶ 69–71). Petitioner also relies on Broadcom's manner of controlling access to secured services, wherein, once proximity is authenticated, an access device "enable[s] access to the requested service," or alternatively, the service "may enable an access device" to perform various functions. *Id.* at 77–78 (citing Ex. 1008 ¶¶ 57, 116–120, 122; Ex. 1003 ¶¶ 126–127).

The plain language of enabling an application, function, or service does not suggest a requirement that information be received from a PDK in exchange for an access key. 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. 21–28. 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. *Id.*

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. 21–28. As Patent Owner argues, "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 20 (citing *Trustees of Columbia Univ. v. Symantec*, 811 F.3d 1359, 1363–64 (Fed. Cir. 2016) (emphasis added)). However, 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 21–28; *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1984).

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 shows various "examples" of "enabling" an application, a function or a service presented in the Specification. Prelim. Resp. 24. In particular, as 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."[6] Ex. 1001,

[6] 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. 23), 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, 9:6–13.

9:6–13 (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 3:21–32 (emphases 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 8:30–42 (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 8:19–29 (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. 21–28. 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*. *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 or a service"

recited in claims 1 and 10 is not limited to receiving information from a PDK in exchange for an access key. We determine no further explicit construction is necessary to resolve the controversy. *See Vivid Techs.*, 200 F.3d at 803.

C. 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.[7] *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

D. Claims 1, 5, 6, 8–11, 13, and 14 as Obvious over Giobbi '157, Giobbi '139, and Dua

Petitioner contends that claims 1, 5, 6, 8–11, 13, and 14 of the '042 patent would have been obvious over by Giobbi '157, Giobbi '139, and alternatively, over Giobbi '157, Giobbi '139, and Dua. Pet. 6–68. In response, Patent Owner contends that the Petition fails to establish that Giobbi '157, Giobbi '139, and Dua "render the challenged claims invalid and unpatentable." Prelim. Resp. 28–31.

We briefly summarize Giobbi '157, Giobbi '139, and Dua below.

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

1. Giobbi '157

Giobbi '157, titled "Two-Level Authentication for Secure Transaction," published on October 18, 2007, with a filing date of May 5, 2007. Ex. 1005, codes (54), (43), (22). Giobbi '157 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." *Id.* at code (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.

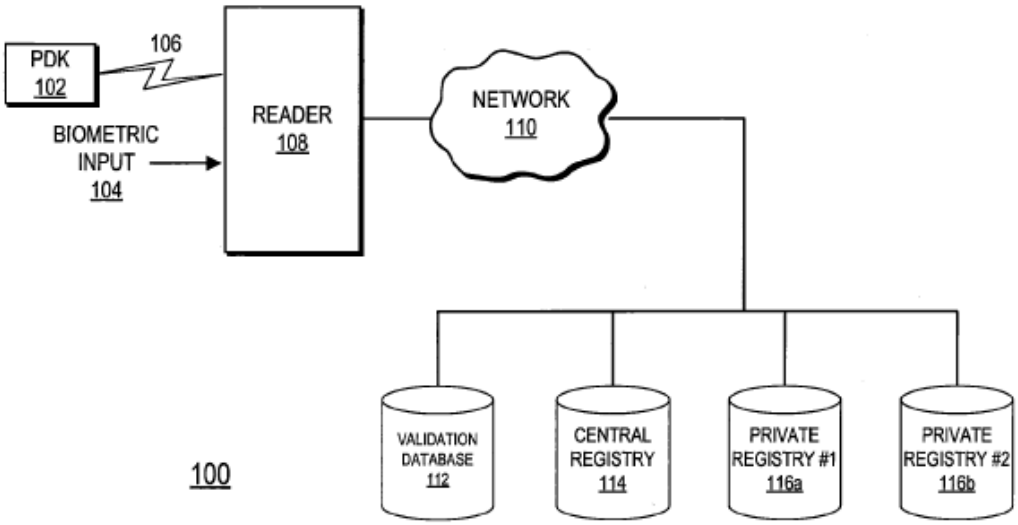


FIG. 1

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.

