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

Paper 33
Entered: April 21, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO. LTD.,
Petitioner,

v.

WARD PARTICIPATIONS B.V.,
Patent Owner.

PGR2022-00007
Patent 10,992,480 B2

Before THU A. DANG, GEORGIANNA W. BRADEN, and JAMES J. MAYBERRY, *Administrative Patent Judges.*

DANG, *Administrative Patent Judge.*

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable

I. INTRODUCTION

A. Background

In response to a Petition (Paper 2, "Pet.") filed by Samsung Electronics Co., Ltd. ("Petitioner"), we instituted a post-grant review of claims 1–19 (the "challenged claims") of U.S. Patent No. 10,992,480 B2 (Ex. 1001, "the '480 patent"). *See* Paper 8 ("Dec. Inst."). During trial, Ward Participations B.V. ("Patent Owner") filed a Response (Paper 11 ("PO Resp."), to which Petitioner filed a Reply (Paper 21, "Pet. Reply."). In turn, Patent Owner filed a Sur-Reply. Paper 28 ("PO Sur-Reply"). An oral hearing was held with the parties on January 26, 2023. A transcript of the hearing has been entered into the record. Paper 32 ("Tr.").

We have jurisdiction under 35 U.S.C. § 6. This Decision is a final written decision under 35 U.S.C. § 328(a) and 37 C.F.R. § 42.73 as to the patentability of claims 1–19 of the '480 patent. We conclude Petitioner has shown by a preponderance of the evidence that those claims are unpatentable.

B. Related Proceedings

Petitioner identifies the '480 patent as the subject of *Ward Participations B.V. v. Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.*, No. 6.21-cv-00806 (W.D. Tex.). Pet. 112. Petitioner also identifies the '480 patent as the subject of IPR2022-00113. *Id.* A final written decision in IPR2022-00113 will issue on the same day as this Decision.

C. The '480 Patent

The '480 patent, titled "Method and System for Performing a Transaction and for Performing a Verification of Legitimate Access to, or

Use of Digital Data," issued on April 27, 2021, from Application No. 16/597,773 (the "'773 application"), with a filing date of October 9, 2019, which is a continuation of Application No. 10/560,579, filed as PCT Application No. PCT/NL2004/00042 (the "'422 application"), with a filing date of June 14, 2004, which in turn claims priority to Foreign (Dutch) Application No. PCT/NL03/00436 (the "'00436 Dutch application"), with a filing date of June 13, 2003. Ex. 1001, codes (54), (45), (21), (22), (63), (30).

The invention described in the '480 patent provides authentication data and authentication software to an electronic device that are stored in a secure storage location inaccessible to the user or the operating system of the device. *Id.* at code (57). An illustration of the embodiment of the '480 patent's computer configuration is depicted in Figure 3, reproduced below:

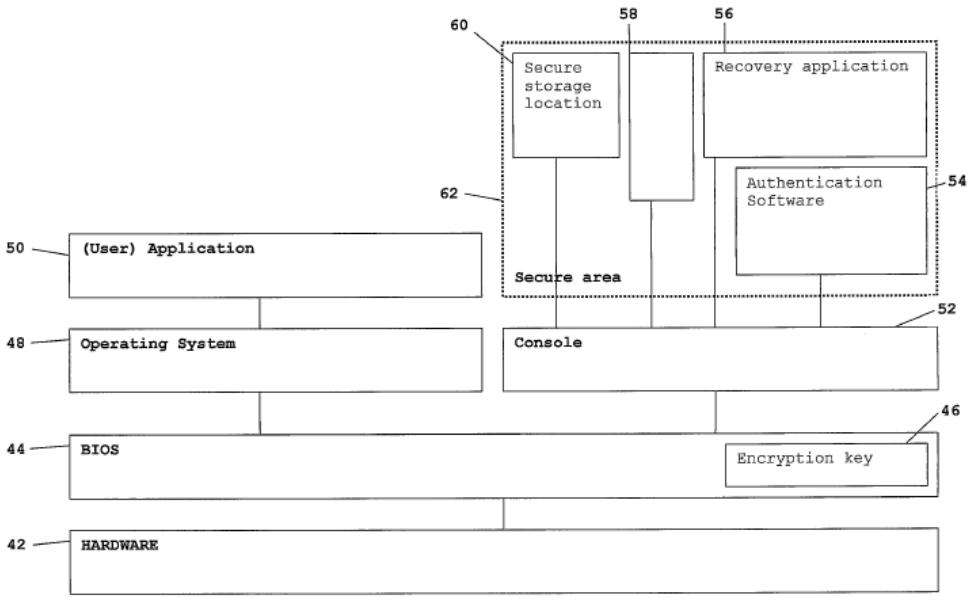


FIG. 3

Figure 3 is a schematic diagram of a computer configuration of a device having authentication software and an authentication table installed in the Basic In Out System (BIOS). *Id.* at 3:14–16. As shown in Figure 3, the

device consists of hardware 42, examples of hardware components being a processor, a hard drive, or other memory and a keyboard. *Id.* at 8:14–17. The hardware devices are controlled by BIOS 44, BIOS 44 being a software package stored in a read-only-memory (ROM) located on a main board, which is one of the hardware components of an electronic device. *Id.* at 8:18–21.

BIOS 44 controls most of the instructions and data flowing from one component to another, wherein BIOS 44 checks whether the instructions to the other component are allowed or not. *Id.* at 8:22–28. As shown in Figure 3, BIOS 44 may comprise encryption key 46 used to encrypt data, and only another party who knows encryption key 46 may be able to decrypt the data. *Id.* at 8:29–32.

Operating system 48 creates a run-time environment for any user application, and is an interface between the user and hardware 42. *Id.* at 8:33–36. When a user instructs operating system 48 to run application 50, application 50 requests data from operating system 48, and operating system 48 in turn requests the data through BIOS 44 from hardware 42, i.e., the hard drive, wherein the data coming from hardware 42 pass through BIOS 44 and operating system 48 before they arrive at requesting application 50. *Id.* at 8:36–43. Accordingly, BIOS 44 controls the accessibility of certain data or devices of hardware 42 and thus the use of particular software, wherein it may prohibit, for example, operating system 48 from accessing certain parts of a hard drive or to starting certain applications. *Id.* at 8:44–48.

Console 52 is an environment that runs all the processes in the computer, wherein, at start-up of the computer, console 52 instructs devices of hardware 42 via BIOS 44 to start and report their status, and in case of errors, BIOS 44 sends error messages coming from hardware 42 to

console 52, which then handles and correct the errors. *Id.* at 8:49–56. Any instructions coming from operating system 48 intended for console 52 may be blocked by BIOS 44. *Id.* at 8:59–61.

In Figure 3, in or behind console 52, there is secure area 62 only accessible to BIOS 44, secure area 62 comprising applications and storage locations not reported to operating system 48, and thus, operating system 48 does not know that the applications and data in the storage locations are present and maybe even running in a separate environment. *Id.* at 8:62–9:1.

As shown in Figure 3, secure area 62 comprises secure storage location 60, recovery application 56, and authentication software 54, wherein an authentication table may be securely stored in secure storage location 60 in a part of the computer commonly seen as part of BIOS 44 but the authentication table is unreachable for operating system 48, and thus for a user. *Id.* at 9:7–11. With the authentication table securely stored in secure storage location 60, authentication software 54 should run in an environment in BIOS 44, thus preventing the authentication table from being accessible to operating system 48 at any time. *Id.* at 9:12–16. Therefore, authentication software 54 may be installed in an application environment in secure area 62 such that it may obtain the authentication table without passing through an unsecured part of the device. *Id.* at 9:16–19. Authentication software 54 preferably has its own unique serial number, software identification (ID) and/or private encryption key. *Id.* 5:39–40.

In a further embodiment, authentication software 54 may be provided with a system for signing a digital signature using a part of a software identification number (software ID) or any other application identifying character string, hereinafter, "private key." *Id.* at 13–31–36. A digital signing algorithm is preferably stored in a secure part of BIOS 44, wherein

this algorithm may be protected like the authentication table in secure storage location 60. *Id.* at 9:27–34.

D. The Challenged Claims

Of the challenged claims, claims 1, 16, 17, and 18 are independent. Independent claim 1 is illustrative of the challenged claims, and is reproduced below:

> 1. A method for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party, the electronic device having an operating system creating a run-time environment for user applications, the method comprising:
>
> providing a private key in a memory of said electronic device, said memory being a secure part of a Basic In Out System or any other secure location in said electronic device, which private key is inaccessible to a user of said electronic device, wherein the private key is encrypted when the private key is stored in said memory, a decryption key for decrypting the private key being incorporated in the electronic device, said decryption key being inaccessible to said user, to any user-operated software and to said operating system, wherein said memory is inaccessible to said operating system of said electronic device, thereby rendering the private key inaccessible to said user, wherein the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software;
>
> providing authentication software in said electronic device, the private key being accessible to said authentication software, wherein authentication software is stored in said secure memory inaccessible to said operating system;
>
> activating the authentication software to generate a digital signature from the private key, wherein the authentication software is run in a secure processing environment inaccessible to said operating system;

providing the digital signature to the second transaction party.

Ex. 1001, 17:64–18:29.

E. Asserted Challenges to Patentability

We instituted post grant review of all claims and all challenges in the Petition. Petitioner asserts that claims 1–19 of the '480 patent are unpatentable on the following basis (Pet. 3–5):

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–19	112(a)	Lack of written description
1, 3, 6, 11, 14–19	103[1]	Ellison[2], Muir[3]
7, 9, 13	103	Ellison, Muir, Al-Salqan[4]
8, 10, 12	103	Ellison, Muir, Searle[5]

Petitioner relies on the Declarations of John R. Black, Jr., Ph.D. (Exs. 1003, 1032) in support of its unpatentability contentions. Patent Owner provides the Declarations of Bart Preneel, Ph.D. Exs. 2001, 2012.

[1] The Leahy-Smith America Invents Act ("AIA") amended 35 U.S.C. § 103. *See* Pub. L. No. 112-29, 125 Stat. 284, 285–88 (2011). As the application that issued as the '480 patent was filed before the effective date of the relevant amendments, the pre-AIA version of § 103 applies.

