

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

SAMSUNG ELECTRONICS CO. LTD.,  
and BANK OF AMERICA, N.A.,<sup>1</sup>  
Petitioner,

v.

WARD PARTICIPATIONS B.V.,  
Patent Owner.

---

IPR2022-00114  
Patent 11,063,766 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  
*35 U.S.C. § 318(a)*

---

<sup>1</sup> Bank of America, N.A. filed a motion for joinder and a petition in Case IPR2022-01077, which were granted, and, therefore, has been joined as petitioner in this proceeding.

## I. INTRODUCTION

### A. *Background*

In response to a Petition (Paper 2, “Pet.”) filed by Samsung Electronics Co., Ltd. (“Petitioner”), we instituted *inter partes* review of claims 1, 3–5, 8–13, and 21–33 (the “challenged claims”) of U.S. Patent No. 11,063,766 B2 (Ex. 1001, “the ’766 patent”). *See* Paper 7 (“Dec. Inst.”). During trial, Ward Participations B.V. (“Patent Owner”) filed a Response, Paper 9 (“PO Resp.”), to which Petitioner filed a Reply (Paper 19, “Pet. Reply”). In turn, Patent Owner filed a Sur-Reply. Paper 27 (“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 31 (“Tr.”).

We have jurisdiction under 35 U.S.C. § 6. This Decision is a Final Written Decision under 35 U.S.C. § 318(a) as to the patentability of the claims on which we instituted trial. Based on the record before us, Petitioner has shown by a preponderance of the evidence that claims 1, 3–5, 8–13, and 21–33 of the ’766 patent are unpatentable.

### B. *Related Proceedings*

Petitioner identifies the ’766 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. 102. Petitioner also identifies two proceedings before the Board that challenge claims of US 10,992,480 B2, a “related child patent.” *Id.* (identifying PGR2022-00007 and IPR2022-00113).

*C. The '766 Patent*

The '766 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 July 13, 2021, from Application No. 10/560,579, filed as PCT Application No. PCT/NL2004/00042, with a filing date of June 14, 2004. Ex. 1001, codes (54), (45), (21), (22) (86).

The invention described in the '766 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 '766 patent's computer configuration is depicted in Figure 3, reproduced below:

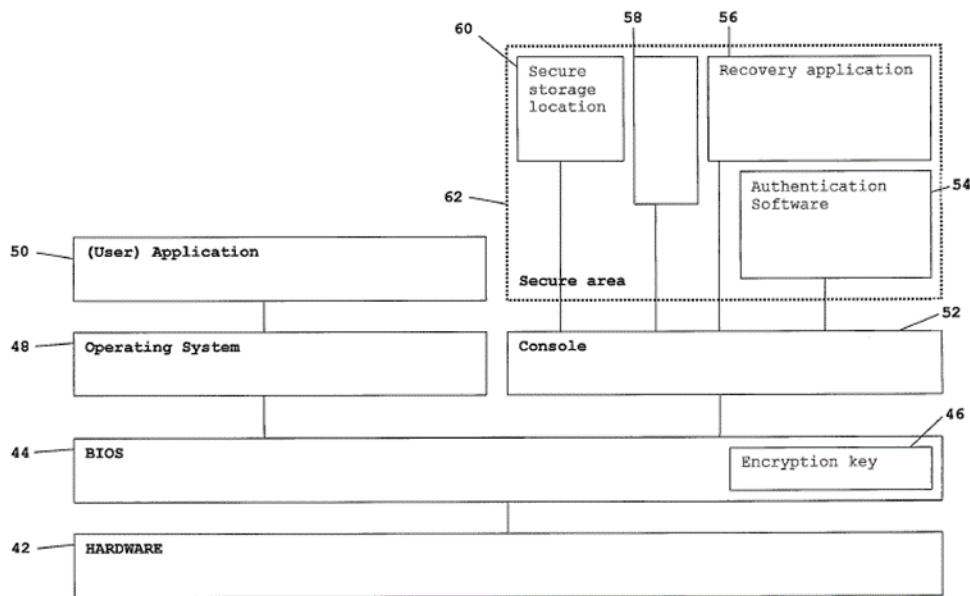


FIG. 3

Figure 3 is a schematic diagram of a computer configuration having authentication software and an authentication table installed in the Basic In Out System (BIOS). *Id.* at 3:25–27. 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 8:30–33.

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 8:34–37.

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 8:38–44. 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 8:45–48.

Operating system 48 creates a run-time environment for any user application, and is an interface between the user and hardware 42. *Id.* at 8:49–52. 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 8:52–59. 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 starting certain applications. *Id.* at 8:60–64.

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 8:65–9:5. Any instruction coming from operating system 48 intended for console 52 may be blocked by BIOS 44. *Id.* at 9:8–10.

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 9:11–17.

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 9:23–27. 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 9:28–32. 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 9:32–35.

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 13:46–51. 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 9:43–47.

*D. The Challenged Claims*

Of the challenged claims (claims 1, 3–5, 8–13, and 21–33), claims 1, 29, and 33 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 and authentication software running in a separate operating environment, independent from and inaccessible to the operating system, the electronic device having a memory comprising storage locations, part of the memory being accessible to the operating system, part of the memory being a secure area,

wherein the electronic device comprises a system for accessing a memory location in the memory, wherein the system for accessing the memory location is configured to selectively report the storage locations of the secure area, wherein the storage locations are not reported to the operating system while at the same time being reported to the authentication software running in the separate operating environment, the method comprising:

providing a private key in the secure area of the electronic device which private key is inaccessible to a user of the electronic device, wherein the secure area is inaccessible to the operating system of the electronic device, thereby rendering the private key inaccessible to the user;

providing authentication software in the electronic device, the private key being accessible to the authentication software, wherein the authentication software is stored in the secure area inaccessible to the 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 the operating system; and

providing by the electronic device the digital signature to the second transaction party.

Ex. 1001, 18:10–45.

*E. Asserted Grounds of Unpatentability*

We instituted *inter partes* review all claims and all challenges in the Petition. Petitioner asserts that claims 1, 3–5, 8–13, and 21–33 of the '766 patent are unpatentable on the following grounds (Pet. 1):

| Claim(s) Challenged      | 35 U.S.C. §      | Reference(s)/Basis                            |
|--------------------------|------------------|-----------------------------------------------|
| 1, 3, 4, 8, 9, 13, 21–33 | 103 <sup>2</sup> | Ellison <sup>3</sup> , Muir <sup>4</sup>      |
| 10, 12                   | 103              | Ellison, Muir, Al-Salqan <sup>5</sup>         |
| 11                       | 103              | Ellison, Muir, Al-Salqan, Searle <sup>6</sup> |

---

<sup>2</sup> 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 '766 patent was filed before the effective date of the relevant amendments, the pre-AIA version of § 103 applies.

<sup>3</sup> U.S. Patent No. 7,082,615 B1, issued July 25, 2006, filed September 22, 2000 (Ex. 1006, “Ellison”).

<sup>4</sup> PCT Patent Publication No. WO 01/93212 A2, published December 6, 2001, filed May 30, 2001 (Ex. 1008, “Muir”).

<sup>5</sup> U.S. Patent No. 6,549,626, issued April 15, 2003, filed October 20, 1997 (Ex. 1007, “Al-Salqan”).