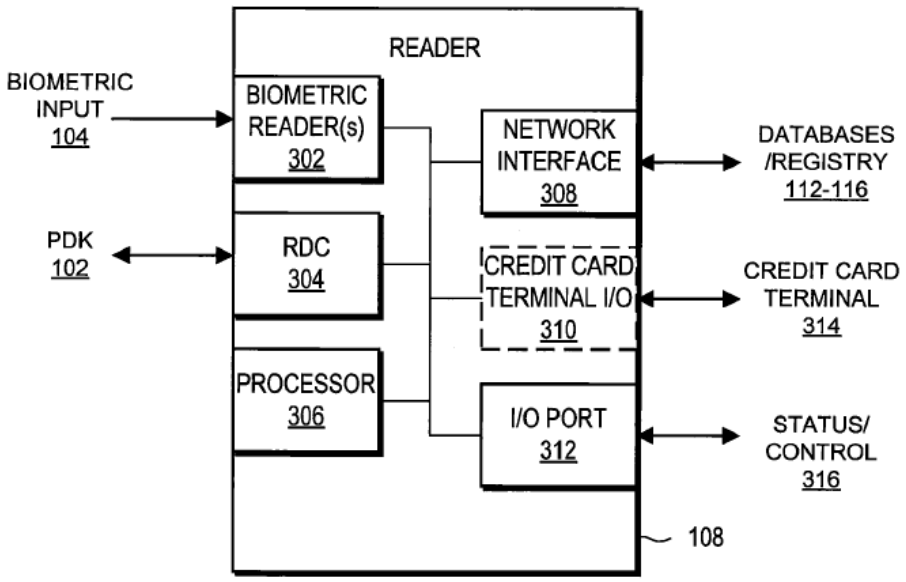


FIG. 3

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.

PDK 102 is depicted in Figure 2, reproduced below.

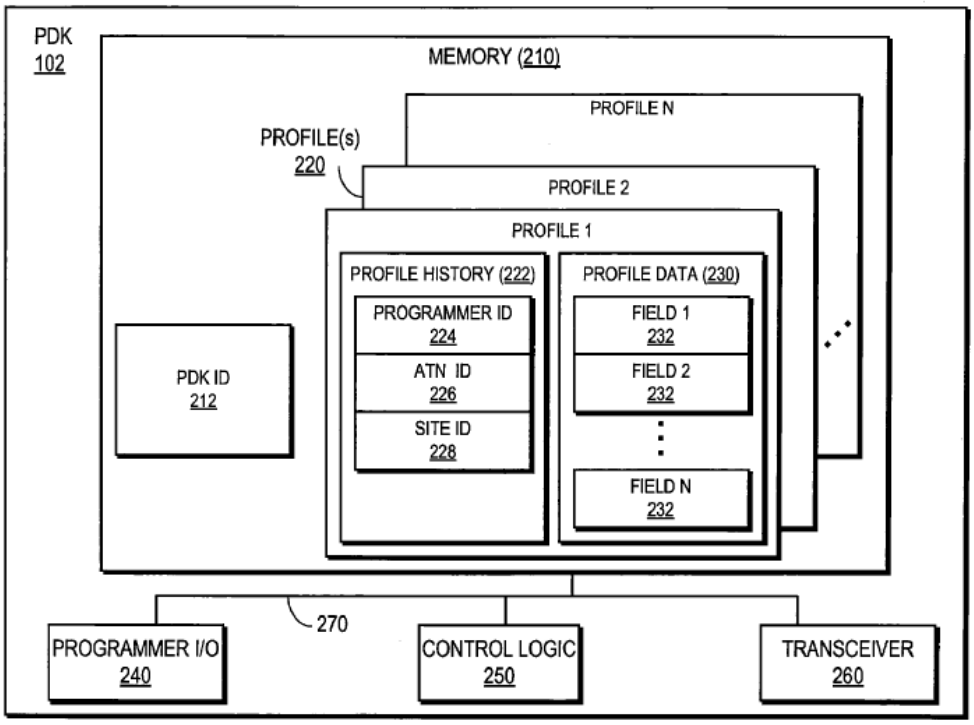


FIG. 2

Figure 2 is a block diagram of PDK 102 comprising memory 210, programmer I/O 240, control logic 250, and transceiver 260, coupled by bus 270. *Id.* ¶ 35. Memory 210 can be any combination of memory types, including physical access secured and tamperproof memories, that stores unique PDK ID 212 and one or more profiles 220. *Id.* ¶ 36. Profiles 220 may comprise a biometric profile, for example, which includes profile data 230 representing physical and/or behavioral information that can uniquely identify the PDK owner. *Id.* ¶ 37.

2. Giobbi '139

Giobbi '139, titled "Digital Content Security System," published on December 16, 2004, with a filing date of May 17, 2004. Ex. 1006, codes

(54), (43), (22). Giobbi '139 discloses a personal digital key digital content security system (PDK-DCSS) that is used to protect computers from unauthorized use and protect the digital content stored on computers from being wrongfully accessed and copied. *Id.* at code (57). Components of the PDK-DCSS are (1) a standard hard drive device, with the addition of a PDK receiver/decoder circuit (PDK-RDC) integrated into the hard drive's controller, and (2) a PDK key associated with the PDK-RDC. *Id.* To save batteries, RDCs use checks for presence of associated PDK key on a periodic basis. *Id.* ¶ 89.

