

IN THE 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
U.S. Patent No. 10,032,171

DECLARATION OF DR. CHUCK EASTTOM Ph.D., D.Sc.

TABLE OF CONTENTS

I.	Introduction.....	8
II.	Analysis	9
	A. LEVEL OF ORDINARY SKILL IN THE ART	10
	B. The ‘171 patent.....	10
	C. EMV Specifications	17
	i. EMV Standard adoption.....	27
	ii. EMV Standards Options.....	31
	iii. Alternatives to EMV standard.....	33
III.	Claim Analysis.....	34
IV.	Technical Background	34
	D. Claim Construction	35
	E. General Comments.....	43
	F. Collinge	44
	iv. General Overview of Collinge	44
	v. Claim [1.A-3]: “... configured to [1] 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”	49
	vi. Claim [1.A-4]: “...[2] 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”	55

vii. Claim [1.B]: “requesting by the application, from the remote computer system, over the wireless network, a first set of data associated with the account;”	57
viii. Claim 1.C “receiving by the application, from the remote computer system, over the wireless network, 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 dat comprising a first non-permanent cryptographic key associated with the account;”	59
ix. Claim [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”	62
x. Claim [1.E-3] “responding to the at least one POS command communication...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;”	64
xi. Claims 4 and 20: “wherein the interrogation conforms to a card specification...”	67
xii. Claims 6 and 22: “The method of claim 1, 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 rspense cryptogram includes a portion, but not all, of the output”	68
xiii. Claim 8	71
xiv. Claim 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; and”	71
xv. Claim 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 non-permanent cryptographic key and the account identifier to the mobile device over the wireless network.”	73
xvi. Claims [10.A]/[27.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;”	74
xvii. Claim 10 B “determining a current non-permanent cryptographic key associated with the account using the account identifier,”	77
xviii. Claim 10 C “calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account ”	78
xix. Claim 15 “The method of claim 1, wherein the application is configured to generate the response cryptogram according to a card specification,”	78
xx. Claim 16 “The method of claim 1, wherein the first and second non-permanent cryptographic key are associated with an issuer master key,”	79
xxi. Claim 17 F “receive by the application, from the remote computer system, over the wireless network, the first set of data associated with the account,”	81
xxii. Claim 17 H-1 “wherein the at least one POS command communication comprises a request for digital credential data,	

the request for digital credential data including a cryptogram request”	82
xxiii. Claim 17.H-2	85
xxiv. Claim 17.I subsequent to the interrogation, request from the remote computer system, over the wireless network, a second set of data associated with the account;	85
xxv. Claim 17.J “receive 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 associated with the account comprising a second non-permanent cryptographic key associated with the account; and”	87
xxvi. Claim 17.K “store 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.”	87
xxvii. Claim 24 “wherein the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation.”	88
xxviii. Claim 25 “The system of claim 17, further comprising the remote computer system, the remote computer system configured to generate non permanent cryptographic keys associated with the account and send each of the non-permanent cryptographic keys and the ccount identifier to the mobile device over the wireless network”	89
G. Fiske	90
xxix. General overview of Fiske	90
xxx. [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”	93

xxxii. Claim [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;.....	94
xxxiii. Claims 4, 5, 20, 21: “The method of claim 1, 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.” “The method of claim 4, wherein the request for digital credential data comprises a request for a first cryptogram according to the card specification and the at least one device response communication comprises a second cryptogram, wherein the second cryptogram is the response cryptogram.	97
xxxiv. Claims 6 and 22: “The method of claim 1, 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”.....	100
xxxv. Claim 8.A: “ <i>The method of claim 1, further comprising, at the remote computer system: 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; and</i> ”	101
xxxvi. Claims 10 and 27 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;”	102
xxxvi. . Claim 10 B. determining a current non-permanent cryptographic key associated with the account using the account identifier;	103
xxxvii. Claim 10.C calculating a calculated cryptogram using the current nonpermanent cryptographic key associated with the account;	104
xxxviii. Claims 11 and 28, 12 and 29	105
xxxix. Claims 13 and 30 “The method of claim 12, wherein the authorization data further comprises values from the transaction.” ...	108
xl. Claims 15 and 32 “The method of claim 1, wherein the application is configured to generate the response cryptogram according to a card specification.”	109
xli. Claim 17	110
xlii. Claim 24 “The system of claim 17, wherein the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation.”	110
xliii. Claim 25 “The system of claim 17, further comprising the remote computer system, the remote computer system configured to generate non-permanent cryptographic keys associated with the account and send each of the non-permanent cryptographic keys and the account identifier to the mobile device over the wireless network.”	111
V. Conclusions.....	111