<sup>6</sup> U.S. Patent No. 6,683,954 B1, issued January 27, 2004, filed October 23, 1999 (Ex. 1009, “Searle”).

| Claim(s) Challenged | 35 U.S.C. § | Reference(s)/Basis                  |
|---------------------|-------------|-------------------------------------|
| 5                   | 103         | Ellison, Muir, Epstein <sup>7</sup> |

Petitioner relies on the Declarations of John R. Black, Ph.D. (Ex. 1003, 1032) in support of its unpatentability contentions. Patent Owner provides the Declarations of Bart Preneel, Ph.D. Exs. 2001, 2009. Dr. Preneel was cross-examined by Petitioner, and a transcript of his deposition was entered into the record. Ex. 1033.

## 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 ’766 patent would have had “a Bachelor’s degree in an academic discipline emphasizing the design of electrical, computer, software technologies, in combination with

---

<sup>7</sup> U.S. Patent No. 6,694,025 B1, issued February 17, 2004, filed June 2, 1999 (Ex. 1030, “Epstein”).

training or at least two years of related work experience with software security technologies such as cryptography or encryption/decryption systems, or in the development of hardware and software for carrying out secure electronic transactions,” wherein “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.” Pet. 2–3 (citing Ex. 1003 ¶¶ 15–16). Patent Owner “adopts Petitioner’s proffered level of ordinary skill in the art because it comports with the technology and claims of the ’766 Patent as well as the asserted prior art.” See PO Resp. 15.

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 ’766 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, 3–5, 8–13, and 21–33 Allegedly Obvious Under 35 U.S.C. § 103*

Petitioner contends that: claims 1, 3, 4, 8, 9, 13, and 21–33 of the ’766 patent would have been obvious over Ellison and Muir (Pet. 6–74); claims 10 and 12 would have been obvious over Ellison, Muir, and Al-Salqan (*id.* at 74–82); claim 11 would have been obvious over Ellison, Muir, Al-Salqan and Searle (*id.* at 82–90); and claim 5 would have been obvious over Ellison, Muir, and Epstein (*id.* at 90–97). Petitioner maintains its arguments pertaining to these grounds and references in its Reply. Pet. Reply 5–19.

Patent Owner counters that the asserted combinations fail to disclose key elements of claim 1. PO Resp. 16–46; see PO Sur-reply 1–4.

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 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. 2 (citing *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Circ. 2011)). Patent Owner does not propose a claim construction but takes issue with the Institution Decision’s analysis of the term “stored” in “the authentication software is stored in the secure area.” PO Resp. 46–50 (citing Dec. Inst. 13). Specifically, Patent Owner contends that, during the relevant period between the filing dates of Ellison, Muir and the application of the ’766 patent, when data or a data file is “stored,” it is stored in “permanent memory” and “remains there until it is deleted.” *Id.* at 47–48.

In light of the parties’ arguments and evidence, we find that it is necessary to construe “wherein the authentication software is *stored* in the secure area inaccessible to the operating system” to the extent necessary to resolve the disputed issues before us. *See* claim 1 (emphasis added).

*“wherein the authentication software is stored in the secure area inaccessible to the operating system” (claims 1, 29, 33).*

Independent claims 1, 29 and 33 recite “providing authentication software the electronic device . . . , wherein the authentication software is *stored* in the secure memory inaccessible to the operating system.”

Ex. 1001, 18:36–39 (emphasis added).

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. 47–48. 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 2. 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 the secure area inaccessible to the operating system.” Pet. Reply 2. 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 10 (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 the secure memory inaccessible to the 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(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, “would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of non-obviousness.<sup>8</sup> *See Graham*, 383 U.S. at 17–18.

---

<sup>8</sup> Neither party presents arguments regarding objective evidence of nonobviousness in the instant proceeding.

### 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, 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 operating system. *Id.* at 2:41–46. An illustration of Ellison’s execution architecture is depicted in Figure 1A, reproduced below.

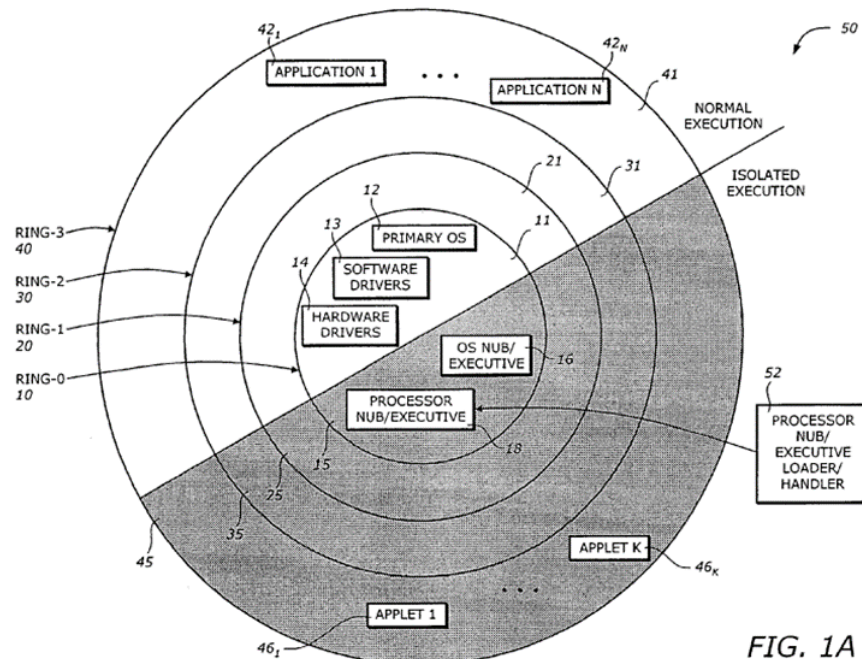


Figure 1A is a diagram illustrating logical operating architecture 50 that includes ring-0 10, ring-1 20, ring-2 30, ring-3 40, and processor nub loader 52. *Id.* at 2:62–3:6. As shown in Figure 1A, logical operating architecture 50 has two modes of operation: normal execution mode (white) and isolated 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, normal execution Ring-0 11 includes primary operating system 12, software drivers 13, and hardware drives 14; while isolated execution Ring-0 15 includes OS nub 16 and processor nub 18. *Id.* at 3:10–16. 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 the isolated area, wherein, from the isolated area, processor nub loader 52 copies processor nub 18 in a non-volatile memory into the isolated area, verifies and logs its integrity, and manages a symmetric key used to protect the processor nub's secrets. *Id.* at 6:47–56.

A memory control hub (MCH) provides control and configuration of memory and input/output devices such as the system memory and the input/output control hub (ICH), wherein the MCH provides interface circuits to recognize and service isolated access assertions on memory reference bus cycles. *Id.* at 5:57–62. The MCH has memory range registers to represent the isolated area in the system memory. *Id.* at 5:62–65. Once configured,

the MCH aborts any access to the isolated area that does not have the access bus mode asserted. *Id.* at 5:65–67.

The ICH represents a known single point in the system having the isolated execution functionality, wherein the ICH includes an isolated bus cycle interface, processor nub loader 52, a digest memory, a cryptographic key storage, an isolated execution logical processor manager, and a token bus interface. *Id.* at 6:27–43.