3. Dua

Dua, titled "Method, System, and Apparatus Having Near Field Communication (NFC) Chip With Configurable Memory That Is Updatable Via a Host Processor," issued on May 26, 2015, with a filing date of September 30, 2014. Ex. 1006, codes (54), (45), (22). Dua discloses the use of Radio Frequency Identification (RFID) technology to exchange communication settings, media capability, and other parameters with an external device that also has integrated RFID technology. *Id.* at code (57). In particular, Dua discloses a media player with cellular phone capability. *Id.* at 6:46–65, Fig. 1. An RFID tag-reader module is attached to or embedded within the media player, wherein 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.* at 12:46–56. Compatibility with these standards gives the media player the ability to not only establish a wireless connection with other electronic devices using RFID for setup, but also allows the media

player to function as an electronic key and wallet (for point-of-sale transactions). *Id.* at 12:56–61.

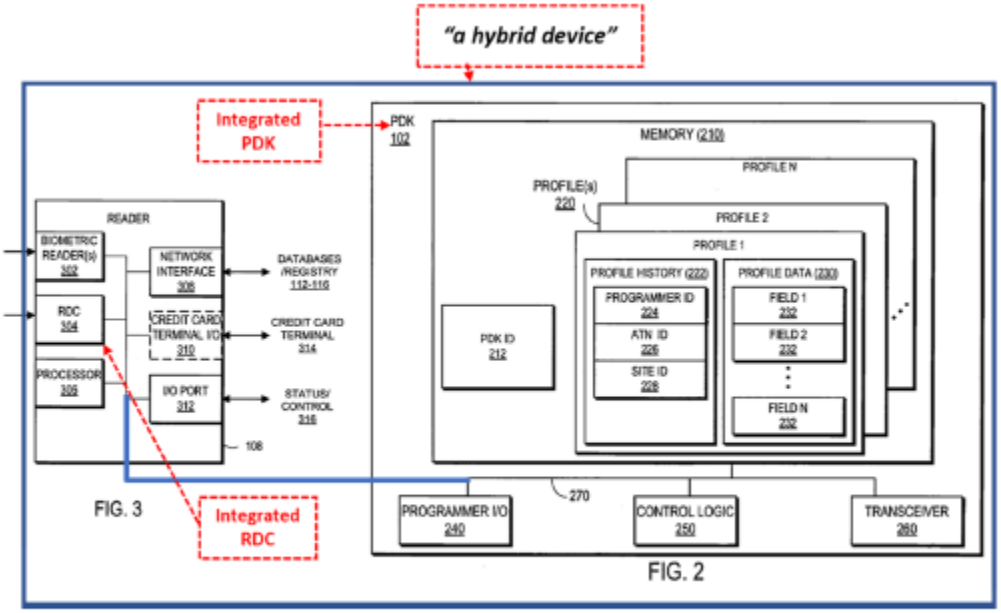
4. Analysis of Claims 1, 5, 6, 8–11, 13, and 14 as being Obvious over Giobbi '157, Giobbi '139, and Dua

Petitioner contends that the claims of the '042 patent are directed to a "hybrid device" that "includes a personal digital key (PDK) and a receiver-decoder circuit (RDC).'" Pet. 5. Petitioner contends that Giobbi '157 similarly teaches an "integrated PDK" that "can communicate with a receiver-decoder circuit (RDC)." *Id.* at 7–8.

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 "hybrid device"

Petitioner contends that, "[t]o the extent that the preamble is limiting, the combination of Giobbi-157 and-139 discloses a '***hybrid device***'" as claimed. Pet. 26 (citing Ex. 1005 ¶¶ 12, 27, 30, 35; Ex. 1006 ¶¶ 22–44; Ex. 1003 ¶ 58). Petitioner provides an annotated combination of Figures 2 and 3 of Giobbi '157, modified to incorporate Giobbi '139's teachings, shown below, to illustrate its contentions.



MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139's teachings).

The above annotated combination of Figures 2–3 of Giobbi '157 in the Petition, according to Petitioner, illustrates "Giobbi-157's cell phone" which "includes an integrated PDK" (second from top dotted red box), and in the combination of Giobbi '157 and Giobbi '139, "this integrated PDK communicates with an integrated RDC" (bottom red box) "all within a ***hybrid device***." Pet. 26–27 (citing Ex. 1005, Figs. 2–3).

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 the preamble. *See generally* Prelim. Resp. 28–31.[8]

[8] Because there is no dispute that Giobbi '157 in view of Giobbi '139 and Dua teaches a hybrid 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)).

