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

Paper 8
Entered: April 26, 2022

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*.

DECISION
Instituting Post-Grant Review
35 U.S.C. § 324

I. INTRODUCTION

A. Background

Samsung Electronics Co., Ltd. ("Petitioner") filed a Petition to institute 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"). Paper 2 ("Pet."). Ward Participations B.V. ("Patent Owner") filed a Preliminary Response. Paper 7 ("Prelim. Resp.").

Section 324(a) of Title 35 of the United States Code provides that a post-grant review may not be instituted "unless . . . the information presented in the petition . . . , if such information is not rebutted, would demonstrate that it is more likely than not that at least 1 of the claims challenged in the petition is unpatentable." Upon consideration of the evidence and arguments in the Petition (including its supporting testimonial evidence) as well as the evidence and arguments in the Preliminary Response, for the reasons below, we determine that the information in the Petition satisfies the threshold provided in 35 U.S.C. § 324(a) and we institute this proceeding.

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.*

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 '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:

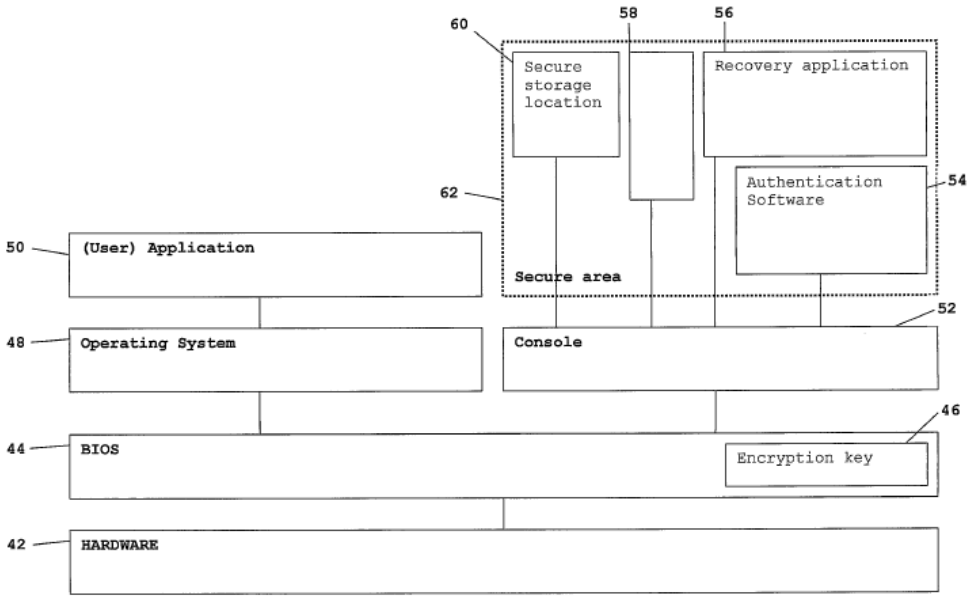

FIG. 3

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 to access certain parts of a hard drive or to start 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

Petitioner challenges the patentability of claims 1–19 of the '480 patent 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	Ellison[1], Muir[2]
7, 9, 13	103	Ellison, Muir, Al-Salqan[3]
8, 10, 12	103	Ellison, Muir, Searle[4]

Petitioner relies on the Declaration of John R. Black, Jr., Ph.D. (Ex. 1003) in support of its unpatentability contentions.

II. ANALYSIS

A. Eligibility for Post-Grant Review

The post-grant review provisions apply only to a patent that contains a claim with an effective filing date on or after March 16, 2013. *See* Leahy-

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

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

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

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

Smith America Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284 (2011), §§ 3(n)(1), 6(f)(2)(A). The statute defines the "effective filing date" as

> (A) if subparagraph (B) does not apply, the actual filing date of the patent or the application for the patent containing a claim to the invention; or
>
> (B) the filing date of the earliest application for which the patent is entitled, as to such invention, to a right of priority under section 119, 365(a), or 365(b) or to the benefit of an earlier filing date under section 120, 121, or 365(c).

35 U.S.C. § 100(i)(1).

Determining whether a patent is subject to the first-inventor-to-file provisions of the AIA, and therefore eligible for post-grant review, is straightforward when the application from which the patent issued was filed before March 16, 2013, or when the application was filed on or after March 16, 2013 without any priority claim. The determination is more complex, however, for a patent that issues from a "transition application," that is, an application filed on or after March 16, 2013 that claims the benefit of an earlier filing date. *See* MPEP § 2159.04. Entitlement to the benefit of an earlier date under 35 U.S.C. §§ 119, 120, 121, and 365 is premised on disclosure of the claimed invention "in the manner provided by § 112(a) (other than the requirement to disclose the best mode)" in the earlier application. *See* 35 U.S.C. §§ 119(e), 120. Thus, a patent that issues from a transition application is not available for post-grant review if the claimed subject matter complies with the written description and enablement requirements of § 112(a) for an ancestor application filed prior to March 16, 2013.