[2] U.S. Patent No. 7,082,615, issued July 25, 2006, filed September 22, 2000 (Ex. 1006, "Ellison").

[3] PCT Patent Publication No. WO 01/93212, published December 6, 2001, filed May 30, 2001 (Ex. 1008, "Muir").

[4] U.S. Patent No. 6,549,626, issued April 15, 2003, filed October 20, 1997 (Ex. 1007, "Al-Salqan").

[5] U.S. Patent No. 6,683,954, issued January 27, 2004, filed October 23, 1999 (Ex. 1009, "Searle").

Dr. Preneel was cross-examined by Petitioner, and a transcript of his deposition was entered into the record. Ex. 1034.

II. ANALYSIS

A. Level of Ordinary Skill in the Art

In determining whether an invention would have been obvious at the time it was made, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). In our analysis, various factors may be considered, including the "type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field." *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (quotation marks omitted). Furthermore, the prior art itself can reflect the appropriate level of ordinary skill in the art. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

Relying on the declaration of Dr. Black, Petitioner contends that a person of ordinary skill in the art (POSITA) related to the '480 patent would have had "a Bachelor's degree in an academic discipline emphasizing the design of electrical, computer, software technologies, or a related field, in combination with training or at least two years of related work experience with software security technologies such as cryptography or encryption/decryption systems." Pet. 5. According to Petitioner, "the person could also hold a Masters or Doctor of Philosophy degree in a relevant academic discipline with less than a year of related work experience in the same discipline." *Id.* (citing Ex. 1003 ¶¶ 15–16). Patent Owner "does not dispute Petitioner's POSITA definition." *See* PO Resp. 8.

Accordingly, we adopt and apply Petitioner's definition of a POSITA at the time of the claimed invention because, based on the record, this proposal is consistent with the '480 patent, the asserted prior art, and is supported by the testimony of Dr. Black. We note that the applied prior art comports with this level of skill. *See Okajima*, 261 F.3d at 1355.

B. Claims 1–19 as Allegedly Lacking Written Description Support Under 35 U.S.C. § 112(a)

The written-description inquiry is a question of fact, is context-specific, and must be determined on a case-by-case basis. *Ariad Pharm., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (en banc). The test for sufficiency of support is whether the disclosure of the application relied upon "reasonably conveys to the artisan that the inventor had possession at that time of the later claimed subject matter." *Vas–Cath Inc. v. Mahurkar*, 935 F.2d 1555, 1563 (Fed. Cir. 1991). "One shows that one is 'in possession' of the invention by describing the invention, with all its claimed limitations," wherein, "[w]hile the meaning of terms, phrases, or diagrams in a disclosure is to be explained or interpreted from the vantage point of one skilled in the art, all the limitations must appear in the specification." *Lockwood v. Am. Airlines, Inc.*, 107 F.3d 1565, 1572 (Fed. Cir. 1997). That is, "it is the specification itself that must demonstrate possession" and "a description that merely renders the invention obvious does not satisfy the [written description] requirement." *Ariad Pharm.*, 598 F.3d at 1351 ("[T]he level of detail required to satisfy the written description requirement varies depending on the nature and scope of the claims and on the complexity and predictability of the relevant technology.").

Petitioner contends that the '480 patent does not describe a "private key" in the manner recited in the claims. Pet. 14. In particular, Petitioner

contends that the following terms in independent claim 1, and similarly recited in independent claims 16–18, lack written description support: "providing a private key in a memory of said electronic device, said memory being a secure part of a Basic In Out System or any other secure location in said electronic device," wherein the private key is "inaccessible to a user of said electronic device," "encrypted when the private key is stored in said memory," and "decrypted in a secure processing environment inaccessible to said user and to any user-operated software." Pet. 10–11, 14–24; *see* Pet. Reply 1–14. Patent Owner disputes these contentions. PO Resp. 8–34; PO Sur-reply 1–5.

We address in detail Petitioner's arguments and Patent Owner's responses with respect to the contested limitations of claim 1.

i. "providing a private key in a memory of said electronic device, said memory being a secure part of a Basic In Out System or any other secure location in said electronic device" wherein the "private key is inaccessible to a user of said electronic device" (claim 1)

According to Petitioner, the '480 patent discloses "a secure area 62 that includes a secure storage location 60, authentication software 54, an authentication table and a memory location 58" which stores "a log file of all actions performed by the BIOS 44," but "the '480 Patent fails to describe where the private key is stored in the electronic device." Pet. 16–17. Petitioner provides an annotated Figure 3 of the '480 patent, shown below, to illustrate its contentions.

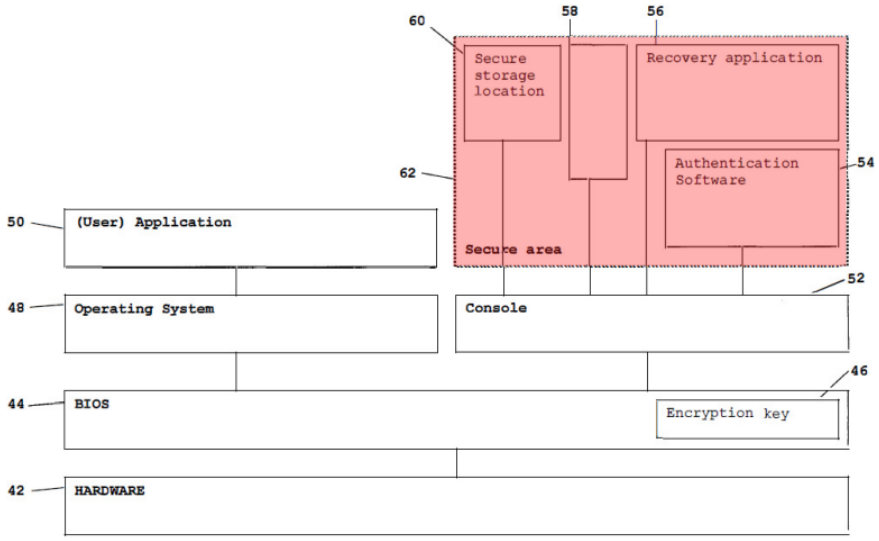


FIG. 3

The Petition's annotated Figure 3 of the '480 patent shows secure area 62 (red), comprising secure storage location 60, memory location 58, recovery application 56, and authentication software 54. Pet. 17.

Petitioner contends that, although the '480 patent explains that secure area 62 is "[i]n or behind the console 52" and is "only accessible to the BIOS [44]," "the '480 Patent fails to describe where the private key is stored in the electronic device and certainly does not teach that the secure area 62 stores the private key." Pet. 17. According to Petitioner, although the '480 patent teaches an "authentication software for signing a digital signature [which] uses a private key" that is "preferably stored in a secure part of the BIOS 44" and is protected "in the secure storage location 60," this disclosure "describes the storage of the ***digital signing algorithm and not of the private key***." *Id.* at 18 (citing Ex. 1001, 9:27–34, 13:31–44; Ex. 1003 ¶ 173). Petitioner contends that "the '480 Patent only reveals that the private key is '***registered at a third party***, for example the authentication software provider ***which supplied said private key***.'" *Id.* (citing Ex. 1001, 13:31–44).

Petitioner then contends that, since there is no teaching in the '480 patent of where the private key is stored or maintained in the user's electronic device "or how the private key may be protected from the user when provided by the third party," the '480 patent "fails to provide written description in support of the private key being inaccessible to a user of the electronic device." Pet. 19 (citing Ex. 1003 ¶¶ 175–176).

Patent Owner argues that the contested limitations are fully supported by the description of the '773 application that issued as the '480 patent, and that a POSITA "would reasonably recognize the claim limitations based on the disclosure of the '773 patent." PO Resp. 16–17. Patent Owner contends that "Petitioner admits that the specification includes description of a private key." *Id.* at 17 (citing Pet. 14). In particular, according to Patent Owner, the '773 application "discloses '[t]he authentication software preferably has its own unique serial number, software ID and/or private encryption key,'" and thus "[a] POSITA would recognize that since the unique serial number [or] software ID of the authentication software is [a] private key, the private key is an integral part of the authentication software component and/or is embedded therein." *Id.* at 17 (citing Ex. 1001, 5:39–40). Patent Owner contends that, "[a]s a result of recognizing the private key can be an integral part of the authentication software because the '773 application states this, a POSITA would recognize that disclosure relating to the authentication software also includes the private key embedded therein." *Id.* at 19 (citing Ex. 1001, 5:39–40; Ex. 2012 ¶¶ 5, 46, 53, 55–56).

We are unpersuaded by Patent Owner's contention that a POSITA would recognize that the '480 patent's "authentication software" would include the "private key" as claimed "embedded therein." PO Resp. 19. In particular, we are unpersuaded by Patent Owner's citation to the

specification of the '480 patent disclosing that "[t]he authentication software preferably has its own unique serial number, software ID and/or private ***encryption*** key" (PO Resp. 17 (citing Ex. 1001, 5:39–40) (emphasis added)), as written description support for the claimed "private key" limitation. As Petitioner points out, "[t]he private encryption key recited in 5:40 of the '480 Patent should not be confused with the private key used to generate a digital signature in the '480 Patent's 13:31–44." Pet. Reply 8, n1. We are persuaded by Petitioner's contention and determine that "[a] key used to encrypt data is not the same as a key used to generate a digital signature," as claimed. *Id*.

Significant to our determination is the limited description of the "private key" in the Detailed Description. *See* Ex. 1001, 5:39–40, 13:31–44. As Petitioner points out, it was only during prosecution of the '773 application, which issued as the '480 patent, that "private key" appeared in the claims by replacing "authentication data" previously recited. Pet. 9; *see* Ex. 1002, 91–96.

Although, as Petitioner acknowledges, the '480 patent does mention a "private key" (Pet. 14–15), the '480 patent only mentions it in one paragraph when discussing signing a digital signature,

> In a further embodiment, the authentication software may be provided with a system for signing a digital signature according to the present invention using at least a part of a software identification number (software ID) or any other application identifying character string, hereinafter referred to as a private key. The private key is registered at a third party, for example the authentication software provider which supplied said private key. The private key may be used to uniquely sign the digital signature and append the signed digital signature to the digital signature, which is sent to the second transaction party. The

> second transaction party is not capable of generating the signed digital signature without the private key. The second transaction party only stores the signed digital signature.