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 established a reasonable likelihood of establishing that the combination of Giobbi '157, Giobbi '139, and Dua teaches a "hybrid device."

ii. "an integrated personal digital key (PDK) . . . communicating wirelessly with at least one external receiver-decoder circuit (RDC)," "an integrated RDC for communicating wirelessly with at least one external PDK . . . coupled to the integrated PDK by a first signal line [and] coupled to at least one other component of the hybrid device by a second signal line"

Petitioner contends that Giobbi '157 "discloses a '***Personal Digital Key (PDK)***,' which is an example of an ***integrated*** secure memory ***for storing information***," wherein the PDK "is ***integrated*** into a hybrid device, such as a cell phone." Pet. 27 (citing Ex. 1005 ¶¶ 11, 35). Petitioner further contends that Giobbi '157 discloses "RDC 304," which wirelessly receives data from the PDK 102 in an encrypted format and decodes the encrypted data for processing. *Id.* at 28 (citing Ex. 1005 ¶¶ 50, 59). According to Petitioner, Giobbi '157 discloses establishing communication between PDK 102 and RDC 304 of reader 108 once PDK 102 is within range of reader 108. *Id.* at 28–29 (citing Ex. 1005 ¶ 59). Thus, Petitioner contends that Giobii '157 discloses that PDK 102 "***communicat[es] wirelessly with at least one external receiver-decoder circuit (RDC)*** [(304)]." *Id.* at 29 (citing Ex. 1003 ¶60).

In addition, Petitioner contends that "Dua's RFID Tag Unit 306 is another example of a '***PDK***' ***for storing information***" and "***capable of***

communicating wireless with at least one external receiver-decoder circuit (RDC) (RFID reader)." Pet. 29 (citing Ex. 1007, 6:46–65, 12:51–64, 13:9–18,14:53–64, 15:42–56, 16:31–34, Figs. 4A, 6; Ex. 1003 ¶ 61).

Petitioner further contends that Giobbi '157 discloses "an integrated RDC '***communicating wireless with at least one external PDK within a proximity zone***,'" because Giobbi '157's reader 108 wirelessly communicates with PDK 102 when PDK 102 is within a proximity zone of reader 108. Pet. 30 (citing Ex. 1005 ¶¶ 26–44). According to Petitioner, Giobbi '157's "hybrid device" includes "an integrated RDC" that is coupled to the integrated PDK by a "signal line for communication." *Id.* (citing Ex. 1005 ¶¶ 12, 27, 30, 35; Ex. 1006 ¶¶ 22–44; Ex. 1003 ¶ 62) (emphasis omitted). Further, Petitioner contends that Giobbi '139 also discloses "an integrated RDC 'communicating wirelessly with the at least one external device within a proximity zone.'" *Id.* at 30–31 (citing Ex. 1006 ¶¶ 26–44; Ex. 1003 ¶ 63).

In addition, Petitioner contends that "Dua's Reader Unit 304 is another example of an '***integrated, reader-decoder circuit (RDC)***'" because "Reader Unit 304 also '***communicat[es] wirelessly with at least one external device within a proximity zone***' and is '***communicatively coupled to [an] integrated PDK***' (the RFID Tag Unit 306)." Pet. 31 (citing Ex. 1007, 6:46–65, 12:51–64, 13:9–18, 14:53–64, 15:42–56, 16:31–34, Figs. 4A, 6; Ex. 1003 ¶ 64).

Petitioner then contends that Giobbi '157 shows "***the integrated RDC 304 coupled by a second signal line*** to the biometric reader 302 (***at least one other component of the hybrid device***.)" Pet. 34 (citing Ex. 1005 ¶¶ 30, 48, 49, 51, 52, 71, Fig. 3). According to Petitioner, "[t]he integrated RDC

compares the biometric input at the biometric reader to the biometric profile data received from a PDK," wherein a POSITA would have found it obvious that "the integrated RDC [is] coupled to at least one other component of the hybrid device by a second signal line." *Id.* (citing Ex. 1005 ¶¶ 30, 48–49, 51–52, 71, Fig. 3; Ex. 1003 ¶ 66) (emphasis omitted). In addition, Petitioner contends that Giobbi '139 also discloses "a storage device ('***at least one other component***') '***of the hybrid device***'" that "can be controlled by a signal line from the RDC to the storage device ('***the integrated RDC coupled to at least one other component of the hybrid device by a second signal line***')." *Id.* at 33 (citing Ex. 1006 ¶¶ 41, 88–90).

Further, Petitioner also contends that "Dua's teachings" render "obvious that ***the integrated RDC*** is ***coupled to at least one other component of the hybrid device by a second signal line***, so that the RDC can enable that component or for the mere fact that the RDC must be connected to a processor, transmitter, memory, or power to function in the mobile device." Pet. 36 (citing Ex. 1007 6:46–65, 12:51–64, 13:9–18, 14:53–64, 15:42–56, 16:31–34, Figs. 4A, 6; Ex. 1003 ¶ 68).

At this stage in the proceeding, Patent Owner does not present arguments in the Preliminary Response addressing the specific merits of Petitioner's contentions with respect to these limitations in claim 1. *See generally* Prelim. Resp. 28–31.