1. Transition Application

As an initial matter, we consider whether the '773 application that eventually matured into the '480 patent is a transition application. Here, as discussed above, the '480 patent issued from the '773 application filed October 9, 2019, which is a continuation of the '422 application filed June 14, 2004, which in turn claims priority to the '436 Dutch application filed June 13, 2003. *See* Ex. 1001, codes (21), (22), (63), (30). As Petitioner contends, the '480 patent purports to be a transition application "because it was filed after March 16, 2013 and claims priority to application filed before March 16, 2013." Pet. 2. That is, the '773 application that matured into the '480 patent is a transition application. *Id.*

2. Written Description Support

Next, we must determine if all of the claims of the '480 patent have written description support prior to March 16, 2013.[5] The written-

[5] If there is adequate written description support for the claims of the '480 patent prior to March 16, 2013, then the '480 patent is not eligible for a post-grant review. Here, we need not address whether the claims have written description support in the '436 Dutch application from which the '422 application claimed priority, as the '422 application was filed prior to March 16, 2013. *See* Ex. 1001, codes (21), (22), (63), (30). If the '422 application does not provide adequate written description support for the claims of the '480 patent, then it has broken the priority chain with respect to those claims and any disclosure in the '436 Dutch application cannot cure that break. Furthermore, if the '773 application (issued as the '480 patent) itself as filed does not provide adequate written description support for the claims of the '480 patent, then there is no priority chain with respect to those claims and any disclosure in the '422 application or in the '436 Dutch application. Thus, if the claims of the '480 patent does not have written description support in the '773 application, we need not address whether the claims have written description support in the '422 application or the '436 Dutch application because the priority chain has been broken.

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.").

To assess the priority claim of the '480 patent, we must determine if the application disclosure of the applications in its priority chain or the '773 application (issued as the '480 patent) itself "describ[ed] the invention, with all its claimed limitations," *Lockwood*, 107 F.3d at 1572, to show "possession of the claimed subject matter as of the filing date," *Ariad Pharm.*, 598 F.3d at 1351. For the reasons discussed below, we determine that the disclosures of the applications in the '480 patent priority chain do

not reasonably convey to an artisan of ordinary skill that the inventor had possession of 1) "providing a private key in a memory of said electronic device, wherein said memory being a secure part of a Basic In Out System or any other secure location in said electronic device operated by the first transaction party," wherein 2) "[the] private key is inaccessible to a user of said electronic device," wherein 3) "the private key is encrypted when the private key is stored in said memory," and wherein 4) "the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software," as required by claim 1. *See* Ex. 1001, 17:64–18:29.

> "*providing a private key in a memory of said electronic device, wherein said memory being a secure part of a Basic In Out System or any other secure location in said electronic device" (claim 1)*

Petitioner contends that the '480 patent "is part of a family of applications that include[s] corresponding European patents, which have been invalidated because the issued claims were not supported by written disclosure," wherein "the same or similar limitations are recited in the '480 Patent and do not have written description support for similar reasons." Pet. 11. According to Petitioner, European patent EP 1634140 (Ex. 1016, "EP 140") and EP 3229099 (Ex. 1017, "EP 099") "were granted on the basis of [the '422 application]," wherein "EP 099 recites claims similar to the '480 Patent." *Id.* at 11–12 (citing Ex. 1001, 17:64–20:47; Ex. 1015 (the Hague Court Judgment), 6–8). Petitioner contends that the Hague court in EP 099 held that claim features "said memory being a secure part of a Basic In Out System *or any other secure location in said electronic device*," and "the authentication data being accessible to said authentication software, *wherein authentication software is stored in said secure memory inaccessible to said*

operating system" were not support by the description in the respective patent disclosure. *Id.* at 12 (citing Ex. 1015, 6, 37–45). Thus, according to Petitioner, "[t]he '480 Patent recites these same features and similarly lacks written description support for them." *Id.*

Patent Owner responds that Petitioner is "conflating European patent law (with its own set of different standards) with United States patent law and cherry-picking European provisional rules for its benefit." Prelim. Resp. 3. According to Patent Owner, the proceedings of EP 099 and EP 140 "were merely suspended ***as it pertains to the Netherlands***," whereas there was no determination made to the validity of the applications "with respect to any of the other European countries." *Id.* at 5.

The '422 application, from which the '773 application (issued as the '480 patent) continued, was filed with 31 original claims on June 14, 2004, before March 16, 2013. *See* Ex. 1014, code (22), 31–35. None of these claims recites a "providing a private key in a memory of said electronic device, wherein said memory being a secure part of a Basic In Out System or any other secure location in said electronic device." *See id.* at 31–35. Figure 1 of the '422 application, as originally filed, shows "five actors: a random table supplier, a trusted third party, a BIOS manufacture, a BIOS and authentication software." *Id.* at 7, Fig. 1. The Detailed Description then describes the installation method as

> a new device relates to any electronic device containing a Basic In Out System ("BIOS", "Boot agent" etc.) with any associated secure storage/memory location, e.g. a computer, server, printer, personal digital assistant, mobile telephone, which is being manufactured, or has been manufactured, but has not yet been delivered to an end-ser, whereas an existing device relates to any electronic device containing a Basic In Out System which has been delivered to an end-user, and may or may not have been used by the end-user. The Basic In Out

> System is only referred to as a system for accessing a memory location in a memory that is direct or indirectly connected to the electronic device. However, as its described hereinafter, the method according to the present invention may employ such a BIOS system to securely store certain digital data and/or such a BIOS system may be provided with an encryption system. A secure storage location and/or an encryption system are not essential to the BIOS system with respect to the present invention.

