

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

RFCYBER CORP.,
Patent Owner.

IPR2022-00412
Patent 9,189,787 B1

Before KEVIN F. TURNER, PATRICK R. SCANLON, and
KEVIN W. CHERRY, *Administrative Patent Judges*.

SCANLON, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining No Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

Apple Inc. (“Petitioner”) challenges claims 1–19 of U.S. Patent No. 9,189,787 B1 (Ex. 1001, “the ’787 patent”). We have jurisdiction under 35 U.S.C. § 6, and this Final Written Decision is issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons that follow, we determine that Petitioner has not shown by a preponderance of the evidence that claims 1–19 of the ’787 patent are unpatentable.

A. Procedural History

Apple Inc. filed a Petition (Paper 1, “Pet.”) requesting an *inter partes* review of the challenged claims. Petitioner also filed a Motion for Joinder to IPR2021-00980. Paper 3. Petitioner indicated that its Petition is substantially identical to the petition in IPR2021-00980.¹ Pet. 5. RFCyber Corp. (“Patent Owner”) filed a Preliminary Response. Paper 9.

We instituted a trial as to all challenged claims. Paper 11 (“Decision on Institution” or “Dec. Inst.”). Because IPR2021-00980 had been terminated prior to our Decision on Institution, we dismissed Petitioner’s motion to join that proceeding as moot. Dec. Inst. 2 n.1.

After institution, Patent Owner filed a Patent Owner Response (Paper 15, “PO Resp.”), Petitioner filed a Reply (Paper 18, “Reply”), and Patent Owner filed a Sur-reply (Paper 23, “Sur-reply”).

Petitioner relies on the Declaration of Gerald W. Smith (Ex. 1003) and the Supplemental Declaration of Gerald W. Smith (Ex. 1042) in support of its contentions. Patent Owner relies on the Declaration of Miguel Gomez (Ex. 2007) in support of its contentions.

¹ The Petition actually refers to the petition in IPR2021-00981, but this appears to be a typographical error.

An oral hearing was held on April 21, 2023. A transcript of the hearing is included in the record. Paper 29 (“Tr.”).

B. Real Parties in Interest

Petitioner identifies itself as the real party in interest. Pet. 2. Patent Owner identifies itself as its real party in interest. Paper 6, 1.

C. Related Matters

The parties identify the following district-court proceedings as related matters involving the ’787 patent: *RFCyber Corp. v. Apple, Inc.*, No. 6:21-cv-00916 (W.D. Tex.); *RFCyber Corp. v. Google LLC*, No. 2:20-cv-00274 (EDTX); *RFCyber Corp. v. LG Electronics, Inc.*, No. 2:20-cv-00336 (EDTX); and *RFCyber Corp. v. Samsung Electronics Co.*, 2:20-cv-00335 (EDTX). Pet. 3; Paper 6, 1 (Patent Owner’s Mandatory Notices).

Petitioner also identifies the following Board proceeding involving the same parties and a related patent: PGR2022-00003 (U.S. Patent No. 10,600,046 B2 (“the ’046 patent”)) (institution denied March 24, 2022). Pet. 4. The parties also identify the following Board proceedings involving the ’787 patent or related patents, filed by Samsung Electronics America, Inc. et al.: IPR2021-00978 (U.S. Patent No. 8,448,855 B1 (“the ’855 patent”)) (institution denied December 14, 2021); IPR2021-00979 (U.S. Patent No. 8,118,218 B2 (“the ’218 patent”)) (institution denied December 14, 2021); IPR2021-00980 (the ’787 patent) (terminated April 11, 2022); and IPR2021-00981 (U.S. Patent No. 9,240,009 B2 (“the ’009 patent”)) (terminated April 11, 2022). Pet. 4; Paper 6, 1. Petitioner also identifies the following Board proceedings involving the ’787 patent or related patents, filed by Google LLC: IPR2021-00954 (the ’855 patent) (terminated October 20, 2021); IPR2021-00955 (the ’787 patent) (terminated October 20, 2021); IPR2021-00956 (the ’009 patent) (terminated October

20, 2021); IPR2021-00957 (the '218 patent) (terminated October 20, 2021); PGR2021-00028 (the '046 patent) (terminated March 25, 2022); and PGR2021-00029 (the '046 patent) (terminated November 16, 2021). Pet. 3.

D. The '787 Patent

The '787 patent relates to commerce over networks, and more specifically, to a method and apparatus for funding an electronic purse (“e-purse”) for use in portable devices configured for both electronic commerce (“e-commerce”) and mobile commerce (“m-commerce”). Ex. 1001, code (57), 1:15–19.

The '787 patent states that there is a “need for a mechanism in devices, especially portable devices, functioning as an electronic purse (e-purse) to be able to conduct transactions over an open network with a payment server without compromising security.” *Id.* at 1:44–48. Although closed systems—such as smart card technology—existed, they were “difficult to be expanded into other areas such as e-commerce and m-commerce” because “stored values and transaction information are stored in data storage of each tag that is protected by a set of keys,” which keys must be “delivered to the card for authentication before data can be accessed during a transaction.” *Id.* at 1:33–39. According to the '787 patent, this required delivery of keys “makes systems using such technology difficult to be expanded to an open environment such as the Internet for e-commerce and cellular networks for m-commerce as the key delivery over a public domain network causes security concerns.” *Id.* at 1:39–43. The '787 patent purports to overcome the limitations of the prior art by providing a system for funding an e-purse stored on a portable device. The e-purse allows for transactions “over an open network with a payment server without compromising security.” *Id.* at 1:60–64.

Figure 2, reproduced below, provides a schematic view of one embodiment of the '787 patent.