On this preliminary record, we are persuaded that Petitioner has made a sufficient showing that the combination of Giobbi '157 in view of Giobbi '139 and Dua teaches "an integrated personal digital key (PDK) . . . communicating wirelessly with at least one external receiver-decoder circuit (RDC)," "an integrated RDC for communicating wirelessly with at least one

external PDK . . . coupled to the integrated PDK by a first signal line [and] coupled to at least one other component of the hybrid device by a second signal line," as recited in claim 1.

iii. "one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service on one or more of the hybrid device and a device associated with the external RDC"

Petitioner contends that Giobbi '157 discloses "[w]hen a PDK [] comes within range of a Reader [], communication is automatically established [] between the RDC . . . and the PDK . . . when it enters a proximity zone of the [RDC].'" Pet. 37 (citing Ex. 1005 ¶¶ 59–63). According to Petitioner, Giobbi '157 then provides for the RDC requesting profile data stored within the external PDK for authentication, and if the profile data received from the "secure memory" of the external PDK is valid, the RDC "completes the transaction," wherein a "transaction" includes "enabling access to secure physical or digital assets," i.e., "***enabling one or more of an application, a function, and service***." *Id.* (citing Ex. 1005 ¶¶ 61, 63).

Petitioner provides an annotated Figure 4 of Giobbi '157, shown below, to illustrate its contentions.

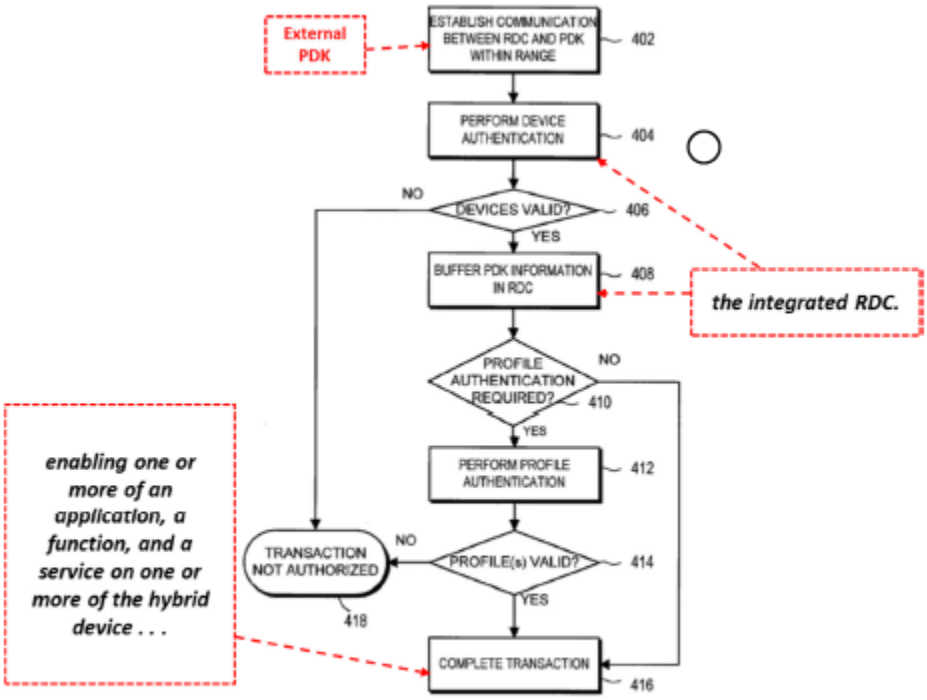


FIG. 4
MS-1005, FIG. 4.

The above annotated Figure 4 of Giobbi '157, as discussed in the Petition, is a block diagram illustrating a method for establishing communication between an RDC and a PDK within range. Pet. 38. In annotated Figure 4 of Giobbi '157, the method begins with the "External PDK" (top dotted red box) "'establish[ing] communication between RDC and PDK within range,'" wherein, upon transaction completion 416, the method "enabl[es] one or more of an application, a function and a service" (bottom dotted red box). *Id.* at 37 (citing Ex. 1005 ¶¶ 59–63) (emphasis omitted).

According to Petitioner, Giobbi '157 "explicitly" teaches that the transaction "enables one or more of an application, a function, and service" when stating that "the transaction includes enabling access to secure physical or digital assets (e.g., unlocking a door, opening a vault, providing access to a secured hard drive, etc.)." Pet. 39 (citing Ex. 1005 ¶ 63;

Ex. 1003 ¶ 71) (emphasis omitted). According to Petitioner, "the external PDK can enable functions on the hybrid device, including 'effectively enabling/disabling the device itself.'" *Id.* at 37–38.

Alternatively, Petitioner contends the "integrated PDK" of the hybrid device in Giobbi '157 also "enabl[es] one or more of an application, a function, and service." Pet. 38 (citing Ex. 1005, code (57), ¶ 11) (emphasis omitted). According to Petitioner, "[t]ransactions in Giobbi–157 are performed by transmitting authenticating information from a PDK ('***the integrated PDK***' of the hybrid device) to an RDC (***the external RDC***), for example, when completing a withdrawal from an ATM (***a device associated with the external RDC)***." *Id.* at 38–39 (citing Ex. 1005 ¶ 65; Ex. 1003 ¶ 70).