Id. at 6–7.

In weighing the limited record before us, we determine that the '422 application does not provide sufficient written description support for the recited "providing a private key in a memory of said electronic device, wherein said memory being a secure part of a Basic In Out System *or any other secure location in said electronic device*" in the '480 patent. Ex. 1001, 18:3–6 (emphasis added). We disagree with Patent Owner that "provisional, non-binding decisions regarding European patents ha[ve] no relevance on the patentability of the '480 Patent." Prelim. Resp. 8. Here, in view of the record before us, we find persuasive, at this stage of the proceeding, the Hague court's unrebutted (even though provisional) determination that a person having ordinary skill in the art would have understood that "the invention requires equipment that has a Basic Input/Output System such as a 'BIOS' or "Boot agent'" (Ex. 1015, 5.20), wherein the '422 application "does not describe any alternative for shutting off the access of the operating system/user of the electronic device to storage locations other than by means of the BIOS." *Id.* at 5.31. That is, "it is clear that the average person skilled in the art will directly and unambiguously deduce from the original application that the security of transactions is achieved by storing the authentication data in a storage location within the BIOS or shield from the operating system by the BIOS," wherein adding the feature that "the

authentication data can also be stored in 'any other secure location' in the electronic device" entailed adding "impermissible matter." *Id.* at 5.32.

Significant to our determination is the lack of any description of the structure of "any alternative for shutting off the access of the operating system/user of the electronic device to storage locations other than by means of the BIOS," as the Hague court points out. Ex. 1015, 5.31. We note Patent Owner does not provide any evidence to support such alternative means.

We determine on the current limited record, 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 being a secure part of any secure location in said electronic device other than a Basic In Out System. That is, the '422 application does not contain an adequate written description of "providing a private key in a memory of said electronic device, wherein said memory being a secure part of a Basic In Out System *or any other secure location in said electronic device*," as required by claim 1 (emphasis added).

Because we determine that the term "providing a private key in a memory of said electronic device, wherein said memory being a secure part of a Basic In Out System or any other secure location in said electronic device" of claim 1 lacks adequate written description support in the '422 application, the earliest filing date for this subject matter is the filing date of the '773 application (issued as the '480 patent) when the subject matter was first introduced, i.e., October 9, 2019. As such, we conclude that the '480 patent is eligible for post-grant review.

private key in a memory of said electronic device . . . inaccessible to a user of said electronic device," "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" (claim 1)

Petitioner contends that 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.

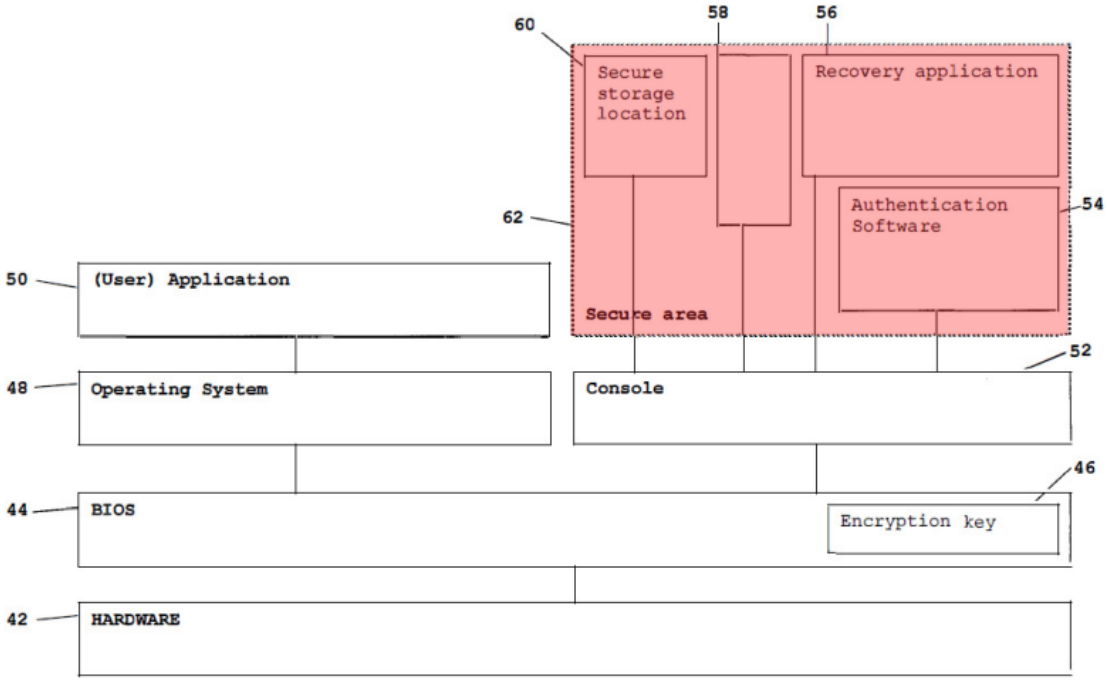

FIG. 3

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." *Id.* at 19 (citing 1003 ¶¶ 175–176). Furthermore, according to Petitioner, "since the '480 Patent describes the private key as being part of a software ID or an application identifying character string, it could have been accessible to the user" because "the '480 Patent does not teach that the software ID or application identifying character string are inaccessible to the user." *Id.* (citing Ex. 1001, 5:39–40, 13:31–44).