Ex. 1001, 13:31–44.

Although, as Patent Owner points out, the '480 patent also discloses that "the authentication software preferably has its own unique serial number, software ID and/or private ***encryption*** key" (*see* PO Resp. 17 (citing Ex. 1001, 5:39–40 (emphasis added))), the '480 patent discloses such unique number "may be advantageously employed in the installation method and in a track and trace method." *See* Ex. 1001, 5:39–40 ("The authentication software preferably has its own unique serial number, software ID and/or private encryption key. Said unique number may be advantageously employed in the installation method and in a track and trace method"). The '480 patent then, in the only paragraph discussing "private key," discloses that "***in a further embodiment***, the authentication software "may be provided with a system for signing a digital signature . . . using . . . a private key." *Id.* at 13:31–44 (emphasis added). We disagree that, from this mention of the private "encryption" key (i.e., a unique number belonging to the authentication software for use in an installation or track and trace method), a POSITA would have recognized that a "private key" for generating a digital signature is "an integral part of the authentication software component and/or is embedded therein." PO Resp. 17.

When an explicit limitation in a claim "is not present in the written description whose benefit is sought it must be shown that a person of ordinary skill would have understood, at the time the patent application was filed, that the description requires that limitation." *Hyatt v. Boone*, 146 F.3d 1348, 1353 (Fed. Cir. 1998) (emphasis added). In other words, where the

written description fails to disclose an element explicitly, "the applicant must show that any absent text is necessarily comprehended in the description provided and would have been so understood at the time the patent application was filed." *Id.* at 1354–55.

We also do not agree with Patent Owner's apparent obviousness contention that "the private key is with the authentication software" because a "second transaction party is not capable of generating the signed digital signature without the private key." PO Resp. 21. To the extent Patent Owner relies upon an obviousness-type argument to assert that the private key limitation is sufficiently described, "a description that merely render the invention obvious does not satisfy the [written description] requirement." *See Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1352 (Fed. Cir. 2010). Here, we agree with Petitioner that "using a private key does not mean that the private key is part of or included in the authentication software." Pet. Reply 8. As Petitioner points out, during his deposition supporting Patent Owner's contention, Dr. Preneel acknowledged that there is no disclosure in the '480 patent that the private key is part of the authentication software wherein the private key ***may also not be part*** of the authentication software. Pet. Reply 5–6 (citing Ex. 1034, 42:20–43:17) (emphasis added). In particular, Dr. Preneel's testified as to the obviousness of the private key limitation as follows:

> Q. So here, when you say "private key can be an integral part of the authentication software," are you saying it's technically possible that the private key is an integral part of an authentication software?
> A. Yes, it is.
> Q. And paragraph 55, you have no citation to that statement you made; is that correct?
> A. That is correct.

> Q. So is it correct that the private key ***can also not be an integral part*** of the authentication software?
> A. ***That is correct***.
> Q. So when you make the statement "the private key can be an integral part of the authentication software," is that - - kind of when you're interpreting the '480 patent in view of the obviousness standard, ***you're saying, "Yeah, it would be obvious that the private key can be an integral part*** of the authentication software"; is that correct?
> A. ***That is correct***, yes.

Ex. 1034, 43:24–44:17 (emphasis added).

We agree with Petitioner that Patent Owner's obviousness contention of the private key being part of or included in the authentication software, as supported by Dr. Preneel, does not satisfy the written description requirement. *See Ariad Pharm.*, 598 F.3d at 1351. Although Patent Owner cites to *Intuitive Surgical* in contending that the Board noted "not all features [must] come from an individual embodiment" to convey with reasonable clarity to a POSITA that the inventors possessed the invention claimed (PO Sur-reply 2 (citing *Intuitive Surgical, Inc. v Ethicon LLC*, IPR2019-01110, Paper 30 at 11–15 (Nov. 20, 2020)), all the limitations must still appear in the specification more than that which "would lead one to speculate as to modifications that the inventor might have envisioned, but failed to disclose." *See Lockwood*, 107 F.3d at 1572. That is, "it is the specification itself that must demonstrate possession" and "a description that merely renders the invention obvious does not satisfy the [written description] requirement." *Ariad Pharm.*, 598 F.3d at 1351. Here, from the limited description of "private key" in the specification of the '480 patent, we are unpersuaded that a POSITA would have recognized that a "private key" for

generating a digital signature is "an integral part of the authentication software component and/or is embedded therein." PO Resp. 17.

For similar reasons, we also agree with Petitioner that there is no written description support for the "private key" being "inaccessible to a user of said electronic device." Pet. 19 (citing Ex. 1003 ¶¶ 175–176). We agree that "there is no disclosure that the private key is stored in a secure part of the BIOS." Pet. Reply 9.

We do not agree with Patent Owner's contention that "a POSITA would recognize that the private key is with the authentication software," wherein "when the authentication software is provide[d] by the third party during the installation of authentication software in a BIOS, . . . the system of the present invention still does not exit[sic]," and thus, "a user cannot access the nonexistent system, . . . cannot access the authentication software (with the private key)." PO Resp. 20–21 (citing Ex. 2012 55–60). As discussed, there is no disclosure in the '480 Patent that satisfies the written description requirement for Patent Owner's contention the private key being stored or embedded in the authentication software. *See* also Pet. Reply 7–8 (Ex. 1032 ¶ 13).

Thus, having considered the evidence and arguments of record, we determine that a person having ordinary skill in the art would not have understood that the patentee was in possession of an invention where a "private key" provided "in a memory of an electronic device, wherein said memory being a secure part of a Basic In Out System or any other secure location in said electronic device," wherein the "private key is inaccessible to a user of said electronic device," as required by claim 1.

ii. private key being "encrypted when the private key is stored in said memory" and "decrypted in a secure processing environment inaccessible to said user and to any user-operated software" (claim 1)

Petitioner contends that the '480 patent also does not teach "the private key is encrypted when the private key is stored in said memory" because it does not disclose "that the private key is stored in the secure memory." Pet. 20. Furthermore, according to Petitioner, the '480 patent explains that "encryption key 46 in BIOS 44 may be used to encrypt data, but the encrypted data is not a private key," wherein the '480 patent does not disclose "***a temporal element*** that the private key is encrypted ***when*** it is stored in the memory" as claimed. *Id.* (citing Ex. 1001, 8:29–30; Ex. 1003 ¶ 178). Although Petitioner acknowledges that "[t]he '480 Patent discloses a 'private encryption key,'" Petitioner contends that "a private encryption key is not the same as an encrypted private key." *Id.* (citing Ex. 1001, 5:39–40; Ex. 1003 ¶ 179) (emphasis omitted). Petitioner then contends that, since it does not disclose an "encrypted private key," the '480 patent "as a whole" also does not provide any disclosure related to "decryption" of the encrypted private key. *Id.* at 21 (citing Ex. 1003 ¶ 180).

Patent Owner repeats its contention that "the authentication software has the private key," and thus contends that "if the authentication software is encrypted when the authentication software is stored in the memory, the private key must also be encrypted when the authentication software (with the private key) is stored in the memory." PO Resp. 22 (citing Ex. 1001, 5:39–40). According to Patent Owner, the '480 patent discloses that the authentication software is encrypted in order to be protected when transmitted from a trusted third party (TTP) to the requesting party. *Id.* at 23

(citing Ex. 1001, 7:33–42). Patent Owner contends that, "[s]ince the authentication software has the private key, the private key is encrypted accordingly." *Id.* (citing Ex. 2012 ¶¶ 58–66). Patent Owner then contends that a "decrypt key" is then used "to decrypt the authentication software and to decrypt the bit string and generate the corresponding table," wherein "[s]ince the authentication software has the private key, the private key is decrypted accordingly." *Id.* at 24–25 (citing Ex. 1001, 7:55–60).

We do not agree with Patent Owner's contention that, because "the authentication software has the private key," the private key is encrypted and decrypted with the authentication software accordingly. PO Resp. 22–25. As discussed, there is no disclosure in the '480 Patent that satisfies the written description requirement for Patent Owner's contention the private key being stored or embedded in the authentication software.

Furthermore, regardless of whether or not the private key is stored or embedded in the authentication software, Patent Owner does not address Petitioner's contention that the '480 patent does not disclose "***a temporal element*** that the private key is encrypted ***when*** it is stored in the memory." Pet. 20; *see* PO Resp. 23. Instead, Patent Owner merely contends that "the authentication software is encrypted in order to be protected ***when transmitted*** from the TTP to the requesting device," and ***then*** "the [already] ***encrypted*** authentication software with its private key ***is stored*** in a secure part of the BIOS." PO Resp. 23 (emphasis added). Based on the complete record before us, we agree with Petitioner that there is no written description support for the "private key" being "encrypted when the private key is stored in said memory."

We further agree with Petitioner that, since the '480 patent does not disclose an encrypted private key, the '480 patent as a whole also does not

provide any disclosure related to "decryption" of the encrypted private key. Pet. 21 (citing Ex. 1003 ¶ 180).

Having considered the evidence and arguments of record, we determine that a person having ordinary skill in the art would not have understood that the patentee was in possession of an invention where a "private key" is "encrypted when the private key is environment inaccessible to said user and to any user-operated software" and "decrypted in a secure processing environment inaccessible to said user and to any user-operated software," as required by claim 1.

iii. Claims 2–19.

Independent claim 16, similar to claim 1, recites "a memory storing a private key, said memory being a secure part of a Basic In Out System or any other secure location in said election device," wherein the private key "is inaccessible to a user of the electronic device," "is encrypted when the private key is stored in said memory," and "a decryption key for decrypting the private key" that is "inaccessible to said user." Ex. 1001, 19:13–45. Independent claim 17 similarly recites "providing a private key in a memory of said electronic device," wherein the private key "is encrypted, when the private key is stored in said memory," and "a decryption key for decrypting the private key" that is "inaccessible to said user." Ex. 1001, 19:46–20:19. Independent claim 18 similarly recites "a memory storing a private key," wherein the private key "is encrypted, when the private key is stored in said memory," and "a decryption key for decrypting the private key" that is "inaccessible to said user." Ex. 1001, 20:20–43. Petitioner contends that these limitations in independent claims 16–18 lack written description support for the same reasons set forth above with respect to illustrative claim 1. *See* Pet. 10–11, 14–24.