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

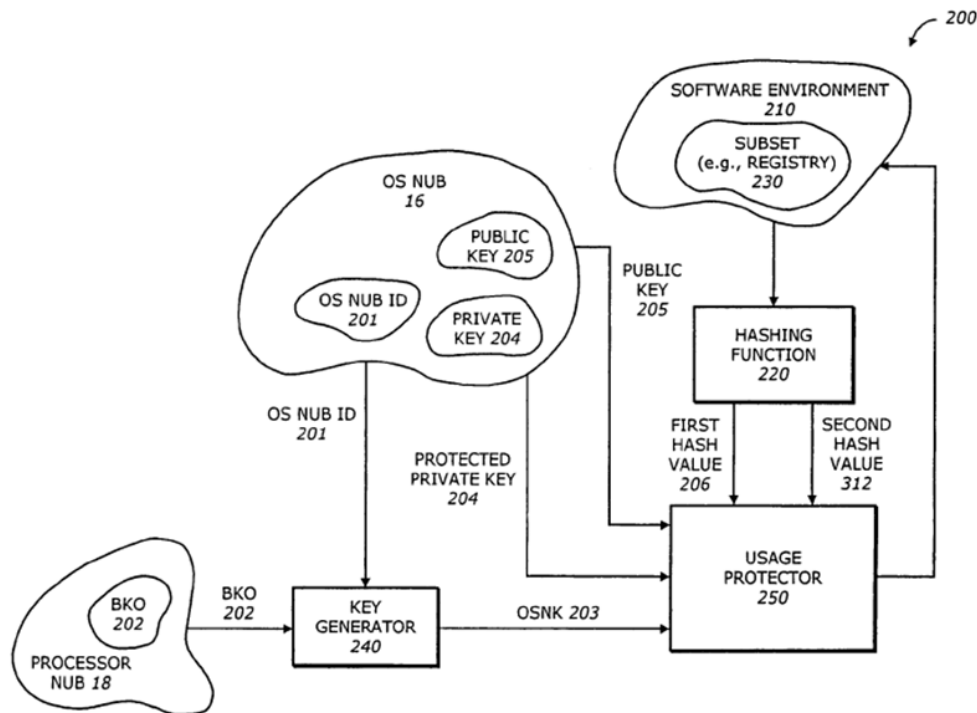


FIG. 2

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).

In one embodiment, the apparatus comprises a virtual smart card driver that receives a request from a user through an application, and creates a restricted memory space (“hidden memory space”) by designating a space as restricted memory space, making it generally inaccessible to the operating system and normal applications running on top of the operating system. *Id.* at 9:10–20.

Muir’s memory space having a hidden memory space is depicted in Figure 6, reproduced below.

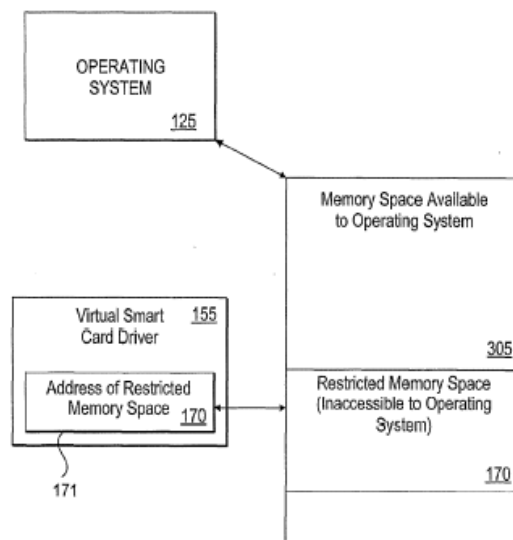


Fig. 6

Figure 6 shows a diagram illustrating operating system 125, virtual smart card driver 155, and memory space 305, wherein memory space 305 is shown including restricted memory space 170. *Id.* at 12:9–13.

In one embodiment, memory space 305 is a fixed disk with some “good” or “usable” sectors that are marked as “bad.” *Id.* at 12:14–15. In another embodiment, memory space 305 is a read-only memory (ROM), random access memory (RAM), flash memory or similar device, which is accessed using address pointers, wherein a portion of the memory is designated as restricted memory space 170 by altering the address pointers used by the operating system to access memory space 305. *Id.* at 12:19–23.

In a further embodiment, restricted memory space 170 stores a private key, wherein the private key is hidden from operating system 125. *Id.* at 12:24–26.

Virtual smart card driver includes address pointer 171 to restricted memory space 170 or alternatively to a number of addresses or locations for restricted memory space. *Id.* at 13:1–4. Virtual smart card driver 155 uses address pointer 171 to send data to and retrieve data from restricted memory space. *Id.* at 5–7.

#### 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 the private key and performing cryptographic operations such as encryption.” Pet. 21.

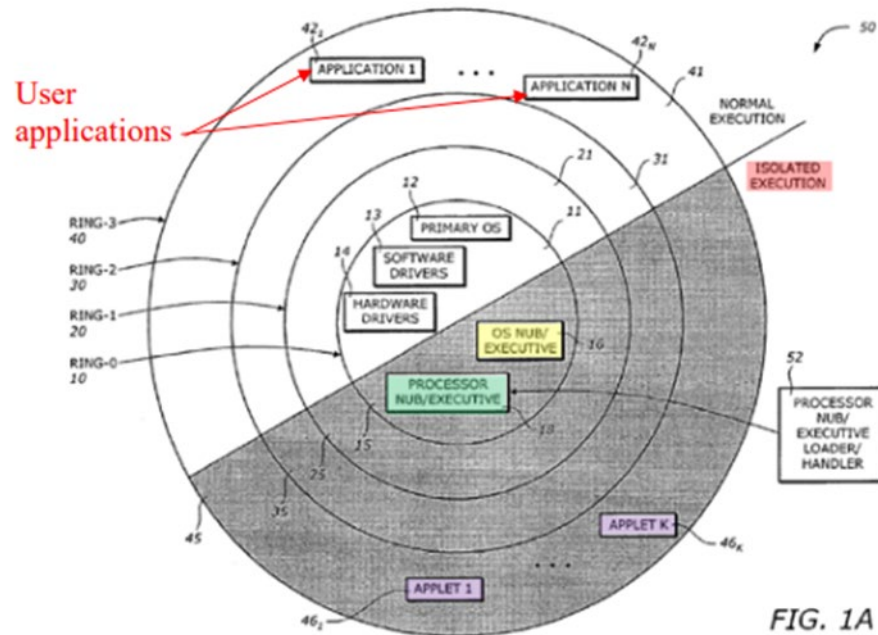
Having reviewed all the arguments and evidence in the complete record, we determine Petitioner has demonstrated by a preponderance of the evidence that claims 1, 29, and 33, and claims 3, 4, 8, 9, 13, 21–28, and 30–32 depending therefrom, would have been obvious over Ellison in view of Muir, notwithstanding Patent Owner’s arguments to the contrary. We similarly determine that dependent claims 10 and 12 would have been obvious over Ellison and Muir in further view of Al-Salqan; that dependent claim 11 would have been obvious over Ellison and Muir in further view of Searle; and that dependent claim 5 would have been obvious over Ellison and Muir in further view of Epstein.

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” and “authentication software running in a separate operating environment, independent from and inaccessible to the operating system” (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 associated with a first transaction party and a second transaction party*).” Pet. 24–25 (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 ¶¶ 97–98). Further, 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 25–26. 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. 26–27. As shown in annotated Figure 1A, logical operating architecture 50 includes processor nub loader 52. 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<sub>1</sub>–46<sub>K</sub> (purple) in the isolated execution mode.