For similar reasons, 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" as discussed. *Id.* at 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). That is, "a private encryption key is not the same as an ***encrypted*** private key." *Id.* (citing Ex. 1003 ¶ 179). Thus, according to Petitioner, 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 responds that the '480 patent discloses that "[t]he authentication software preferably has its own unique serial number, software ID and/or private encryption key," wherein a person of ordinary skill in the art "would recognize that since the authentication software has a private encryption key, the private key forms an integral part of the authentication software component and/or is embedded therein." Prelim. Resp. 13 (quoting Ex. 1001, 5:39–40; citing Ex. 2001 ¶ 62). That is, "a POSITA would recognize that the private key is with the authentication software." *Id.* (citing Ex. 2001 ¶ 62). Furthermore, according to Patent Owner, "FIG.3 of the '480 Patent clearly discloses authentication software 54 installed and stored in secure area 62," and thus, "[s]ince the authentication software 54 includes the private key contained or embedded therein, the private key would be provided in secure memory location 54 of the Secure Area 62." *Id.* at 15 (citing Ex. 1001, Fig. 3; Ex. 2001 ¶ 65).

Patent Owner then contends that "[e]ncryption of the authentication software and thus its private key is supported, for example, at step 20 in FIG. 1 of the '480 Patent," wherein "the authentication software may be

encrypted, or not." Prelim. Resp. 17 (quoting Ex. 1001, 11:44–45). Thus, Patent Owner contends that a POSITA "would recognize that if the authentication software with the private key is encrypted, it would be inaccessible to a user of the device." *Id.* (citing Ex. 2001 ¶ 67). According to Patent Owner, a person of ordinary skill in the art would have understood that "if the operating system 48 cannot gain specified access, such access is also denied to the user." *Id.* (citing Ex. 2001 ¶ 68).

Patent Owner further contends that the '480 patent discloses "the principles of the decryption, re-encryption and re-encrypted storage of an authentication table." Prelim. Resp. 19 (citing Ex. 1001, Figs. 1, 2). Thus, Patent Owner contends that "[a] POSITA would understand that this principle can be readily applied to any authentication data that are used to perform unique digital signing" according to the '480 patent, "including the private key of the authentication software." *Id.* (citing Ex. 2001 ¶ 70). According to Patent Owner, a person of ordinary skill in the art would have recognized that the written description in the '480 patent "supports the authentication software including a private key and describes the secure processing environment (not accessible to user-operated software programs) in which the authentication software decrypts authentication data (which the private key is)." *Id.* at 23 (citing Ex. 2001 ¶ 73).

The '773 application, which matured into the '480 patent, was filed with 25 original claims and with claims 26–28 added by preliminary amendment. *See* Ex. 1002, 212–218. None of these claims recite "providing a *private key* in a memory of said electronic device," wherein the private key is "inaccessible to a user of said electronic device," is "encrypted" *when* the "private key is *stored in said memory*," and "decrypted in a secure processing environment inaccessible." *See id.*

(emphasis added). Instead, the claims as filed merely recite "providing *authentication data* in a memory of said electronic device, ..." *See id.* (emphasis added). As Petitioner points out, during prosecution of the '773 application, the claims were amended by replacing "authentication data" with "private key," and the application was allowed thereafter. Pet. 9; *see* Ex. 1002, 91–96.

Figure 3 of the '480 patent shows secure area 62 comprising secure storage location 60, memory location 58, recovery application 56, and authentication software 54. *See* Ex. 1001, Fig. 3. The Detailed Description then describes the authentication software as preferably having "its own unique serial number, software ID ***and/or*** private encryption key," wherein "a *unique serial number* . . . , or *the unique software ID* [is] embedded in the authentication software." *Id.* at 5:39–49 (emphasis added). Thus, as described in the Detailed Description, in this embodiment, the authentication software comprises a unique serial number, a unique software ID ***and/or*** a private encryption key, wherein the unique serial number or the unique software ID is embedded therein. *Id.* The Detailed Description then describes a further embodiment, wherein the authentication software may be provided with a system for signing a digital signature "using at least a part of a . . . software ID[] ***or*** any other application identifying character string, hereinafter referred to as a private key," wherein "[t]he private key is registered at a third party, for example the authentication software provider which supplied said private key." *Id.* at 13:31–38. That is, in this embodiment, the authentication software is used for signing a digital signature using a software ID or a private key. *Id.*

In weighing the limited record before us, we agree with Petitioner that the '480 patent does not explicitly describe where the private key is stored in

the electronic device. Pet. 16–17. 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 (emphases added).