Having considered the evidence and arguments of record, we determine that a person having ordinary skill in the art similarly would not have understood that the patentee was in possession of an invention with the "private key" as set forth in claims 16–18. That is, we determine that the "private key" as set forth in independent claims 16–18 lack written description support for the same reasons set forth above with respect to the similarly recited "private key" in illustrative claim 1. We also determine that claims 2–15, depending from claim 1, and claim 19, depending from claim 18, all incorporating by reference the "private key" of the independent claims, lack written description support for the same reasons.

C. Claims 1–19 as Allegedly Obvious Under 35 U.S.C. § 103

Petitioner contends that: 1) claims 1, 3, 6, 11, and 14–19 of the '480 patent would have obvious over Ellison and Muir (Pet. 51–89); 2) claims 7, 9, and 13 would have been obvious over Ellison, Muir, and Al-Salqan (*id.* at 89–97); and 3) claims 8, 10, and 12 would have been obvious over Ellison, Muir and Searle (*id.* at 97–104). Petitioner maintains its arguments pertaining these grounds and references in its Reply. Pet. Reply 16–26.

Patent Owner counters that the asserted combinations fail to disclose key elements of claim 1. PO Resp. 34–70; *see* PO Sur-reply 5–8.

1. 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

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 Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) ("The Board is required to construe 'only those terms that . . . are in controversy, and only to the extent necessary to resolve the controversy.'") (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

Petitioner submits that "[n]o formal claim constructions are necessary because 'claim terms need only be construed to the extent necessary to resolve the controversy.'" Pet. 5 (citing *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011)). Patent Owner does not propose a claim construction but takes issue with the Institution Decision's analysis of the term "stored" in "authentication software is stored in said secure memory." PO Resp. 70–74. Specifically, Patent Owner contends that, during the relevant period between the filing dates of Ellison, Muir and the application of the '480 patent, when data/ a data file is "stored," it is stored in "permanent memory" and "remains there until it is deleted." *Id.* at 72.

In light of the parties' arguments and evidence, we construe "wherein authentication software is ***stored*** in said secure memory inaccessible to said operating system" to the extent necessary to resolve the disputed issues before us. *See* claim 1 (emphasis added).

> "*wherein authentication software is stored in said secure memory inaccessible to said operating system" (claims 1, 16); "providing authentication software in said electronic device" (claim 17); "a memory storing authentication software" (claim 18).*

Claim 1 recites "providing authentication software in said electronic device . . . , wherein authentication software is *stored in said secure memory* inaccessible to said operating system." Ex. 1001, 18:19−23 (emphasis added). Claims 16, 17 and 18 similarly recite this limitation.

We do not agree with Patent Owner's argument that during the relevant period, when data is "stored," it is stored in "permanent memory" "until it is deleted." PO Resp. 74. As Petitioner points out, the phrase "permanent memory" is not required by the claims, wherein Patent Owner's argument is untethered to the claim language and appears to inappropriately incorporate limitations from the specification. Pet. Reply 15. That is, although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. *See In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993).

Similarly, we also do not agree with Patent Owner's contention that "stored" data remains in the permanent memory "until it is deleted." We agree with Petitioner that whether the data remains at the original memory location is not relevant to whether that data can then be "stored in said secure memory inaccessible to said operating system." Pet. Reply 15. As Petitioner points out, in his deposition, Dr. Preneel acknowledged that reading and writing operations "involve[] some sort of buffering" and that buffering involves "stor[ing] the data on a buffer at least temporarily." Pet. Reply 3 (citing Ex. 1033, 82:20–84:24). That is, Dr. Preneel acknowledged that "stored" does not necessarily need to be in "permanent memory."

Ex. 1033, 81:25–82:11 (Q. When the authentication software is stored in the allocated memory space, . . . is the authentication software stored in a permanent memory space necessarily? . . . WITNESS: From external memory, which is nonvolatile memory, and gets stored into RAM, which is obviously temporary memory.")

Accordingly, we maintain that the term "stored in said secure memory inaccessible to said operating system" encompasses being held in any secure location that is inaccessible to the operating system for an undefined amount of time.

2. Principles of Law

A patent claim is unpatentable under 35 U.S.C. § 103 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.[6] *See Graham*, 383 U.S. at 17–18.

3. Overview of Cited Prior Art

a. Ellison

Ellison, titled "Protecting Software Environment in Isolated Execution," issued on July 25, 2006, with a filing date of September 22,

[6] Neither party presents arguments regarding objective evidence of nonobviousness in the instant proceeding.

2000. Ex. 1006, codes (54), (45), (22). Ellison discloses a method and apparatus to protect a subset of a software environment, wherein a key generator generates an operating system nub key (OSNK) that is unique to an operating system (OS) nub that is part of an OS in a secure platform, and a usage protector uses the OSNK to protect usage of a subset of the software environment. *Id.* at code (57). One principle for providing security in a computer system or platform is the concept of an isolated execution architecture which includes logical and physical definitions of hardware and software components that interact directly or indirectly with an OS. *Id.* at 2:41–46. An illustration of Ellison's execution architecture is depicted in Figure 1A, reproduced below.

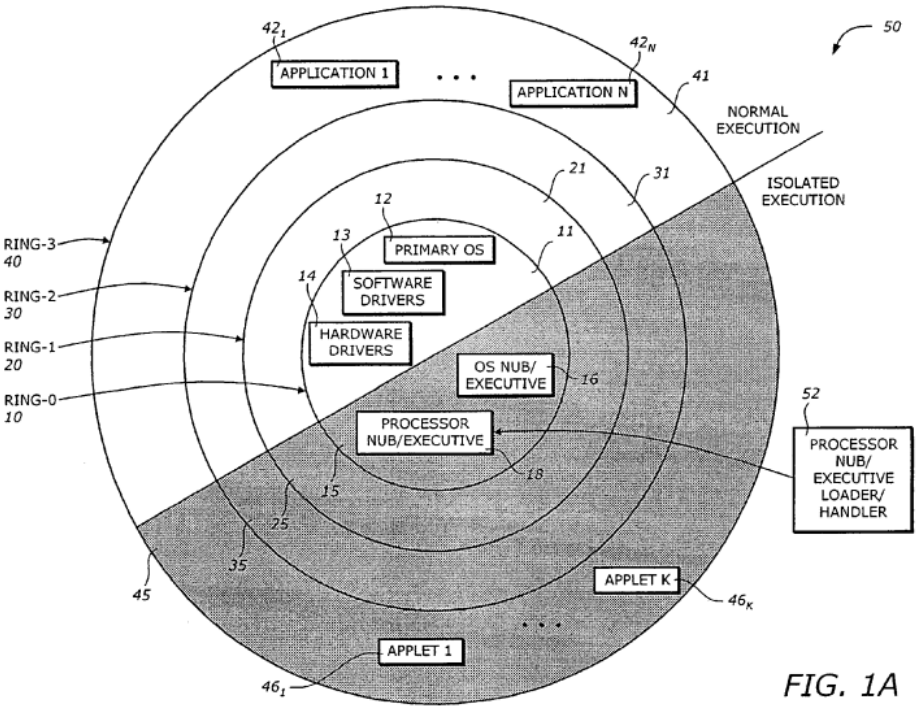


Figure 1A is a diagram illustrating logical operating architecture 50 that includes ring-0 10, ring-1 20, ring-2 30, ring-3 40, and processor nub

loader 52. *Id.* at 2:62–3:6. As shown in Figure 1A, logical operating architecture 50 has two modes of operation: normal execution mode (white) and isolated execution mode (gray). *Id.* at 3:4–6. Each ring in logical operating architecture 50 can operate in both modes, but processor nub loader 52 operates only in the isolated execution mode. *Id.* at 3:6–8. In Figure 1A, isolated execution Ring-0 15 includes OS nub 16 and processor nub 18. *Id.* at 3:15–16. One concept of the isolated execution architecture is the creation of an isolated area protected by both the processor and chipset in the computer system. *Id.* at 3:32–40.

In operation, processor nub loader 52 is invoked by execution of an appropriate isolated instruction and is transferred to isolated area 70, wherein from isolated area 70, processor nub loader 52 copies processor nub 18 in non-volatile memory 160 into isolated area 70, verifies and logs its integrity, and manages a symmetric key used to protect the processor nub's secrets. *Id.* at 6:47–56.

Ellison's secure platform is depicted in Figure 2, reproduced below.

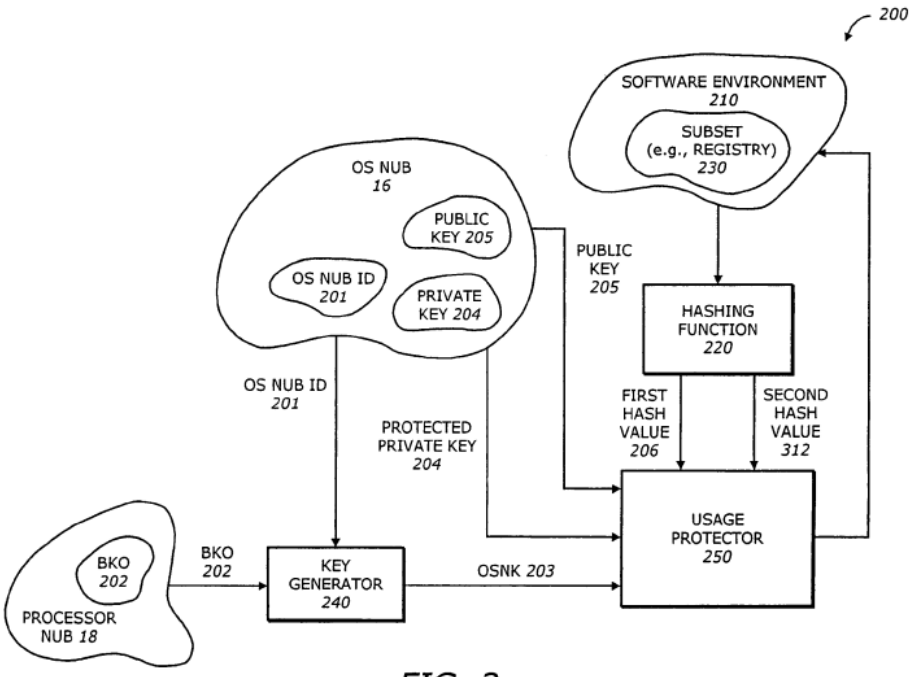


FIG. 2

Figure 2 is a diagram illustrating secure platform 200, which includes OS nub 16, processor nub 18, key generator 240, hashing function 220, and usage protector 250, all operating within the isolated execution environment. *Id.* at 8:25–30.

b. Muir

Muir, titled "Apparatus and Methods for Using a Virtual Smart Card," published on December 6, 2001, with a filing date of May 30, 2001. Ex. 1008, codes (54), (43), (22). Muir discloses an apparatus that includes a smart card interface and a virtual smart card configured to emulate a physical smart card as if a smart card is connected with the smart card interface. *Id.* at code (57).