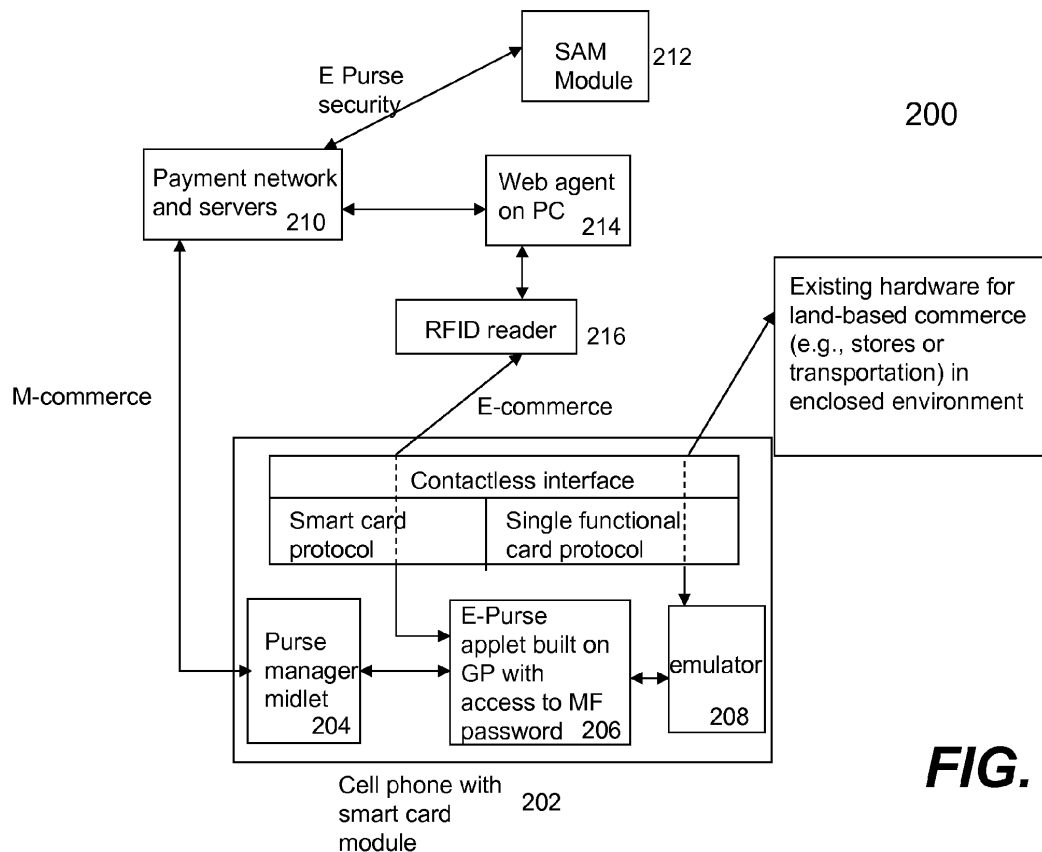


FIG. 2

Figure 2 shows an exemplary architecture diagram 200 according to one embodiment of the '787 patent. Ex. 1001, 3:6–7.

As shown in Figure 2, a portable device is pre-loaded with smart card module 202 comprising emulator 208, e-purse applet 206, and purse manager midlet 204. *Id.* at 5:1–48. The portable device may be a cellphone that is “near field communication (NFC) enabled” and includes an RFID interface “that allows the cellphone to act as a tag.” *Id.* at 5:4–10.

Purse management midlet 204 “is a software component” that “acts as an agent to facilitate communications between an e-purse applet 206 and one or more payment network and servers 210 to conduct transactions.” *Id.* at 5:16–20. E-purse applet 206 is built on a global platform and “acts as a

gatekeeper to regulate or control the data exchange.” *Id.* at 4:55–57, 5:11–13. Emulator 208 is “a hardware device or a program that pretends to be another particular device or program that other components expect to interact with.” *Id.* at 4:47–50.

In one embodiment of the ’787 patent, a user may fund the e-purse from a bank account by a process conducted via the m-commerce path shown in Figure 2. *Id.* at 7:22–30. Figure 4C, reproduced below, “shows an exemplary block diagram 450 of related blocks interacting with each other to achieve the process” of funding the e-purse. *Id.* at 7:26–28.

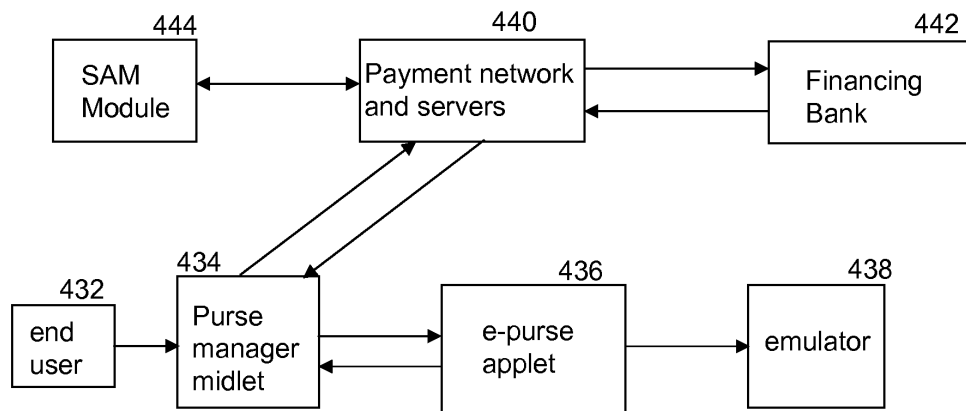


Figure 4C “shows an exemplary block diagram of related blocks interacting with each other to achieve the process” of financing an e-purse according to one embodiment of the ’787 patent. Ex. 1001, 3:21–23.

End user 432 enters a personal identification number (PIN), which, if valid, activates purse manager midlet 434. *Id.* at 7:34–37. The purse manager midlet “communicates with the e-purse applet 436 for a response that is then sent to the payment network and server 440.” *Id.* at 7:44–47. Payment network and server 440 “verifies that the response is from an authorized e-purse originally issued therefrom with a SAM module 444.” *Id.* at 8:1–4. “After the response is verified, the payment network and server 440 sends a request to the [user’s] financing bank 442.” *Id.* at 8:4–7. Upon

receiving authorization from the financing bank, “the server 440 will either reject the request or form a network response to be sent to the midlet 434.” *Id.* at 8:9–12. “The e-purse verifies the authenticity (e.g., in APDU format) and sends commands to the emulator 438 and updates the transaction logs.” *Id.* at 8:13–15. According to the ’787 patent, “[b]y now, the e-purse finishes the necessary steps and returns a response to the midlet 434 that forwards an (APDU) response in a network request to the payment server 440.” *Id.* at 8:15–18.