At this stage of the proceeding, we do not find persuasive Patent Owner's contention that a person of ordinary skill in the art would have recognized that authentication software has a "private key" that forms an "integral part of the authentication software component and/or is embedded therein" (Prelim. Resp. 13 (quoting Ex. 1001, 5:39–40)), in view of the cited section in the Detailed Description describing the authentication software as comprising the unique serial number, the unique software ID ***and/or*** a private encryption key, but only the unique serial number or the unique software ID is embedded therein. *See* Ex. 1001, 5:39–49. That is, we are unpersuaded at this stage of the proceeding that the person of ordinary skill in the art will directly and unambiguously deduce from the '773 application as filed that the "private encryption key" is embedded in the authentication software, as Patent Owner contends. Prelim. Resp. 13. Instead, we find persuasive Petitioner's contention that the '480 patent (i.e., the '773 application) merely teaches storing the digital signing algorithm in a secure part of the BIOS 44 but is silent as to storage of the private key. Pet. 18 (citing Ex. 1001, 9:27–34, 13:31–44; Ex. 1003). As Petitioner contends, the

'480 patent only discussed the private key as being "registered at a third party, for example the authentication software provider which supplied said private key." *Id.* (citing Ex. 1001, 13:31–44).

We also do not find persuasive Patent Owner's contention that the '480 patent provides support for private key being encrypted at, for example, "step 20 in FIG. 1 of the '480 Patent." Prelim. Resp. 17. Although the cited portion of the Detailed Description states that "the authentication software may be encrypted, or not" (see Ex. 1001, 11:44–45), we agree with Petitioner that this cited portion of the '480 patent does not disclose "***a temporal element*** that the private key is encrypted ***when*** it is stored in the memory," wherein "a private encryption key is not the same as an ***encrypted*** private key." Pet. 20 (citing Ex. 1001, 8:29–30; Ex. 1003 ¶¶ 178–179).

Here, 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 that "private key" appeared in the claims by replacing "authentication data" previously recited. Pet. 9; *see* Ex. 1002, 91–96.

We determine, on this limited record, 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 provided in a memory of an electronic device that is inaccessible to a user, wherein the private key is encrypted when the private key is stored in the memory. That is, the '773 application does not contain an adequate written description of "providing a private key ***in a memory*** of said electronic device ***inaccessible to a user*** of said electronic device," the private key being "***encrypted when*** the private key is ***stored in said memory***," as required by claim 1 (emphasis added).

On this record, we determine that the terms "providing a private key in a memory of said electronic device . . . inaccessible to a user of said electronic device," the private key being "encrypted when the private key is stored in said memory," and therefore "decrypted in a secure processing environment inaccessible to said user and to any user-operated software," as recited in claim 1 of the '480 patent, lack adequate written description support in the '773 application.

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

Petitioner contents that the terms "providing a private key in a memory of said electronic device, wherein said memory being a secure part of a Basic In Out System or any other secure location in 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" lack written description support. Pet. 16–24. Patent Owner disputes these contentions. Prelim. Resp. 13–24.

As we determined above in connection with our analysis of whether the '480 patent is eligible for post-grant review, the terms lack written description support in the '773 application (issued as the '480 patent) itself and/or the '422 application (from which the '773 application was filed as a continuation). Thus, we determine that the information in the Petition demonstrates that it is more likely than not that the Challenged Claims are unpatentable as failing to comply with the written description requirement under 35 U.S.C. § 112(a) with respect to these terms. We will, however, revisit our preliminary determination with respect to this ground for these terms on a complete record.

C. Claims 1–19 as 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). In response, Patent Owner contends that neither Ellison nor Muir teaches or suggests a "decryption key for decrypting a private key," or "authentication software [] stored in said secure memory inaccessible to said operating system," that is "run in a secure processing environment inaccessible to said operating system." Prelim. Resp. 29–40.

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 contends that "[n]either Ellison nor Muir disclose **storing** authentication software in a secure memory," but instead "Ellison's usage protector 250 is 'located in a secure platform 200.'" Prelim. Resp. 34. In light of the parties' arguments and evidence, we find that it is necessary to 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.

Petitioner relies on Ellison's usage protector 250 to disclose "authentication software stored in said secure memory." Pet. 55–58. In particular, Petitioner contends that Ellison's Figure 2 describes "a ***secure platform*** 200 that 'includes . . . a usage protector 250, [] ***operating within the isolated execution environment***." *Id*. at 58 (citing Ex. 1006, 8:25–32; Ex. 1003 ¶ 95). Patent Owner responds that "Ellison does make clear that usage protector 250 is **not** stored in the isolated area 70" because critical modules such as usage protector 250 "are *loaded into* the execution space by

processor numb loader 52." Prelim. Resp. 35 (citing Pet. 71; Ex. 2001 ¶ 93). Patent Owner contends that "Petitioner relies on where Ellison's usage protector is 'located' when it is executed," but "the location of execution fails to disclose storage in secure memory." *Id.* at 36. Thus, Patent Owner appears to be contending that software that is "loaded" into a secure "location of execution" is not software is that is "stored" in a secure "memory" location, whereas, to be "stored" in a secure "memory" location, the software must be "stored in the isolated area 70." *Id.* at 35–36.

