Trials@uspto.gov
571-272-7822

Paper No. 37
Date: March 19, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MASTERCARD INCORPORATED AND
MASTERCARD INTERNATIONAL INCORPORATED,
Petitioner,

v.

OV LOOP, INC.,
Patent Owner.

IPR2023-01289
Patent 10,032,171 B2

Before JAMES A. TARTAL, RYAN H. FLAX, and BRENT M. DOUGAL, *Administrative Patent Judges*.

TARTAL, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 314

We have jurisdiction to conduct this *inter partes* review under 35 U.S.C. § 6. This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a) (2018) and 37 C.F.R. § 42.73 (2021). Mastercard Incorporated and Mastercard International Incorporated ("Petitioner") bears the burden of proving unpatentability of each claim it has challenged by a preponderance of the evidence, and the burden of persuasion never shifts to OV Loop, Inc. ("Patent Owner"). *See* 35 U.S.C. § 316(e) (2018); 37 C.F.R. § 42.1(d); *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). For the reasons discussed below, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–33 ("the Challenged Claims") of U.S. Patent No. 10,032,171 B2 (Ex. 1001, "the '171 patent") are unpatentable.

I. INTRODUCTION

A. Summary of Procedural History

Petitioner[1] filed a Petition (Paper 1, "Pet.") pursuant to 35 U.S.C. §§ 311–319 requesting an *inter partes* review of the Challenged Claims. We instituted an *inter partes* review of the Challenged Claims on all grounds of unpatentability asserted in the Petition. Paper 15. Patent Owner[2] filed a Response. Paper 22 ("PO Resp."). Petitioner filed a Reply to the Patent Owner Response. Paper 26 ("Pet. Reply"). Patent Owner filed a Sur-reply

[1] Petitioner identifies no additional real parties in interest. Pet. 10.

[2] Patent Owner identifies no additional real parties in interest. Paper 4, 2.

in support of the Patent Owner Response.[3] Paper 29 ("PO Sur-reply"). Following oral argument, we entered a transcript of the hearing in the record. Paper 35 ("Tr.").

B. Related Proceedings

The Parties identify the '171 patent as a subject of *OV Loop, Inc. v. Mastercard Incorporated*, Case 7:23-cv-01773 (S.D.N.Y.). Pet. 10; Paper 4, 1. Additionally, Petitioner filed a parallel petition in IPR2023-01290 seeking *inter partes* review of the Challenged Claims based on different grounds, which was not instituted. IPR2023-01290, Papers 1, 15.

II. BACKGROUND

A. The '171 Patent

The '171 patent issued July 24, 2018, from an application filed on August 30, 2012, and is directed to using a mobile device for a secure payment transaction through interrogation with a point-of-sale ("POS") terminal. Ex. 1001, 1:25–30, codes (21), (22), (45), (57). The '171 patent refers back to three provisional applications, the earliest of which was filed on August 30, 2011. *Id.* at code (60). Patent Owner has stipulated that it "will not allege in the IPR2023-01289 proceeding that any of claims 1–33 of the '171 Patent are entitled to a priority date any earlier than the August 30, 2012 filing date of the non-provisional application for the '171

[3] In email correspondence to the Board, Patent Owner also identified four instances in Petitioner's Reply that Patent Owner argues are beyond the proper scope of a reply and requested leave to file a motion to strike. Ex. 3001. We denied Patent Owner's request, explaining that the relief sought was an exceptional remedy not shown to be warranted and that Patent Owner's arguments are a part of the record as Exhibit 3001. Paper 28, 3–4. We addressed Patent Owner's arguments concerning the proper scope of a reply in our analysis below.

Patent." Paper 14, 6. Accordingly, in this proceeding August 30, 2012, is the priority date of the '171 patent.

According to the '171 patent, in some prior payment system "a microchip referred to as a 'Secure Element' (SE) is embedded into a payment card, a payment fob (medallion), a cell phone, or other mobile device that may be used for making payments." Ex. 1001, 1:34–40 (further explaining that any "device that houses the SE" is "referred to as a 'card' or 'card device"). The '171 patent states that "it is important to note that the SE may be an emulated software based SE," and that "virtually any electronic device with a digital memory and processor or controller may be adapted to emulate and pretend to be an SE." *Id.* at 1:45–49. As further background, the '171 patent explains that "to extract information from the SE, an interrogator," also referred to as "a reader," "is required to interact electrically with the SE" and "typically follows standards set forth by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and by application providers (such as VISA and MASTERCARD)."[4] *Id.* at 1:50–56. The '171 patent further explains as follows:

> Cards containing an SE are typically presented to an RFID (Radio Frequency Identification) reader device as the interrogator that extracts the information from the card and delivers the data to the POS terminal and then forwarded by the POS terminal on to a card processor for authorization. Mobile phones that contain NFC (Near Field Communication) functionality with embedded SEs have the ability to pretend to be (or emulate) a card that contains an SE. In this case the mobile phone may be presented to the RFID reader just as a card would be presented, and the information may be extracted from the SE

[4] We further discuss the applicable standards. *See infra* Section III.D.4.

> that is on the mobile phone and delivered to POS, which then forwards the data on to a card processor for authorization.

Id. at 6:3–15. The '171 patent also includes an illustration of "a protocol level communication between a reader and an SE," and notes that "[t]he protocol layer is a standard protocol" referred to as the "Application Protocol Data Unit" ("APDU"), which is typically "defined by ISO/IEC specification 7816." *Id.* at 6:16–20, Fig. 1. The '171 patent states that a shortcoming of the prior systems was the requirement to "have physical possession of a card that matches the authorization capabilities of a merchant's system where a purchase is made," which was "inconvenient." *Id.* at 1:34–60.

The '171 patent seeks to provide "more flexible and convenient systems and methods for authorizing financial transactions," and so proposes "systems and methods . . . to facilitate transactions at a point-of-sale terminal where it is not necessary for the user (e.g., the purchaser) to have physical possession of a card with a magnetic stripe or possession of a secure element." *Id.* at 1:61–62, 9:11–15.

In one embodiment, the '171 patent describes the use of "a remote permanent cryptographic key" stored at a "remote source" away from the mobile device "to calculate an expected cryptogram that is expected to include at least a portion of the digital credential data." *Id.* at 1:66–2:10. An interrogation between the POS terminal and the mobile device includes sending at least one POS command communication from the POS terminal to the mobile device requesting the digital credential data and at least one device response communication from the mobile device to the POS terminal including the expected cryptogram, such that the financial transaction is authorized. *Id.* at 2:10–21.

The '171 patent states that "cryptogram" refers to "encrypted data" and "cryptographic key" refers to "a key used, at least in part, to calculate a cryptogram." *Id.* at 25:37–45. The '171 patent identifies a multiple "[e]xamples of cryptograms at the time of this filing" that are "defined" by various "card specifications" listed in Table 4. *Id.* at 25:52–63. A "dynamic" cryptogram "is always changing from one interrogation (transaction) to the next over the life a digital credential (SE representation)." *Id.* at 25:64–67. The '171 patent provides in Table 4, reproduced below, "[e]xamples of cryptograms at the time of this filing" that are "defined" by certain "card specifications."

TABLE 4

Card specification	Cryptogram Designator or Name
MASTERCARD PAYPASS MSD	CVC3
VISA Contactless MSD	dCVV
DISCOVER ZIP MSD	dCVV
EMV, VISA QVSDC, VISA VSDC, MASTERCARD MCHIP	AC, TC, AAC, ARQC

Id. at 25:55–63. Table 4, reproduced above, includes a left column listing various card specifications and a right column listing the corresponding cryptogram designator or name. *Id.*

A "'permanent cryptographic key' refers to a cryptographic key that is unchanging (or static) throughout the life of a card, SE, mobile device, or digital credential." *Id.* at 27:29–32. A "temporary cryptographic key" "changes (or is dynamic) from one interrogation to the next over the life of a digital credential (e.g., an SE representation)." *Id.* at 27:33–36.

Figure 15 of the '171 patent is reproduced below.

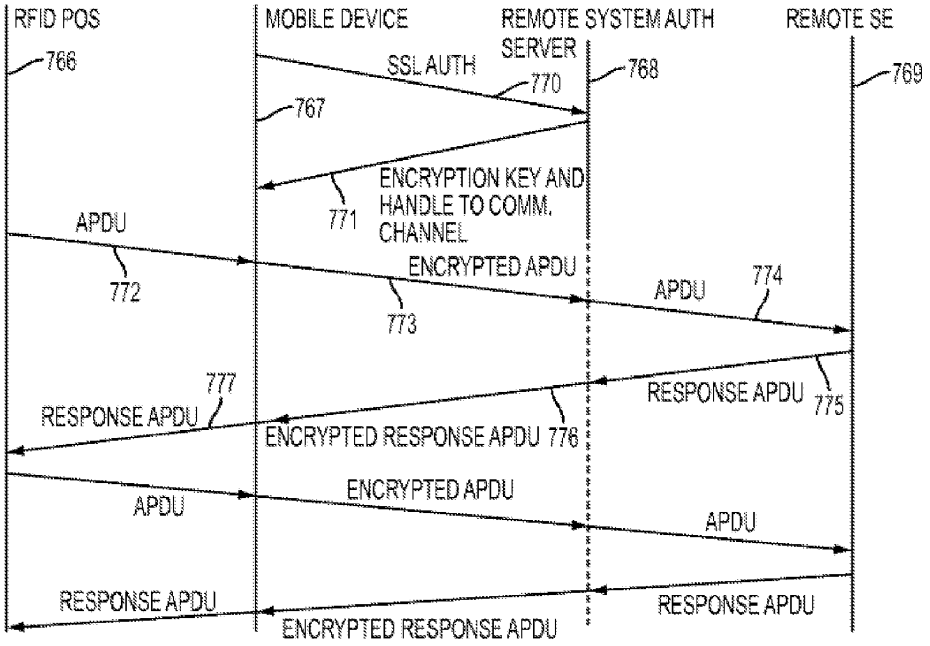

FIG. 15

Figure 15 "illustrates an embodiment of a data flow diagram including authorization between a mobile device and a remote hosted SE." *Id.* at 4:3–5. Figure 15 shows four vertical lines identified from left to right as RFID POS entity 766, mobile device 767, remote system authorization server 768, and remote hosted SE 769. *Id.* at 17:47–52. A series of sloping arrows between the vertical lines illustrates in Figure 15 how mobile device 767 interacts with remote authorization server 768 to facilitate the access of digital credential data from remote SE 769. *Id.* at 17:52–56. Adjacent to the sloping lines in Figure 15 is "APDU." *Id.* at 3:34–36. The '171 patent explains that APDU corresponds to a "protocol level communication" where "[t]he protocol layer is a standard protocol referred to as APDU," which stands for "Application Protocol Data Unit" and typically "is defined by ISO/IEC specification 7816," a "broad specification

with different sections directed toward different 'layers' of communication protocols." *Id.* at 3:34–36, 6:17–23. The '171 patent further describes the communications illustrated in Figure 15 as follows:

> a communication channel is opened between the RFID POS 766 and the remote SE 769. Authorization over SSL is initiated where credentials 770 are sent to the remote authorization server 768. The remote authorization server 768 verifies the credentials and sends back a successful response 771 which contains a handle to a communication channel and an encryption key. The mobile device 767 may then open a channel to the remote SE 769. At that point APDU command and response APDUs may be sent securely between the RFID POS reader 766 and the remote SE 769 and back through the mobile device 767. An APDU command 772 is sent from the RFID POS reader 766 to the mobile phone 767, which may encrypt that APDU as command 773 and forwards an APDU command 773 on to the remote system 768 and on to the remote SE 769 as APDU command 774. In some embodiments the command communications 773 and 774 comprise at least a portion of the command communication 772 from the RFID POS 766 to the mobile device 767. In some embodiments the mobile device 767 may know ahead of time what the RFID POS 766 will command the mobile device 767 in the APDU command 772 in advance of actually interacting with the RFID POS 766. In such cases the command 773 may have been sent already sent [SIC] by the mobile device 767 before the command 772 was received by the mobile device 767 from the RFID POS 766. The return APDU response from the SE is delivered back to the RFID POS through the communication channel using the handle provided by the response 771, via communications 775, 776, and 777.

Id. at 17:57–18:19.

B. Illustrative Claim

Petitioner challenges claims 1–33 of the '171 patent. Pet. 12. Claims 1 and 17 are independent claims. Claims 2–16 depend from claim 1 and claims 18–33 depend from claim 17.