E. Challenged Claims

As noted above, Petitioner challenges claims 1–19 of the ’787 patent. Pet. 6–7. Of the challenged claims, claims 1 and 11 are independent. Ex. 1001, 8:49–9:4, 9:49–10:14. Claim 1, reproduced below, is illustrative of the subject matter recited in the challenged claims (bracketing added).

1. **[PREAMBLE]** A portable device for commerce, the portable device comprising:

[1a] an emulator loaded in a smart card module for storing security values and updated transaction logs, and **[1b]** an e-purse applet to cause the portable device to function as an electronic purse (e-purse), **[1c]** wherein both of the emulator and e-purse applet are already personalized via a personalization process built on a first security channel so that the emulator is set to store a set of keys for subsequent data access authentication and the e-purse applet is configured to conduct a transaction with a network server over a second security channel;

[1d] a first interface configured to perform field communication (NFC) with a reader to perform electronic commerce with the e-purse applet against a fund stored in the emulator;

[1e] a second interface configured to perform mobile commerce with a payment server via an application against the fund stored in the emulator, and

[1f] a purse manager midlet being executed in the portable device to act as an agent to facilitate communications between the e-purse applet and a payment server to conduct transactions therebetween.

Ex. 1001, 8:49–9:4.

F. Instituted Ground of Unpatentability

We instituted *inter partes* review of the challenged claims based on the following ground of unpatentability asserted by Petitioner:

Claims Challenged	35 U.S.C. §	References
1–19	103 ²	Dua, ³ GlobalPlatform, ⁴ Philips ⁵

Dec. Inst. 35; Pet. 6–7.

II. ANALYSIS

A. Legal Standards

To prevail in its challenge, Petitioner must demonstrate by a preponderance of the evidence that the claims are unpatentable. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d) (2020). “In an IPR, the petitioner has the burden from the onset to show with particularity why the patent it challenges

² The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), amended 35 U.S.C. § 103. The ’787 patent claims benefit of a September 24, 2006, filing date, which is before the effective date of the applicable AIA amendments. Ex. 1001, code (63). Petitioner does not contest the ’787 patent’s priority date. Pet. 7. Thus, we refer to the pre-AIA version of 35 U.S.C. § 103.

³ US 2006/0165060 A1, published July 27, 2006 (Ex. 1004).

⁴ GlobalPlatform, Card Specification, Version 2.1.1, March 2003, (Ex. 1006).

⁵ Philips Semiconductors SmartMX, P5CT072, Secure Dual Interface PKI Smart Card Controller, Rev. 1.3, Oct. 4, 2004 (Ex. 1012).

is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (2012) (requiring *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)). This burden of persuasion never shifts to the patent owner. See *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (discussing the burden of proof in *inter partes* review).

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) when in evidence, objective indicia of non-obviousness (also called secondary considerations), such as commercial success, long-felt but unsolved needs, and failure of others. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). We analyze grounds based on obviousness in accordance with the above-stated principles.⁶

B. Level of Ordinary Skill in the Art

In determining whether an invention would have been obvious at the time it was made, 35 U.S.C. § 103 requires us to resolve the level of ordinary skill in the pertinent art at the time of the effective filing date of the

⁶ The record does not include any evidence of objective indicia of non-obviousness.

claimed invention. *Graham*, 383 U.S. at 17. The person of ordinary skill in the art is a hypothetical person who is presumed to have known the relevant art. *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995). Factors that may be considered in determining the level of ordinary skill in the art include, but are not limited to, the types of problems encountered in the art, the sophistication of the technology, and educational level of active workers in the field. *Id.* In a given case, one or more factors may predominate. *Id.*

Petitioner contends that an ordinarily skilled artisan for the '787 patent “would have been knowledgeable regarding mobile payment methods and systems pertinent to the '787 patent.” Pet. 11 (citing Ex. 1003 ¶¶ 27–28). Petitioner also contends that an ordinarily skilled artisan “would have had at least a bachelor’s degrees [sic] in computer science, computer engineering, electrical engineering or an equivalent, and one year of professional experience relating to mobile payment technology,” and that “[l]ack of professional experience could be remedied by additional education, and vice versa.” *Id.* (citing Ex. 1003 ¶¶ 27–28).

Patent Owner argues that “[a] person of ordinary skill in the art would have had a Bachelor’s degree in Computer Science, Computer Engineering, or Applied Mathematics, with 2 or more years of academic or industry experience in computer security, network security or mobile payment technology.” PO Resp. 10 (citing Ex. 2007 ¶¶ 32–33).

In its Reply, Petitioner argues that, although Patent Owner did not dispute Petitioner’s proposed level of ordinary skill in its Preliminary Response, the Patent Owner Response “quietly removes a requirement for mobile payment experience,” but “does not acknowledge this definition shift, nor does it provide any justification for removing this key requirement.” Reply 2–3 (citing PO Resp. 10). Relying on the declaration

testimony of Mr. Smith, Petitioner contends that mobile payment experience is required. *Id.* at 3 (citing Ex. 1042 ¶¶ 4–10). According to Petitioner, Patent Owner is seeking to redefine the ordinary skill in the art because its expert, Mr. Gomez, is “an unqualified declarant who [has] admitted he has no specific mobile payment technology experience, no experience with e-purses, no experience with the relevant protocols, and no educational experience to remedy his professional deficiencies.” *Id.* (citing Ex. 1041, 8:11–19, 9:7–20:4, 37:8–39:9, 50:15–51:18). Petitioner also contends that the Board should accord Mr. Gomez’s unqualified testimony little to no weight. *Id.* (citing *Best Med. Int. ’l, Inc. v. Elekta Inc.*, 46 F.4th 1346, 1353–54 (Fed. Cir. 2022)).