In addition, Petitioner contends Giobbi '139 discloses "a use case where an integrated RDC can be incorporated into cell phones, PDAs, and MP3 players." Pet. 40 (citing Ex. 1006 ¶ 88). According to Petitioner, in Giobbi '139, "[i]f an authorized PDK is used in conjunction with the integrated RDC the application/function/service runs on the device," e.g., "the hybrid device 'plays the digital content,' such as music ('***enables one or more of an application, a function, and service***')." *Id.* (citing Ex. 1006 ¶ 37; Ex. 1003 ¶ 72).

Patent Owner responds that the exchanged information referenced by the Petitioner in Giobbi '157 is not "received in exchange for an access key provided to the PDK." Prelim. Resp. 29. According to Patent Owner, Giobbi '157 does not teach or suggest that "this unsecure[d] 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." *Id.* at 30. Patent Owner contends the second exchange in Giobbi '157 likewise does not disclose providing an access key. *Id.* In particular, according to Patent Owner, "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." *Id.* Patent Owner also contends that "Giobbi '139 also fails to disclose that the 'activation code' is provided in exchange for an access key provided by the playing device." *Id.* at 31. Accordingly, Patent Owner contends that "neither Giobbi '157 nor Giobbi '139 disclose 'enabling one or more of an application, a function, and a service.'" *Id.*

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. 29–31) that is not consistent with 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, and does not require, "receiv[ing] information from a PDK in exchange for an access key."

Giobbi '157 teaches, for example, an RDC requesting profile data stored within the external PDK for authentication, wherein, if the profile data received from the external PDK is valid, the RDC completes the transaction, which includes enabling access to secure physical or digital assets. *See* Ex. 1005 ¶¶ 61, 63, Fig. 4. We are persuaded by Petitioner's reliance on Giobbi '157's "transaction" wherein upon its completion

"'enabl[es] access to secure physical or digital assets' ('***enabling one or more of an application, a function, and service***')." *See* Pet. 37.

On this preliminary record, we are persuaded that Petitioner has made a sufficient showing that the combination of Giobbi '157 in view of Giobbi '139 and Dua teaches "one or more of the integrated RDC and integrated RDC and integrated PDK enabling one or more of an application, a function, and a service on one or more of the hybrid device and a device associated with the external RDC," as recited in claim 1.

iv. Claims 5, 6, 8–11, 13, and 14 as Obvious over Giobbi '157, Giobbi '139, and Dua

Petitioner provides detailed explanations as to how the combination of Giobbi '157, Giobbi '139, and Dua renders the limitations as recited in claims 5–6, 8–11, and 13–14 obvious, citing Dr. Traynor's testimony for support. Pet. 40–68 (citing Ex. 1005, code (57), ¶¶ 9, 11–12, 26–30, 33, 35, 37, 43–44, 47, 49–59, 61–68, 74, Figs. 1–4, 7D; Ex. 1006 ¶¶ 36–37, 55, 67–69, 71, 87–91; Ex. 1007 18:60–22:6, Figs. 4A–B; Ex. 1003 ¶¶ 73–114). At this stage in the proceeding, Patent Owner does not address separately these explanations and supporting evidence by Petitioner regarding claims 5–6, 8–11, and 13–14. *See generally* Prelim. Resp. 28–31.

Having reviewed Petitioner's arguments and supporting evidence in the present record, we are persuaded that Petitioner has made a sufficient showing that the combination of Giobbi '157, Giobbi '139, and Dua teaches the subject matter of claims 5, 6, 8–11, 13, and 14.

v. Conclusion

For the foregoing reasons, we determine that the evidence and arguments presented show a reasonable likelihood that Petitioner would

prevail in establishing that the subject matter of claims 1, 5, 6, 8–11, 13, and 14 would have been obvious over Giobbi '157, Giobbi '139, and Dua.

5. Analysis of Claims 1, 5–6, 8–11, and 13–14 as Obvious over Giobbi '157 and Giobbi '139

Petitioner contends that claims 1, 5–6, 8–11, and 13–14 of the '042 patent would also have been obvious over just Giobbi '157 and Giobbi '139, but provides the same arguments discussed above for the obviousness ground over Giobbi '157, Giobbi '139, and Dua. Pet. 6–68. Patent Owner responds with the same arguments discussed above for the obviousness ground based on Giobbi '157, Giobbi '139, and Dua. Prelim. Resp. 28–31. Thus, at this stage of the proceeding, we do not separately address Petitioner's obviousness ground based on Giobbi '157 and Giobbi '139. Nonetheless, Patent Owner may raise arguments regarding this obviousness ground in the Response after institution.