Claim 1 is illustrative of the claimed subject matter and is reproduced below, with bracketed labels annotated by Petitioner:

> 1. [1.PRE] A method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising:
>
> [1.A-1] at a mobile device, executing an application in an operating system of the mobile device, [1.A-2] the application interrogable by an electronic reader, over a first communications channel, for digital credential data corresponding to an account having a corresponding digital credential and [1.A-3] configured to request, from a remote computer system hosting the corresponding digital credential, over a wireless network that is separate from the first communications channel, data associated with the account and [1.A-4] generate cryptograms requested during interrogations over the first communications channel using the data associated with the account received from the remote computer system, wherein the application does not access a permanent cryptographic key issued for the digital credential during the interrogations;
>
> [1.B] requesting by the application, from the remote computer system, over the wireless network, a first set of data associated with the account;
>
> [1.C] receiving by the application, from the remote computer system, over the wireless network, the first set of data associated with the account, the first set of data associated with the account usable by the application to formulate an application protocol data unit response, the first set of data comprising a first non-permanent cryptographic key associated with the account;
>
> [1.D] locally storing the first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;
>
> [1.E] participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising:

[1.E-1] receiving at least one POS command communication sent by the POS terminal over the first communications channel, wherein the at least one POS command communication comprises a request for digital credential data to authorize a transaction against the account, the request for digital credential data including a cryptogram request;

[1.E-2] generating a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and

[1.E-3] responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to an electronic reader through the communication channel, the at least one device response communication comprising at least one response application data protocol unit containing the response cryptogram and an account identifier for the account;

[1.F] subsequent to the interrogation, requesting by the application, from the remote computer system, over the wireless network, a second set of data associated with the account;

[1.G] receiving by the application, from the remote computer system, over the wireless network, the second set of data associated with the account, the second set of data comprising a second non-permanent cryptographic key associated with the account; and

[1.H] storing the received second non-permanent cryptographic key as the local cryptographic key associated with the account to change the local cryptographic key associated with the account between at least two interrogations.

Ex. 1001, 50:61–51:65; Pet. 1–2.[5] Claim 17 recites "[a] system for secure application-based participation by a mobile device in point-of-sale interrogations" comprised of features that generally correspond to the limitations of the method recited in claim 1. Ex. 1001, 53:15–54:22.

C. Asserted Grounds of Unpatentability

Petitioner asserts that the Challenged Claims are unpatentable based on the following grounds:

Claims Challenged	35 U.S.C. §[6]	Reference/Basis
1–33	103(a)	Collinge[7]
1–4, 6–20, 22–33	102	Collinge
1–33	102	Fiske[8]
1–33	103(a)	Fiske

Pet. 13.

[5] Claim 1 recites in limitation 1[C] "application protocol data unit" and in limitation 1[E-3] "application data protocol unit." The term "application data protocol unit" does not appear in the Specification of the '171 patent outside of the claims. There is no dispute that "application data protocol unit" refers to an "application protocol data unit" or "APDU." *See* Ex. 1050 ¶ 39 n.3; Ex. 2009 ¶ 25; Ex. 1021, 35; Pet. Reply 14 n.12; *see also* PO Resp. 21 (referring to "APDUs for communications between the terminal and the 'Card'").

[6] The Leahy-Smith America Invents Act ("AIA") included revisions to 35 U.S.C. §§ 102 and 103 that became effective on March 16, 2013. We apply the pre-AIA version of §§ 102 and 103 here, because the '171 patent issued from an application filed before the effective date of the AIA. *See* Ex. 1001, code (22).

[7] U.S. Patent App. Pub. No. US 2013/0262317 A1, published Oct. 3, 2013 (Ex. 1011, "Collinge").

[8] U.S. Patent No. 11,080,693 B2, issued Aug. 3, 2021 (Ex. 1012, "Fiske").

Petitioner relies on, among other evidence, the supporting Declaration of Stuart Fiske, D. Phil., dated August 11, 2023, and the Supplemental Declaration of Stuart Fiske, dated September 20, 2024.[9] Exs. 1006 and 1050. Petitioner also relies on the declaration of Brian Byrne, dated August 3, 2023 (Ex. 1018) and the declaration of Sylvia Hall-Ellis, Ph.D., dated August 10, 2023 (Ex. 1032), both of which primarily address the authenticity and public availability of certain documents. Patent Owner's arguments are supported by, among other evidence, the Declaration of Dr. Chuck Easttom, Ph.D., D.Sc., dated June 28, 2024. Ex. 2009.

III. ANALYSIS

A. Legal Standards for Anticipation and Obviousness

Petitioner contends under two grounds that certain Challenged Claims are anticipated. Pet. 13. A claim is anticipated if a single prior art reference either expressly or inherently discloses every limitation of the claim. *Orion IP, LLC v. Hyundai Motor Am.*, 605 F.3d 967, 975 (Fed. Cir. 2010). "A single prior art reference may anticipate without disclosing a feature of the claimed invention if such feature is necessarily present, or inherent, in that reference." *Allergan, Inc. v. Apotex Inc.*, 754 F.3d 952, 958 (Fed. Cir. 2014) (citing *Schering Corp. v. Geneva Pharm.*, 339 F.3d 1373, 1377 (Fed. Cir. 2003)).

[9] In this Decision "Fiske" refers to the reference entered as Exhibit 1012 and "Dr. Fiske" refers to the individual providing supporting testimony on behalf of Petitioner.

Petitioner contends under two grounds that the Challenged Claims are unpatentable based on obviousness. Pet. 13. 35 U.S.C. § 103(a) sets forth as follows:

> [a] patent may not be obtained . . . if the differences between the subject matter sought to be patented 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.

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

An obviousness analysis "need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007). However, Petitioner cannot satisfy its burden of proving obviousness by employing "mere conclusory statements." *In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016).

B. Level of Ordinary Skill in the Art

In determining the level of ordinary skill in the art, 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) (citation omitted). Petitioner contends that a person of ordinary skill in the art would have had "a Bachelor's degree in Electrical Engineering or

Computer Engineering, or equivalent knowledge, with sufficient mathematical background to understand basic cryptographic techniques, and with two to four years of academic or industry experience in payment systems." Pet. 24. Petitioner further contends "[a]dditional education could compensate for less practical experience and vice versa." *Id.*

Patent Owner asserts that a person of ordinary skill in the art would have had "the equivalent of an undergraduate degree in electrical and computer engineering (or a related field) and approximately two years of work experience in the field of secure payment system," and that "[a]dditional education in the field could be substituted for industry experience, and vice versa." PO Resp. 4. Patent Owner does not suggest that its proposed level of ordinary skill materially differs from the level of skill proposed by Petitioner. *See id.*

We find, on the current record, that the '171 patent and the cited prior art references reflect the appropriate level of skill at the time of the claimed invention and that the level of appropriate skill reflected in these references and in the '171 patent is consistent with the definition of a person of ordinary skill in the art proposed by Petitioner. Accordingly, we adopt Petitioner's proposed level of ordinary skill. We would have reached the same conclusions in this Decision had we adopted Patent Owner's proposed level of ordinary skill in the art.

C. Claim Construction

We apply the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. § 282(b). 37 C.F.R. § 42.100(b). Under that standard, claim terms "are generally given their ordinary and customary meaning" as would have been understood by a person of ordinary skill in the art at the time of the invention. *Phillips v.*

AWH Corp., 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc)). "In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence." *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17). Extrinsic evidence is "less significant than the intrinsic record in determining 'the legally operative meaning of claim language.'" *Phillips*, 415 F.3d at 1317.

Petitioner states that it "gives the terms their ordinary and customary meaning, as understood by a [person of ordinary skill in the art] at the time of the invention and in the context of the patent disclosure." Pet. 24. Patent Owner does not propose an express construction of any claim term. *See* PO. Resp. 11.

Claims 1 and 17 each recite "at least one response application data protocol unit containing the response cryptogram and an account identifier for the account." Petitioner argues this limitation is "potentially subject to at least two alternative constructions." Pet. 24–25. In particular, Petitioner asserts that the limitation may be construed either as "one or more response application data protocol units, collectively containing the response cryptogram and an account identifier for the account" (the "First Construction") or as "one or more response application data protocol units, each of which contains both the response cryptogram and an account identifier for the account" (the "Second Construction"). *Id.* Petitioner states that the Second Construction is "likely correct," and further contends there is no need to expressly construe the limitation because the Challenged Claims are unpatentable under either construction. *Id.* at 25.

In response, Patent Owner appears to dispute the First Construction, arguing that "Petitioner does not provide any support for its contention that [the First Construction] is supported by the specification of the '171 patent." PO Resp. 24. Patent Owner further states that "Patent Owner does not contend that [the First Construction] is consistent with the plain and ordinary meaning of the claim." *Id.* (citing Pet. 49). Patent Owner does not dispute Petitioner's Second Construction. *See id.* at 28–29.

In light of the lack of any dispute over the Second Construction, a construction we find consistent with the ordinary and customary meaning of the claim language, we need not resolve whether the claim language also encompasses Petitioner's First Construction. Moreover, as explained below, we find Collinge renders obvious the subject matter of the limitation under either construction. *See infra* Section III.D.5. For the foregoing reasons, we find that an express construction of any claim term is not necessary for purposes of this Decision. *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))).

D. Alleged Obviousness Based on Collinge

Petitioner contends the subject matter of the Challenged Claims would have been obvious over Collinge. Pet. 36–65; Pet. Reply 8–22. Petitioner's contentions are supported by Dr. Fiske. Ex. 1006 ¶¶ 81–163; Ex. 1050 ¶¶ 24–58. Patent Owner disputes Petitioner's contentions based on Collinge primarily in regard to whether Petitioner has sufficiently set forth (1) how Collinge is prior art and (2) how Collinge discloses or teaches certain limitations of the Challenged Claims. PO Resp. 5–49; PO Sur-reply 3.

Patent Owner's arguments are supported by Dr. Easttom. Ex. 2009 ¶¶ 74–194.

We determine that Petitioner has shown that the Challenged Claims would have been obvious over Collinge and adopt as our own determination Petitioner's contentions, as supported by the evidence cited by Petitioner. *See* Pet. 36–65; Pet. Reply 8–22. We focus our discussion below on the arguments in opposition raised by Patent Owner, which we disagree with for the reasons that follow. We begin with a brief summary of Collinge, address the availability of Collinge as prior art, provide a brief summary of the '095 Provisional that Collinge incorporates by reference, discuss the EMV Specifications and PayPass Specifications, and, finally, turn to our analysis of each of the Challenged Claims.

1. Summary of Collinge

Collinge is a patent application directed "to provisioning of payment credentials to a mobile device lacking a secure element," specifically, "for use in conducting a near field financial transaction." Ex. 1011 ¶2. Figure 1 of Collinge, reproduced below, illustrates "a system for generating and provisioning payment credentials to a mobile device." *Id.* ¶ 16.

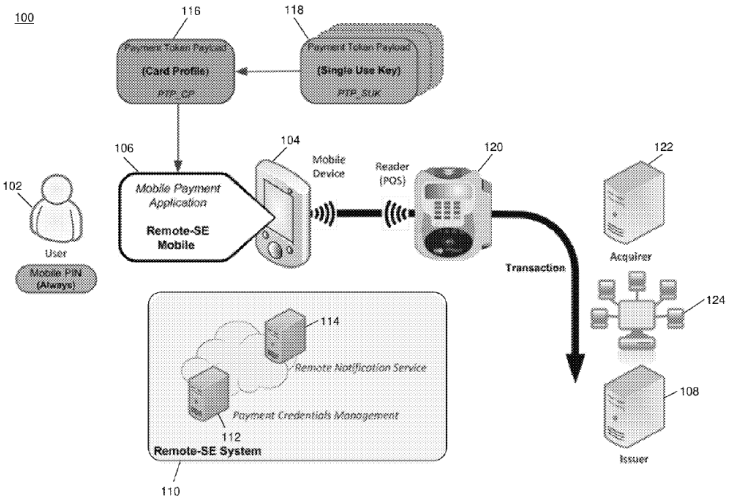

FIG. 1

As shown in Figure 1, system 100 includes user 102 in possession of mobile device 104, which may include payment application 106. *Id.* ¶¶ 40–41. User 102 may use mobile device 104 for payment transactions that rely on a payment account with issuer 108, where "[p]ayment credentials corresponding to the payment account may be stored by a remote-SE (remote-secure element) system 110 for provisioning to the mobile device 104." *Id.* ¶ 42. In particular, remote-SE system 110 may use a token payload, including card profile 116 and single use key 118, to provision payment credentials to mobile device 104. *Id.* ¶ 43. "[C]ard profile 116 may include the payment credentials, and the single use key 118 may be a single use (e.g., one-time use) key used to generate a payment cryptogram valid for a single payment transaction." *Id.*

For payment transactions, "mobile device 104 may be further configured to transmit a generated payment cryptogram and payment credentials to a point-of-sale terminal 120 at a merchant," where "point-of-sale terminal 120 may be any type of point-of-sale terminal or device suitable for receiving payment credentials via near field communication (NFC)." *Id.* ¶ 44. Point-of-sale terminal 120 may submit payment credentials and other transaction information to acquirer 122 for authorization, which includes using payment network 124 to query issuer 108. *Id.* ¶¶ 44–45.