The fact that Patent Owner did not dispute Petitioner’s proposed level of ordinary skill in its Preliminary Response does not preclude Patent Owner from disputing the proposed definition at trial. Nevertheless, we agree with Petitioner that the Patent Owner Response fails to provide a sufficient basis for the proposed level of ordinary skill. *See* Reply 2–3. Indeed, the Patent Owner Response provides no explanation in support of the proposed definition. *See* PO Resp. 10. Nor does Mr. Gomez adequately support his opinion, which merely repeats the proposed level of ordinary skill from the Patent Owner Response, without objective evidence or analysis. *See* Ex. 2007 ¶¶ 32–33.

Patent Owner, however, argues in its Sur-reply that its proposed level of ordinary skill is correct because, unlike Petitioner’s proposal, it addresses claimed features such as “storing security values,” “security channel[s],” and “a set of keys.” Sur-reply 3. Patent Owner also argues that the ’787 patent “highlights ‘a mechanism . . . to enable a portable device to conduct transactions . . . *without compromising security*’” and shows a “three-tier

security model based on which the present invention is contemplated.” *Id.* (citing Ex. 1001, code (57), 3:1–3) (alterations in original). In contrast, Patent Owner argues that “Petitioner seeks to limit the field of relevant experience *exclusively* to ‘mobile payment technology,’” and ignores claim limitations relating to computer or network security. *Id.* at 3–4 (citing Reply 2–3); *see also* Tr. 34:2–4 (arguing that Petitioner’s proposed level of ordinary skill “ignores security and requires only mobile payments”).

On the full record before us, we agree with Petitioner that a person of ordinary skill in the art should have some level of experience relating to mobile payment technology. For example, the title of the ’787 patent, “Method and Apparatus for Conducting E-commerce and M-commerce,” provides a strong indication that mobile payments are a key aspect of the disclosed invention. *See* Ex. 1001, code (54). The ’787 patent describes its technical field as: “The present invention is generally related to commerce over networks. Particularly, the present invention is related to electronic purses that can be advantageously used in portable devices configured for both electronic commerce (a.k.a., e-commerce) and mobile commerce (a.k.a., m-commerce),” which reinforces that mobile payment technology is a key aspect. *See id.* at 1:17–21. In addition, we credit Mr. Smith’s uncontroverted testimony that mobile payment experience is required, which we find persuasive and supported by evidence. *See* Ex. 1042 ¶¶ 4–10.

On the other hand, we agree with Patent Owner that network security is an important aspect of the ’787 patent’s invention. But to the extent that Patent Owner is asserting that mobile payment technology and computer or network security are distinct concepts such that the proper level of ordinary skill would include experience in one or the other but not both, we disagree. Rather, we view the ’787 patent as relating to methods and apparatuses for

conducting e-commerce and m-commerce (*see, e.g.*, Ex. 1001, code (54), 1:17–21) and describing security as being an *aspect* of the commerce (*see id.* at code (57) (“[A] mechanism is provided to enable a portable device to conduct transactions over an open network with a payment server without compromising security.”), 2:16–19 (“During a transaction, the security keys are used to establish a secured channel between an embedded e-purse and an SAM (Security Authentication Module) or backend server.”)).

For the above reasons, we find Petitioner’s contentions on this issue more persuasive on the full record before us. In order to avoid any doubt that we consider computer or network security to be an element of mobile payment technology, we determine for the purposes of this Decision that one of ordinary skill in the art would have at least a Bachelor’s degree in computer science, computer engineering, electrical engineering or an equivalent, and one year of professional experience relating to mobile payment technology, including computer or network security. In addition, a lack of professional experience could be remedied by additional education, and vice versa.

Regarding Petitioner’s assertion that Mr. Gomez’s testimony should be given little to no weight, Patent Owner argues that Mr. Gomez is well qualified under both proposed levels of ordinary skill. Sur-reply 4–5. During the hearing, Petitioner modified its position somewhat, arguing that Mr. Gomez’s “testimony should be accorded little to no weight, *particularly where he weighs in on issues specific to financial transactions and smart cards.*” Tr. 8:15–18 (emphasis added). Petitioner stated further that “[w]e’re simply asking the Board to take into the account each individual expert’s background knowledge on a per issue basis.” *Id.* at 59:26–60:2. Based on the full record, we disagree that *all* of Mr. Gomez’s testimony

should be given little to no weight. When considering any expert testimony, we take into account the declarant's background knowledge on a per issue basis.

C. Claim Construction

In *inter partes* reviews, the Board interprets claim language using the district-court-type standard, as described in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). *See* 37 C.F.R. § 42.100(b). Under that standard, we generally give claim terms their ordinary and customary meaning, as would be understood by a person of ordinary skill in the art at the time of the invention, in light of the language of the claims, the specification, and the prosecution history. *See Phillips*, 415 F.3d at 1313–14. Although extrinsic evidence, when available, may also be useful when construing claim terms under this standard, extrinsic evidence should be considered in the context of the intrinsic evidence. *See id.* at 1317–19.

Petitioner contends that all claim terms, except “emulator” and “midlet,” should have their plain and ordinary meaning. Pet. 12. As to the claim terms “emulator” and “midlet,” Petitioner contends that the ’787 patent expressly defines those terms “so those definitions are controlling.” *Id.* (citing Ex. 1001, 4:47–50, 5:20–22). Patent Owner argues that “claim construction is not required to resolve any issues” in this proceeding. PO Resp. 9.

We determine that we need not expressly construe any claim term to resolve the parties’ disputes because doing so would have no effect on the analysis below. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017); *see also 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)).

D. Asserted Obviousness Based on Dua, GlobalPlatform, and Philips

Petitioner asserts that claims 1–19 of the ’787 patent are unpatentable under 35 U.S.C. § 103(a) based on Dua, GlobalPlatform, and Philips. Pet. 15–57. Patent Owner provides arguments addressing this asserted ground of unpatentability. PO Resp. 10–35. We first summarize the references and then address the parties’ contentions.

1. Dua (Ex. 1004)

Dua is a published U.S. patent application entitled “Method and Apparatus for Managing Credentials Through a Wireless Network.” Ex. 1004, code (54). Dua discloses a “system and methodology for conducting financial and other transactions using a wireless device.” *Id.* at code (57). Dua’s wireless device includes a “wallet application” that receives, stores, manages, and transmits multiple payment, identification, and other confidential information electronically. *Id.* ¶ 41. Card issuers like banks or merchants can develop custom “extensions” which are installed in the wallet application and stored in an embedded smart card. *Id.* ¶¶ 289, 295. One example of an extension is a stored-value card extension for paying subway fare. *Id.* ¶¶ 290, 293. The stored value card extension “need[s] to be programmed” to support “over-the-air reload,” i.e., wireless funding of the e-purse. *Id.* ¶ 293.