We reproduce annotated Figure 1B of Ellison below:

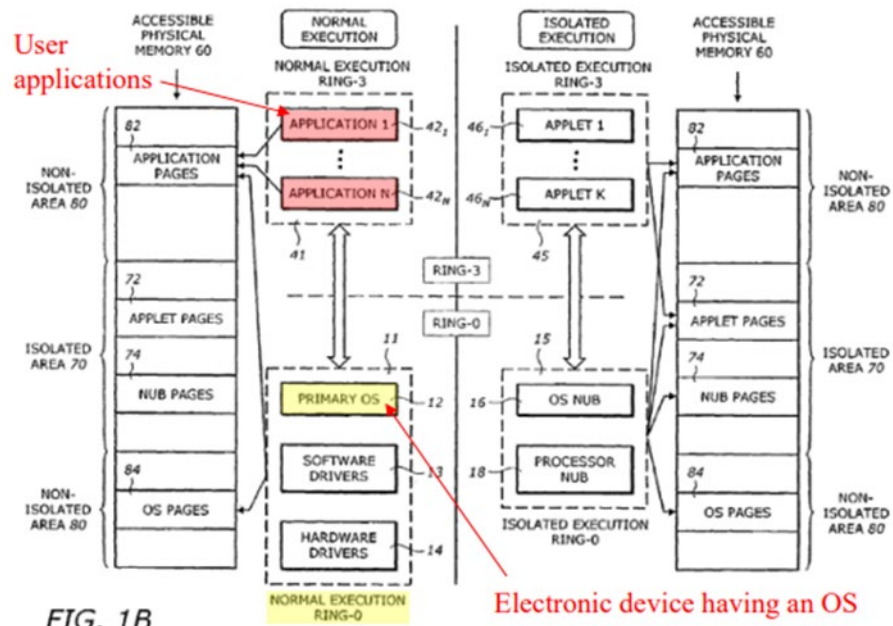


Figure 1B of Ellison, shown above, is a diagram illustrating accessibility of various elements in the Ellison's operating system and processor. Ex. 1006, 1:61–63. Annotated Figure 1B of Ellison in the Petition shows normal execution mode and isolated execution mode side-by-side, wherein primary OS 12 (yellow) is shown interacting with applications 42<sub>1</sub>–42<sub>N</sub> (red) in the normal execution mode. Pet. 28. 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<sub>1</sub>–42<sub>N</sub> which can be executed*

in the normal execution mode and are isolated from components of the isolated execution rings.” *Id.* at 26 (citing Ex. 1006, 3:9–61, 4:1–29, 2:57–61), 28.

Petitioner then contends that Ellison’s electronic device also includes “**authentication software in the form of usage protector 250**, which is part of secure platform 200 in the electronic device (e.g., Muir’s device 256) associated with the first party and **runs within the isolated execution environment** (‘*separate operating environment*’).” Pet. 29 (citing Ex. 1006, 8:25–32, Fig. 2). Petitioner provides annotated Figure 2 of Ellison, shown below, to illustrate its contentions.

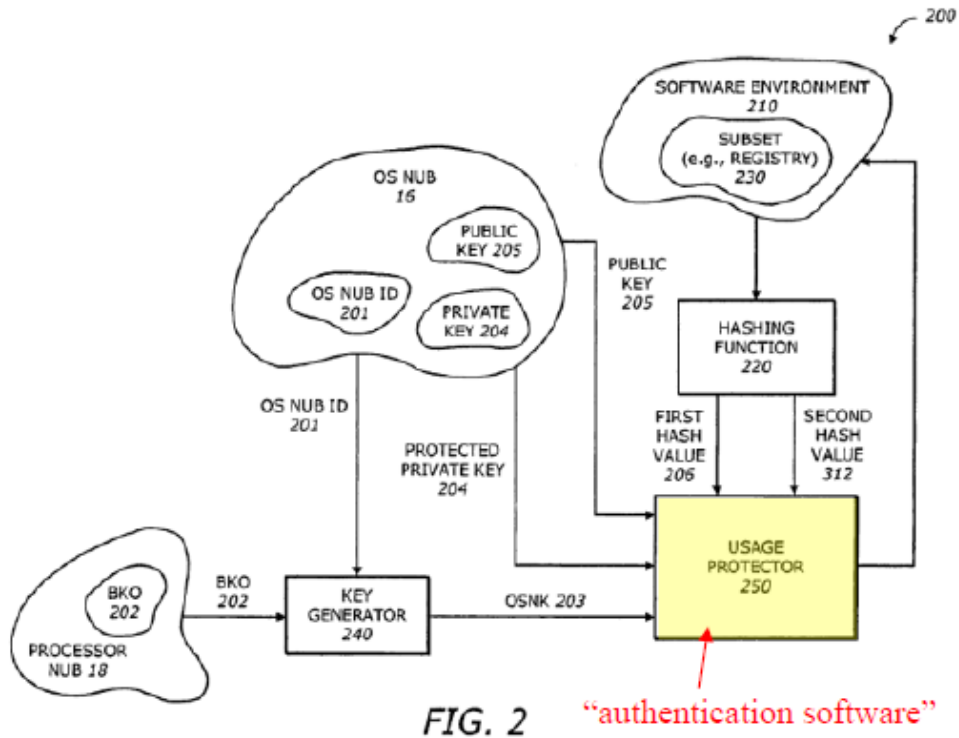


Figure 2 of Ellison, shown above, is a diagram illustrating secure platform 200, which includes OS nub 16, processor nub 18, key generator 240, hashing function 220, and usage protector 250, all operating within the isolated execution environment. Ex. 1006, 8:25–30. Annotated Figure 2 of

Ellison in the Petition, according to Petitioner, illustrates an “usage protector 250” (yellow) that is “run in the isolated execution environment and is independent from and inaccessible to OS 12 (*‘the operating system’*) by virtue of its placement within the isolated execution environment.” Pet. 29 (citing Ex. 1006, 3:9–61, 4:1–29, 4:57–5:27, 8:25–32, Figs. 1A–1B).

Patent Owner contends that “[i]t is clear that Petitioner wrongly equates the ‘primary operating system 12’ of Ellison with ‘operating system’ in the ’766 Patent” and thus “misapprehends that the ‘separate operating environment’, independent from and inaccessible to the ‘operating system.’” PO Resp. 20. In particular, Patent Owner contends that “[a]pplications 42<sub>1</sub>–42<sub>N</sub> and applets 46<sub>1</sub>–46<sub>K</sub> are all user applications,” wherein a POSITA would understand that the counterpart of “user applications” of the ’766 patent includes “applications 42<sub>1</sub>–42<sub>N</sub> and applets 46<sub>1</sub> to 46<sub>K</sub>,” and that the counterpart of “operating system” of the ’766 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 23–24. Thus, 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.* at 24; *see also* PO Sur-reply 1–2 (citing Ex. 1006, 2:62–65, Figs. 1A–C, 2).

Patent Owner acknowledges that “Petitioner relies on Ellison’s usage protector 250 to allegedly disclose authentication software.” PO Resp. 24 (citing Pet. 29). Patent Owner then repeats its contention that “the counterpart of ‘operating system’ of the ’766 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 25. Therefore, according to Patent Owner, “[s]ince the Usage protector 250 is accessible to isolated execution mode of the operating system, the Usage protector 250 is accessible to the operating system,” even though they are inaccessible to normal execution mode of the operating system. *Id.*

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 1. Here, Ellison discloses OS 12, which is a “primary ***operating system.***” Ex. 1006, 3:10–15 (emphasis added). 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.” Pet. Reply 6. That is, claim 1 merely requires an “operating system” for “creating a run-time environment for user applications.”

We also do not agree with Patent Owner that a POSITA would understand that the counterpart of “user applications” of the ’766 patent includes “applications 42<sub>1</sub>–42<sub>N</sub> and applets 46<sub>1</sub> to 46<sub>K</sub>.” PO Resp. 23–24. As Petitioner points out, Patent Owner “concedes that Ellison’s applets 46<sub>1</sub>–46<sub>K</sub> [] are ‘user applications,’” wherein “claim 1 does not recite ‘all user applications’ or any other limitations that require all applets (or even both applets 42<sub>1</sub>–42<sub>K</sub> and applets 46<sub>1</sub>–46<sub>K</sub>) in Ellison’s system to be mapped to the claimed ‘user application.’” Pet. Reply 7.