2. Collinge as Prior Art

Collinge is a patent application filed on March 14, 2013, and published on October 3, 2013. Ex. 1011, codes (22), (43). Under the heading "Related Applications," Collinge refers back to a series of provisional applications and expressly states as follows:

> This application claims the priority benefit of commonly assigned U.S. Provisional Application No. 61/619,095, filed Apr. 2, 2012, entitled "Method and System for Processing mobile Payments for Devices Without Secure Elements" [(Ex. 1009, "the '095 Provisional")]; U.S. Provisional Application No. 61/639,248, filed Apr. 18, 2012, entitled "Method and System for Processing mobile Payments by Provisioning Credentials to Mobile Devices Without Secure Elements" [(Ex. 1010, "the '248 Provisional")]; U.S. Provisional Application No. 61/735,383, filed Dec. 10, 2012, entitled "Systems and Methods for Processing Mobile Payments by Provisioning Credentials to Mobile Devices Without Secure Elements," by Mehdi Collinge et al.; and U.S. Provisional Application No. 61/762,098, filed Feb. 7, 2013, entitled "Systems and Methods for Processing Mobile Payments by Provisioning Credentials to Mobile Devices Without Secure Elements." by Mehdi Collinge et al., [collectively, the "Collinge Provisionals"] *which are each herein incorporated by reference in their entirety*.

Id. ¶ 1 (emphasis added).

The date Collinge was filed, March 14, 2013, is after the August 30, 2012, priority date of the '171 patent stipulated to by Patent Owner in this proceeding. Petitioner asserts that "Collinge is pre-AIA 102(e) prior art as of its priority date of April 2, 2012," the filing date of the '095 Provisional.[10] Pet. 25, 28–33; *see also Lynk Labs, Inc. v. Samsung Electronics Co., Ltd.*, No. 2023-2346, slip. op. at 10 (Fed. Cir. Jan. 14, 2025) ("the plain language of §§ 311(b) and 102(e)(1) permits IPR challenges based upon published patent applications, and such published patent applications can be deemed prior art in IPRs as of their filing date").

[10] Petitioner also asserts that the '248 Provisional provides written description support for all elements of at least one independent claim of Collinge, but provides no supporting analysis in the Petition. *See* Pet. 28.

For Collinge to be § 102(e) prior art as of the filing date of the '095 Provisional, the '095 Provisional must provide written description support for: (1) the subject matter of at least one claim of Collinge, and (2) the subject matter Petitioner relies upon in Collinge to show the unpatentability of the Challenged Claims of the '171 patent. *See In re Giacomini*, 612 F.3d 1380, 1383 (Fed. Cir. 2010); *Dynamic Drinkware*, 800 F.3d at 1382.

As to the first consideration, Petitioner provides a detailed claim chart identifying how Petitioner contends the '095 Provisional provides written description support for each limitation of claim 20 of Collinge. Pet. 29–33. As to the second consideration, using Petitioner's allegations directed to claim 1 of the '171 patent as an example, Petitioner provides a detailed analysis of how it contends Collinge discloses or teaches each limitation of claim 1 of the '171 patent with supporting citations to both Collinge and to the '095 Provisional. *Id.* at 36–52. We find Petitioner's contentions are sufficiently supported by a preponderance of the evidence to show that Collinge is prior art. Petitioner also contends, and we agree, that the Collinge Provisionals are expressly incorporated by reference by Collinge. *See* 37 C.F.R. § 1.57(c)(1) (providing that an incorporation by reference must use "the root words 'incorporat(e)' and 'reference'" and must "[c]learly identify the referenced . . . publication"); Pet. 36 n.5; Pet. Reply 3; Ex. 1011 ¶ 1.

We disagree with Patent Owner's arguments disputing the sufficiency of Petitioner's showing that Collinge is prior art and that Collinge also incorporated by reference the Collinge Provisionals, for the following reasons. *See* PO Resp. 5–12. Patent Owner argues that "provisional applications are not themselves prior art under § 102(e)(1)

because they are not applications published under § 122(b)." *Id.* at 7 (citing *Amgen Inc. v. Sanofi, Aventisub LLC*, 872 F.3d 1367, 1380, n. 5 (Fed. Cir. 2017)). According to Patent Owner, Petitioner may not rely on "nonpublic information solely disclosed in a provisional application" even if that information is later expressly incorporated by reference in subsequent published application. *Id.* at 8 (citing *In re Lund*, 376 F.2d 982, 991 (CCPA 1967)). Patent Owner reasons that "[b]ecause Collinge's attempt to incorporate the Collinge Provisional by reference could not—for the purposes of prior art—be effective until its relevant disclosure became publicly available, the disclosures found solely in the Collinge Provisional do not qualify as 'described in' Collinge under 102(e)." *Id.* at 9.

Petitioner argues, and we agree, that the subject matter taught in the Provisional Applications was properly incorporated by reference with Collinge and constitutes prior art as of the publication date of Collinge, as part of Collinge. Pet. Reply 1–4. Petitioner explains that the Federal Circuit has made clear that "[m]aterial not explicitly contained in the single, prior art document may still be considered for purposes of anticipation if that material is incorporated by reference." *Id.* (quoting *Advanced Display Sys., Inc. v. Kent State University*, 212 F.3d 1272, 1282–83 (Fed. Cir. 2000)) (alteration in original). Petitioner further explains that material incorporated by reference by Collinge need only be publicly available as of the date of publication of Collinge and that the Collinge Provisionals were publicly available at least as of the date Collinge was published. *Id.* at 2–3 (citing *In re Hawkins*, 486 F.2d 569, 574 (CCPA 1973); *In re Lundak*, 773 F.2d 1216, 1222 (Fed. Cir. 1985); 37 C.F.R. § 1.14(a)(1)(iv)–(v)). Patent Owner does

not dispute that the Collinge Provisionals were publicly available at least as of the date Collinge was published.[11] *See* PO Sur-reply 1–3.

3. The '095 Provisional[12]

As explained above, Collinge incorporates by reference the '095 Provisional, titled "System and Methods for Processing Mobile Payments for Mobile Devices Without Secure Elements." Ex. 1011 ¶ 1; Ex. 1009, p.1. The '095 Provisional is directed to "directed to a method and system providing technical solutions for processing electronic payments initiated from a mobile device without requiring a secure element (SE) in the mobile device using in part a financial transaction card processing system or network as a part thereof." Ex. 1009 ¶ 1.

---

[11] The nonprecedential Board decision Patent Owner relies on does not persuasively support Patent Owner's arguments. PO Resp. 7–8; PO Sur-reply 2 (citing *Sequenom, Inc. v. Bd. of Trustees of the Leland Stanford Junior University*, IPR2014-00337, Paper 14 (PTAB Sep. 23, 2014)). As the Board explained in *Sequenom*, a petition for *inter partes* review was denied because the asserted reference, a provisional U.S. patent application, was "neither a patent nor an application for patent published under 35 U.S.C. § 122(b), and, therefore, [was] not one of the two types of documents that may be relied upon under 35 U.S.C. § 102(e) to show that claims are unpatentable." IPR2014-00337, Paper 14, 3. The Board further stated in *Sequenom* that the petitioner failed to show support for the notion that "a ground of unpatentability under § 102(e) may be predicated on a provisional application, without reference to a corresponding patent or application for patent published under § 122(b)." *Id.* In this case, Petitioner relies on Collinge, a published application that expressly incorporated by reference the Collinge Provisionals, not merely on a provisional application.

[12] With our authorization Petitioner filed a corrected copy of Exhibit 1009 on October 24, 2024. Paper 28 (granting Petitioner's request to file corrected version of Exhibit 1009 to correct clerical errors with the formatting of figures appearing at pages 49 to 56 over Patent Owner's opposition).

The '095 Provisional states as background as follows:

> [A] a user who has an NFC-capable mobile device may not be able to use it as a payment device if their mobile device lacks a secure element (SE).
>
> Accordingly, what is further needed are systems and methods that allow mobile devices without an SE to complete mobile payments using a Cloud-based transaction data generation system which can authenticate and generate payment credentials (i.e., tokens) associated with one or more existing payment accounts, such as, but not limited to, a PayPass® account, so that the user can conduct PayPass® transactions at PayPass®-enabled merchants with a mobile device without having to use an SE and without requiring their acquirer or merchant to make significant changes to their host system(s).

Id. ¶¶ 2–3. The '095 Provisional describes in detail "[e]xemplary processes for authentication, payment, and synchronization." *Id.* ¶¶ 55–60. In Table 1, the '095 Provisional further details "[e]xemplary data flow stages." *Id.* ¶ 61. For example, the '095 Provisional states, in regard to authentication, that "[i]f the validation of the CAP Token is successful, the Cloud generates the CVC3 value . . . and returns an encrypted payload to the Mobile Payment Application." *Id.* ¶ 56.

Dr. Fiske explains that "Mastercard's PayPass Specifications" (for credit card account transactions) are "the brand-specific implementations" of the EMV Specifications (Exs. 1019–1029). Ex. 1050 ¶ 12; *see also id.* ¶ 38 (stating that "CVC3 and Application Cryptogram (AC) are well known in the art to be names of response cryptograms generated by the payment application for authorization of a transaction in an EMV-compliant transaction") (citing Ex. 1037, 54, 57; Ex. 1052, 14:63–65.

4. EMV Specifications and PayPass Specifications

Relevant to Petitioner's contentions and to our analysis, as background, is an understanding of EMV card specifications, also referred to as standards ("EMV Specifications"). Petitioner provides EMV Specifications from June 2008 as Exhibits 1019–1022 and from March 2011 as Exhibits 1023 to 1029.[13] *See* Pet. vi.–vii. Petitioner contends, for example, that a person of ordinary skill "reading Collinge" would have understood that Collinge "discloses contactless payment techniques compatible with EMV infrastructure" and that an EMV transaction is performed in accordance with EMV Specifications. *Id.* at 38 (citing, e.g., Exs. 1021, 1023, 1026, 1027). Petitioner's contention is that, as a necessity in the field, these Specifications were well known to those of ordinary skill in the art.

According to Petitioner, "as of August 2011, chip cards . . . of major payment brands such as Mastercard and Visa, as well as corresponding POS readers, conformed to or were migrating to industry standards known as the EMV Specifications." *Id.* at 17–18 (citing Ex. 1006 ¶ 49). Petitioner and Dr. Fiske explain that "well before August 2011, EMV chip cards were already the mainstream form of payment cards in most parts of Europe," and that the "EMV Specifications . . . are maintained and published by a technical body known as EMVCo, a technical body formed in February 1999 by three major payment brands—Europay International,

[13] Petitioner provides a declaration from Brian Byrne who, based on personal knowledge, states that Exhibits 1019–1022 were publicly available in 2008 and that Exhibits 1023 to 1029 were publicly available in 2011. Ex. 1018.

MasterCard International and Visa International.[14] *Id.* at 18; Ex. 1006 ¶ 49 (citing Exs. 1019–1029; Ex. 1041, 6; Ex. 1042).

Dr. Easttom also discusses at length the EMV Specifications in his declaration (Ex. 2009), noting, for example, that "even by December 2013, adoption of EMV was far from widespread," (¶ 39) that a person of ordinary skill "at the time would have considered . . . alternatives," (¶ 40), that the "Payment Card Industry Data Security Standards from 2010 state '[m]ost environments processing EMV transactions today are hybrid environments, handling both EMV and non-EMV transactions'" (¶ 41), and that some of the EMV Specifications were optional (¶ 45).[15] *Id.* ¶¶ 27–51. Accepting Dr. Easttom's testimony as correct, his testimony does not refute Petitioner's showing that a person of ordinary skill in the art would have been aware of, and well-versed in, the EMV Specifications, even if not all of the EMV Specifications were mandatory, if there were alternative specifications, or if adoption of the EMV Specifications in the United States was ongoing.

As Patent Owner recognizes, a person of ordinary skill in the art would have had "approximately two years of work experience in the field of secure payment system," and the evidence shows a person of ordinary skill in the art would have been familiar with the EMV Specifications that were commonly applied to electronic transactions in many instances at the

---

[14] In discussing his qualifications, Dr. Fiske states that from 1999 to 2013 as a "lead consultant and relationship manager" he "led projects covering many aspects of the migration of the American Express card payment product to EMV," including "development of the specification and implementation of the American Express EMV application on the MULTOS platform." Ex. 1006 ¶ 7.