2. GlobalPlatform (Ex. 1006)

GlobalPlatform Card Specification version 2.1.1 describes the “[s]pecifications that shall be implemented on GlobalPlatform smart cards.” Ex. 1006, 16. GlobalPlatform describes its own security architecture and commands for use in installing and personalizing applications on

GlobalPlatform cards. Ex. 1006, 65–67, 88–90. GlobalPlatform is a “hardware-neutral,” “vendor-neutral,” and “Application independent” “chip card standard,” which “provides a common security and card management architecture.” Ex. 1006, 16; Ex. 1008, 290. “GlobalPlatform is intended to run on top of any secure, multi-application card runtime environment” including Java Card. Ex. 1006, 16 (§1), 29 (§3.1). GlobalPlatform specifies the card architecture, security architecture, Life Cycle models for smart cards and their Applications, the Card Manager, Security Domains for key management, and establishing Secure Channels. Ex. 1003 ¶¶ 66–78. GlobalPlatform describes sequences of commands for installing, personalizing, and deleting applications on multi-application smart cards. Ex. 1006, 65–67, 88–90.

3. Philips (Ex. 1012)

Philips is a short form specification describing a Secure PKI Smart Card Controller for the SmartMX (Memory eXtension) multiple interface option platform, which is identified as the P5CT072 device. Ex. 1012, 1. The Smart Card Controller can be used as data memory and program memory. *Id.* The interface technology is well established in all products of the MIFARE interface platform. *Id.* at 2. “Compatibility with existing MIFARE® reader infrastructure and the optional free of charge emulation modes of MIFARE® 1K and MIFARE® 4K enable fast system integration and backward compatibility of standard MIFARE® and ProX family based cards.” *Id.*

4. Independent Claims 1 and 11

Petitioner contends that the combination of Dua, GlobalPlatform, and Philips discloses each limitation of independent claims 1 and 11. Pet. 19–46. To support its arguments, Petitioner identifies certain passages in the

cited references and explains the significance of each passage with respect to the corresponding claim limitation. *Id.* At a high level, Petitioner maps Dua’s wireless devices to the portable device of claim 1, Dua’s “wallet application” to the midlet, Dua’s secure value card extension (“SVCE”) to the e-purse applet, Dua’s Wireless Credential Manager (“WCM”) to the e-purse SAM, and Philips’s MIFARE emulator to the claimed emulator. *Id.* at 19. Petitioner also articulates reasons to combine the relied-upon aspects of Dua, GlobalPlatform, and Philips. *Id.* at 15–19. Specifically, Petitioner asserts that it would have been obvious to one of ordinary skill in the art “to use GlobalPlatform with Dua’s smart cards, wallet application, and extensions” (*id.* at 17 (citing Ex. 1003 ¶ 17)), and “to use a Philips smart card in Dua’s wireless device” (*id.* at 18–19 (citing Ex. 1003 ¶¶ 108–112, 122–125)).

Claim 1 recites the limitation (limitation [1c]):

wherein both of the emulator and e-purse applet are already personalized via a personalization process built on a first security channel so that the emulator is set to store a set of keys for subsequent data access authentication and the e-purse applet is configured to conduct a transaction with a network server over a second security channel.

Similarly, claim 11 recites the limitation (limitation [11c]):

personalizing the emulator and the e-purse applet via a personalization process built on a first security channel so that the emulator is set to store a set of keys for subsequent data access authentication and the e-purse applet is configured to conduct a transaction with a network server over a second security channel

We focus our analysis on these related limitations because they are dispositive as to claims 1 and 11.

Regarding limitation [1c], Petitioner contends that “well before the ’787 patent, ‘personalizing’ smart card applications was ubiquitous and well-known to” an ordinarily skilled artisan, *id.* at 23 (citing Ex. 1006, 88–89; Ex. 1008, 598, Fig. 10.1; Ex. 1001, 4:22–32, 4:52–57, 5:61–63), and that an ordinarily skilled artisan would have known that the personalization process “involves, *inter alia*, creating cryptographic keys to ensure secure communication,” *id.* (citing Pet. 1–2). Petitioner also contends that, in any event, “Dua in view of GlobalPlatform and Philips disclose and render obvious this limitation in two different ways.” *Id.*

As to the “first way,” Petitioner contends that “[i]t is obvious to use GlobalPlatform with Dua’s smart cards and extensions (e.g., SVCEs),” and “[t]o install and use Dua’s SVCE in a smart card, the extension must be paired with a GlobalPlatform Security Domain.” *Id.* at 23–24 (citing Pet. 15–19; Ex. 1006, 30, 44; Ex. 1003 ¶¶ 144–147). Petitioner contends that an ordinarily skilled artisan would have utilized GlobalPlatform’s Application Provider Security Domain (“APSD”) as the security domain for Dua’s SVCE (e-purse applet), “because [APSD] allows ‘the use of keys that are completely isolated’ from other entities.” *Id.* at 25 (citing Ex. 1006, 30, 86 (quotation omitted)). According to Petitioner, “[t]he ASPD can establish its own Secure Channels to communicate with off-card entities. *Id.* (citing Ex. 1006, 87–88).

Petitioner contends that, “[a]fter an application is installed, ‘a personalization process built on a first security channel’ is conducted to provide sets of keys for subsequent data access authentication.” *Id.* at 26 (citing Ex. 1006, 88). Petitioner contends that GlobalPlatform describes

using triple DES keys for cryptographic communications.⁷ *Id.* (citing Ex. 1006, 185, 195–196, 203, 219. Petitioner then contends that Philips also describes using triple DES keys for cryptographic communications, and that these keys must be personalized for Philips’s MIFARE emulator to operate over a GlobalPlatform Secure Channel because an ordinarily skilled artisan would have known that MIFARE memory structures are protected against unauthorized access. *Id.* (citing Ex. 1012, 1, 5, 7; Ex. 1003 ¶¶ 149–150; Ex. 1019, 199, 201). Thus, Petitioner contends, the prior art teaches an emulator “already personalized via a personalization process built on a first security channel so that the emulator is set to store a set of keys for subsequent data access authentication,” as claimed in limitation [1c]. *Id.* (citing Ex. 1003 ¶ 150).