E. Claims 10, 11, 13, and 14 as obvious over Broadcom

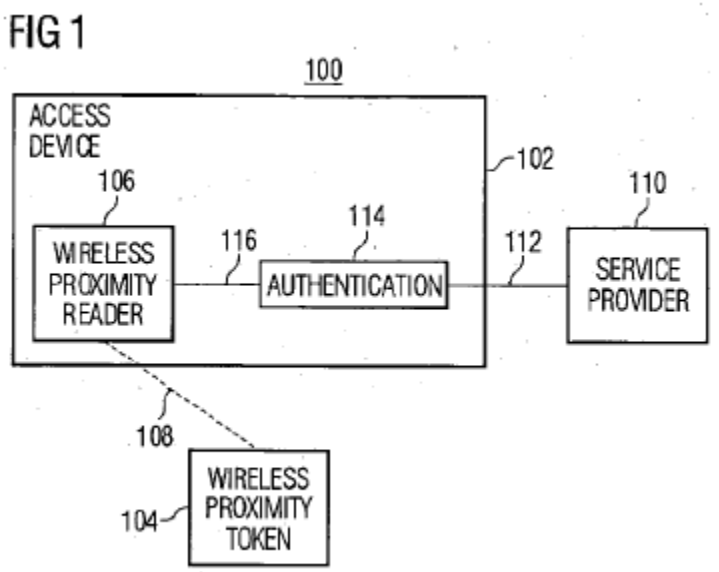
Petitioner contends that claims 10, 11, 13, and 14 of the '042 patent also would have been obvious over Broadcom (Pet. 68–84). In response, Patent Owner contends that Petitioner fails to demonstrate that Broadcom discloses or renders obvious the claim limitations. Prelim. Resp. 31–34.

We briefly summarize Broadcom below.

1. Broadcom

Broadcom, titled "Proximity Authentication System," published on June 1, 2005, with a filing date of September 30, 2004. Ex. 1008, codes (54), (43), (22). Broadcom 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. *Id.* at code (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 Broadcom's proximity-based authentication system is depicted in Figure 1, reproduced below.

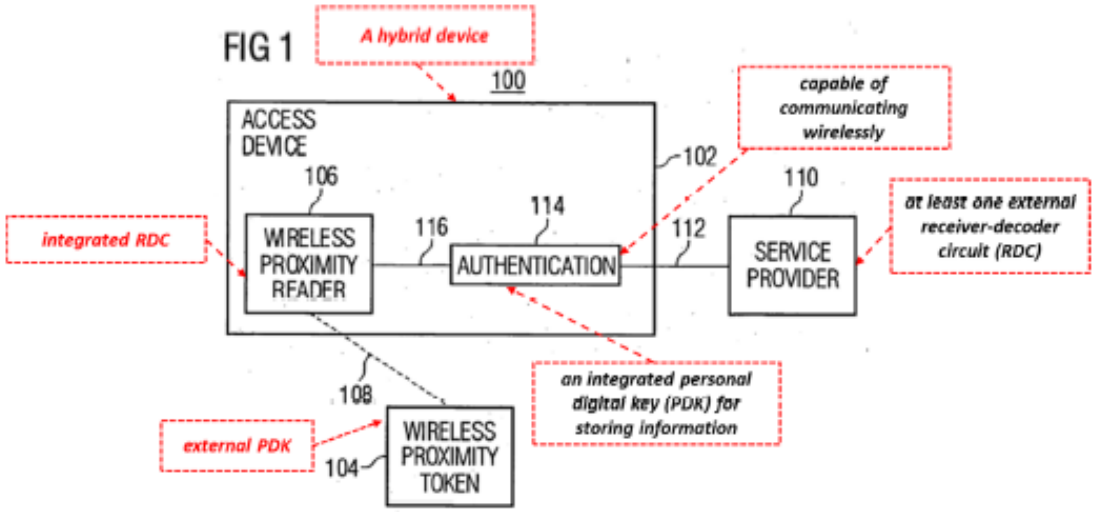


Broadcom's Figure 1 is a block diagram of system 100 comprising access device 102 used to determine whether wireless token 104 assigned to a user or users is proximate to access device 102. *Id.* ¶¶ 110–111. As shown in Figure 1, wireless proximity reader 106 is configured to receive signals 108 from 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. Analysis of Claims 10, 11, 13, and 14 as Obvious over Broadcom

Petitioner contends that Broadcom teaches "a system for secured access to a service based on a wireless device coming within[] the proximity of a reader," wherein a user's credentials are stored on an RFID token and this token and associated authentication credentials are then read by an RFID reader. Pet. 68 (citing Ex. 1008, code (57), ¶¶ 9–16). In particular, according to Petitioner, the Access Device including the reader authenticates the RFID token and permits access to the secured service after authentication. *Id.* (citing Ex. 1003 ¶ 115). According to Petitioner, Broadcom teaches securing authentication information securely within memory that is tamper resistant and not exposed in the mobile device. *Id.* at 70 (citing Ex. 1008 ¶¶ 13, 134, 167, 187, 192; Ex. 1003 ¶ 116).

Petitioner provides an annotated Figure 1 of Broadcom, shown below, to illustrate its contentions.



MS-1008, FIG. 1 (annotated).