[15] Dr. Easttom identifies "EMV, and related standards and technologies" as an example of an area within which he has "expertise." Ex. 2037, 45–46.

relevant time. *See* PO Resp. 4; Ex. 1006 ¶ 49 (citing Exs. 1019–1029; Ex. 1041, 6; Ex. 1042); *see also* Pet. Reply 5 n.4 (arguing that low adoption of EMV in the U.S. was "irrelevant" and that a person of ordinary skill in the art would have been "motivated to build EMV-compliant products, due to its worldwide importance and expected adoption in U.S. terminals") (citing Ex. 2009 ¶ 37; Ex. 1050 ¶ 13; Ex. 1041, 2).

In further support of its contention that a person of ordinary skill in the art reading Collinge "would have done so in light of their knowledge of common payment specification, especially EMV, . . . and the brand-specific implementations of those EMV standards, such as Mastercard's PayPass specification," Petitioner emphasizes that the '171 patent, itself, "expressly relies on the [person of ordinary skill]'s knowledge of EMV and PayPass to provide necessary disclosure." Pet. Reply 5 (citing Ex. 1001, 26:50–27:33, 49:32–39; 31:57–64; 25:50–62).

In this regard, the '171 patent states as follows:

> The details of an interrogation between a point-of-sale and a digital credential, card, SE representation, and mobile device are defined in "card specifications" and implemented in point-of-sale terminals. Examples of these card specifications at the time of this filing are MASTERCARD PAYPASS-Mag Stripe v3.3, Contactless EMV, DISCOVER NETWORK RF Contactless Specification-Supplement Guide For Functional Support, AMEX ALIS v 1.7, and VISA Contactless Payment Specification v2.0.2. As used herein the term "card specification" refers to a specification or reference within the specification to other specifications and so on that a point-of-sale terminal must adhere to in order to interrogate a card, SE, mobile device as expected by that card specification. A point-of-sale terminal, as the interrogator, controls the interrogation. The card specification that defines the details of an interrogation may also define the details of a cryptogram request, calculation, and delivery from the card, SE, or mobile device to the point-of-sale

> as part of the interrogation sequence. Card specifications may include references to other specifications and those other specifications to even more specification wherein the card specification may be defined by the card specification in conjunction with other supporting documents sited within a card specification. Card specifications typically consist of an application layer that defines an interrogation sequence and calculations that are to be performed by both the card, SE, mobile device and also the interrogator or point-of-sale. Both a mobile device and a point-of-sale are expected to be operating under the direction of a card specification during an interrogation.

Ex. 1001, 26:50–27:12. Petitioner also shows that other contemporaneous patents corroborate that a person of ordinary skill would have been familiar with EMV Specifications when reading Collinge. *See* Pet. Reply 7.

Patent Owner argues for the first time in its Sur-reply that the EMV Specifications (Exs. 1019–1029) are "non-prior art references." PO Sur-reply 3. Patent Owner does not otherwise explain its argument and did not seek to exclude the EMV Specifications. To be clear, unlike Collinge, Petitioner did not rely on the EMV Specifications *as prior art* asserted against the Challenged Claims in a ground of unpatentability, but that does not mean the EMV Specifications are not "prior art." In an obviousness analysis "the background knowledge possessed by a person having ordinary skill in the art" is always a consideration, and unasserted prior art may well provide evidence of that background knowledge. *See*, *e.g.*, *KSR*, 550 U.S. at 401. Petitioner's contention is that it is with this background knowledge that the ordinarily skilled artisan would have read and understood the asserted prior art, i.e., Collinge, here.

In sum, the evidence presented shows that, before the priority date of the '171 patent, a person of ordinary skill in the art would have been aware of the EMV Specifications as an objective industry standard, would have

followed standard industry guidance for interrogations, and would have interpreted Collinge with the background knowledge of the EMV Specifications, particularly in regard to the "details of an interrogation" using EMV, as expressly recognized by the '171 patent. *See*, *e.g.*, Ex. 1001, 26:50–27:12; *see also* Ex. 1012, 1:58–64 (stating that "[m]any electronic payment systems use the EMV (Euro-pay®, Mastercard, Visa®) transaction protocols, as defined for example in the EMV 4.2 Specifications or the EMV Contactless Specifications for Payment Systems, which are publicly available and published by EMVCo. LLC"). In short, we find a preponderance of the evidence establishes that the EMV Specifications (Exs. 1019–1029) are part of the background knowledge of a person of ordinary skill at the relevant time and that this background knowledge would have informed such an ordinarily skilled artisan's reading and analysis of Collinge and Fiske.[16] *See Wellman, Inc. v. Eastman Chemical Co.*, 642 F.3d 1355, 1367 (Fed. Cir. 2011) (stating that "[w]ell known industry standards need not be repeated in a patent").

Patent Owner also argues that Exhibit 1058 ("PayPass – Mag Stripe Technical Specification") and Exhibit 1059 (PayPass – M/Chip Card Technical Specification") are not "prior art" because the date printed on the documents "provides insufficient evidence of public accessibility" and the documents state the information they contain is "proprietary and

[16] Patent Owner also argues for the first time in its Sur-reply that Petitioner's reliance on the EMV Specifications "goes well beyond illustrating the background knowledge in the art," because "Petitioner relies on them for alleged disclosure of claim limitations that are missing from the asserted prior art." PO Sur-reply 3–4. To the extent Patent Owner argues Petitioner relied on background knowledge to supply a particular missing limitation of a claim, we address those arguments in our analysis of claims below.

confidential." PO Sur-reply 3–5. First, we do not rely directly on Exhibits 1058 and 1059 as evidence of prior art asserted against the Challenged Claims. Second, the Federal Circuit, has found that in an *inter partes* review proceeding, the Board "may rely on evidence other than just prior art" and a petitioner may "rely on evidence beyond the asserted prior art." *Yeda Research and Dev. v. Mylan Pharma. Inc.,* 906 F. 3d 1031, 1041 (Fed. Cir. 2018) (explaining that the Board has recognized that non-prior art evidence of what was known "cannot be applied, independently, as teachings separately combinable" with other prior art, but "can be relied on for their proper supporting roles, e.g., indicating the level of ordinary skill in the art, what certain terms would mean to one with ordinary skill in the art, and how one with ordinary skill in the art would have understood a prior art disclosure").

5. Independent Claim 1

Petitioner contends that the subject matter of claim 1 would have been obvious over Collinge. Pet. 36–52. In describing the disclosure of Collinge, Petitioner states (*id.* at 26), in part, as follows:

> Collinge teaches a remote system (100) separate from a user mobile device, that generates payment credentials, including a "single use key" transmitted "to the mobile device, wherein the mobile device is not required to have a secure element." [Ex. 1011 ¶¶ 7, 39, 43, cl. 1]. The "single use key" is used by the user's mobile device to "generate a payment cryptogram valid for a single payment transaction." [Ex. 1011 ¶ 43]; *see also* [Ex. 1009 ¶ 10; Ex. 1010 ¶ 10]. The remote system and the mobile device "may communicate using dual channel communication." [Ex. 1011 ¶ 43].
>
> Collinge discloses a mobile device including a mobile payment application 194 configured to conduct payment transactions with a POS terminal via NFC without the use of a SE. [Ex. 1009 ¶¶ 2, 3, 33, 75; Ex. 1010 ¶¶ 2, 3].

Petitioner also provides a limitation-by-limitation discussion of how Collinge discloses the features and recited stapes/elements of claim 1 and, to the extent a limitation was not expressly disclosed in Collinge, why it would have been obvious to a person of ordinary skill based on Collinge's disclosure in light of the knowledge of a person of ordinary skill in the art. *Id.* at 36–52. We determine that Petitioner has shown that claim 1 would have been obvious over Collinge and adopt as our own determination Petitioner's contentions, as supported by the evidence cited by Petitioner. *See id.*; Pet. Reply 8–16.

Patent Owner argues that Petitioner fails to show how Collinge renders obvious limitations 1.A-3, 1.C, 1.E-2, and 1.E-3 of claim 1. PO Resp. 13–29; PO Sur-reply 5–16; *see also supra* Section II.B (quoting the claim and including Petitioner's sub-numbering for its steps and elements). We focus our discussion below on these disputed limitations and disagree with Patent Owner's arguments for the reasons that follow.

> Limitation [1.A-3]: [at a mobile device, executing an application in an operating system of the mobile device, the application . . .] configured to request, from a remote computer system hosting the corresponding digital credential, over a wireless network that is separate from the first communications channel, data associated with the account

Patent Owner argues that "Collinge does not disclose or render obvious a 'request [for] data associated with the account."[17] PO Resp. 13–17 (emphasis omitted, alteration in original). As shown by Petitioner, Collinge states that "[p]ayment credentials corresponding to the

[17] Patent Owner does not provide additional argument in its Sur-reply in regard to limitation [1.A-3]. *See generally* PO Sur-reply.

payment account may be stored by a remote SE (remote-secure element) system 110 for provisioning to the mobile device 104." Pet. 38 (quoting Ex. 1011 ¶ 42). We agree with Petitioner that when the mobile payment application of Collinge transmits a CAP token to the remote-SE system it corresponds to a "request" for "data associated with the account," because it "causes the remote-SE system to generate and return payment credentials in an encrypted payload after verification of CAP token." *Id.* (citing Ex. 1006 ¶ 87; Ex. 1011 ¶¶ 81–84, 85).

Patent Owner argues that the "CAP token's purpose is simply to authenticate the mobile device," and that the mere fact that account information is subsequently returned after verification of the CAP token "simply illustrate[s] the relative order of stages." PO Resp. 13–14 (citing Ex. 2009 ¶¶ 84–87) (emphasis omitted). The order of stages referred to by Patent Owner, however, supports the showing that transmitting a CAP token to the remote-SE system corresponds to a "request." Patent Owner does not dispute that in Collinge the remote SE system provides data associated with the account to the mobile device in response to the mobile device transmitting a CAP token to the remote SE system. Indeed, Patent Owner does not suggest any purpose for authenticating the mobile device using the CAP token other than to enable the remote SE system to send a response to the mobile device. Thus, while the CAP token may also serve to authenticate the mobile device, transmitting the CAP token to the remote-SE system in the process of obtaining account information in response constitutes a "request," as required by claim 1.

We reach the same determination notwithstanding Patent Owner's argument that there are "several additional stages" involving authentication between when the mobile payment application of Collinge transmits a CAP

token to the remote-SE system and when, in response, the remote-SE system returns payment credentials in an encrypted payload after verification of CAP token to the mobile device. *Id.* at 14–15 (citing Ex. 2009 ¶¶ 85–90). Claim 1 recites a "method comprising" a series of steps, which does not preclude additional steps, Patent Owner does not argue that claim 1 precludes intervening stages, and any intervening stages do not alter the fact that in Collinge it is the transmission of the CAP token to the remote-SE system (i.e., a "request") that causes the remote-SE system to generate and return payment credentials to the mobile device. *See* Ex. 1001

We have considered Dr. Easttom's opinions in this regard on behalf of Patent Owner and are not persuaded that in Collinge "[t]he CAP token sent in stage 3 has one purpose, which is to validate the mobile application." Ex. 2009 ¶ 88. Patent Owner does not show any suggestion in Collinge of any need to authenticate the mobile application in Collinge but for the primary purpose of transmitting account information from the remote computer system back to the mobile device. Dr. Easttom also states that "[t]he occurrence of action B temporally after action A does not in any way teach that action A was a request for action B," and that a person of ordinary skill "reading Collinge would not understand it this way." *Id.* ¶ 91 (emphasis omitted). Dr. Easttom, however, does not explain what more a "request" requires, in the context of claim 1, than the initiation of a process by the mobile device through which the remote computer system is contacted by the mobile device and then returns data associated with the account to the mobile device. In other words, Patent Owner does not suggest Collinge teaches any other process whereby the mobile device obtains account information from the remote computer system other than by first transmitting a "request" from the mobile device in the form of a CAP

token to the remote computer system. Accordingly, we find Petitioner has shown by a preponderance of the evidence that Collinge discloses the subject matter recited in limitation [1.A-3].

> Limitation [1.C]: receiving by the application, from the remote computer system, over the wireless network, the first set of data associated with the account, the first set of data associated with the account usable by the application to formulate an application protocol data unit response, the first set of data comprising a first non-permanent cryptographic key associated with the account

Petitioner shows that "Collinge discloses that the mobile payment application can receive an encrypted payload and payment credentials from the cloud system over a wireless network," that the "encrypted payload can include a 'single use key' including a generating key for generation of a CVC3 cryptogram or Application Cryptogram, and that the "generating key may be a KS_{UN} . . . which is nonpermanent (unique to each transaction) and associated with the account." Pet. 43 (citing Ex. 1009 ¶¶ 68–71; Ex. 1011 ¶¶ 9, 1, 50, 83, 141, Fig. 17). Petitioner also shows that "KS_{UN} is uniquely, mathematically, and deterministically associated with the account, because it is generated from a card-level key K_{DUN}, which is in turn generated from the account number (PAN)." Pet. Reply 10 (citing Ex. 1009 ¶¶ 69–71; Ex. 1050 ¶ 30); Pet. 43.