As to the claimed personalization of the e-purse, Petitioner also contends that Dua’s SVCE would “need to obtain its personalization data, including its own keys and Cardholder-specific data.” *Id.* at 27 (quoting Ex. 1006, 88). Petitioner contends that, “[a]fter the APSD is loaded, installed, and personalized, a Load File for loading Dua’s SVCE into the smart card can be sent from the off-card entity (e.g., Dua’s WCM) and a check is performed to ensure the APSD is present on the card.” *Id.* (citing Ex. 1006, 63–64). Petitioner contends that a secure channel between Dua’s SVCE and the WCM could be implemented using GlobalPlatform’s Secure Channel Protocol, in either direct or indirect mode. *Id.* at 27–29 (citing Ex. 1006, 89, 102; Ex. 1003 ¶¶ 71–78, 151). Petitioner points to GlobalPlatform’s “Secure Channel Protocol ‘02” as an example protocol for creating a secure channel between the SVCE and the WCM. *Id.* at 29–31

⁷ “DES” refers to “Data Encryption Standard.” Ex. 1006, 189.

(citing Ex. 1006, 87–88, 213–234 (Fig. E-1); Ex. 1003 ¶¶ 153–154; Ex. 1004 ¶ 247). Thus, Petitioner contends, an ordinarily skilled artisan would have known that Dua’s e-purse applets were also “already personalized via a personalization process built on a first security channel” so that “the e-purse applet is configured to conduct a transaction with a network server over a second security channel,” as also claimed in limitation [1c]. *Id.* at 31 (citing Ex. 1003 ¶¶ 151–155).

Petitioner also contends that “Dua in view of Philips also discloses limitation [1c] in a second way.” *Id.* As to Dua’s e-purse applets being “already personalized via a personalization process built on a first security channel” so that “the e-purse applet is configured to conduct a transaction with a network server over a second security channel,” Petitioner contends that an ordinarily skilled artisan “would have understood that Dua’s SVCEs are personalized,” *id.* at 31–32 (citing Ex. 1004 ¶¶ 57–58, 215, 289, 293, 297–306; Ex. 1003 ¶ 157; Ex. 1008, 954), and that “Dua’s wallet application makes SIP communication capability available to such extensions,” *id.* at 32 (citing Ex. 1004 ¶¶ 293–294, 311, 323; Ex. 1003 ¶ 158).⁸ Petitioner contends that the claimed “first security channel” may be created using a TLS-secured SIP message, and that this initial security channel “can include another security channel ‘built on’ the TLS security channel using S/MIME (Secure/Multipurpose Internet Mail Extensions)” to secure SIP MIME message bodies.⁹ *Id.* at 32–33 (citing Ex. 1004 ¶¶ 102, 109, 125, 201, 204, 207–209, 212, 215; Ex. 1003 ¶¶ 70, 96, 98–99, 159–163; Ex. 1026 ¶ 201).

⁸ “SIP” refers to a “Session Initiation Protocol.” Ex. 1004 ¶ 42.

⁹ “TLS” refers to “Transmission Layer Security.” Ex. 1004 ¶ 101.

And, as for the emulator being “already personalized via a personalization process built on a first security channel so that the emulator is set to store a set of keys for subsequent data access authentication,” as recited in limitation [1c], Petitioner argues that the MIFARE emulator would need to be personalized with keys to be able to access the emulator’s memory and function properly. *Id.* at 34 (citing Ex. 1012, 1–3; Ex. 1019, 199, 201). According to Petitioner, “to implement [Phillips’s] MIFARE® with Dua’s SVCEs,” it would have been obvious “for Dua’s SVCEs to communicate with Philips’s MIFARE® emulator to, for instance, ensure proper RF communications with the mobile device’s contactless interface and facilitate over-the-air reloads, as expressly disclosed by Dua.” *Id.* at 34 (citing Ex. 1004 ¶¶ 293–296, 311, 313; Ex. 1012, 1–3; Ex. 1003 ¶ 164).

Petitioner asserts that the combination of Dua, GlobalPlatform, and Philips discloses limitation [11c] for the same reasons asserted in connection with limitation [1c]. 44.

Regarding Petitioner’s “first way” argument, Patent Owner disputes the assertion that Philips discloses using triple DES keys for cryptographic communications. PO Resp. 26 (citing Pet. 26). Instead, Patent Owner argues that “the only evidence [Petitioner] cites is that Philips includes a Triple key DES-3 co-processor,” and this disclosure “says nothing about the MIFARE emulator using DES keys.” *Id.* (citing Pet. 26; Ex. 1012, 1).

We agree with Patent Owner. The disclosure in Philips relied on by Petitioner merely identifies a “Dual / Triple key DES-3 co-processor” to be an element of the P5CT072 device without explaining how this co-processor operates or how it interacts with other elements. Ex. 1012, 1. Neither the Petition nor Mr. Smith’s original declaration directs us to any explicit disclosure in Philips that ties the MIFARE emulator to the triple key DES-3

co-processor. Pet. 26; Ex. 1003 ¶¶ 149–150. We are not persuaded that the mere presence of the triple key DES-3 co-processor is sufficient to establish that the MIFARE emulator would use triple DES keys personalized using a GlobalPlatform secure channel. Indeed, the triple key DES-3 co-processor is just one of several co-processors identified in Philips. *See* Ex. 1012, 1 (identifying a “PKI (Public KEY Infrastructure) co-processor” and an “AES co-processor”), 5 (identifying a “[h]igh speed CRC co-processor,” a “[h]igh speed AES co-processor,” and a “PKI Co-processor”). Petitioner provides no corroboration for Mr. Smith’s bare contention that the *emulator* and not the *application* is what communicates via the GlobalPlatform Secure Channel.