We agree with Petitioner that Ellison’s Figure 1B “clearly depicts primary OS 12 in the normal execution region,” wherein “Ellison explains that OS 12 interacts with OS pages 84, application pages 82, and applets 42<sub>1</sub>–42<sub>K</sub>, which are user applications in the non-isolated region.” Pet. Reply 6–7 (citing Ex. 1006, 2:57–4:29, Figs. 1A–1B). According to Petitioner, on the other hand, “applets 46<sub>1</sub>–46<sub>K</sub> run 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.” *Id.* at 7 (citing Ex. 1006, 2:57–4:29, Figs. 1A–1B; Ex. 1032 ¶ 16).

We reproduce Figure 1B of Ellison below:

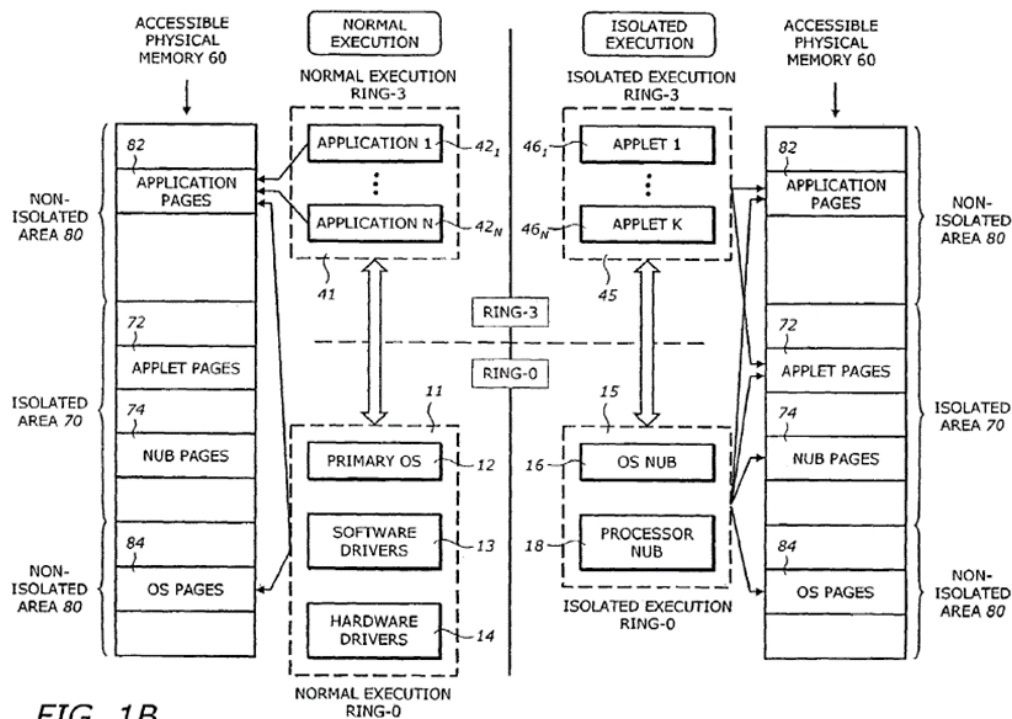


Figure 1B of Ellison shows primary OS 12, software drivers 13, and hardware drivers 14 (bottom left hashed box) interacting (left bidirectional

arrow) with applications 42<sub>1</sub>–42<sub>N</sub> (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<sub>1</sub>–46<sub>N</sub> (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. 29; Pet. Reply 7. 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 7.

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,” wherein a POSITA would understand that “the counterpart of ‘user applications’ of the ’766 Patent includes applications 42<sub>1</sub>–42<sub>N</sub> and applets 46<sub>1</sub> to 46<sub>K</sub>.” PO Resp. 23–24; PO Sur-reply 1–2. Instead, we agree with Petitioner that Ellison discloses an operating system (primary OS 12) creating a run-time environment for user applications (42<sub>1</sub> to 42<sub>N</sub>), as claimed. *See* Ex. 1006, Figs. 1A–1B.

Although Patent Owner contends that Ellison’s usage protector 250 is “accessible to the operating system” because it is “accessible to isolated execution mode of the operating system” (PO Resp. 25), Patent Owner’s contention hinges on its contention that Ellison’s “operating system” includes normal execution mode *and* isolated execution mode. *Id.*

at 23–24. As discussed above, we agree with Petitioner that the claimed “operating system” encompasses Ellison’s primary operating system, OS 12, wherein Ellison “clearly depicts primary OS 12 in the normal execution region,” which interacts with applets 42<sub>1</sub>–42<sub>K</sub> that “are user applications in the non-isolated region.” Pet. Reply 6–7.

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” and “authentication software running in a separate operating environment, independent from and inaccessible to the operating system,” as recited in claim 1, regardless of whether or not the preamble is limiting.<sup>9</sup> Furthermore, 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. 19–24. As Petitioner explains, and as supported by Dr. Black’s testimony, “doing so would have simply involved combining prior

---

<sup>9</sup> 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 using an electronic device, the electronic device having an operating system creating a run-time environment for user applications and authentication software running in a separate operating environment, independent from and inaccessible to the operating system, 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”).

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 24 (citing Ex. 1003 ¶ 72).

- ii. *the method comprising “providing authentication software in the electronic device,” wherein a provided private key is “accessible to said authentication software,” and said “authentication software is stored in the secure memory inaccessible to the operating system” (claim 1)*

As discussed above regarding the preamble, Petitioner contends that “Ellison’s electronic device also includes authentication software in the form of usage protector 250, which is part of secure platform 200 in the electronic device (e.g., Muir’s device 256) associated with the first transaction party,” and which “runs within the isolated execution environment (‘separate operating environment’).” Pet. 29 (citing Ex. 1006, 8:25–32, Fig. 2) (emphasis omitted). According to Petitioner, usage protector 250 “is independent from and inaccessible to OS 12 (‘the operating system’) by virtue of its placement within the isolated execution environment.” *Id.* (citing Ex. 1006, 3:9–61, 4:1–29, 4:47–5:27, 8:25–32, Figs. 1A, 1B; Ex. 1003 ¶ 101) (emphasis omitted). Thus, Petitioner contends that it would have been obvious to a POSITA that “the usage protector 250 would have been stored in secure memory (e.g., isolated area) inaccessible to elements outside of the isolated execution environment, such as OS 12.” *Id.* at 49 (citing Ex. 1003 ¶ 126).

Petitioner then contends that Ellison’s “private key 204 is stored in cryptographic key storage 155 and in a multiple key storage of non-volatile

flash memory 160,” wherein “*[o]nly the OS nub 16 can retrieve and decrypt the encrypted private key* for subsequent use.” Pet. 32 (citing Ex. 1006, 8:33–65, Fig. 1C). According to Petitioner, “Ellison’s 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.* at 32–33 (citing Ex. 1003 ¶ 104). On the other hand, according to Petitioner, “private key 204 is accessible to usage protector 250.” *Id.* at 46 (citing Ex. 1006, 10:1–3, 10:63–12:26, 8:40–65, Fig. 2; Ex. 1003 ¶ 123).