Patent Owner argues that "Collinge does not disclose or render obvious a non-permanent cryptographic key associated with the account." PO Resp. 18–20 (emphasis omitted); PO Sur-reply 5–6. Patent Owner recognizes that Petitioner contends K_{SUN} is associated with the account because "it uses the account-specific ATC," and "it uses an account-specific key (K_{DUN}), which itself comes from the account number, in its generation."

PO Resp. 18 (citing Pet. 43). Patent Owner argues that "the disclosures in the Collinge Provisional that Petitioner relies on (i.e., [Ex. 1009 ¶¶ 68–71] were not carried forward into Collinge, could not have been ascertained by reading Collinge alone, and cannot be used as prior art disclosures in this proceeding." PO Resp. 18–19.

As explained above (*see supra* Section III.D.2), we disagree with Patent Owner in this regard and have determined that Collinge properly incorporated by reference disclosures in the '095 Provisional (Ex. 1009) relied upon here by Petitioner. Thus, the '095 Provisional's disclosure *is* Collinge's disclosure (and Collinge is prior art).

Patent Owner next argues that "Petitioner makes no assertion and provides no evidence that Collinge discloses" the recited "first set of data associated with the account usable by the application to formulate an application protocol data unit response." PO Resp. 20–22; PO Sur-reply 6–7. To clarify Patent Owner's position, we note that the recited "first set of data" of limitation [1.C] is the "data associated with the account" of limitation [1.A-3], which we found above was shown by Petitioner to be disclosed by Collinge.

Petitioner shows that Collinge discloses the recited "first set of data" for the same reasons Collinge discloses the recited "data associated with the account," as these two elements refer to the same data. Pet. 43 (referring back to the analysis of limitation [1.A-3] and explaining that "Collinge discloses that the mobile payment application can receive an encrypted payload and payment credentials from the cloud system over a wireless network," that the "encrypted payload can include a 'single use key' including a generating key for generation of a CVC3 cryptogram or Application Cryptogram," and that the "generating key may be a

KSUN . . .which is nonpermanent (unique to each transaction) and associated with the account." *Id.* (citing Ex. 1009 ¶¶ 68–71; Ex. 1011 ¶¶ 9, 13, 50, 82, 83, 141, Fig. 17). Accordingly, the remaining issue raised by Patent Owner over the issue is whether a person of ordinary skill in the art would have found it obvious for the "first set of data" to be "usable" by the application of Collinge "to formulate an application protocol data unit response [APDU], " as required by claim limitation 1[C].

Petitioner further shows by a preponderance of the evidence that it would have been obvious for the "first set of data" to have been usable to formulate an APDU response in light of Collinge's disclosure. *Id.* at 43–44 (citing Ex. 1006 ¶ 95; Ex. 1021 § 6.5; Ex. 1037, 46–48). Dr. Fiske explains in this regard as follows:

> It is well known in the art that, during the interrogation, commands issued by the terminal and responses from the 'Card' are communicated in command- and response-application protocol data units (C-APDUs and R-APDUs), respectively and it would be obvious to implement Collinge in this way to ensure interoperability with EMV-standardized devices.

Ex. 1006 ¶ 95 (citing Ex. 1021 § 6.5; Ex. 1037, 46–48); *see also* Pet. Reply 11 (explaining that Collinge expressly enabled "a PayPass (EMV-compliant) transaction," that "nearly all smart card payment systems at that time did and still do globally" use APDU messages, and that a person of ordinary skill would have known that "APDUs are simply standardized messages exchanged between smart cards and smart card POS terminals, [and] that any response message, including the cryptogram, would be conveyed via an APDU" (citing, *e.g.*, Ex. 1021 §§ 6.1–6.2; Ex. 1037, 46–47; Ex. 1050 ¶¶ 33–34). Dr. Fiske additionally explains that "APDU messages are standard communication format for both contactless and contact readers

and payment, as defined in ISO/IEC 7816-4 standard, a fact acknowledged by the '171 Patent itself." Ex. 1050 ¶ 33 (citing Ex. 1001, Table 1).

We disagree with Patent Owner's arguments in opposition to Petitioner's obviousness allegations. PO Resp. 20–22; PO Sur-reply 6–7. Patent Owner argues that "Petitioner cannot prove obviousness simply by asserting that there could be a benefit . . . to using APDUs for communications between the terminal and the 'Card,'" that Petitioner fails to show an expectation of success "in modifying Collinge to use an [APDU] response," and that Petitioner has not shown that the cited exhibits (Exhibits 1021 and 1037) are prior art for purposes of supplying "a limitation that is plainly absent from Collinge." PO Resp. 21–22 (emphasis omitted); *see also* PO Sur-reply, 7 (arguing that "Petitioner provides no contention that the technology here is unusually simple or straightforward, and it is not").

We disagree with Patent Owner's arguments because here Petitioner is not relying on some other disclosure to fill a missing limitation absent from Collinge, but is instead relying only on Collinge and the knowledge a person of ordinary skill in the art would possess when appreciating the teachings of Collinge. Petitioner is not suggesting Collinge needed to be modified to add the use of an APDU, but, rather, that Collinge's disclosure already contemplated it based on the well-known background of the art. Petitioner shows by a preponderance of the evidence that "the Collinge Provisionals state the disclosures therein are intended to be used in a 'standard' PayPass transaction," and that a person of ordinary skill in the art would have considered "the PayPass Specification (and EMV Specifications, with which the PayPass Specification complies) when reading Collinge." Pet. Reply 8 (citing Ex. 1009, 8, 14–15, 22–23; Ex. 1050 ¶ 22).

In sum, Petitioner shows that Collinge describes a process to be used in a "standard" PayPass transaction and that a person of ordinary skill in the art would have known, at a minimum, that it would have been obvious from Collinge that the "first set of data" (i.e., the encrypted payload in Collinge) would have been "usable" by the application of Collinge "to formulate an application protocol data unit response," as required by limitation [1.C]. Petitioner further demonstrates how Collinge discloses that the "first set of data" was "useable by the application to formulate" an APDU response in addressing limitation [1.E–3], which specifically requires "generating a response." *See* Pet. Reply 11 (explaining that "[d]etails of how [the encrypted payload] is used to formulate an APDU response are explained where that is separately claimed"); *see also id.* (citing Pet. 48–50 (addressing limitation [1.E-3])).

> Limitation [1.E-2]: generating a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and

Petitioner demonstrates that Collinge discloses a mobile device that "sends a generated payment cryptogram and payment credentials to the POS terminal," which may be, for example "an application cryptogram or a dynamic card validation code (CVC3)." Pet. 46–47 (citing Ex. 1009 ¶¶ 44, 61, 64, Table 1; Ex. 1011 ¶¶ 44, 55, 70, 77). Collinge makes clear that the mobile payment application generates "the payment CVC3 value using the information in the encrypted payload." Ex. 1011 ¶ 85. Petitioner further shows that "the encrypted payload can include KS_{UN}, an unpredictable cryptographic key, which is locally stored," and that "[u]sing a single-use

key, such as KS_{UN} to generate a cryptogram results in a cryptogram that does not include the single-use key." Pet. 47 (citing Ex. 1006 ¶ 103; Ex. 1009 ¶¶ 61, 71; Ex. 1011 ¶¶ 9, 13, 83, 85, Fig. 17; Ex. 1034, 17–18; Ex. 1039). Dr. Fiske further explains in this regard that a person of ordinary skill in the art would have found such an implementation of Collinge to be "standardized operations in secure payment transactions" and merely the application of "a known technique (MAC computation using key known only by both parties) to yield predictable results (e.g., allowing issuer to verify card authenticity)." Ex. 1006 ¶¶ 103–104 (citing Ex. 1034, 17–18; Ex. 1039).

Patent Owner argues "Collinge does not disclose or render obvious "wherein the response cryptogram does not include the local cryptographic key."[18] PO Resp. 22–25 (emphasis omitted). Specifically, Patent Owner argues that, "[b]ecause Collinge itself does not describe the "CVC3 calculation" from Exhibit 1009 that Petitioner relies on, that disclosure cannot be used here." *Id.* at 23 (citing Ex. 2009 ¶¶ 118–122). As explained above (*see supra* Section III.D.2), we disagree with Patent Owner in this regard and have determined that Collinge properly incorporated by reference disclosures in the '095 Provisional (Ex. 1009) relied upon here by Petitioner. Patent Owner also asserts that according to Dr. Easttom "there are numerous ways to generate a cryptogram using a cryptographic key, including techniques that would include the generating key in the cry[p]togram." *Id.* at 24 (citing Ex. 2009 ¶ 122; Ex. 2035, 29:20–30:19).

[18] Patent Owner does not provide additional argument in its Sur-reply in regard to limitation [1.E-2]. *See generally* PO Sur-reply.

We disagree with Patent Owner's argument for several other reasons. First, even if there were alternatives that would "include the generating key," that does not suggest that a method that excluded the generating key was not obvious. Second, we give little weight to Dr. Easttom's opinion in this regard because he cites no evidence in support of his opinion that there were "numerous ways to generate a cryptogram using a cryptographic key, including techniques that would include the generating key." Ex. 2009 ¶ 122. Third, Patent Owner cites the testimony of Dr. Fiske as support for Patent Owner's argument, but Dr. Fiske's testimony merely says that "there are alternative mechanisms for generating cryptograms to those in EMV," but that a person of skill would have also understood "that, to have any usefulness in payments, the appropriate form would be to use the EMV standards." Ex. 2035, 30:14–19. Regardless, Dr. Fiske also explains that "Collinge, via its incorporation of the Collinge Provisionals, recites an explicit formula for CVC3 generation by using K_{SUN} as an encryption key to perform DES3 cryptographic operation." Ex. 1050 ¶ 35 (citing Ex. 1009, 29–30); *see also id.* ¶ 36 (explaining that if cryptographic calculations like DES3 included the generating key "anyone with the cryptogram could use the included key to create a valid yet fraudulent payment request—undermining the entire purpose of using encryption").

> Limitation [1.E-3]: responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to an electronic reader through the communication channel, the at least one device response communication comprising at least one response application data protocol unit containing the response cryptogram and an account identifier for the account

As discussed above (*supra* Section III.C), Petitioner offers two alternative ways of construing this limitation. In the absence of any dispute by Patent Owner with regard to the Second Construction, we first address how Petitioner shows the limitation would have been obvious over Collinge construing the recited "at least one device response communication comprising at least one response application data protocol unit containing the response cryptogram and an account identifier for the account" to mean "one or more response application data protocol units, each of which contains both the response cryptogram and an account identifier for the account." *See* Pet. 24–25; PO Resp. 25–29.

Petitioner explains how Collinge discloses "generating a response cryptogram" by the mobile device, as required by limitation [1.E-2], which we also discuss above. *See* Pet. 46–47. Limitation [1.E.3] further requires "responding" by the mobile device to the point-of sale terminal with an APDU that includes both the "response cryptogram" and "an account identifier." Petitioner shows that "Collinge discloses that the mobile device sends payment credential data," and that a person of ordinary skill in the art would have understood that credential data "to include generated payment cryptogram and other 'common payment credential information' such as account information (e.g., PAN)[] to the POS terminal in response to a POS communication." Pet. 48–49 (citing, *e.g.*, Ex. 1009 ¶¶ 61, 64, Table 1; Ex. 1011 ¶¶ 44, 55, 70, 77;). Petitioner also shows for the same reasons discussed above that "the card (or device) being interrogated would respond to a command APDU (C-APDU) from the POS terminal with a response APDU." *Id.* at 48.

As Dr. Fiske further explains, a person of ordinary skill in the art would have understood from Collinge that it discloses a process "compatible

with EMV transactions," and that "in an EMV mode contactless Visa transaction, the POS Kernel issues a GPO command, and the "Card" may return a cryptogram as well as Track 2 Equivalent Data, which contains, among other things, a PAN (Application PAN)." Ex. 1006 ¶ 109 (citing Ex. 1027 § 2.4.1, Table E-6). Petitioner further shows that "in an EMV mode contactless Visa transaction, the POS Kernel issues a GPO command, and the 'Card' may return a cryptogram as well as Track 2 Equivalent Data, which contains, among other things, a PAN (Application PAN)."[19] Pet. 50 (citing Ex. 1027 § 2.4.1, Table E-6).