4. Analysis

Petitioner contends that, in the combination of Ellison and Muir, "each device involved in a transaction would have been connected through a computer network," wherein the individual devices "would have included

Ellison's isolated execution architecture and one or more parts of Muir's system" such as "restricted memory space for storing private key and performing cryptographic operations such as encryption." Pet. 48.

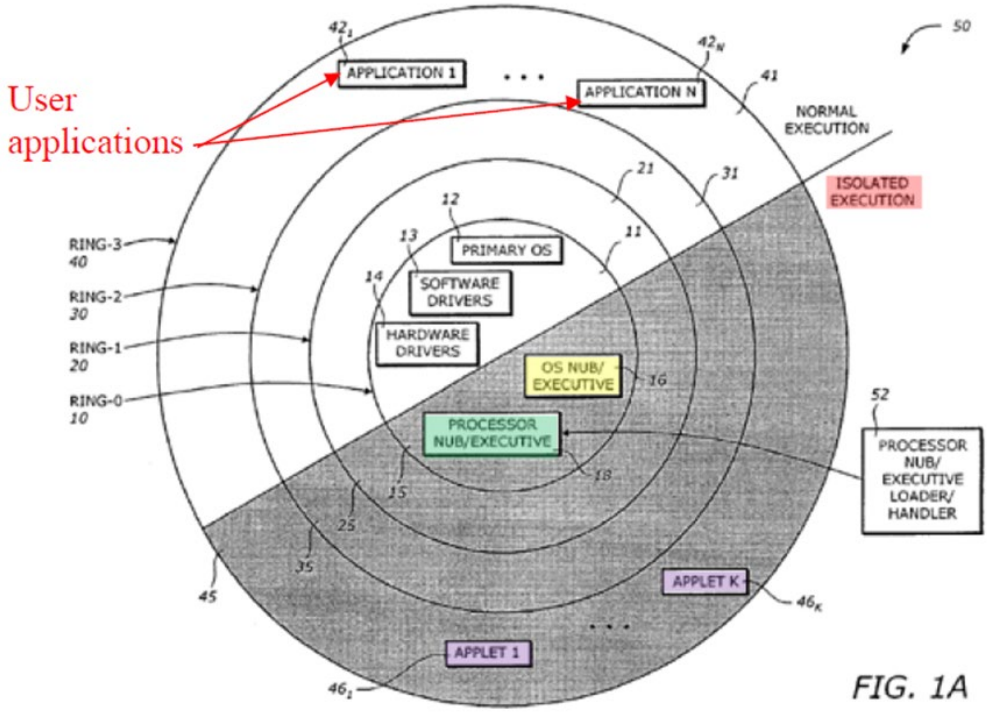
Having reviewed all the arguments and evidence in the complete record, we determine Petitioner has demonstrated by a preponderance of the evidence that claims 1, 16–18, and claims 3, 6, 11, 14, 15, and 19 depending therefrom, would have been obvious over Ellison in view of Muir, notwithstanding Patent Owner's arguments to the contrary. We similarly determine that dependent claims 7, 9, and 13 would have been obvious over Ellison and Muir in further view of Al-Salqan; and that dependent claims 8, 10, and 12 would have been obvious over Ellison and Muir in further view of Searle.

We first address in detail Petitioner's arguments and Patent Owner's responses with respect to the limitations of claim 1.

> *i. Preamble, a "method for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party, the electronic device having an operating system creating a run-time environment for user applications" (claim 1)*

Petitioner contends that, to the extent the preamble is limiting, the combination of Ellison and Muir teaches "cryptographic systems and methods can be used to protect sensitive data used in an e-commerce transaction ('***method for performing an electronic transaction'***)," wherein "the transaction can be conducted ***between the electronic devices of two transaction parties*** (e.g., first and second transaction parties)." Pet. 51 (citing Ex. 1008, 1, 9, 11–12, Fig. 5; Ex. 1006, 4:56, 3:9–8:13–13:3,

Figs. 1A–1C, 2, 3C–3D; Ex. 1003 ¶ 88). Furthermore, Petitioner contends that "Ellison's 'isolated execution architecture' would have been implemented in Muir's electronic devices including the electronic device of the first transaction party." *Id.* at 52. Petitioner provides annotated Figures 1A–1B of Ellison as modified by Muir, shown below, to illustrate its contentions.



SAMSUNG-1006, FIG. 1A

Figure 1A of Ellison, shown above, is a diagram illustrating a logical operating architecture as disclosed in Ellison. Ex. 1006, 1:59–60. Annotated Figure 1A of Ellison in the Petition, according to Petitioner, illustrates an "isolated execution architecture" that has been "implemented in Muir's electronic device of the first transaction party." Pet. 52. As shown in annotated Figure 1A, logical operating architecture 50 includes processor nub loader 52. *See* Ex. 1006, 2:62–3:6. As shown in annotated Figure 1A,

logical operating architecture 50 has two modes of operation: normal execution mode (white) and isolated execution mode (gray), wherein OS nub 16 (yellow) and processor nub 18 (green) are shown interacting with applets 46_1–46_K (purple) in the isolated execution mode.

We reproduce annotated Figure 1B of Ellison below:

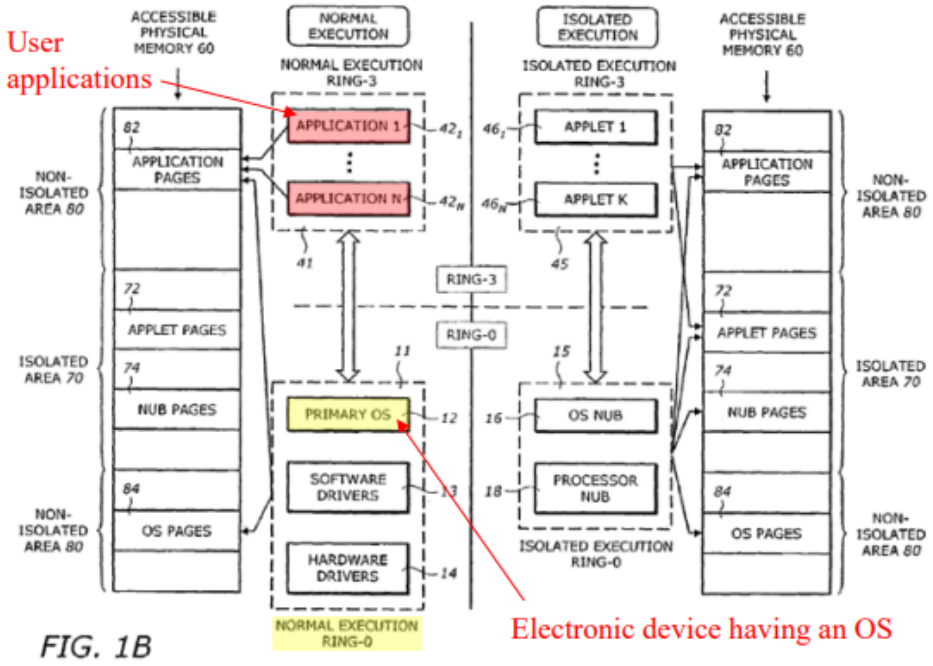


FIG. 1B

SAMSUNG-1006, FIG. 1B

Figure 1B of Ellison, shown above, is a diagram illustrating accessibility of various elements in the Ellison's operating system and processor. Ex. 1006, 1:61–63. Annotated Figure 1B of Ellison in the Petition shows normal execution mode and isolated execution mode side-by-side, wherein primary OS 12 (yellow) is shown interacting with applications 42_1–42_N (red) in the normal execution mode. Pet. 29. According to Petitioner, along with annotated Figure 1A, annotated Figure 1B of Ellison in the Petition depicts "***a primary operating system (OS) 12 that creates a run-time environment for user applications, such as applications 42_1-42_N*** which can be executed

in the normal execution mode and are isolated from components of the isolated execution rings." Pet. 55 (citing Ex. 1006, 3:9–61, 4:1–29, 2:57–61).

Patent Owner contends that "[i]t is clear that Petitioner wrongly equates the 'primary operating system 12' of Ellison with 'operating system' in the '480 Patent" and thus "misapprehends that the 'isolated environment region' is not accessible to the operating system.'" PO Resp. 55. In particular, Patent Owner contends that a POSITA would understand that the counterpart of "user applications" of the '480 patent includes "applications 42_1-42_N and applets 46_1 to 46_K," and that the counterpart of "operating system" of the '480 patent in Ellison is "the operating system including normal execution mode and isolated execution mode, not only the primary operating system (OS) 12 operating in the normal execution mode." *Id.* at 46. Therefore, Patent Owner contends that Ellison's "operating system should include the processor nub 18 and the operating system nub 16 which operate in the isolated execution mode." *Id.*; *see also* PO Sur-reply 5–6 (citing Ex. 1006, 2:62–65, Figs. 1A–C, 2).

We find Patent Owner's contentions unavailing. In particular, we find unavailing Patent Owner's contention that "Petitioner incorrectly (solely) maps Ellison's OS 12 to the operating system" of the challenged claims. PO Sur-reply 5–6. As Petitioner points out, "OS 12 satisfies [Patent Owner's] description of an operating system." Pet. Reply 18. We agree with Petitioner that, although Patent Owner's contention appear to hinge on the argument that to be properly mapped to the claimed operating system, primary OS 12 operating in normal execution mode must also include processor nub 18 and operating system nub 16 executing the isolated execution mode, "neither the intrinsic record nor the prosecution history

impose such a requirement on the claimed OS." *Id.* That is, claim 1 merely requires an "operating system" for "creating a run-time environment for user applications."