In addition, we are not persuaded by Petitioner’s assertion that the triple DES “keys must be personalized for the emulator to operate over a GlobalPlatform Secure Channel” because an ordinarily skilled artisan would have known that MIFARE memory structures are protected against unauthorized access. *See* Pet. 26 (citing Ex. 1012, 1, 5, 7; Ex. 1003 ¶¶ 149–150; Ex. 1019, 199, 201). Mr. Smith’s testimony repeats this assertion. Ex. 1003 ¶ 150.

As an initial point, we agree with Patent Owner that personalizing *keys* is not equivalent to personalizing *an emulator*, as required by claims 1 and 11. *See* PO Resp. 26. We note, however, that Mr. Smith also testifies that the “keys need to be personalized *into the Philips MIFARE emulator*.”¹⁰ Ex. 1003 ¶ 150 (citing Ex. 1012, 3) (emphasis added). But, even to the extent that Petitioner intended to assert that the triple DES keys must be

¹⁰ During the hearing, Petitioner argued that “personalized into the emulator” means stored in the emulator. Tr. 20:1–4.

personalized *into the emulator* for the emulator to operate over a GlobalPlatform Secure Channel, we do not find this assertion persuasive. First, the disclosures of Philips from pages 1, 5, and 7 relied on by Petitioner do not support the assertion. As mentioned above, Philips identifies a triple key DES-3 co-processor as an element of the P5CT072 device. Ex. 1012, 1. Philips also identifies a “**High speed DES-3 co-processor** (64 bit parallel processing DES engine)” as a product specific feature. *Id.* at 5. Neither of these disclosures are sufficient to establish that Philips’ MIFARE emulator uses the DES keys—let alone that the keys would be stored in the emulator. Philips also lists a “High speed Triple-DES co-processor (two or three keys loadable)” as a family standard feature. *Id.* at 7. Again, there is no indication of how this co-processor functions or interacts with other elements to suggest that the MIFARE emulator uses the DES keys. The simple mention of “two or three keys loadable” in connection with the co-processor is insufficient to establish that the keys are loaded into the emulator. As Patent Owner contends, this discussion is consistent with the applets, e.g., the e-purse applet, being personalized and using the GlobalPlatform Secure Channel, not the emulator. *See* Ex. 2007 ¶ 87.

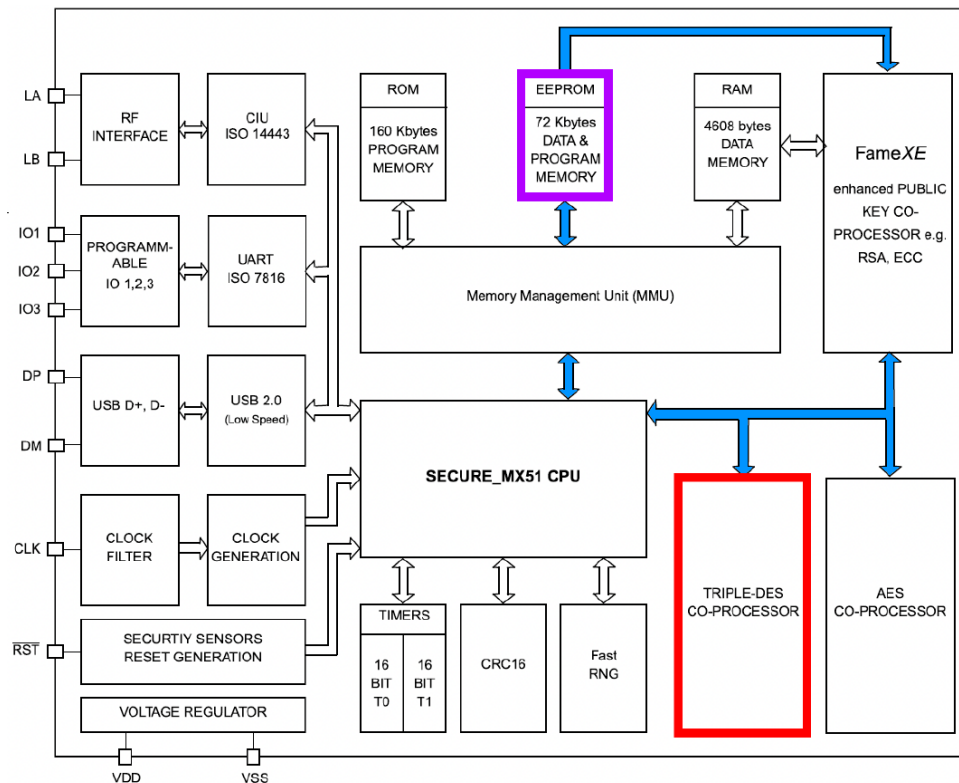
Second, we do not find persuasive Mr. Smith’s testimony that the “keys need to be personalized into the Philips MIFARE emulator so that it can ‘access 4 Kbytes of EEPROM memory using the MIFARE command set.’” Ex. 1003 ¶ 150 (citing Ex. 1012, 3). The passage of Philips quoted by Mr. Smith in support of his testimony states that the MIFARE “emulation offers the possibility to access 4 Kbytes of EEPROM memory using the MIFARE® command set.” Ex. 1012, 3. Mr. Smith, however, does not provide sufficient reasoning or analysis to explain why this disclosure would suggest that the *MIFARE emulator* would need triple DES keys downloaded

via the GlobalPlatform Secure Channel to access the memory. Moreover, Philips also discloses that, instead of using triple DES keys to secure the memory, “[a]ccess rights for the user OS and the MIFARE® 4K emulation on accessing the EEPROM memory can be configured via the so called ACM (Access Condition Matrix).” Ex. 1012, 3. We are not directed to any disclosure indicating that the ACM uses or relates to triple DES keys. As such, we disagree that the MIFARE emulator requires keys to access the EEPROM memory.