Patent Owner argues "Collinge does not disclose or render obvious a 'device response communication comprising at least one response application data protocol unit containing the response cryptogram and an account identifier for the account.'" PO Resp. 25–29 (emphasis omitted); PO Sur-reply 7–8; Pet. 24–25. We do not agree with Patent Owner's opposing arguments. First, Patent Owner again argues that the disclosures in the Collinge Provisionals were "not carried forward into Collinge." PO Resp. 27–28. As explained above (*see supra* Section III.D.2), we disagree with Patent Owner in this regard and have determined that Collinge properly incorporated by reference disclosures in the '095 Provisional (Ex. 1009) relied upon here by Petitioner.

Next, Patent Owner argues that Petitioner "provides no explanation as to how 'CVC3' and 'application cryptogram,'" would have informed a person of ordinary skill "that Collinge is compatible with *any* EMV

[19] Petitioner also shows that a person of ordinary skill in the art would have understood that a PAN is an account number corresponding to the recited "account identifier" of claim 1. Pet. 49 n.6 (citing Ex. 1006 ¶ 107 n.3).

transactions." PO Resp. 28. We credit the testimony of Dr. Fiske in this regard, who explains that "based on Collinge's references to well-known transaction systems such as "PayPass" [Ex. 1009 ¶ 2], and terminologies (e.g. "CVC3," "application cryptogram"), [Ex. 1011 ¶ 50]," a person of ordinary skill "reading Collinge would understand it as disclosing devices, systems, and methods compatible with mainstream contactless payment transactions including EMV transactions." Ex. 1006 ¶ 73. Dr. Easttom's testimony in support of Patent Owner on this point is not convincing because it is premised on his view that the PayPass disclosures in Collinge's provisional "are not carried forward into Collinge," which we reject as explained above. *See* Ex. 2009 ¶¶ 125–126.

Additionally, Petitioner also shows Collinge discloses the recited "at least one device response communication comprising at least one response application data protocol unit containing the response cryptogram and an account identifier for the account" if construed to mean to mean "one or more response application data protocol units, collectively containing the response cryptogram and an account identifier for the account," in accordance with Petitioner's First Construction. *See* Pet. 24–25, 48–50. Petitioner shows that Collinge, in the '095 Provisional, discusses the PayPass card specification and that it would have been known to a person of ordinary skill in the art, as follows, that:

> during interrogation for a contactless transaction including a Mastercard Paypass transaction, the 'Card' (user device) would provide, in R-APDUs, account information such as a Primary Account Number (PAN) in response to a READ RECORD command, and a response cryptogram (CVC3 or Application Cryptogram) in response to a COMPUTE CRYPTOGRAPHIC CHECKSUM or GENERATE AC command APDU.

Pet. 49–50 (citing Ex. 1006 ¶ 108; Ex. 1026 §§ 3.4.2, 3.4.3, 3.8.1–3.8.3, 5.2, 5.3; Ex. 1048 ¶¶ 17, 18).

We do not agree with Patent Owner's opposing arguments addressing Petitioner's contentions based on the First Construction. PO Resp. 25–29; PO Sur-reply 7–8. First, Patent Owner again argues that the disclosures in the Collinge Provisionals were "not carried forward into Collinge." PO Resp. 25–26. As explained above (*see supra* Section III.D.2), we disagree with Patent Owner in this regard and have determined that Collinge properly incorporated by reference disclosures in the '095 Provisional (Ex. 1009) relied upon here by Petitioner. Next, Patent Owner argues that the cited EMV Specification (Ex. 1026) refers to "PayPass" only once under "Implementation Options," which is insufficient to show "that a 'Mastercard interrogation' is being implanted," and that the "Mastercard interrogation" implementations "are not mandatory for EMV compliance and may not be implemented in a particular installation." PO Resp. 26–27.

We disagree with Patent Owner's arguments. Patent Owner offers no explanation for why addressing "PayPass" only once in Exhibit 1026 is insufficient or why a person of ordinary skill in the art would only have knowledge of "mandatory" specifications. We agree with Petitioner and find that a preponderance of the evidence shows that a person of ordinary skill in the art "reviewing Collinge would [have been] familiar with the PayPass specification, and [would have known] that PayPass is Mastercard's implementation of contactless EMV-compliant transactions." Pet. Reply 14.

6. Independent claim 17

Petitioner contends the subject matter of claim 17 would have been obvious over Collinge. Pet. 63–65. As noted above, claim 17 recites "[a] system for secure application-based participation by a mobile device in

point-of-sale interrogations" comprised of features that generally correspond to the steps and limitations of the method recited in claim 1. Ex. 1001, 53:15–54:22. Petitioner provides a limitation-by-limitation discussion that substantially relies upon its analysis of corresponding features of claim 1 to show how Collinge discloses the features of claim 17 and, to the extent a limitation was not expressly disclosed, why it would have been obvious to a person of ordinary skill in the art based on their reading of Collinge. Pet. 36–52, 63–65. Additionally, with regard to the "controller" exclusively recited in claim 17, Petitioner shows mobile device 104 of Collinge "necessarily has a controller configured to route communications over a communication channel from an electronic reader," and that a controller was well-known to a person of ordinary skill as hardware "necessary to allow NFC communications." *Id.* at 62 (citing Ex. 1006 ¶¶ 145, 146; Ex. 1011 ¶ 70).

Patent Owner argues that Petitioner's contentions challenging claim 17 based on Collinge "fail for the same reasons" as those for claim 1.[20] PO Resp. 13–29, 49. We disagree with Patent Owner's arguments for the reasons provided above in our discussion of claim 1. We determine that Petitioner has shown that claim 17, like claim 1, would have been obvious over Collinge and adopt as our own determination Petitioner's contentions, as supported by the evidence cited by Petitioner. *See* Pet. 63–65.

[20] More precisely, Patent Owner addresses claims 17, 24, and 25 together and states that Petitioner's contentions fail for the "same reasons" as "claims 1, 8, and 17." PO Resp. 49. Elsewhere Patent Owner clearly addresses claims 1 and 17 based on the same arguments. *See, e.g.*, *id.* at 13 (arguing that "Collinge does not anticipate or render obvious claim 1 (or 17)" (emphasis omitted).

7. Dependent claims 4 and 20

Claim 4 depends from claim 1 and further recites "wherein the interrogation conforms to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification." Ex. 1001, 52:7–10. Claim 20 depends from claim 17 and recites essentially the same limitation as claim 4. *Id.* at 54:32–35.

Petitioner shows that the '095 Provisional, incorporated by reference by Collinge, "expressly references making transactions compliant with the PayPass card specification." Pet. 54 (citing Ex. 1009 ¶¶ 29–32, 40). Petitioner further shows that "card specifications were well known in the art," and that a person of ordinary skill in the art "would have been motivated to make their systems compliant with such specifications including Mastercard PayPass or EMV Specifications to expand their market opportunity by allowing interoperability with existing and expected future payment infrastructure." *Id.* (citing Ex. 1006 ¶ 118). On this basis, alone, we find that Petitioner has shown that Collinge renders obvious the subject matter of claims 4 and 20.

Additionally, Petitioner also argues that Collinge "refers to 'm/chip payment transactions,'" which a person of ordinary skill in the art would have understood "to refer to known EMV-compliant payment system specifications defining sets of inputs and responses."[21] *Id.*; Ex. 1006 ¶ 117; *see also* Ex. 1011 ¶ 49 (stating that "[t]he m/chip payment credentials 206

[21] Both the Petition and Dr. Fiske cite as support Exhibit 1011 ¶ 44, which we understand to be a typographical error intended to cite ¶ 49, which expressly discusses "m/chip payment transactions."

may include data elements specific to m/chip payment transactions, such as issuer action codes, risk management data, and offline data authentication object lists."). Patent Owner argues that because "m/chip" and "m/chip payment transactions" are terms that do not appear in the Collinge Provisionals, it is subject matter that was not carried forward from the Collinge Provisional.[22] PO Resp. 12, 41–43. Petitioner argues that the absence of the specific term "m/chip" in the Collinge Provisionals is "irrelevant," because a person of ordinary skill in the art would have "understood that PayPass Specifications include PayPass-M/Chip, published in September 2008." Pet. Reply 21 (citing Ex. 1050 ¶ 51).

We agree with Petitioner on this argument because the issue is not whether the language "m/chip" appears in the Collinge Provisionals to be carried forward to Collinge, but whether a person of ordinary skill in the art, reading Collinge, which includes the disclosure of the '095 Provisional, would have found it obvious that the "interrogation conforms to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification," as required by claims 4 and 20. The '095 provisional discloses just that, including, for example, a process in which "[t]he PayPass Terminal executes the standard payment transaction process." Ex. 1009 ¶ 61, Table 1. This disclosure regarding using "standard" processes invokes the knowledge of such standards and specifications the ordinarily skilled artisan would have had reading Collinge.

---

[22] Patent Owner refers in its argument to claims 4 and 21, which we understand to be a typographical error intended to refer to claim 20, because the language of claim 20, not claim 21, mirrors the language of claim 4. *See* PO Resp. 41.

Patent Owner also argues, again, that "Petitioner's reference to 'PayPass' disclosure in the Collinge Provisional is not allowed since Collinge does not carry forward that disclosure." PO Resp. 41 n.7. As explained above (*see supra* Section III.D.2), we disagree with Patent Owner in this regard and have determined that Collinge properly incorporated by reference disclosures in the '095 Provisional (Ex. 1009) relied upon here by Petitioner. We determine that Petitioner has shown that claims 4 and 20 would have been obvious over Collinge and adopt as our own determination Petitioner's contentions, as supported by the evidence cited by Petitioner. *See* Pet. 54; Pet. Reply 21.

8. Dependent claims 6 and 22

Claim 6 depends from claim 1 and further recites "wherein generating the response cryptogram comprises encrypting the set of inputs using the local cryptographic key according to a digital encryption standard (DES) calculation to generate an output, wherein the response cryptogram includes a portion, but not all, of the output." Ex. 1001, 52:16–21. Claim 22 depends from claim 17 and recites essentially the same limitation as claim 4. *Id.* at 54:42–47.

Collinge, including the incorporated disclosure of the '095 Provisional, expressly states that "the cryptographic process uses the triple Data Encryption Standard (DES) algorithm to generate the CVC3 value." Ex. 1009, cl. 6. We further credit the testimony of Dr. Fiske in this regard, who explains with cited support that the "message authentication code (MAC) is generated by DES," that "CVC3 is a MAC," and that the '095 Provisional discloses using DES to generate a CVC3 value. Ex. 1006 ¶ 121. Thus, Petitioner shows that a person of ordinary skill in the art would have known that "a response cryptogram like CVC3 is generated using DES

calculation because it is the predominant symmetric encryption algorithm in financial applications—specifically, triple DES (DES executed three times)," and that "[b]ecause only two bytes of the longer cryptogram are included in the response, the response includes less than the entire output." Pet. 56 (citing Ex. 1006 ¶ 121; Ex. 1009 ¶ 71; Ex. 1016 ¶ 53; Ex. 1034, 17–18; Ex. 1043).

Patent Owner argues in opposition that Petitioner "points to no disclosure in Collinge as to any particular technique for generating the alleged response cryptogram, let alone any digital encryption standard."[23] PO Resp. 45–46 (emphasis omitted). Patent Owner also argues that there were alternatives to DES known in the art and that "[i]t is not sufficient to show that DES was known." *Id.* at 46. Patent Owner disregards the express disclosure in the '095 Provisional presumably based on its argument that it is not a part of Collinge. As explained above (*see supra* Section III.D.2), we disagree with Patent Owner in this regard and determine that Collinge properly incorporated by reference disclosures in the '095 Provisional (Ex. 1009) relied upon here by Petitioner; *see also* Ex. 1050 ¶ 54 (Dr. Fiske explaining that "[t]he Collinge Provisionals disclose that the 'DES3' algorithm is used to calculate the cryptogram" (citing Ex. 1009 ¶ 71)). Given the express disclosure in Collinge, the potential availability of alternatives is irrelevant. Moreover, Dr. Fiske explains that the use of DES was merely the application of "standard operation in the industry." Ex. 1006 ¶¶ 122 (citing Ex. 1020 §§ 8.1.2, A1.2, A1.3, B1.1). We determine that Petitioner has shown that claims 6 and 26 would have been obvious over

[23] Patent Owner provides no further argument in its Sur-reply in regard to the additional limitations of claims 6 or 22. *See generally* PO Sur-reply.

Collinge and adopt as our own determination Petitioner's contentions, as supported by the evidence cited by Petitioner. *See* Pet. 56; Pet. Reply 21–22.