As Petitioner points out, Ellison's OS 12 provides a run-time environment for user applications, wherein Ellison's Figure 1B "clearly depicts primary OS 12 in the normal execution region" and "Ellison explains that OS 12 interacts with OS pages 84, application pages 82, and applets 42_1–42_K, which are user applications in the non-isolated region." Pet. Reply 18 (citing Ex. 1006, 2:57–4:29, Figs. 1A–1B).

We reproduce Figure 1B of Ellison below:

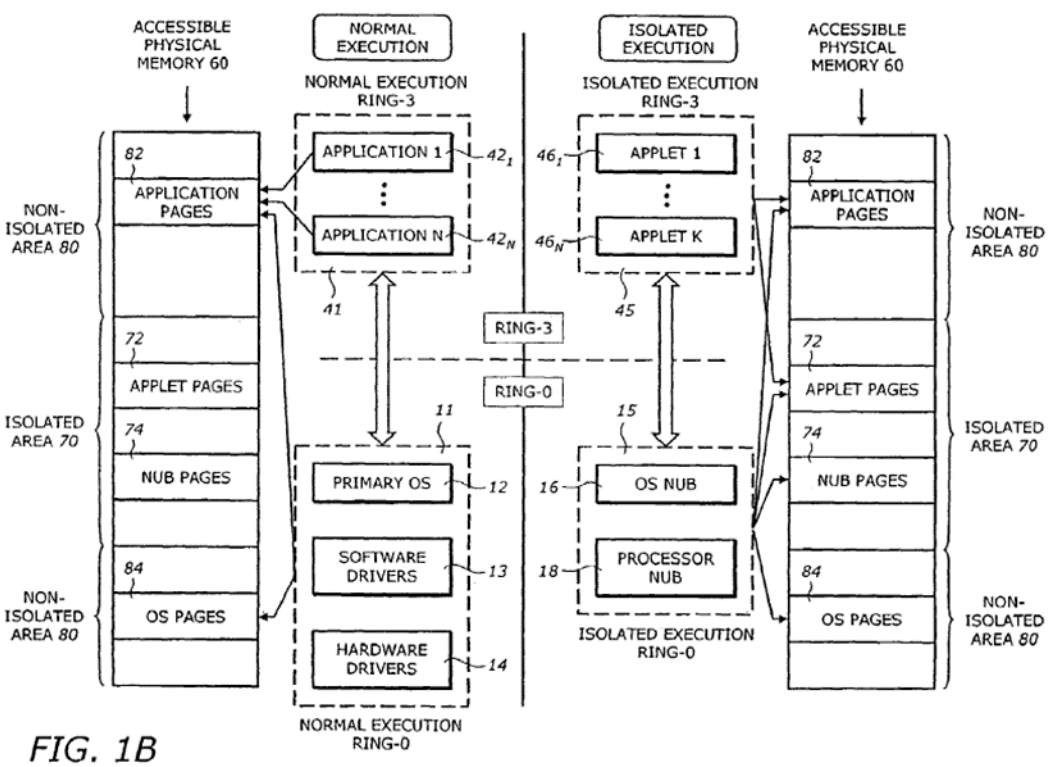


FIG. 1B

Figure 1B of Ellison shows primary OS 12, software drivers 13, and hardware drivers 14 (bottom left hashed box) interacting (left bidirectional

arrow) with applications 42_1–42_N (top left hashed box) in the normal execution mode; and OS nub 16 processor nub 18 (bottom right hashed box) interacting (right bidirectional arrow) with applets 46_1–46_N (top right hashed box) in the isolated execution mode. As Petitioner pointed out during oral argument, as shown in Figure 1B, only OS nub 16 and processor nub 18 are interacting with the isolated execution region, and that normal execution modules such as primary OS 12 do not have any access to the isolated execution region. Tr. 59:1–8; *see also* Pet. 55; Pet. Reply 18–19. We agree with Petitioner that, as shown in Figure 1B of Ellison, "OS nub 16 is distinct and separate entity from OS 12," wherein it "operates within the isolated execution area," while "primary OS does not." *See* Tr. 23:23–25; Pet. Reply 18–19.

Accordingly, we find unavailing Patent Owner's contention that Ellison's "operating system should include the processor nub 18 and the operating system nub 16 which operate in the isolated execution mode." PO Resp. 59; PO Sur-reply 5–6. As Petitioner explains, Ellison's processor nub 18 and operating nub 16 interact with applets 46_1–46_N running in the isolated execution area (e.g., isolated execution ring-3) that is "a separate operating environment, independent from and inaccessible to, the OS 12." Pet. Reply 18–19 (citing Ex. 1006, 2:57–4:29, Figs. 1A–B; Ex. 1032 ¶ 36).

Based on the complete record presented, we determine Petitioner has demonstrated that the combination of Ellison and Muir teaches a "method for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party, the electronic device having an operating system creating a run-time environment for user applications" as recited in claim 1, regardless

of whether or not the preamble is limiting.[7] Furthermore, as discussed in detail below in section (II)(4)(C)(vi), we also agree with Petitioner that a POSITA would have been motivated to combine Ellison and Muir to arrive at the method of claim 1 with a reasonable expectation of success. Pet. 46–51. As Petitioner explains, and as supported by Dr. Black's testimony, "the combination would have simply involved combining prior art elements (Muir's computer system with restricted memory space and secure cryptographic operations) according to known methods (Ellison's isolated execution architecture) to yield the predictable result of performing electronic transactions securely between two parties." *Id.* at 51 (citing Ex. 1003 ¶ 72).

ii. "providing a private key in a memory of said electronic device, said memory being a secure part of a Basic In Out System or any other secure location in said electronic device, which private key is inaccessible to a user of said electronic device, wherein the private key is encrypted when the private key is stored in said memory" (claim 1)

Petitioner contends that Ellison's "isolated execution regions '***is accessible only to elements of the operating system and processor operating in isolated execution mode***,'" and that "isolated mode applets 46[1]

[7] The issue of whether the preamble is limiting need not be resolved because, regardless of whether the preamble is limiting, Petitioner shows sufficiently, and Patent Owner does not dispute, that the combination of Ellison and Muir teaches a method for performing an electronic transaction between first and second transaction parties using an electronic device having an operating system creating a run-time environment for user applications, as recited in the preamble. *See Realtime Data*, 912 F.3d at 1375 (noting that we need only construe "only those terms that . . . are in controversy").

to 46_K and their data are tamper-resistant and monitor-resistant from all software attacks from other applets and OS 12." Pet. 56 (citing Ex. 1006, 4:1–22). According to Petitioner, "[a] user is not an element of the operating system and processor operating in isolated execution mode, and therefore ***cannot access elements within the isolated execution region***." *Id.* (citing Ex. 1003 ¶ 92).

Petitioner then contends that Ellison discloses "a ***secure platform*** 200 that 'includes the OS nub 16, the processor nub 18, a key generator 240, . . . , ***all operating within the isolated execution environment***.'" Pet. 58 (citing Ex. 1006, 8:25–32; Ex. 1003 ¶ 95). Petitioner also contends that "the private key 204 can be stored in the cryptographic key storage 155 and in a multiple key storage of the non-volatile flash memory 160," and "only the OS nub 16 can retrieve the private key." *Id.* at 59–60. According to Petitioner, because "the OS nub 16 is within the secure platform and isolated environment," it would have been obvious to a person of ordinary skill in the art (POSITA) that "the cryptographic key storage 155 and the non-volatile flash memory 160 are secure storage locations so that the private key 204 can be accessed securely by OS nub 16." *Id.* (citing Ex. 1003 ¶ 96). Thus, Petitioner contends that "Ellison explicitly teaches that the OS nub 16 and private key 204 shown in platform 200 ***all operate within the isolated execution environment***," which "would indicate to a POSITA that private key 204 is stored in a secure memory and is inaccessible to a user of said electronic device." *Id.* Nevertheless, Petitioner argues that Muir "explicitly teaches ***a private key 167 stored in a restricted memory space 170 which is inaccessible to the operating system***." *Id.* at 60 (citing Ex. 1008, 7–9, 3).

Petitioner then contends that Ellison's OS nub 16 "retrieves the encrypted private key 204 and decrypts it for use in the isolated

environment." Pet. 61 (citing Ex. 1006, 8:33–65, 11:1–12:26). Thus, Petitioner concludes "Ellison and Muir render obvious ***the private key 204 being encrypted when stored in a secure memory (e.g., memory 160 or Muir's restricted memory space 170)*** and obtained therefrom by OS nub 16." *Id.* at 63 (citing Ex. 1003 ¶ 99).

Patent Owner contends that the combination of Ellison and Muir "will not teach or suggest" the limitation "providing a private key," as claimed. *See* PO Resp. 47. In particular, Patent Owner contends that Ellison's "private key 204" is "for the protection of the isolated environment itself," but "not for the protection of digital transactions involving two parties." *Id.*

We find unavailing Patent Owner's contention which is directed to Ellison alone, and not to the combination of Ellison and Muir proposed by Petitioner. *See* PO Resp. 47. We agree with Petitioner's contention that Ellison's private key 204 "can be used 'to encrypt a digest of a message producing a signature" (*see* Ex. 1006, 60–65 ("In the digital signature generation process, the protected private key 204 is used as an encryption key to encrypt a digest of a message producing a signature")), wherein "Muir clearly discloses using a digital signature for transactions between two parties." Pet. Reply 25 (citing Ex. 1006, 8:59–65; Ex. 1008, 2, 3, 6, 9, 10, 12, 18; Ex. 1032 ¶ 29). Thus, contrary to Patent Owner's contention, we agree with Petitioner's position regarding the combination of Ellison and Muir for teaching that "private key 204" is "for the protection of digital transactions involving two parties." PO Resp. 47.

Based on the complete record presented, we determine Petitioner has demonstrated sufficiently that a POSITA would have been motivated to combine Ellison and Muir, wherein the combination of Ellison and Muir teaches "providing a private key in a memory of said electronic device," the

memory being "a secure part of a . . . secure location in said electronic device," the private key being "inaccessible to a user of said electronic device," and "encrypted when the private key is stored in said memory," as recited in claim 1.