Last, we do not find Petitioner’s reliance on Exhibit 1019 persuasive. *See* Pet. 26 (citing Ex. 1019, 199, 201). Exhibit 1019 is a textbook titled RFID Handbook that Mr. Smith uses as background information. Tr. 15:18–24. The cited portions of Exhibit 1019 describe a MIFARE transponder whose memory is divided into 16 segments or sectors, with each sector being protected against unauthorized access by two keys. Ex. 1019, 199, 201. Mr. Smith does not explain adequately, however, why a disclosure of a MIFARE *transponder* having keys would have suggested to one of ordinary skill in the art that Philips’ MIFARE emulator would have triple DES keys. *See* Ex. 1003 ¶ 150. Even if Exhibit 1019 somehow suggests that the MIFARE emulator *could have been* provisioned with triple DES keys, that would still be insufficient to establish obviousness. *See Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) (“[O]bviousness concerns whether a skilled artisan not only *could have made* but *would have been motivated to make* the combinations or modifications of prior art to arrive at the claimed invention.”).

In the Reply, Petitioner argues that Patent Owner is wrong in asserting “that Philips ‘says nothing’ about the Mifare emulator using DES keys” because “[t]he Mifare emulator includes its own key set for accessing secure

Mifare memory structures.”¹¹ Reply 17–18 (citing Pet. 26; Ex. 1003 ¶ 150; Ex. 1042 ¶¶ 31–37). For the reasons discussed above, we are not persuaded that either the Petition or Mr. Smith’s original declaration adequately establish that Philips’ MIFARE emulator uses the DES keys downloaded via the GlobalPlatform Secure Channel. In his supplemental declaration, Mr. Smith testifies that “Patent Owner’s position that reference [in Philips] to a Triple key DES-3 coprocessor does not mean that the emulator has access to triple DES keys is incorrect.” Ex. 1042 ¶ 33. To support this statement, Mr. Smith provides an annotated version of a block diagram depicting Philips’ controller, which we reproduce below.



¹¹ Patent Owner contends that this is “a completely new argument” (Sur-reply 16), but we disagree because the emulator’s “own key set” appears to correspond to the triple DES keys discussed in the Petition. *See e.g.*, Ex. 1042 ¶ 32 (equating the emulator’s own set of stored keys to the triple DES keys).

Id. (citing Ex. 1012, 9). For this annotated diagram, Mr. Smith adds (1) a purple outline to the EEPROM, (2) a red outline to the TRIPLE-DES CO-PROCESSOR, and (3) blue overlay to the connections between these and other components. *Id.* Mr. Smith then states that this annotated diagram shows that “the Triple-DES co-processor is logically linked to EEPROM where the emulator is stored.” *Id.* We do not find this testimony persuasive, however. The mere fact that the EEPROM is “logically linked” to the triple-DES co-processor is not sufficient to establish that the MIFARE emulator uses the triple DES keys downloaded via the GlobalPlatform Secure Channel.

For the above reasons, we determine, based on the full record, that the combination of Dua, GlobalPlatform, and Philips does not disclose an emulator personalized via a personalization process built on a first security channel in the “first way” asserted by Petitioner.

Turning to Petitioner’s “second way” argument, Patent Owner argues that this position fails for similar reasons as Petitioner’s “first way;” namely, Petitioner “provides no reason or evidence that the emulator itself needs to be personalized.” PO Resp. 27 (citing Pet. 34). We agree with Patent Owner that, with respect to personalization of the emulator, Petitioner’s “second way” is similar to its “first way.” Indeed, the Petition states: “*As explained above*, when the extension is a subway SVCE (e.g., for MIFARE®), a corresponding emulator would need to be personalized with keys as well to be able to access the emulator’s memory to function properly with Dua’s subway SVCE,” and relies on much of the same evidence (i.e., Philips and Exhibit 1019) that was relied on in the “first way.” Pet. 34 (citing Ex. 1012, 1–3; Ex. 1019, 199, 201) (emphasis added). Accordingly, we determine on the record before us that the combination of Dua,

GlobalPlatform, and Philips does not disclose an emulator personalized via a personalization process built on a first security channel in the “second way” for the same reasons discussed above in connection with the “first way.”¹²

In view of the above, we are not persuaded that Petitioner has met its burden of showing, by a preponderance of the evidence, that independent claims 1 and 11 are unpatentable over the combination of Dua, GlobalPlatform, and Philips. Because we are not persuaded Petitioner has demonstrated sufficiently that the combination of Dua, GlobalPlatform, and Philips renders claims 1 and 11 obvious, we need not reach Patent Owner’s assertions that Philips does not qualify as prior art. *See* PO Resp. 11–13.

5. Dependent Claims 2–10 and 12–19

Claims 2–10 depend from claim 1, and each of these dependent claims thus contains all the limitations of claim 1. Claims 12–19 depend from claim 11, and each of these dependent claims thus contains all the limitations of claim 11. Petitioner’s challenges to dependent claims 2–10 and 12–19 do not overcome the deficiencies of the combination of Dua, GlobalPlatform, and Philips with respect to claims 1 and 11. *See* Pet. 46–57. Accordingly, for the same reasons discussed above in connection with claims 1 and 11, we also determine Petitioner has not demonstrated, by a preponderance of the evidence that claims 2–10 and 12–19 are unpatentable over the combination of Dua, GlobalPlatform, and Philips.

¹² We also note the inherent tension in the “second way.” The Petition’s basis for asserting the triple DES keys were used with the emulator was the presence of the triple-DES coprocessor and the use of GlobalPlatform. Without GlobalPlatform, the rationale for using the triple DES key with the SIP connection of Dua becomes substantially, if not fatally, weaker.

III. CONCLUSION

In summary:

Claims	35 U.S.C. §	Reference(s)/Basis	Claims Shown Unpatentable	Claims Not shown Unpatentable
1–19	103	Dua, GlobalPlatform, Philips		1–19
Overall Outcome				1–19

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–19 of U.S. Patent No. 9,189,787 B1 are not determined to be unpatentable; and

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

IPR2022-00412
Patent 9,189,787 B1

FOR PETITIONER:

Adam P. Seitz
Paul R. Hart
ERISE IP, P.A.
Adam.Seitz@eriseip.com
Paul.Hart@eriseip.com
PTAB@eriseip.com

FOR PATENT OWNER:

Vincent J. Rubino, III
Peter Lambrianakos
Richard Cowell
FABRICANT LLP
vrubino@fabricantllp.com
plambrianakos@fabricantllp.com
rcowell@fabricantllp.com