I. Introduction

1. My name is William C. Easttom II (Chuck Easttom), I have 30 years of experience in the computer science industry including extensive experience with computer science and computer security including cryptography, smart cards, NFC, and credit card payment processing. I have authored 42 computer science books, including textbooks used at over 60 universities around the world. I also have authored over 70 research papers and am an inventor with 26 computer science patents.

2. I hold a Doctor of Science (D.Sc.) degree in Cyber Security from Capitol Technology University (Dissertation Topic: “A Comparative Study of Lattice Based Algorithms for Post Quantum Computing”). I also hold a Doctor of Philosophy (Ph.D.) in Technology focused on nanotechnology (Dissertation Topic: “The Effects of Complexity on Carbon Nanotube Failures”) from Capitol Technology University. I also have a Doctor of Philosophy (Ph.D.) in Computer Science from the University of Portsmouth (Dissertation Topic: topic “A Systematic Framework for Network Forensics Using Graph Theory”). I also hold four master’s degrees (one in Applied Computer Science, one in Education, one in Defense and Strategic Studies, and one in Systems Engineering).

3. I am currently an Adjunct Lecturer for Georgetown teaching graduate courses in requirements engineering and cryptography. I am also an adjunct for Vanderbilt

University teaching graduate computer science courses, specifically quantum computing, secure software engineering, and digital forensics. I also developed a graduate course in digital forensics for the University of Dallas and taught that course from 2019 to 2022.

4. I am a Senior member and Distinguished Speaker for the Association of Computing Machinery (ACM) and a Senior Member and Distinguished Visitor of the Institute for Electrical and Electronics Engineering (IEEE). The IEEE is the world's largest and most preeminent engineering organization. Among other activities, the IEEE creates industry standards for a wide range of engineering disciplines, including software development standards. I am also a Distinguished Visitor of the IEEE. I have been involved in IEEE standards creation for several years.

5. My full CV is included as Exhibit 2037.

6. I have been asked to review U.S. Patent No. 10,032,171, the IPR filed by the petitioner in IPR2023-01289 and all attached exhibits, and to form my own independent scientific opinions. I have done so.

7. I am being compensated at my usual rate of \$550 per hour. My combination is not dependent in any way upon my conclusions or the outcome of this matter.

II. Analysis

8. This section contains my analysis of the ‘171 patent, the asserted references relied on in the petition, the assertions made by the petitioner, and the analysis of the petitioner’s expert, Dr. Fiske.

A. LEVEL OF ORDINARY SKILL IN THE ART

9. In determining the level of one of ordinary skill in the art I considered the ‘171 patent itself, the state of the art at the time of the invention (no later than August 30, 2011), and the prior art referenced in the ‘171 patent itself. I note that Dr. Fisk uses the filing date of August 30, 2012, rather than the filing of the provisional patent application. Using Dr. Fiske’s date would not change my analysis.

10. I arrived at the conclusion that a person of ordinary skill in the art (POSITA) as of August 30, 2011, would have 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 systems. Additional education in the field could be substituted for industry experience, and vice versa.

11. I was at least a person of ordinary skill in the art at the time of the invention of the ‘171 patent.

B. The ‘171 patent

12. The ‘171 patent relates to using a mobile computing device in combination with a remotely hosted Secure Element representation to make payments, authorizations or exchange information with other devices. (‘171 1:25-30). The ‘171

patent involves assurance that the data being delivered came from a particular Secure Element (SE) or card ('171 4:65-5:1).