> *iii. "a decryption key for decrypting the private key being incorporated in the electronic device, said decryption key being inaccessible to said user, to any user-operated software and to said operating system, . . . , wherein the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software" (claim 1)*

Petitioner contends that Ellison discloses decryptor 325 decrypting encrypted private key 204 using operating system nub key (OSNK) 203, thereby yielding unencrypted private key 325. Pet. 61–62 (citing Ex. 1006, 8:35–65 11:1–12:26, Figs. 3C–3D; Ex. 1003 ¶ 98). Petitioner contends that Ellison's "***OSNK 203 is used as a decryption key for decrypting the private key 204***," wherein it is "generated by the key generator 240, which is part of the isolated execution environment in the electronic device of the first transaction party." *Id.* at 63 (citing Ex. 1006, 8:25–65, 9:1–14, 11:11–30, Figs. 2, 3C). According to Petitioner, "OSNK 203 ('***decryption key***') is generated and used within the ***isolated environment region, which is not accessible to a user, any user-operated software, and the operating system (OS) 12*** of the electronic device in the normal execution mode." *Id.* at 64 (citing Ex. 1006, 8:25–65, 11:1–12:26, 9:1–14, Figs. 2, 3C, 3D). That is, according to Petitioner, "Ellison explicitly discloses that OSNK 203 'is provided only to the OS Nub 16,' which may further 'supply the OSNK 203

to trusted agents, such as the usage protector 250.'" *Id.* at 30 (citing Ex. 1006, 9:1–14).

Patent Owner responds that Ellison's OSNK 203 "is used to decrypt the register values or to sign the software to be run in the secure processing environment—not to sign a transaction between a first and second transaction party." PO Resp. 40 (citing Ex. 2012 ¶ 77). In particular, Patent Owner contends that "Ellison discloses that OSNK 203 is input to the usage protector 250," and "can be used to decrypt the register values or to decrypt a private key 204 that is used to digitally sign[] the software to be run in the secure processing environment," wherein "the usage protector is not used to sign a transaction between a first and second transaction party." *Id.* at 44 (citing Ex. 2012 ¶ 97).

Patent Owner then contends that "Petitioner admits that Ellison disclose the decryption key and the memory key . . . are accessible to isolated execution mode of the operating system, such as can be 'accessed securely by OS nub 16.'" PO Resp. 61. Patent Owner repeats its contention that "the counterpart of 'operating system' of the '480 Patent in Ellison is the operating system including normal execution mode and isolated execution mode," and "not only the primary operating system (OS) 12 operating in the normal execution mode." *Id.* Thus, according to Patent Owner, since the decryption key and the memory are accessible to isolated execution mode of the "operating system" in Ellison, "the decryption key and the memory are accessible to the operating system even though they are inaccessible to normal execution mode of the operating system." *Id.*

We find Patent Owner's arguments, similar to its above arguments in sections II(C)(4)(i)–(ii), unavailing. In particular, as to Patent Owner's argument that Ellison's private key 204 is used to sign the software to be run

in the secure processing environment and not used to sign a transaction between two parties, as discussed above in section II(C)(4)(ii), Patent Owner's contention is directed to Ellison alone, and not to the combination of Ellison and Muir proposed by Petitioner. PO Resp. 44. Contrary to Patent Owner's contention, as discussed in section II(C)(4)(ii), we are persuaded by Petitioner's reliance on the combination of Ellison and Muir for teaching that OSNK 23 is used to decrypt the register values or to decrypt private key 204 that is used to digitally sign a transaction between two transaction parties. *See, e.g.*, Ex. 1006, 8:59–65; Ex. 1008, 9.

As to Patent Owner's contention that Ellison's decryption key and memory are accessible to the operating system even though they are inaccessible to normal execution mode of the operating system (PO Resp. 59–60), Patent Owner's contention appear to hinge on the argument that to be properly mapped to the claimed operating system, primary OS 12 operating in normal execution mode must also include processor nub 18 and operating system nub 16 executing the isolated execution mode. *See* Pet. Reply 18. As discussed above in section II(C)(4)(i), we find unavailing Patent Owner's contention that "the counterpart of 'operating system' of the '480 Patent in Ellison is the operating system including normal execution mode and isolated execution mode." *Id.*

As Petitioner explains, Ellison's processor nub 18 and operating nub 16 interact with applets 46_1–46_N running in the isolated execution area (e.g., isolated execution ring-3) that is "a separate operating environment, independent from and inaccessible to, the OS 12." Pet. Reply 18–19 (citing Ex. 1006, 2:57–4:29, Figs. 1A–B; Ex. 1032 ¶ 36). Thus, we agree with Petitioner's contention that Ellison's OS nub 16 and processor nub 18

"operate within an isolated execution environment," wherein "OSNK 203 is generated and used in the same isolated environment of secure platform 200." *Id.* at 19 (citing Ex. 1006, 8:12–32).

Based on the complete record presented, we determine Petitioner has demonstrated sufficiently that a POSITA would have been motivated to combine Ellison and Muir, wherein the combination of Ellison in view of Muir teaches "a decryption key for decrypting the private key being incorporated in the electronic device, said decryption key being inaccessible to said user, to any user-operated software and to said operating system," and the "private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software," as recited in claim 1.

iv. "providing authentication software in said electronic device, the private key being accessible to said authentication software, wherein authentication software is stored in said secure memory inaccessible to said operating system" (claim 1)

Petitioner contends "Ellison's isolation execution architecture ***provides authentication software in the electronic device in the form of the usage protector 250***, which is part of the secure platform 200 in the electronic device." Pet. 67. Petitioner contends that Ellison's "private key 204 is accessible to the usage protector 250 ('***authentication software***')." *Id.* at 69 (citing Ex. 1006, 10:1–3, 10:63–12:26, 8:40–65; Ex. 1003 ¶ 106). According to Petitioner, "the ***usage protector 250 ('authentication software')*** is located in a ***secure*** platform 200 and ***operates within the isolated execution environment***." *Id.* at 71 (citing Ex. 1006, 8:25–32). Accordingly, Petitioner contends that it would have been obvious

to a POSITA that "the usage protector 250 would have been stored in secure memory" wherein "all or at least the authentication portion of the usage protector 250 and its operational software/code would have been stored in secure memory of the isolated execution environment." *Id.* at 71–72 (citing Ex. 1003 ¶ 109).

Patent Owner responds that neither Ellison nor Muir teaches or suggests authentication software stored in a secure area inaccessible to the operating system. PO Resp. 67. In particular, although Patent acknowledges that Petitioner relies on Ellison's usage protector 250 for the claimed "authentication software" (*id.* (citing Pet. 71)), Patent Owner argues that "[t]he execution environment of Ellison's usage protector 250 is not the same as where usage protector 250 is stored." *Id.* at 40 (citing Ex. 2012 ¶ 82). According to Patent Owner, Ellison's failure to disclose the storage location of usage protector 250 "implies the primary OS 12 would have access to usage protector 250 for running in the normal execution environment." *Id.* at 41 (citing Ex. 2012 ¶ 87).

Patent Owner then repeats its contention that "the operating system of Ellison includes two execution modes: normal execution mode and isolated execution mode." PO Resp. 67. According to Patent Owner, although usage protector 250 "operates in secure processing environment that is not accessible to the OS 12," it "can be accessed by the processor nub 18 and the operating system nub 16 which operate in the isolated execution mode." *Id.* at 67–68. That is, according to Patent Owner, OS nub 16 "is part of the operating system" running on platform 200. PO Sur-reply 8.

We find Patent Owner's arguments unavailing. In particular, as to Patent Owner's argument that the execution environment of Ellison's usage protector 250 is not the same as where usage protector 250 is stored (PO

Resp. 40), Patent Owner is relying on a claim construction of "stored" that precludes a "location" where the software is "loaded into." As discussed above in Section II(C)(1), however, such an interpretation does not comport with the aforementioned construction of being held in a secure location that is inaccessible to the operating system.

As Petitioner points out, Ellison's usage protector 250 is located in a secure location, i.e., secure platform 200 and operates within the isolated execution environment. Pet. 71; Ex. 1006, 8:25–32. Given the claim construction above, we agree with Petitioner's contention that it would have been obvious to a POSITA that Ellison's usage protector 250 is held, i.e., "stored" in "secure memory of the isolated execution environment" for execution. Pet. 71–72 (citing Ex. 1003 ¶ 109).

As to Patent Owner's contention that Ellison's usage protector 250 "can be accessed by the processor nub 18 and the operating system nub 16 which operate in the isolated execution mode" (PO Resp. 67–68), Patent Owner's contention hinges on its contention that Ellison's OS nub 16 "is part of the operating system" running on platform 200. PO Sur-reply 8. As discussed above in section II(C)(4)(i), we find such contention unavailing.

Based on the complete record presented, we determine Petitioner has demonstrated sufficiently that a POSITA would have been motivated to combine Ellison and Muir, wherein the combination of Ellison in view of Muir teaches "providing authentication software in said electronic device, . . .wherein authentication software is stored in said secure memory inaccessible to said operating system," as recited in claim 1.

v. Remaining limitations of claim 1

Petitioner provides detailed explanations as to how the combination of Ellison and Muir teaches the remaining claim limitations as recited in independent claim 1, citing Dr. Black's testimony for support. Pet. 72–74 (citing Ex. 1006, 3:6–61, 4:1–29, 4:57–5:27, 8:55–65, 10:63–11:30, Figs. 1A, 1B, 3C; Ex. 1008, 2, 3, 6, 9, 10, 12, 18; Ex. 1003 ¶¶ 110–112). In particular, Petitioner contends that Ellison's Figure 3C "depicts an illustration of the usage protector 250 in which ***the signature generator 320 generates a digital signature*** 304 for the subset 230 ***using private key 328***, which is a decrypted version of encrypted private key 204." *See id.* at 72. According to Petitioner, Ellison's usage protector 250 "is run in an isolated environment ('***secure processing environment***') that is not accessible to the OS 12 ('***said operating system***')," and "Muir teaches that the ***generated digital signature is provided to another user ('second transaction party')*** connected in the networking environment to the computer system 20 to allow the other user 'to determine the identify' of the first transaction party." *Id.* at 73.