Patent Owner contends “[u]sage protector 250 operates in secure processing environment that is not accessible to the OS 12, but can be accessed by the processor nub 18 and the operating system nub 16 which operate in the isolated execution mode.” PO Resp. 30. That is, according to Patent Owner, “usage protector 250 [is] stored in a secure area accessible to the operating system.” *Id.*

Patent Owner further contends that “Ellison does not teach or suggest authentication software for securing user transactions, but only authentication software to authenticate the code of the secure processing environment (processor nub 18).” PO Resp. 40. According to Patent Owner, “Ellison cannot be combined with Muir’s pointer 171 to restricted memory space 170 without also incorporating Muir’s Virtual Smart Card Driver 155,” wherein “[a]ny combination of Ellison and Muir would require Muir’s Virtual Smart Card Driver 155, which also runs openly accessible to the operating system.” *Id.* at 40–41. Thus, Patent Owner contends that “the authentication software in any combination will be accessible to the

operating system and any request to create a digital signature would come through the primary OS 12 operating with the drive 155 without even touching the isolated execution environment of Ellison.” *Id.* at 41.

Patent Owner’s contention that usage protector 250 is stored in an area accessible to the operating system hinges on its repeated contention that Ellison’s “operating system” includes normal execution mode and isolated execution mode. PO Resp. 23–24. As discussed above, we agree with Petitioner that the claimed “operating system” encompasses Ellison’s primary operating system, OS 12. Pet. Reply 6–7. We agree with Petitioner’s argument, supported by the teachings of Ellison and the testimony of Dr. Black that, “*usage protector 250 is a trusted agent*,” wherein “it would have been obvious to a POSITA that the usage protector 250 would have been stored in secure memory (e.g., isolated area) and would have been inaccessible to elements outside of the isolated execution environment such as OS 12.” Pet. Reply (citing Pet. 49–50; Ex. 1006, 3:15–25, 4:19–22, 8:25–32, 9:2–8; Ex. 1032 ¶ 34).

We also disagree with Patent Owner’s contention that, in the combination of Ellison and Muir, “any request to create a digital signature would come through the primary OS 12 operating with the drive 155,” wherein Patent Owner provides no citation or support for the contention. PO Resp. 41. Instead, we agree with Petitioner that “Ellison’s use of the private key and generation of a digital signature does not involve the OS 12,” and likewise, in the combination of Ellison and Muir, “OS 12 would similarly not be involved.” Pet. Reply 14–15.

In particular, we agree with Petitioner’s argument, supported by Dr. Black’s testimony, that “neither Ellison nor Muir disclose an OS, such as

Ellison's OS 12, having access to a restricted memory space and the private keys." Pet. Reply 15 (citing Ex. 1032 ¶ 30). As discussed above, we agree with Petitioner that, as shown in Figure 1B of Ellison, OS 12 is a distinct and separate entity from isolated execution modules such as OS nub 16, wherein OS nub 16 "operates within the isolated execution area," while "primary OS [12] does not." *See* Tr. 23:23–25; Pet. Reply 7. Further, Muir teaches that "[v]irtual smart card 151 includes virtual smart card driver and memory 140," wherein memory 140 is "a restricted memory space 170 used for storing private keys 167," and "[r]estricted memory space 170 and private key 167 are normally inaccessible to operating system 125 and applications." *See* Ex. 1008, 7, 9, Fig. 6.

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 "authentication software running in a separate environment, independent from and inaccessible to the operating system," wherein a provided private key is "accessible to said authentication software," and said "authentication software is stored in the secure memory inaccessible to said operating system," as recited in claim 1.

- iii. *“a memory comprising storage locations, part of the memory being inaccessible to the operating system, part of the memory being a secure area,” “a system for accessing a memory location in the memory” that is “configured to selectively report the storage locations of the secure area,” wherein the storage locations “are not reported to the operating system while at the same time being reported to the authentication software” (claim 1)*

Petitioner contends that, in the combined system of Ellison and Muir, the electronic device “has a memory comprised of non-volatile memory 160, accessible physical memory 60, in addition to other memory structures such as mass storage device 170, digest memory 154, and cryptographic key storage 155.” Pet. 30 (citing Ex. 1006, 6:44–7:58). According to Petitioner, “[t]he ***non-volatile memory 160 and the accessible physical memory 60*** (which is part of system memory 140) would have been understood by a POSITA to ***include storage locations*** because a memory must include storage locations,” wherein “[a]ccessible physical memory 60 includes an isolated area 70 (***‘part of the memory being a secure area’***) and a non-isolated area 80 (***‘part of the memory being accessible to the operating system’***).” *Id.* (citing Ex. 1006, 4:14–16, 6:1–26; Ex. 1003 ¶ 102).

Further, Petitioner contends that Ellison’s Memory Controller Hub (MCH) 130 “provides control and configuration of memory,” and that “an input/output controller hub (ICH) 150 can be integrated with MCH 130,” which “controls access and connection to non-volatile memory 160,” and “support[s] the isolated execution mode in addition to the traditional I/O functions.” Pet. 35 (citing Ex. 1006, 4:38–56, 5:57–67, 6:27–7:32, Fig. 1C; Ex. 1003 ¶¶ 107–108). Petitioner contends “[b]ecause MCH 130 and ICH 150 control and configure system memory 140 (which includes physical

memory 60 and isolated (memory) area 156/70) and memory 160,” it would have been obvious to a POSITA that Ellison’s MCH 130 and ICH 150 “would have *access to a memory location in the isolated area 70 and the memory 160* and would have been ‘*configured to selectively report the storage locations of the secure area*’ as part of its control and configuration of system memory 140.” *Id.* (citing Ex. 1006, 5:57–6:26; Ex. 1003 ¶ 108).

According to Petitioner, in Ellison, “[r]eporting of the secure locations would have been selective” because “such locations would not have been reported to components (e.g., OS 12) that are not allowed to access the secure locations while being reported to other components (e.g., processor 110 in isolated execution mode 115) with access.” Pet. 35. Further, according to Petitioner, “Muir’s driver 155 ‘includes an address pointer 171 to restricted memory space 170’ that ‘may point to a number of addresses or locations for restricted memory space’” to send data to and retrieve data from restricted memory space 170. *Id.* at 36 (citing Ex. 1008, 13; Ex. 1003 ¶ 109).

Petitioner contends that it would have been obvious to a POSITA that “Ellison’s MCH 130 and ICH 150 would have included an address pointer 171 to selectively report the storage locations of the secure area” when sending and receiving data from the restricted memory spaces such as restriction portion of memory 160 or isolated area 156/70. *Id.* at 37 (citing Ex. 1003 ¶ 110). According to Petitioner, such an address pointer “would have selectively not reported storage locations to the OS 12 and/or addresses in the unrestricted portions of the memory.” *Id.*

Moreover, Petitioner contends that “Ellison’s usage protector 250 (*‘authentication software’*) runs within the isolated execution environment

(‘*separate operating environment*’),” and “performs a number of operations (e.g., encoding, decoding) involving private key 204 and other data that are available in the isolated execution environment and stored in the restricted memory.” Pet. 38–39 (citing Ex. 1006, 8:25–65, 10:4–13:3, Figs. 1C, 2, 3A–3E). Thus, according to Petitioner, to perform such operations, it would have been obvious to a POSITA that “storage locations such as that of the private key 204 that are not reported to the OS 12, would have been reported to usage protector 250” so that usage protector 250 “would be able to perform its operations by obtaining data, such as private key 204, from the reported storage locations.” *Id.* at 39–40 (citing Ex. 1003 ¶ 113).