13. The patent describes methods for securely authorizing digital credentials from a mobile device in transactions, even when the device lacks access to a locally stored permanent cryptographic key. Specifically, it addresses the generation of a cryptogram during an interrogation process with a point-of-sale system that expects the mobile device to compute the cryptogram using both a permanent cryptographic key and unpredictable data received from the point-of-sale system.

14. The '171 patent describes the utilization of two separate cryptograms. There is an expected cryptogram that is calculated from unpredictable data and a permanent cryptographic key ('171 2:27-35; 2:54-58; 32:2-6). There is also an unexpected cryptogram that can be substituted in place of the expected cryptogram during the interrogation step ('171 2:36-44). The unexpected cryptogram is used synonymously with unpredictable cryptogram ('171 28:20-21). That unexpected cryptogram can be sent from a mobile device to a point of sale during interrogation ('171 28:22-29).

15. Figure 2 from the '171 patent demonstrates a portion of the process according to one embodiment:

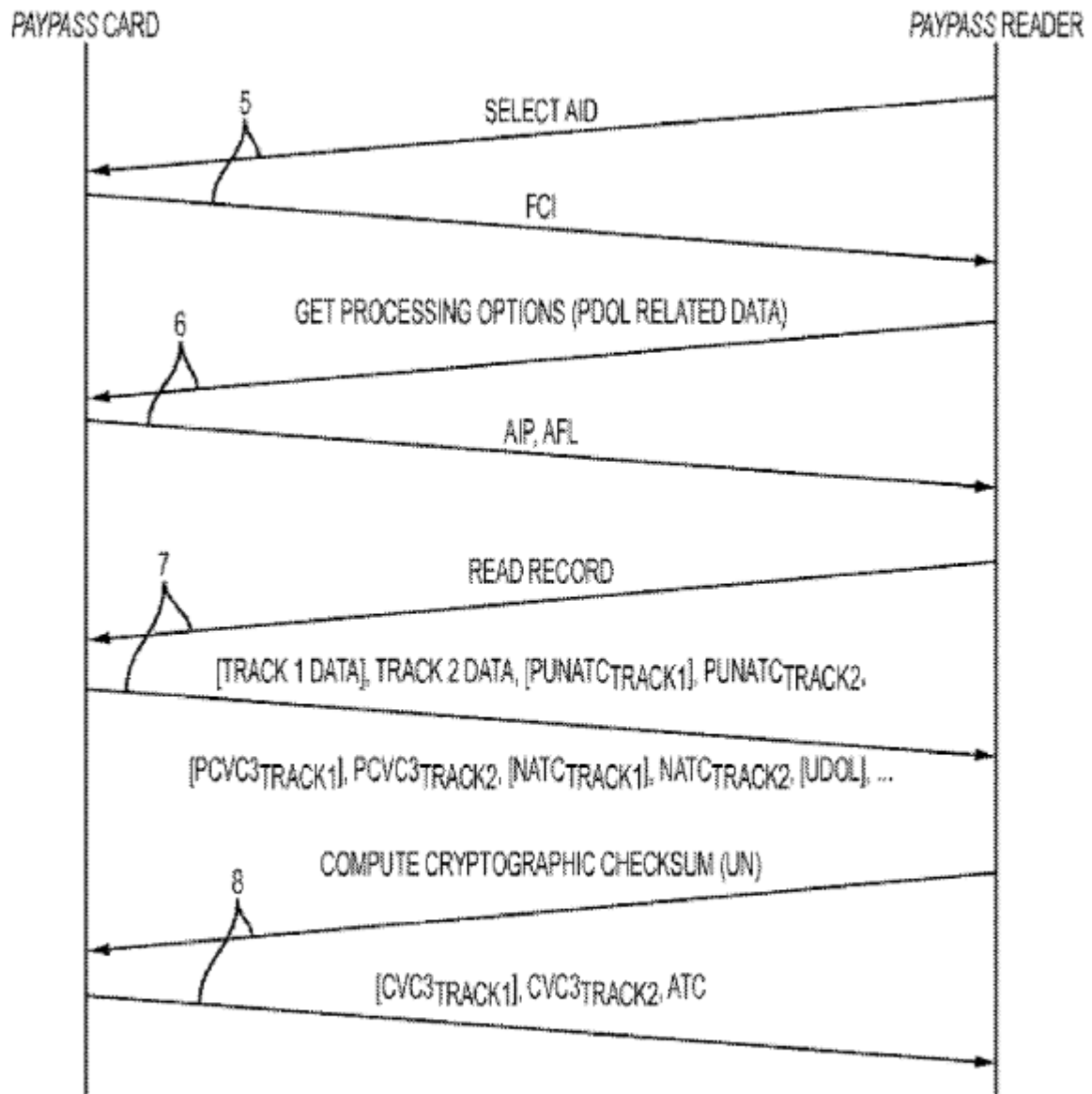


FIG. 2

16. Figure 6 provides an overview of the process:

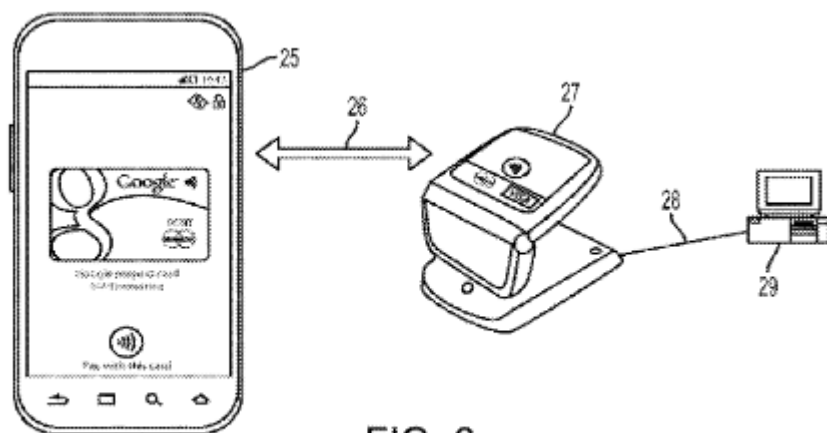
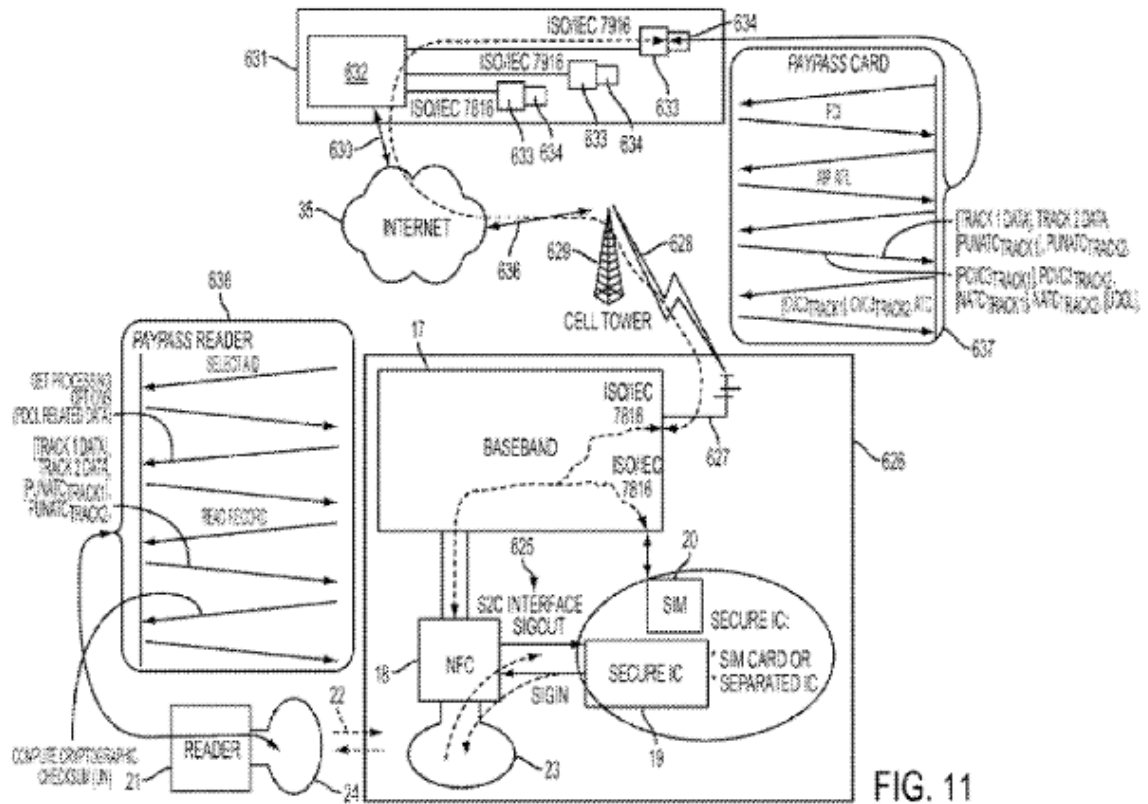