9. Dependent claims 8 and 9

Claim 8 recites as follows:

> at the remote computer system:
> [8.A] prior to the interrogation, generating the first non-permanent cryptographic key at the remote computer system, associating the first non-permanent cryptographic key with the account, and sending the first non-permanent cryptographic key and the account identifier to the mobile device over the wireless network;
> [8.B] after the interrogation, generating the second non-permanent cryptographic key at the remote computer system, associating the second non-permanent cryptographic key with the account and sending the second nonpermanent cryptographic key and the account identifier to the mobile device over the wireless network

Ex. 1001, 52:25–38. Claim 9 further depends from claim 8.

Petitioner contends that the subject matter of claim 8, which depends from claim 1, would have been obvious over Collinge based on the same arguments and evidence upon which Petitioner relies for showing the obviousness of the limitations of claim 1. Pet. 57. Like the Petition, Dr. Fiske, in his Declaration, testimony also refers back to reasons he earlier discusses regarding the limitations of claim 1 as showing how Collinge also renders obvious the limitations of claim 8. Ex. 1006 ¶ 126 (relying on "reasons discussed in [1.A-3], [1.B], [1.C], and [1.E-3] to show that a person of ordinary skill "would have understood or found it obvious that Collinge discloses" [8.A]); ¶ 127 (relying on "reasons discussed in [1.F] and [1.G]" to show "Collinge discloses" limitation [8.B]).

Patent Owner argues with regard to limitation [8.A] that Petitioner fails to make the necessary showing to carry its burden. PO Resp. 37–39;

PO Sur-reply 18–21. In regard to Petitioner relying on its [1.A-3] contentions, Patent Owner argues that Petitioner relies on the PAN as the account identifier and that Collinge "makes no mention of the encrypted payload including the PAN." PO Resp. 38. In regard to Petitioner relying on its [1.B] contentions, Patent Owner argues that Petitioner "contends that the application makes a request for a first set of data, which is a digital credential associated with the account, but makes no mention of the PAN." *Id.* In regard to Petitioner relying on its [1.C] contentions, Patent Owner argues that "Petitioner contends that the mobile payment application can receive payment credentials from the cloud system over a wireless network, but is silent as to the PAN." *Id.* In regard to Petitioner relying on its [1.E-3] contentions, Patent Owner argues that "Petitioner contends that the mobile device sends payment credential data, which a [person of ordinary skill in the art] would understand to include generated cryptogram and 'other common payment credential information' such as the PAN," but that claim 8 is directed to an account identifier sent to the mobile device, not from the mobile device. *Id.* at 38–39. According to Patent Owner, Petitioner alleges the remote-SE sends an "encrypted payload" to the mobile device, but provides no supported contention in the Petition that Collinge includes the PAN in the encrypted payload. *Id.* at 39 (citing Ex. 2009 ¶ 142).

We recognize that Petitioner did not separately address in the Petition the limitations in claim 8 and relies, instead, on arguments and evidence Petitioner addressed under claim 1, making it more difficult for both Patent Owner and the Board to distinguish between arguments pertaining only to claim 1 from those that also apply to claim 8. Nevertheless, because the subject matter of claim 8 pertains directly to the limitations of claim 1, the analysis of which is cited by Petitioner, a thorough consideration of the

evidence Petitioner relies on leads us to disagree with Patent Owner's argument for several reasons.

First, to the extent Patent Owner implies the recited "account identifier" of claim 8 must be in the same encrypted payload Petitioner relies on to show how the recited "first non-permanent cryptographic key" is sent to the mobile device, Patent Owner's argument is beyond the scope of limitation 8[A], which only requires that *both* "the first non-permanent cryptographic key and the account identifier" are *sent* "to the mobile device over the wireless network" *prior* to the interrogation. Second, even if claim 8 were understood to require "sending the first non-permanent cryptographic key and the account identifier to the mobile device over the wireless network" *together*, Patent Owner's arguments are directed only to how Petitioner explained Collinge discloses the features of claim 1, without addressing whether, for the same reasons, Collinge discloses or suggests limitation 8[A]. *See* PO Resp. 38–39 (citing Pet. 48–49. Ex. 2009 ¶ 141) (Patent Owner arguing that Petitioner contends that the mobile device sends payment credential data, which a [person of ordinary skill would have understood] to include generated cryptogram and 'other common payment credential information' such as the PAN," but that it "does not satisfy claim 8, which is directed to an account identifier sent to the mobile device, not to information sent from the mobile device").

Contrary to Patent Owner's argument, Petitioner shows, in its discussion of limitation 1[A][3], that "Collinge states that "[p]ayment credentials corresponding to the payment account may be stored by a remote SE (remote-secure element) system 110 for provisioning to the mobile device 104." Pet. 38 (quoting Ex. 1011 ¶ 42). Collinge's disclosure in paragraph 42 must be understood in the full context of what Collinge

describes. Collinge explains in further detail that the "remote-SE system 110 may build a payment token payload in order to provision the payment credentials to the mobile device 104 for use in a payment transaction," that the "payment token payload may include a card profile 116," that the card profile 116 "may include payment credentials," that the "payment credentials included in the card profile 116 may include common payment credentials 202," and that "common payment credentials 202 may include . . . payment account number [i.e., "PAN"]," and that "the payment token payload may include the card profile 116 and the single use key 118." *Id.* ¶¶ 43, 48, 49; *see also id.* at ¶ 50 (stating that the "single use key 118 may be a payment token used one time to generate a payment cryptogram"). In sum, although Petitioner could have been more diligent in explaining exactly how its discussion of limitation 1[A][3] relates to limitation 8[A], we find the portions of Collinge cited, as further explained in Collinge, demonstrate that Collinge discloses a method whereby the remote computer system sends the account identifier to the mobile device, as well as the first non-permanent cryptographic key, over the wireless network prior to interrogation. *See* Ex. 1011 ¶ 9.

Additionally, in its Reply, Petitioner argues that "the Petition specifically cites to Collinge [0009] as explaining what 'payment credentials' are received from the remote computer system." Pet. Reply 19 (citing Pet. 43). In this regard, Collinge expressly states as follows:

> Another method for generating and provisioning payment credentials to a mobile device . . . includes: storing, in a database, at least a storage key, a plurality of dynamic card validation code keys, and an application transaction counter associated with a mobile application program; provisioning, to the mobile device, at least the storage key, an authentication

> component, and static payment credentials, wherein the static payment credentials are associated with a payment account.

Ex. 1011 ¶ 9. Petitioner argues that this disclosure in Collinge "suggests that the remote system sends 'static payment credentials' (which a [person of ordinary skill would have understood] include the account number) as well as the dynamic KS_{UN}."[24] Pet. Reply 19–20.

Patent Owner argues that "Petitioner's contention as to how a [person of ordinary skill would have understood] 'static payment credentials' is pure speculation by counsel with no evidentiary support." Sur-reply 20. We disagree because Dr. Fiske explained that "[t]raditional magnetic stripe cards contain static data, such as primary account number ("PAN"), expiration date, and CVV verification code." Ex. 1006 ¶ 50. Although Dr. Fiske was most directly addressing "static data" in the context of "traditional magnetic stripe cards," it stands to reason that the meaning of static data similarly applies in the context of payment credentials. Patent Owner offers no evidence or argument to the contrary to dispute the meaning of "static payment credentials" as used in Collinge and explained by Dr. Fiske. *See* PO Sur-reply 20.

Patent Owner also argues with regard to limitation [8.B] that Petitioner fails to make the necessary showing. PO Resp. 39–40; PO Sur-reply 21–22. In regard to Petitioner relying on its [1.F] and [1.G] contentions (*see* Pet. 51–52), Patent Owner argues that limitations [1.F]

---

[24] Patent Owner asserts this argument is outside the scope of a proper reply. *See* PO Sur-reply 20; Ex. 3001. We disagree because it addresses an issue raised by Patent Owner in its Response and refers to an argument made in the Petition where the portion of Collinge at issue was cited. *See* PO Resp. 37–39.

and [1.G] require the application of the mobile device to request and receive a second nonpermanent cryptographic key from the remote computer system after the interrogation, but do not require that the remote computer generate that second nonpermanent cryptographic key "after the interrogation," as required by [8.B]. PO Resp. 40. Patent Owner reasons that the second nonpermanent cryptographic key "could readily be generated prior to interrogation and need not be generated by the remote computer system." *Id.* (citing Ex. 2009 ¶ 145).

We credit the testimony of Dr. Fiske in this regard, who explains that Collinge's disclosed $KS_{UN,}$ the second nonpermanent cryptographic key, can only be generated at the remote computer system (Ex. 1050 ¶ 49 (citing Ex. 1011 ¶ 83) and that a person of ordinary skill in the art would have understood that "when the mobile device uses up the one-time key KS_{UN} in a transaction after an interrogation, it should request a new KS_{UN} from the remote computer for the next transaction, and in response, the remote computer system would generate a KS_{UN} associated with that account and send it to the mobile device in an encrypted payload in response to such a request."[25] Ex. 1050 ¶ 49.

Lastly, Patent Owner argues that KS_{UN} is not an account identifier. PO Sur-reply 22. Our discussion above of how Collinge discloses "[p]ayment credentials corresponding to the payment account may be stored by a remote SE (remote-secure element) system 110 for provisioning to the

[25] We disagree with Patent Owner's assertion that this is an improper reply argument because it is responsive to Patent Owner's argument in its Response that the Petition fails to show the steps being performed after the interrogation. *See* PO Resp. 40; Ex. 3001.

mobile device 104," is not limited by its own terms only to communication *before* the interrogation. Ex. 1011 ¶ 42. Dr. Fiske explains that "it would be obvious to send an account identifier along with the key, so that the mobile device knows which account's key it is receiving, which a [person of ordinary skill in the art would have understood] would be useful when designing a card capable of being used with multiple accounts or a credential wallet that could be used with multiple issuers and accounts."[26] Ex. 1050 ¶ 48. Although we give less weight to Dr. Fiske's testimony in this regard because it fails to identify any supporting evidence, we note there is no evidence to the contrary and Dr. Fiske's conclusion as an expert is entitled to some weight.

Claim 9 depends from claim 8 and further recites "wherein the digital credential comprises a secure element representation maintained at the remote computer system." Ex. 1001, 52:39–41. Patent Owner contends that Petitioner's showing as to claim 9 is insufficient for the same reasons as claim 8. PO Resp. 39. As explained above, we disagree with Patent Owner's arguments directed at claim 8. We determine that Petitioner has shown that claims 8 and 9 would have been obvious over Collinge and adopt as our own determination Petitioner's contentions, as supported by the evidence cited by Petitioner. *See* Pet. 57; Pet. Reply 19–20.

[26] We disagree with Patent Owner's assertion that this is an improper reply argument because it is responsive to Patent Owner's argument in its Response that "Petitioner makes no obviousness argument." *See* PO Resp. 40; Ex. 3001. The Petition alleged claim 8 would have been obvious and Dr. Fiske's additional testimony supports that contention.

10. Dependent claims 10 and 27 (and claims 11–13 and 28–30, which, respectively, depend therefrom)

Claim 10 depends from claim 1 and further recites as follows:

> further comprising, at the remote computer system, performing an authorization process comprising:
> [10.A] receiving an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the response cryptogram and the account identifier;
> [10.B] determining a current non-permanent cryptographic key associated with the account using the account identifier;
> [10.C] calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account;
> [10.D] verifying a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram; and
> [10.E] sending an authorization response to the POS terminal, wherein the data contained in the authorization response is determined, at least in part, by the verifying the correctness of the response cryptogram.

Ex. 1001, 52:42–61. Claim 27 depends from claim 17 and recites essentially the same limitations as claim 10. *Id.* at 54:64–55:14. Claims 11–13 further depend from claim 10 and claims 28–30, which are similar, further depend from claim 27. We determine that Petitioner has shown that claims 10–13 and 27–30 would have been obvious over Collinge and adopt as our own determination Petitioner's contentions, as supported by the evidence cited by Petitioner. *See* Pet. 58–60. We discuss below Patent Owner's arguments in opposition. *See* PO Resp. 30–37; PO Sur-reply 8–18.

Patent Owner argues that claim 10 recites "at the remote computer system," which corresponds to the "same remote computer system" recited

in claim 1. PO Resp. 30. According to Patent Owner, Petitioner relies on "remote-SE system 110" as the remote computer system of claim 1. *Id.* (citing Pet. 38–39; Ex. 2035, 74:15–75:9). Patent Owner further argues that for the recited "remote computer system" limitations of claim 10, Petitioner relies on a "payment network," the "acquirer server 312," "the issuer processing server 308," and the "payment credentials management system," shown as element 704, all of which, Patent Owner argues, are "not part of 'remote SE 110.'" *Id.* at 32; *see also id.* at 36–37 (Patent Owner arguing that the Payment Credentials Management System is "distinct from issuer processing server 308," and that "Petitioner presents no evidence or argument that these distinct components are part of the same remote computer system") (citing Ex. 2009 ¶ 153).