Patent Owner does not address separately Petitioner's explanations and supporting evidence regarding the remaining limitations in claim 1. *See generally* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (discussing the burden of proof in *inter partes* review).

Based on the complete record presented, we determine that Petitioner has demonstrated that the combination of Ellison in view of Muir teaches the remaining limitations recited in claim 1.

Petitioner has shown sufficiently that Ellison and Muir teach all of the limitations of claim 1. Accordingly, Petitioner has proven, by a preponderance of the evidence, that claim 1 would have been obvious based on Ellison and Muir under 35 U.S.C. § 103(a).

vi. Proposed Combination of Ellison and Muir

Petitioner contends that Ellison discloses "an isolated execution architecture that improves security in a computer system or platform by implementing several levels of hierarchy and normal and isolation execution modes for the operating system and processor." Pet. 46–47 (citing Ex. 1006, 1:12–15, 2:40–61, Fig. 1). Although Petitioner acknowledges that Ellison "does not reveal details of [] a system or transaction between multiple parties," Petitioner relies on Muir for such teaching. *Id.* at 47. According to Petitioner, a POSITA looking to implement Ellison's isolated execution architecture in a computer with multiple devices "would have looked to Muir's teachings to implement a secure electronic transaction between two parties," because "both Ellison and Muir are related to providing improved security for transactions involving keys using cryptographic techniques." *Id.* at 48 (citing Ex. 1006, 1:38–51; Ex. 1008, 7, 8, 11; Ex. 1003 ¶ 66).

We agree with Petitioner's motivation to combine the teachings of Ellison and Muir, as supported by Dr. Black's testimony (Pet. 46–51 (citing Ex. 1003 ¶¶ 64–71), and find unavailing Patent Owner's contention that "a POSITA would not have looked to Muir to cure the deficiencies of Ellison." PO Resp. 39. Although Patent Owner contends that "Petitioner fails to show with particularity the *why* and *how* required for its obviousness combinations" (PO Resp. 68), we agree with Petitioner's contention that, in the combination of Ellison and Muir, "each device involved in a transaction would have been connected through a computer network such as Mui's

network shown in FIG. 5," and "[t]he individual devices would have included Ellison's isolated execution architecture and one or more parts of Muir's system." Pet. 48. We credit the testimony of Dr. Black as sufficient support for Petitioner's contention, when he explains, "a POSITA would have viewed extension of Ellison's system to include the multi-party transactions described by Muir to have been a natural and obvious extension," wherein a "a POSITA would have been motivated to enable such multi-party transaction [] in Ellison's system to increase the functionality and usefulness of Ellison's system." *See* Ex. 1003 ¶ 69. Thus, we find unavailing Patent Owner's contention that Petitioner "has not established its prima facie case." PO Resp. 68.

Based on the complete record presented, we determine Petitioner has demonstrated that a POSITA would have found it obvious to combine the teachings of Ellison and Muir, wherein claim 1 would have been obvious over the combination of Ellison and Muir.

vii. Claims 3, 6, 11, 14–19 Allegedly Obvious Over Ellison and Muir

Petitioner provides detailed explanations as to how the combination of Ellison and Muir renders the limitations as recited in claims 3, 6, 11, and 14–19 obvious, citing Dr. Black's testimony for support. *See* Pet. 74–89 (citing Ex. 1006, 4:23–29, 4:57–5:27, 6:1–26, 6:51–57, 7:19–32, 8:25–65, 9:9–22, 9:31–35, 9:48–10:62, 11:1–13:20, Figs. 1A–1C, 2, 3A–3E, 4; Ex. 1008, 1, 8–9, 11, 15; Ex. 1003 ¶¶ 113–114, 116–119, 128–129, 135–168). In particular, as to claim 3, Petitioner contends that "Ellison's ***usage protector 250 has its own encryption key in the form of the operating system nub key (OSNK) 203***," wherein "usage protector 250 ***uses the OSNK 203 as an encryption key to encrypt the first hash value 206***

obtained from subset 230." *Id.* at 74–75. As to claim 6, Petitioner contends that OS nub 16, processor nub 18, key generator 240, hashing 220 and "***usage protector 250, all operat[e] within the isolated execution environment***" and "form part of the secure platform 200 ('secure area')," wherein it would have been obvious to a POSITA that "the usage protector 250 ('***authentication software***') is installed in an application environment in the secure area" to "operate securely within the isolated execution environment." *Id.* at 76. As for claim 11, Petitioner repeats its contention that "private key 204 is decrypted by decryptor 325, which is part of the usage protect 250 ('***authentication software***')." *Id.* at 78.

As for claim 14, Petitioner contends that "Muir discloses that, before performing encryption and decryption operations, a user provides a user ID/password to confirm an identification of the user," wherein a POSITA would have found it obvious to combine the teachings of Ellison and Muir "so that a user identity can be verified prior to conducting a secure transaction between two transaction parties." Pet. 80. As for claim 15, Petitioner contends that Ellison's usage protector 250 has OSNK 203 that is "used for encrypting various data," and thus a POSITA "would have found it obvious that Ellison encrypts digital data." *Id.* at 81–82.

As for independent claims 16–18 reciting similar limitations as claim 1, Petitioner repeats its contentions with respect to claim 1 (Pet. 82–88), and adds that: "Muir's FIG. 5 [] discloses the network interface for an electronic transaction between a first transaction party and a second transaction party" (*id.* at 80); "Ellison teaches that processor 110 also includes an 'isolated execution circuit 115 [that] provides hardware and software support for the isolated execution mode" (*id.* at 85); and that it would have been obvious to a POSITA that "processor 110 would have also

been configured to activate the usage protector 250 ('***authentication software***') as part of its control and configuration of the isolated execution mode and/or the isolated area 70" (*id.* at 86–87). As for dependent claim 19, Petitioner adds that "Muir's electronic devices may include, for example, cellular phones, personal data assistants, and smart cards." *Id.* at 89.

Patent Owner does not provide substantive arguments addressing these explanations and supporting evidence by Petitioner regarding claims 3, 6, 11, and 14–19. *See generally* PO Resp. 69. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Here, Patent Owner contends that independent claims 16–18 "are similar to claim 1" and "contain similar elements to claim 1," wherein, "[s]imilar to argued above," Ellison in view of Muir does not teach the contested limitations. *See* PO Resp. 69. Patent Owner then contends that dependent claims 3, 6, 11, 14–15 and 19 "are not obvious over Ellison in view of Muir for at least the same reasons." *Id.*

Based on the complete record presented, we determine Petitioner has demonstrated that claim 3, 6, 11, and 14–19 would have been obvious over the combination of Ellison and Muir.

viii. Claims 7, 9 and 13 over Ellison, Muir, and Al-Salqan; claims 8, 10, and 12 over Ellison, Muir, and Searle

Petitioner provides detailed explanations as to how the combination of Ellison, Muir and Al-Salqan renders the limitations as recited in claims 7, 9, and 13 as obvious (Pet. 89–97 (citing Ex. 1006, 6:60–67, 8:33–65, 11:1–12:26, Figs. 3C–3D; Ex. 1007, 1:21–2:63, 4:4–5:35, Figs. 2–3; Ex. 1003 ¶¶ 72–79, 121, 124–125, 133–134)); and how the combination of

Ellison, Muir and Searle renders the limitations as recited in claims 8, 10, and 12 obvious (*id.* at 97–104 (citing Ex. 1006, 2:7–12, 10:63–11:40, Figs. 3C–3D; Ex. 1009, 2:13–40, 3:66–4:11, 4:48–5:28, 5:65–6:27, Figs. 1–2; Ex. 1003 ¶¶ 81–86, 122–123, 126–127, 130–132)). In particular, as to claims 7, 9, and 13, Petitioner contends that "Al-Salqan discloses a decryption that uses an asymmetric decryptor 314 and symmetric decryptor 330 to remove [] two lawyers of encryption," wherein "using two encryption layers . . . the private key generated based on Ellison and Al-Salqan would have additional layers of protection." *Id.* at 89–97.

As to claims 8, 10, and 12, Petitioner contends that "Searle discloses encrypting 'a key [(second key)] using another key [(first key)] that is unique and particular to a given client," wherein a POSITA would have been motivated to look to Searle "to apply the details of that key encryption to implement the key encryption of Ellison" to obtain "an enhanced level of security and protection from intruders." Pet. 97–104.

Patent Owner does not provide substantive arguments addressing these explanations and supporting evidence by Petitioner regarding claims 7–10, 12, and 13. *See generally* PO Resp. 70. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Here, Patent Owner contends that these grounds "fail for the reasons noted above with regard to the combination of Ellison and Muir." PO Resp. 70.

Based on the complete record presented, we determine Petitioner has demonstrated that claims 7, 9, and 13 would have been obvious over the combination of Ellison, Muir and Al-Salqan, and that claims 8, 10, and 12 would have been obvious over the combination of Ellison, Muir and Searle.

III. CONCLUSION[8]

For the reasons above, we are persuaded on the record at hand that Petitioner has demonstrated by a preponderance of the evidence that claims 1–19 of the '480 patent are unpatentable, as shown in the following table:

Claims	35 U.S.C §	Reference(s)/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–19	112(a)	Lack of written description	1–19	
1, 3, 6, 11, 14–19	103	Ellison, Muir	1, 3, 6, 11, 14–19	
7, 9, 13	103	Ellison, Muir, Al-Salqan	7, 9, 13	
8, 10, 12	103	Ellison, Muir, Searle	8, 10, 12	
Overall Outcome			1–19	

[8] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

IV. ORDER

For the reasons given, it is

ORDERED that, based on the preponderance of the evidence, claims 1–19 of the '480 patent have been shown to be unpatentable; and

FURTHER ORDERED that, because this is a final written decision, parties to this proceeding seeking judicial review of our decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

For PETITIONER:

W. Karl Renner
Jeremy J. Monaldo
Usman A. Khan
FISH & RICHARDSON P.C.
axf-ptab@fr.com
jjm@fr.com khan@fr.com

For PATENT OWNER:

William P. Ramey, III
Melissa D. Schwaller
RAMEY & SCHWALLER, LLP
wramey@rameyfirm.com
mschwaller@rameyfirm.com