Patent Owner responds that “neither Ellison nor Muir teach or suggest to selectively report the storage locations of the secure memory,” because “‘hidden’ does not mean the same thing as either ‘inaccessible or ‘restricted.’” PO Resp. 32. According to Patent Owner, even if Muir’s private key is “hidden,” the private key “can still be reported to the operating system,” and thus “the private key can still be accessible.” *Id.* That is, according to Patent Owner, Muir’s memory “marked ‘bad’ can still report to the operating system,” wherein in Muir, “‘storage locations’ are reported to the operating system regardless of whether the operating system is fooled not to access certain storage locations because they are ‘hidden,’ designated ‘restricted,’ or ‘marked as bad.’” *Id.* at 32–33.

Patent Owner contends that, in Muir, “the ‘control and configuration function of system memory 140’ which is volatile cannot be analogized to non-volatile memory to disclose the feature of selective reporting of the storage locations of a secure area,” and thus, a POSITA would not have looked to Muir to cure the deficiencies in Ellison. PO Resp. 33. According

to Patent Owner, “[c]ombining Muir and Ellison would nullify the purpose of Ellison because any request to create a digital signature would come through the primary OS 12 operating with the Virtual Smart Card Driver 155 without even touching the isolated execution environment of Ellison.” *Id.* Moreover, according to Patent Owner, “there is a fundamental difference between Ellison and [the ’766 patent] in terms of goals of the system,” wherein “Ellison excludes transactions by applications to be executed in the isolated execution environment,” while “in [the ’766 patent] the goal is to protect user transactions.” *Id.* at 34–35.

We do not agree with Patent Owner’s argument that neither Ellison nor Muir teach or suggest to selectively report the storage locations of the secure memory, because “‘hidden’ does not mean the same thing as either ‘inaccessible or ‘restricted.’” PO Resp. 32. Muir discloses that OS 125 does not access certain parts of restricted/hidden memory according to their markings. *See, e.g.*, Ex. 1008, 12, 15. That is, in Muir, by marking a part of the memory “bad” or by altering pointers to that hidden part, the OS is restricted from accessing that part of the memory. *Id.* In other words, the OS is fooled into thinking that part of memory is not accessible, and thus, that part of memory is made inaccessible to the OS. *Id.* Thus, we disagree with Patent Owner that being “fooled” from accessing a part of memory would not encompass making that hidden part of memory inaccessible. PO Resp. 32–33.

We agree with Petitioner that, in Ellison, “[r]eporting of the secure locations would have been selective” because “such locations would not have been reported to components (e.g., OS 12) that are not allowed to access the secure locations while being reported to other components (e.g.,

processor 110 in isolated execution mode 115) with access.” Pet. 35. Further, as Petitioner points out, “Muir’s driver 155 ‘includes an address pointer 171 to restricted memory space 170’” to send data to and retrieve data from restricted memory space 170. *Id.* at 36 (citing Ex. 1008, 13; Ex. 1003 ¶ 109). That is, Muir discloses that certain parts of memory are hidden from OS 125. *See* Ex. 1008, 12, 15. Although Patent Owner contends that Muir’s memory “marked ‘bad’ can still report to the operating system,” wherein Muir’s “‘storage locations’ are reported to the operating system regardless of whether the operating system is fooled not to access certain storage locations” (PO Resp. 32–33), we find that, in the combined teachings of Ellison and Muir, “hidden” from OS 125 would not encompass being reported to OS 125.

We also disagree with Patent Owner’s contention a POSITA would not have looked to Muir to cure the deficiencies in Ellison because volatile memory cannot be analogized to non-volatile memory. PO Resp. 33. Patent Owner appears to be contending that it would not have been obvious to a POSITA to bodily incorporate part of the system of Muir into the system of Ellison. *See id.* However, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference. Rather, the test is what the combined teachings of those references would have suggested to those of ordinary skill in the art. *See In re Keller*, 642 F.2d 413, 425 (CCPA 1981).

As Petitioner points out, “Ellison’s isolated execution architecture improves security in a computer system or platform” and “can be applied to systems involving ‘[e]lectronic commerce (E-commerce) and business-to-business (B2B) transactions’” (Pet. 19–20 (citing Ex. 1006, 1:12–15, 1:17–

30, 2:40–61, Fig. 1); whereas “Muir’s computer network includes multiple devices involved in electronic transactions, e.g., e-commerce” (*id.* at 20 (citing Ex. 1008, 1, 9, 11). We agree with Petitioner that “[a] POSITA looking to implement Ellison’s isolated execution architecture in a computer system with multiple devices would have looked to Muir to implement a secure electronic transaction between the two parties.” *Id.* at 21 (citing Ex. 1003 ¶ 67).

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 “a memory comprising storage locations, part of the memory being inaccessible to the operating system, part of the memory being a secure area,” and “a system for accessing a memory location in the memory” that is “configured to selectively report the storage locations of the secure area,” wherein the storage locations “are not reported to the operating system” as recited in claim 1.

*iv. Remaining limitations of claim 1*

Petitioner provides detailed explanations as to how the combination of Ellison and Muir teaches the remaining claim limitations recited in independent claim 1, citing Dr. Black’s testimony for support. Pet. 40–51 (citing Ex. 1006, 2:41–61, 3:9–4:29, 4:57–5:27, 8:33–65, 9:2–8, 10:1–3, 10:63–12:26, Figs. 1A–1C, 2, 3A–3E; Ex. 1008, 2, 3, 6–10, 12, 18; Ex. 1003 ¶¶ 114–130). In particular, Petitioner contends that Ellison’s “isolated execution regions ‘[are] **accessible only to elements of the operating system and processor operating in isolated execution mode,**’” and that “isolated mode applets 46<sub>1</sub> to 46<sub>K</sub> and their data are tamper-resistant and monitor-

resistant from all software attacks from other applets and OS 12.” Pet. 40–41 (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.* at 41 (citing Ex. 1003 ¶ 115).

Petitioner also contends that Ellison’s isolation execution architecture includes an isolated execution region in which “entities, such as OS nub 16 and processor nub 18 operate in a secure environment in an isolated execution mode.” Pet. 40 (citing Ex. 1006, 3:9–25, 2:41–61, Fig. 1B; Ex. 1003 ¶ 114). Petitioner contends that “**protected private key 204 . . . can be stored in the multiple key storage . . . of the non-volatile flash memory 160,**” and “can be []programmed into the fuses of a **cryptographic key storage 155** of the ICH 150 or elsewhere in persistent storage within platform 200.” *Id.* at 42 (citing Ex. 1006, 8:33–65, Fig. 1C; Ex. 1003 ¶ 117). According to Petitioner, because “the OS nub 16 is within the secure platform and isolated environment,” it would have been obvious to a POSITA that “the cryptographic key storage 155 and the non-volatile flash memory 160 include secure storage locations so that the private key 204 can be accessed securely by OS nub 16.” *Id.* at 43–44 (citing Ex. 1003 ¶ 119).

According to Petitioner, “Ellison’s 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.” Pet. 44. Nevertheless, Petitioner contends that Muir teaches “**a private key 167 being stored in a restricted memory space 170 which is inaccessible to the operating system.**” *Id.* (citing Ex. 1008, 7–9, 3).

Patent Owner does not present arguments in the Patent Owner Response addressing the specific merits of Petitioner's contentions with respect to these claim limitations. *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).

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 and a person of ordinary skill in the art would have been motivated to combine the references' teachings to arrive at the method of claim 1 with a reasonable expectation of success. 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. Claims 3, 4, 8, 9, 13, and 21–33 Allegedly Obvious Over Ellison and Muir*

Petitioner provides detailed explanations as to how the combination of Ellison and Muir renders the limitations recited in claims 3, 4, 8, 9, 13, and 21–33 obvious, citing Dr. Black's testimony for support. Pet. 51–74 (citing Ex. 1006, 1:58–67, 3:1–9:40, 10:9–13:3, Figs. 1A–1C, 2, 3A–3E; Ex. 1008, 7–9, 11, Fig. 5; Ex. 1003 ¶¶ 131–134, 139–146, 157–93).