Petitioner explains, and we agree, that Petitioner's identification of the remote computer system of Collinge was not limited to the "remote-SE system 110," but included other aspects of the Collinge computer system that Petitioner expressly relies upon, as shown in the annotated version of Collinge Figure 7 provided by Petitioner in Reply. Pet. Reply 16–18. We find no discrepancy in this regard with the portions of Dr. Fiske's testimony cited by Patent Owner, which does not suggest he relied on "different" remote computer systems to meet the additional limitations of claim 10. *See* PO Resp. 30 (citing Ex. 2035: 74:15–75:9); Pet. Reply. 18.

Next, Patent Owner argues in regard to limitation [10.B] that Petitioner fails to show how Collinge discloses "determining a current non-permanent cryptographic key . . . using the account identifier." PO Resp. 34–35 (emphasis omitted). In regard to limitation 10[B], Petitioner shows that "Collinge discloses that 'the issuer processing server 308 may validate the payment CVC3 value using at least the UN_{READER}, UN_{CLOUD},

and application transaction counter,' by retrieving ('determining') the UN_{CLOUD} and KS_{UN} . . . values that were used by the Payment Credential Management System to generate ("calculating") the CVC3 value." Pet. 59 (citing Ex. 1009, ¶ 61 (Table 1, Step 19a-19b); Ex. 1011 ¶87). According to Patent Owner, "Petitioner makes no mention of issuer processing server 308 determining K_{SUN} using the PAN (i.e., the alleged account identifier)," and that Collinge instead provides that "the 'ATC provided in the Payment Transaction' is 'used to retrieve UN_{CLOUD} and K_{SUN} values.'" *Id.* (citing Ex. 1009 ¶ 23). We disagree with Patent Owner's argument and credit the testimony of Dr. Fiske who explains that, in Collinge, retrieval of KS_{UN} does not use only the ATC (citing Ex. 1009 ¶ 23) and that a person of ordinary skill would have understood that the use of an account identifier such as PAN was also necessary to determine the correct key because "KS_{UN} is generated uniquely with and for a PAN and is specific to a PAN." Ex. 2050 ¶ 45.

Last, Patent Owner argues in regard to limitation [10.C] that Petitioner's reliance on the Collinge statement that "the issuer processing server 308 may validate the payment CVC3 value" and that "[m]ethods for validating a CVC3 will be apparent to persons having skill in the relevant art" are insufficient to show Collinge discloses "calculating a calculated cryptogram," as required by claim 10. Specifically, Patent Owner again argues that the disclosures in the Collinge Provisionals were "not carried forward into Collinge." PO Resp. 35–36 (alteration in original). As explained above (*see supra* Section III.D.2), we disagree with Patent Owner in this regard and have determined that Collinge properly incorporated by reference disclosures in the '095 Provisional (Ex. 1009) relied upon here by Petitioner. Further, Dr. Fiske explains that "Collinge's statement that the

technique for validating a message authentication code, such as CVC3 was 'apparent'" to a person of ordinary skill is supported by "payment-related textbook materials, which make clear that this technique for verifying a cryptogram is basic common sense in the industry." Ex. 1050 21 (citing Ex. 2037, 57–58). We determine that Petitioner has shown that claims 10–13 and 27–30 would have been obvious over Collinge and adopt as our own determination Petitioner's contentions, as supported by the evidence cited by Petitioner. *See* Pet. 58–61; Pet. Reply 24–25.

11. Dependent claims 15 and 32

Claim 15 depends from claim 1 and further recites "wherein the application is configured to generate the response cryptogram according to a card specification." Ex. 1001, 53:9–11. Claim 32 depends from claim 17 and recites essentially the same limitation as claim 15. *Id.* at 56:11–13.

In the Petition and Reply, Petitioner relies on its analysis of claims 4 and 20, which recite "wherein the interrogation conforms to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification," to also show how Collinge discloses the subject matter of claims 15 and 32. Pet. 62; Pet. Reply 21; Ex. 1001, 52:7–10. In short, Petitioner shows that Collinge, which includes the disclosures of the '095 Provisional, discloses a system enabling PayPass transactions "where the interrogation is standardized, including by the PayPass Specification," which a person of ordinary skill would have understood. Pet. Reply 21 (citing, e.g., Ex. 1050 ¶ 50).

Patent Owner argues that Petitioner's contentions fail for the same reasons as Patent Owner argues in regard to claims 4 and 20.[27] PO Resp. 43–44. We disagree for the same reasons explained above in regard to claims 4 and 20. *See supra* Section III.D.7.

Patent Owner also argues that Petitioner fails to show "that either the Mastercard Paypass or EMV Specifications specify how a response cryptogram is generated" or that "conducting a transaction according to either specification involves generating a response cryptogram according to the card specification." *Id.* at 44. Patent Owner also argues that Dr. Fiske "admitted, a transaction could comply with EMV Specifications even when generating a cryptogram using a technique that is different from the optional technique disclosed in the EMV Specifications." *Id.* (citing Ex. 2009 ¶ 154; Ex. 2035, 29:20–30:19, 61:1–62:1) (emphasis omitted). We credit the testimony of Dr. Fiske in this regard, who, contrary to Patent Owner's argument, explains that "[t]he EMV standards include specifications for how cryptograms can be generated, and a person of skill in the art in 2012 would be familiar with those specifications," and that "a person of skill in the art would . . . know that there are alternative mechanisms for generating cryptograms to those in EMV," "[b]ut they would also understand that, to have any usefulness in payments, the appropriate form would be to use the EMV standard." Ex. 2035, 30:1–19. We determine that Petitioner has shown that claims 15 and 32 would have been obvious over Collinge and adopt as our own determination Petitioner's contentions, as supported by the evidence cited by Petitioner. *See* Pet. 62; Pet. Reply 21.

---

[27] Patent Owner provide no further argument in its Sur-reply in regard to the additional limitations of claims 15 or 32. *See generally* PO Sur-reply.

12. Dependent claims 16 and 33

Claim 16 depends from claim 1 and further recites "wherein the first and second non-permanent cryptographic key are associated with an issuer master key." Ex. 1001, 53:12–14. Claim 33 depends from claim 17 and recites essentially the same limitations as claim 16. *Id.* at 56:15–17.

Petitioner shows that "Collinge, via the provisional application incorporated by reference, explains that the non-permanent, single-use keys (KSUN) are associated with an issuer master key [('IMK')] because those keys are generated using an intermediate key (using KD_{UN}) which itself is generated from an issuer master key IMK." Pet. 62 (citing Ex. 1009 ¶ 71; Ex. 1011 ¶ 83). In addition to the express disclosure of Collinge, Petitioner further shows that a person of ordinary skill in the art would have known "using issuer keys to generate card-specific and transaction specific keys for generating authentication cryptograms was well known." Ex. 1006 ¶ 143 (citing, e.g., Ex. 1009 ¶ 71). For example, Dr. Fiske explains that the "EMV Integrated Circuit Cart Specification for Payment" provides that "the 'Session Key' used for generation of the cryptogram, as its name suggests, is generated 'for each transaction performed by the application' using an ICC Master Key—specifically, by 'enciphering an n-byte diversification value with the k-bit ICC Master Key (MK) to produce a k-bit ICC Session Key (SK)'"). *Id.* (citing Ex. 1020 §§ A1.3) (emphasis omitted); *see also* Pet. Reply 22 (showing that "the use of Issuer Master Keys to derive keys used to generate MAC cryptograms is a fundamental principle known to [persons of ordinary skill]") (citing Pet. 62; Ex. 1011 ¶ 83; Ex. 1020 §§ 8.1.2, A1.3.1, A1.4; Ex. 1037, 58; Ex. 1050 ¶ 57).

Patent Owner again argues that the disclosures in the Collinge Provisionals were "not carried forward into Collinge."[28] PO Resp. 47–48. As explained above (*see supra* Section III.D.2), we disagree with Patent Owner in this regard and have determined that Collinge properly incorporated by reference disclosures in the '095 Provisional (Ex. 1009) relied upon here by Petitioner. Patent Owner also argues that "EMV does not mandate any technique for generating session keys." *Id.* at 49. Whether an industry specification is mandated or optional, Petitioner sufficiently shows that a person of ordinary skill would have been familiar with the applicable standards. *See, e.g.*, Ex. 1006 ¶ 143. Thus, in light of the express disclosure in Collinge, as well as the demonstrated background knowledge of a person of ordinary skill, we disagree with Patent Owner's assertion that Petitioner was obligated to further demonstrate "why a [person of ordinary skill" would choose to generate sessions keys in Collinge using an issuer maser key . . . [and] would expect such an application to be successful." *See* PO Resp. 49. We determine that Petitioner has shown that claims 16 and 33 would have been obvious over Collinge and adopt as our own determination Petitioner's contentions, as supported by the evidence cited by Petitioner. *See* Pet. 62; Pet. Reply 22.[29]

13. Dependent claims 24 and 25

Patent Owner does not raise any additional arguments in opposition to Petitioner's contentions directed to dependent claims 24 and 25 beyond the

---

[28] Patent Owner provide no further argument in its Sur-reply in regard to the additional limitations of claims 16 or 33. *See generally* PO Sur-reply.

[29] We do not rely on the last sentence on page 22 of the Reply, which Patent Owner argues is improper new argument.

arguments Patent Owner raises with regard to claims 1, 8, and 17. PO Resp. 49. We determine that Petitioner has shown that the claims 24 and 25 would have been obvious over Collinge and adopt as our own determination Petitioner's contentions, as supported by the evidence cited by Petitioner, as our own determination. *See* Pet. 65 (relying upon analysis of claims 1, 8, and 17).

14. Dependent claims 2, 3, 5, 7, 14, 18, 19*, 21, 23, 26, and 31*

Patent Owner does not raise any additional arguments in opposition to Petitioner's contentions directed to dependent claims 2, 3, 5, 7, 14, 18, 19, 21, 23, 26, and 31 beyond the arguments Patent Owner raises with regard to claims 1 and 17. *See* PO Resp. 13 n.3. We determine that Petitioner shows that the subject matter of claims 2, 3, 5, 7, 14, 18, 19, 20, 23, 26, and 31 would have been obvious over Collinge and adopt as our own determination Petitioner's contentions, as supported by the evidence cited by Petitioner, as our own determination. *See* Pet. 52–57, 60–62.

E. Alleged Anticipation Based on Collinge

Petitioner contends claims 1–4, 6–20, and 22–33 of the '171 patent are anticipated by Collinge. Pet. 36–65; Pet. Reply 8–22. Having already determined that a preponderance of the evidence shows that claims 1–4, 6–20, and 22–33 are unpatentable, it is unnecessary to address this additional grounds.

F. Alleged Anticipation and Obviousness Based on Fiske

Petitioner contends the Challenged Claims are anticipated by and would have been obvious over Fiske. Pet. 66–84. Having already determined that a preponderance of the evidence shows that the Challenged Claims are unpatentable, it is unnecessary to address these additional grounds.

IV. CONCLUSION[30]

For the foregoing reasons, we determine that Petitioner demonstrates by a preponderance of the evidence that the Challenged Claims are unpatentable. Our conclusions are summarized in the following table.

Claims	35 U.S.C. §	Reference /Basis	Claims Shown Unpatentable	Claims Not shown Unpatentable
1–33	103(a)	Collinge	1–33	
1–4, 6–20, 22–33	102	Collinge[31]		
1–33	102	Fiske[32]		
1–33	103(a)	Fiske[33]		
Overall Outcome			1–33	

[30] Should Patent Owner wish to pursue amendment of the Challenged Claims in a reissue or reexamination 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 '171 patent, Patent Owner has a 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).

[31] Because we determine that claims 1–4, 6–20, and 22–33 would have been obvious over Collinge, we do not address Petitioner's additional arguments that claims 1–4, 6–20, 22–33 are anticipated by Collinge.

[32] Because we determine that claims 1–33 would have been obvious over Collinge, we do not address Petitioner's additional arguments that claims 1–33 are anticipated by Fiske.

[33] Because we determine that claims 1–33 would have been obvious over Collinge, we do not address Petitioner's additional arguments that claims 1–33 would have been obvious over Fiske.

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that Petitioner demonstrates by a preponderance of the evidence that claims 1–33 of U.S. Patent 10,032,171 B2 are unpatentable; and

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

PETITIONER:

Eliot D. Williams
Jennifer Tempesta
BAKER BOTTS L.L.P
eliot.williams@bakerbotts.com
jennifer.tempesta@bakerbotts.com

PATENT OWNER:

Seth Lindner
Brett Cooper
BC LAW GROUP, P.C.
slindner@bc-lawgroup.com
bcooper@bc-lawgroup.com

Robert A. Auchter
AUCHTER PLLC
robert@auchterlaw.com