The Specification of the '480 patent discloses secure area 62 only accessible to BIOS 44, comprising applications and storage locations not reported to operating system 48 (Ex. 1001, 8:62–9:1), wherein, as shown in Figure 3, secure area 62 comprises secure storage location 60, recovery application 56, and authentication software 54. *Id.* at 9:7–11. That is, the Specification shows "secure memory inaccessible to said operating system" as a location that holds software not accessible to operating system 48. *Id.* Nothing in the Specification, or the general knowledge in the art, limits "secure memory inaccessible to said operating system" to Ellison's "isolated storage area 70," or precludes Ellison's "secure platform 200," as Patent Owner proposes. Prelim. Resp. 35–36. In fact, nothing in the Specification or the general knowledge in the art limits the "storage" to any amount of time in the secure memory.

We are unpersuaded by Patent Owner's apparent position that software that is *loaded* into a secure *location of execution* is not software that is "stored" in a "secure memory" location. Prelim. Resp. 35–36.

In view of the Specification and the general knowledge in the art, we determine 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. Our determination here is preliminary, and the parties are invited to address this claim construction issue at trial, if so desired.

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

3. Ellison

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

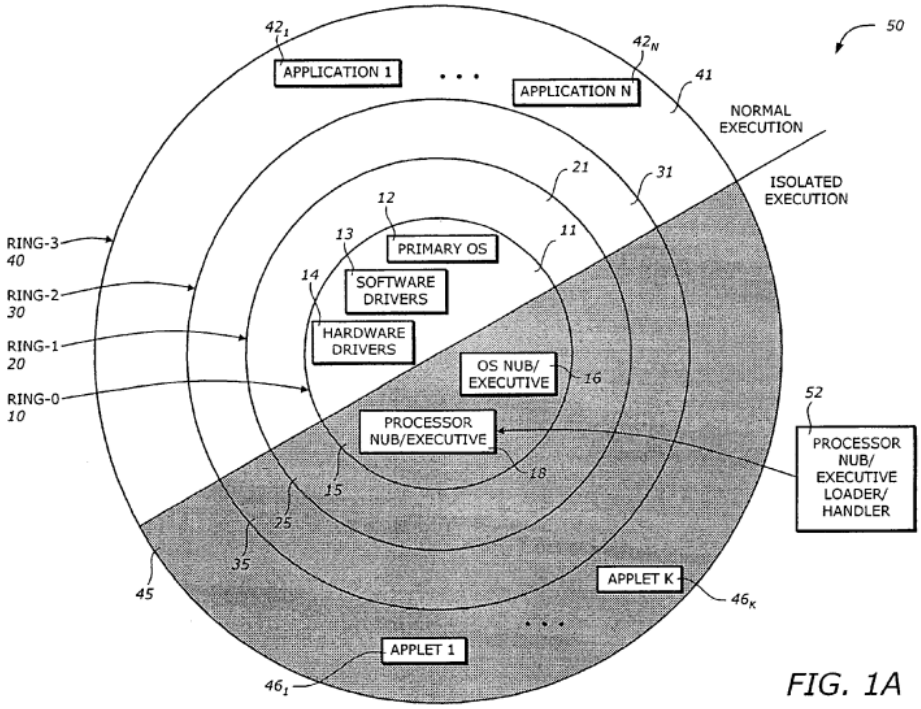

FIG. 1A

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.