The above annotated Figure 1 of Broadcom in the Petition illustrates access device 100, which requests access to service provider 110 and "verif[ies]

that the information sent from the token 104 includes a credential associated with an authorized user and or access device." Pet. 69–70 (citing Ex. 1008 ¶¶ 113–119).

We address in detail Petitioner's contentions and Patent Owner's arguments with respect to the limitations of representative claim 10.

i. "generating an enablement signal enabling one or more of an application, a function and a service on one or more of the hybrid device and a device associated with an external RDC" (claim 10)

Petitioner contends that Broadcom discloses that, its "access device 102" sends "'authentication-related information [('***enablement signal***')] to the service provider 110 to indicate that the token 104 is proximate to the access device 102,'" which then "'enable[s] access to the requested service (block 208).'" Pet. 78 (citing Ex. 1008 ¶¶ 116–119). According to Petitioner, Broadcom discloses that the term "access" may include, "for example, acquiring, using, invoking, etc.," and thus, "'data may be accessed by providing a copy of the data to the access device,' from ***a device associated with an external RDC***." *Id.* (citing Ex. 1008 ¶ 122; Ex. 1003 ¶ 126).

Alternatively, Petitioner contends Broadcom discloses its service may enable an access device to perform various functions including "'access[ing] a processing application' ('***generating an enablement signal enabling one or more of an application, a function and a service on . . . the hybrid device***,'" for example, "'invoking, interacting with or using the application or loading the application onto the access device.'" *Id.* (citing Ex. 1008 ¶¶ 120, 122; Ex. 1003 ¶ 127).

Patent Owner responds that Broadcom accesses services by way of an RFID token broadcasting credentials when activated by a reader, subsequently passed to a service provider for access. Prelim. Resp. 32. Although Patent Owner acknowledges that "Broadcom [] teaches sending messages containing credential information from a token activated by proximity," Patent Owner contends that, "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." *Id.* at 32–33. According to Patent Owner, "no key is provided in [the] exchange for the information." *Id.* at 33.

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. 32–33), which is inconsistent with our claim construction discussed above. Thus, we are unpersuaded by Patent Owner's contention that Broadcom fails to disclose the "enabling" limitation because "Broadcom [] teaches sending messages containing credential information from a token activated by proximity." *Id.*

Here, as Patent Owner acknowledges, Broadcom teaches sending messages containing credential information for access to a service. Prelim. Resp. 32. We agree with Petitioner's reliance on Broadcom's manner of "[controlling] access to secured services [] based on the proximity of wireless token" for teaching "enabling" a service. Pet. 77–78; *see* Ex. 1008 ¶¶ 57, 116–119, 122.

On this preliminary record, we are persuaded that Petitioner has made a sufficient showing that Broadcom teaches "generating an enablement

signal enabling one or more of an application, function and a service on one or more of the hybrid device and a device associated with an external RDC," as recited in claim 10.

ii. Remaining limitations of claim 10, and claims 11, 13, and 14

Petitioner provides detailed explanations as to how Broadcom teaches the remaining claim limitations as recited in independent claim 10 and claims 11, 13, and 14 depending therefrom, citing Dr. Traynor's testimony for support. Pet. 71–77, 79–84 (citing Ex. 1008 ¶¶ 9–10, 110–119, 125, 130, 133–142, 148, 156–159, 162–168, 184, 195, Figs. 1, 3, 6; Ex. 1003 ¶¶ 120–125, 128–135). At this stage in the proceeding, Patent Owner does not address separately Petitioner's explanations and supporting evidence regarding the remaining limitations in claim 10 and claims 11, 13, and 14. *See* generally Prelim. Resp. 31–34.

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 independent claim 10, and claims 11, 13, and 14 depending therefrom, would have been obvious over Broadcom.

v. Conclusion

For the foregoing reasons, we determine that the evidence and arguments presented show a reasonable likelihood that Petitioner would prevail in establishing that the subject matter of claims 10, 11, 13, and 14 would have been obvious over Broadcom.

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) (2020). 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, 5, 6, 8–11, 13, and 14 of the '042 patent to determine whether:

1) claims 1, 5, 6, 8–11, 13, and 14 are unpatentable under 35 U.S.C. § 103 as obvious over Giobbi '157, and Giobbi '139;
2) claims 1, 5, 6, 8–11, 13, and 14 are unpatentable under 35 U.S.C. § 103 as obvious over Giobbi '157, Giobbi '139, and Dua;
3) claims 10, 11, 13, and 14 are unpatentable under 35 U.S.C.§ 103 as obvious over Broadcom; and

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:

W. Karl Renner
Roberto J. Devoto
Usman Khan
Jonathan Driesslein
FISH & RICHARDSON P.C.
axf-ptab@fr.com
devoto@fr.com
khan@fr.com
driesslein@fr.com

For PATENT OWNER:

David L Hecht
James Zak
HECHT PARTNERS LLP
dhecht@hechtpartners.com
jzak@hechtpartners.com