FIG. 6

17. Figure 11 illustrates an embodiment of a diagram of a mobile device that contains NFC capabilities and how that device may allow access to secure elements.



18. The '171 patent has a total of 30 figures, the preceding figures are simply exemplary.

19. The '171 patent describes several embodiments. One embodiment is a method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction. Another embodiment provides another method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction. A further embodiment provides a

method for acquiring digital credential data by a point-of-sale terminal from a secure mobile device for authorization of a financial transaction.

20. The '171 patent describes the ISO/IEC 7816 standard. As one example, "The commands and responses illustrated in FIG. 1 and FIG. 2 are comprised of a string of data that conforms to ISO/IEC 7816 specification." ('171 14:4-6).

21. The '171 patent also provides explanations of some terms used. One example is given here: "As used herein the term "cryptogram" refers to encrypted data that may or may not be able to be un-encrypted. Encrypted data that cannot be un-encrypted is many times called a "hash." A cryptogram is typically calculated from a series of input data that comprises some data and a cryptographic key, where the cryptographic key is used to encrypt some data. As used herein the term "cryptographic key" refers to a key used, at least in part, to calculate a cryptogram. A cryptogram is calculated based on an algorithm or calculation formula. As use herein the term "calculation formula" refers to an algorithm or formula that is specified by a card specification as the method to calculate a cryptogram" ('171 2:37-49)

22. Another example is: "As used herein the term "card data" or "credential data" may refer to the data used to create a proper APDU response to credential specific APDU commands such "read record" 7, and data used in "compute cryptographic checksum" 8. It is common for an application system in a software representation of

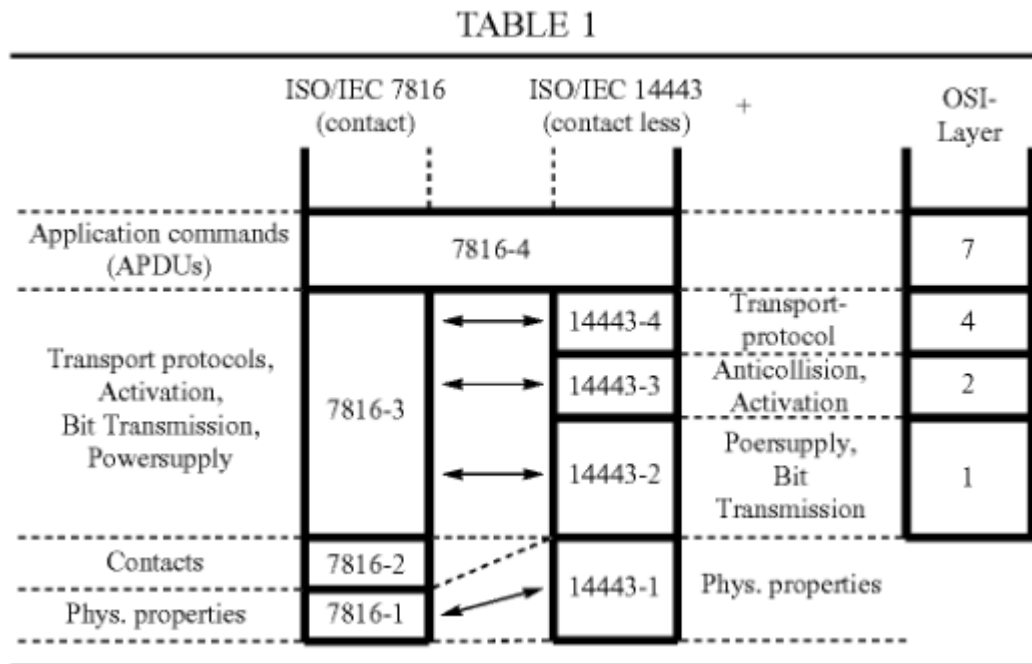
a plurality of remote secure element repository to have access to all the data to properly create a valid APDU response." ('171 31:14-21)