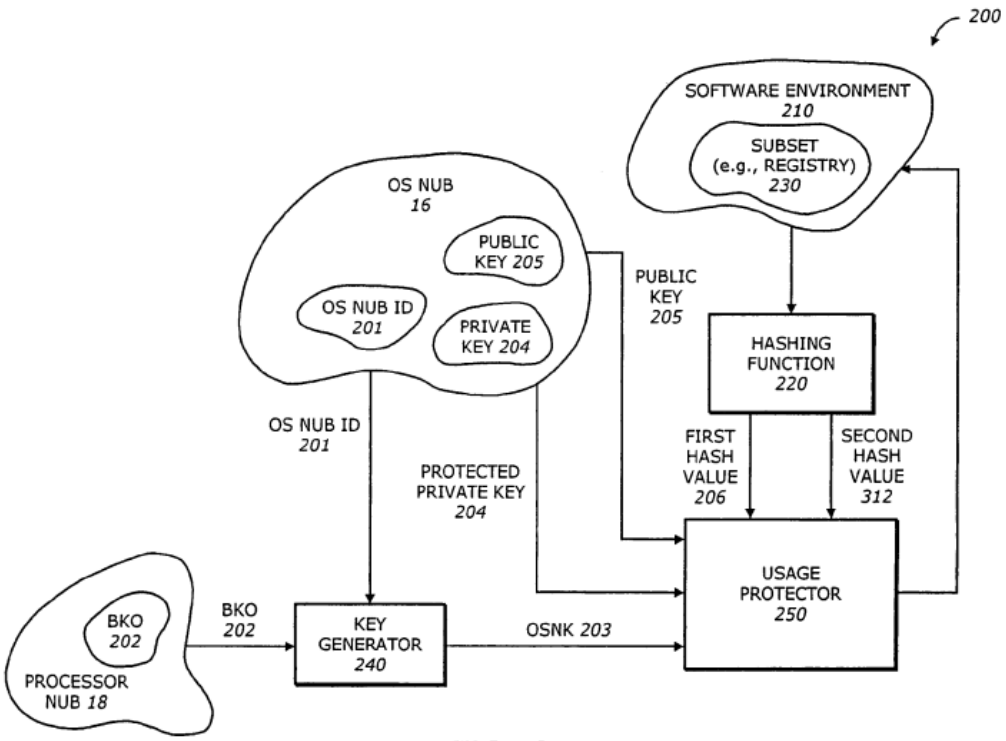

FIG. 2

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.

4. 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).

5. 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.

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 that the preamble is limiting, the combination of Ellison and Muir teaches that "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.

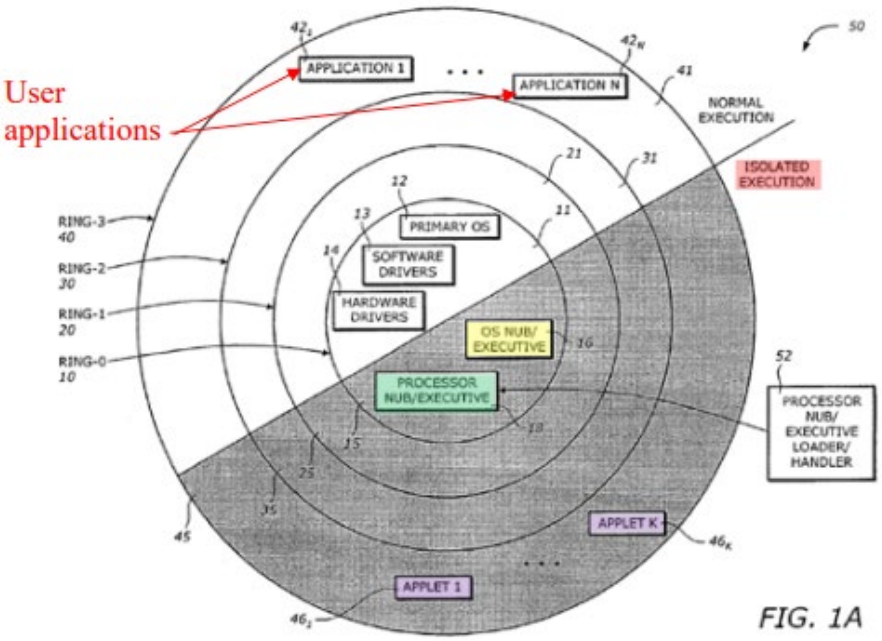

FIG. 1A

SAMSUNG-1006, FIG. 1A

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).

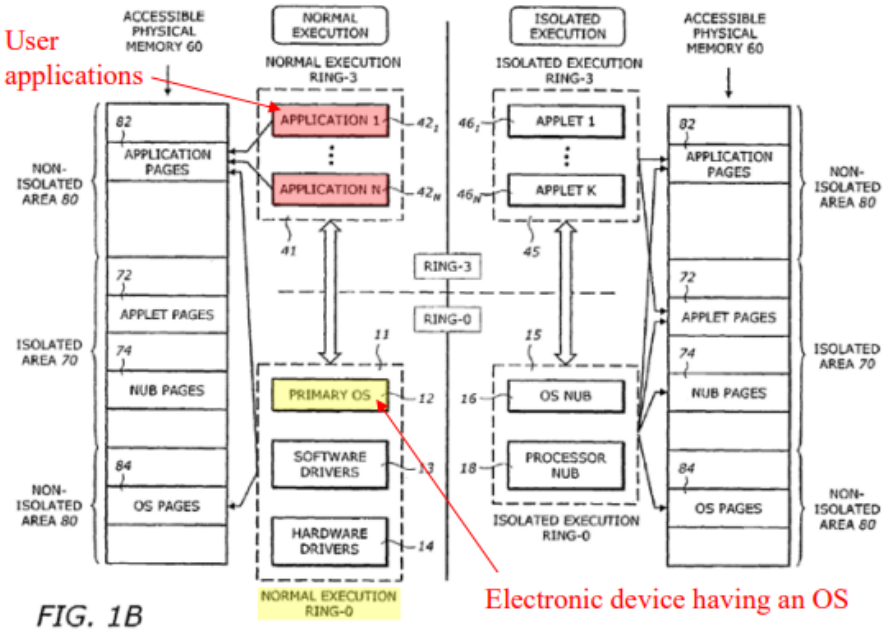

FIG. 1B

SAMSUNG-1006, FIG. 1B

Along with annotated Figure 1A, annotated Figure 1B of Ellison in the Petition, according to Petitioner, 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).

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. 28–39.[6]

Having reviewed all of Petitioner's assertions regarding the preamble, as well as the supporting evidence, we determine on this record that Petitioner has demonstrated that it is more likely than not that the combination of Ellison and Muir teaches a "method for performing an electronic transaction" recited in the preamble of claim 1.