In particular, as to claim 3, Petitioner contends that Ellison's "signature algorithm used by signature generator 320 may be [a] public-key digital signature algorithm," wherein, "based on Ellison's disclosure of using public DSA, it would have been obvious to a POSITA that the second

transaction device would have received the digital signature from the first transaction party,” and that “the first transaction party device’s public key . . . would have been stored at the second transaction party device.” Pet. 51–52. As to claim 8, Petitioner contends that when Ellison’s system obtains private key 204 for perform operations, “the private key have to be provided to ICH 150,” wherein “a POSITA would have understood that ICH 150 and MCH 130 correspond to a BIOS.” *Id.* at 54–55. As to claim 9, 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 56–57. As for claim 13, Petitioner contends that Muir’s Figure 3C “illustrates usage protector 250, which includes a decryptor 325, a signature generator 320, a storage medium 322, and a signature verifier 330,” wherein “*decryptor 325 accepts the OS numb’s encrypted private key (i.e., protected) 204, and decrypts it* using the OSNK 203.” *Id.* at 58–59 (citing Ex. 1006, 10:63–11:30, Fig. 3C)

As to claims 21–23, Petitioner contends that “Muir’s electronic device 256 is adapted to be connected to the second transaction party over a network 255,” and that “the second transaction party in the electronic transaction can be server 258,” wherein it would have been obvious to a POSITA “that server 258 would have been used to perform operations such as facilitating logging in of client devices, such as PDA 256, into the networking environment 250.” Pet. 59–62. As to claim 24, Petitioner contends that a POSITA would have understood that Ellison’s “OSNK 23 is a private (encryption) key and is not shared with another party.” *Id.*

at 63–65. Petitioner repeats its contention with respect to the preamble of claim 1 for limitations similarly recited in claim 25. *Id.* at 65 (citing Ex. 1003 ¶ 167). As to claim 26, Petitioner contends that “Ellison’s system 100 is a ‘system for controlling instructions and data flowing between hardware components of the electronic device,’” wherein it would have been obvious to a POSITA that, “when processing and controlling the data, OS 12 is also controlling instructions for current or subsequently processing or storage of the data.” *Id.* at 67–69. Petitioner repeats its contention with respect to claim 8 for limitations similarly recited in claim 27. *Id.* at 69 (citing Ex. 1003 ¶ 173). As to claim 28, Petitioner contends that a POSITA would have understood that “Ellison’s isolated execution environment serves as a console.” *Id.* at 69–72.

Petitioner repeats its contention with respect to claim 1 for limitations similarly recited in independent claims 29 and 33. Pet. 72–74 (citing Ex. 1003 ¶¶ 178–185, 189–193). Petitioner then repeats its contention with respect to claims 21–23 for limitations similarly recited in claims 30–32, respectively. *Id.* at 73 (citing Ex. 1003 ¶¶ 186–188).

Patent Owner does not address separately these explanations and supporting evidence by Petitioner regarding claims 3, 4, 8, 9, 13, and 21–33. *See generally* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Based on the complete record presented, we determine that Petitioner has demonstrated that claim 3, 4, 8, 9, 13, and 21–33 would have been obvious over the combination of Ellison and Muir.

- vii. *Claims 10 and 12 Allegedly Obvious Over Ellison, Muir, and Al-Salqan; Claim 11 Allegedly Obvious Over Ellison, Muir, Al-Salqan and Searle; Claim 5 Allegedly Obvious Over Ellison, Muir, and Epstein*

Petitioner provides detailed explanations as to: how the combination of Ellison, Muir and Al-Salqan renders the limitations recited in claims 10 and 12 obvious; how the combination of Ellison, Muir, Al-Salqan and Searle renders the limitations recited in claim 11 obvious; and how the combination of Ellison, Muir and Epstein renders the limitations recited in claim 5 obvious, citing Dr. Black’s testimony for support. *See* Pet. 74–97 (citing Ex. 1006, 6:60–67, 8:33–65, 11:1–12:26, Figs. 2, 3C–3D; Ex. 1007, 1:21–2:63, 4:4–6:27, Fig. 2–3; Ex. 1009, 2:13–40, 3:66–4:11, 4:48–5:28, 5:65–6:27, Figs. 1–2; Ex. 1030, 1:8–11, 2:4–66, 3:43–5:8, 5:50–6:6, Fig. 2; Ex. 1003 ¶¶ 73–96, 136–138, 147–153). In particular, as to claims 10 and 12, Petitioner contends that “Al-Salqan discloses a decryption method that uses an asymmetric decryptor 314 and symmetric decryptor 330 to remove [] two layers 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 74–81.

As to claim 11, 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. 82–90. As to claim 5, Petitioner contends that “Epstein discloses ‘a method for securely distributing private keys’ to address security vulnerabilities in the generation of public/private keys,”

wherein a POSITA would have combined Epstein’s private key generation with Ellison and Muir for “generating or obtaining private keys in a secure manner in a network.” *Id.* at 90–97.

Patent Owner does not address separately these explanations and supporting evidence by Petitioner regarding claims 5 and 10–12. *See generally* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Based on the complete record presented, we determine that Petitioner has demonstrated that claims 10 and 12 would have been obvious over the combination of Ellison, Muir and Al-Salqan, that claim 11 would have been obvious over the combination of Ellison, Muir, Al-Salqan and Searle, and that claim 5 would have been obvious over the combination of Ellison, Muir and Epstein.

### III. CONCLUSION<sup>10</sup>

For the foregoing reasons, we determine on the record at hand that Petitioner has demonstrated by a preponderance of the evidence that the challenged claims of the ’766 patent are unpatentable.

---

<sup>10</sup> 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).

In summary:

| <b>Claims</b>                  | <b>35<br/>U.S.C.<br/>§</b> | <b>Reference(s)/Basis</b>   | <b>Claims<br/>Shown<br/>Unpatentable</b> | <b>Claims<br/>Not Shown<br/>Unpatentable</b> |
|--------------------------------|----------------------------|-----------------------------|------------------------------------------|----------------------------------------------|
| 1, 3, 4, 8,<br>9, 13,<br>21–33 | 103                        | Ellison, Muir               | 1, 3, 4, 8, 9,<br>13,<br>21–33           |                                              |
| 10, 12                         | 103                        | Ellison, Muir,<br>Al-Salqan | 10, 12                                   |                                              |
| 11                             | 103                        | Ellison, Muir,<br>Searle    | 11                                       |                                              |
| 5                              | 103                        | Ellison, Muir,<br>Epstein   | 5                                        |                                              |
| <b>Overall<br/>Outcome</b>     |                            |                             | 1, 3–5, 8–13,<br>21–33                   |                                              |

#### IV. ORDER

For the reasons given, it is

ORDERED that, based on the preponderance of the evidence, claims 1, 3–5, 8–13, and 21–33 of the '766 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.

IPR2022-00114  
Patent 11,063,766 B2

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

William M. Fink  
Marc J. Pensabene  
Benjamin M. Haber  
O'MELVENY & MYERS LLP  
tfink@omm.com  
mpensabene@omm.com  
bhaber@omm.com

For PATENT OWNER:

William P. Ramey, III  
Jacob Henry  
RAMEY LLP  
wramey@rameyfirm.com  
jhenry@rameyfirm.com