> *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 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

[6] The issue of whether the preamble is limiting need not be resolved at this stage of the proceeding because, regardless of whether the preamble is limiting, Petitioner shows sufficiently for purposes of institution, 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, 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").

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 contends 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 contends that "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).

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 these claim limitations. *See generally* Prelim. Resp. 28–39.

Having reviewed all of Petitioner's assertions regarding these claim limitations, as well as the supporting evidence, we determine on this record that Petitioner has demonstrated more likely than not that 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," but, "[e]ven if key generator 240 is part of the isolated environment, where is the software stored when it is not in main memory?" Prelim. Resp. 32 (citing Ex. 2001 ¶ 87). In particular, according to Patent Owner, "[i]t is unclear where the OSNK key 203 is stored or whether it is generated every time it is needed." *Id.* (citing Ex. 2001 ¶ 88).

We find Patent Owner's arguments unavailing. In particular, Patent Owner's argument that Ellison must be clear as to "where the OSNK key 203 is stored" is not commensurate in scope with the language of claim 1. Claim 1 does not require that the storage location OSNK 203 be known, but rather merely requires that a key such as OSNK 203 be "incorporated in" the electronic device. *See* Ex. 1001, 18:9–10.

Nevertheless, even assuming *arguendo* that claim 1 requires that OSNK be "stored," Patent Owner is again relying on a claim construction of

"stored" as excluding being held in an isolated execution environment. Prelim. Resp. 32. As discussed above in Section C(1), such interpretation does not comport with the aforementioned construction of being held in any secure location that is inaccessible to the operating system.

In Ellison, as Petitioner points out, "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." Pet. 64 (citing Ex. 1006, 8:25–65, 11:1–12:26, 9:1–14, Figs. 2, 3C, 3D) (emphasis added). We are persuaded by Petitioner's contention that Ellison's OSNK 203, being generated and used ***within*** the secure location in the electronic device is therefore "incorporated in" the electronic device.

On this preliminary record, we are persuaded that Petitioner has demonstrated more likely than not that 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," wherein "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 "[n]either Ellison nor Muir disclose **storing** authentication software in a secure memory." Prelim. Resp. 34. In particular, according to Patent Owner, "the 'location' of usage protector that Petitioner refers to is where the usage protector 250 is loaded ***into*** in order to ***execute***," but "the execution environment is not the same as where something is ***stored***." *Id.* (citing Ex. 2001 ¶ 92).

We find Patent Owner's arguments unavailing. In particular, Patent Owner is again relying on a claim construction of "storing" that precludes a "location" where the software is "loaded into," but, as discussed above in Section C(i), 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, and Patent Owner agrees, 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; Prelim. Resp. 34; Ex. 1006, 8:25–32. Given the claim construction above, we are persuaded by 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).

On this preliminary record, we are persuaded that Petitioner has demonstrated more likely than not that 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).

At this stage in the proceeding, Patent Owner does not address separately Petitioner's explanations and supporting evidence regarding the remaining limitations in claim 1. *See generally* Prelim. Resp.

Having reviewed Petitioner's arguments and supporting evidence in the present record, we determine that the information in the Petition demonstrates that it is more likely than not that at least claim 1 of the Challenged Claims is unpatentable, and we institute trial for all Challenged

Claims and all grounds. Further, we also address certain of the merits of the other asserted grounds below, to help guide the parties in developing the complete record during trial.

v. Claims 3, 6, 11, 14–19 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).

At this stage in the proceeding, Patent Owner does not address separately these explanations and supporting evidence by Petitioner regarding claims 3, 6, 11, and 14–19. *See generally* Prelim. Resp.

Having reviewed Petitioner's arguments and supporting evidence in the present record, we determine Petitioner has demonstrated that it is more likely than not that it will prevail on its assertion that claim 3, 6, 11, and 14–19 would have been obvious over the combination of Ellison and Muir.

vi. 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)).

At this stage in the proceeding, Patent Owner does not address separately these explanations and supporting evidence by Petitioner regarding claims 7–10, 12, and 13. *See generally* Prelim. Resp.

Having reviewed Petitioner's arguments and supporting evidence in the present record, we determine Petitioner has demonstrated that it is more likely than not that it will prevail on its assertion 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

For the reasons above, we determine that the information in the Petition demonstrates that it is more likely than not that the Challenged Claims are unpatentable and we institute a post-grant review proceeding on all Challenged Claims and grounds.

IV. ORDER

For the reasons given, it is

ORDERED that pursuant to 35 U.S.C. § 324(a), the Petition is granted and trial is instituted on claims 1–19 of the '480 patent to determine whether:

1) claims 1–19 lack written description under 35 U.S.C. § 112(a);

2) claims 1, 3, 6, 11, and 14–19 would have been obvious over Ellison and Muir;

3) claims 7, 9, and 13 would have been obvious over Ellison, Muir, and Al-Salqan; and

4) claims 8, 10, and 12 would have been obvious over Ellison, Muir and Searle; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 324(d) 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 Order.

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