23. Yet another example is: "As used herein the term "interrogation" or "interrogation sequence" refers to all the APDU command requests and APDU responses between a mobile device and a point-of-sale using RFID (NFC) required to deliver a complete credential for authorizing a financial transaction to a point-of-sale as defined by a card specification. Typically, an NFC interrogation does not span multiple NFC field entrances and exits. Typically, the beginning of an interrogation starts when a mobile device enters the NFC field of a point-of-sale and ends at least prior to when the mobile device exits the NFC field." ('171 42:54-64).

24. I also note that the petitioner and Dr. Fiske assert that the term APDU is subject to two possible constructions. "The term is potentially subject to at least two alternative constructions: "one or more response application data protocol units, collectively containing the response cryptogram and; an account identifier for the account" ("Construction 1") or "one or more response application data protocol units, each of which contains both the response cryptogram and an account identifier for the account" ("Construction 2")."

25. The '171 describes an APDU as follows: "The protocol layer is a standard protocol referred to as APDU. APDU stands for Application Protocol Data Unit and typically the protocol is defined by ISO/IEC specification 7816. This specification

(commonly referred to as “ISO 7816” is a broad specification with different sections directed toward different “layers” of communication protocols, as seen in Table 1.” (‘171 6:16-19)



26. I note that neither the petitioner nor Dr. Fiske even mentions ISO 7816. This is surprising since the ‘171 not only states the APDUs are compliant with 7816, but also the ‘171 patent mentions ISO 7816 over 40 times. ISO 7813 defines track data in the ‘171 patent (‘171 8:47-49; 21:24-27; 21:34-37) but is also never mentioned by the petitioner nor Dr. Fiske.

C. EMV Specifications

27. The petitioner and Dr. Fiske relies heavily on a set of exhibits (1019-1029) they refer to as the “EMV Specifications.” I will use “EMV Specifications” or “EMV standards” throughout my declaration to refer to these exhibits.

28. Exhibit 1027 to the petition is titled *Contactless Specifications for Payment Systems Book C-3 Kernel 3 Specification* describes the GET PROCESSING OPTIONS (GPO) command and the PDOL (Processing Options Data Object List). Specifically, this exhibit states “Kernel 3 processing for a transaction starts with sending a GET PROCESSING OPTIONS (GPO) command to the card. This includes the data elements requested by the card in the PDOL returned in the response to the SELECT command, which will include the Terminal Transaction Qualifiers”. This is the kernel sending a command to the card, rather than the card beginning the process.

29. Furthermore, the PDOL is Tag 9F38: Processing Options Data Object List (PDOL). Not all credit card vendors even use PDOL, master card does not, but Visa does. A transaction can be processed with or without PDOL¹. "PDOL (Processing Options Data Object List) is a necessary set of parameters that a device has to transmit to a card for further processing in the next command."² PDOL may contain information such as country code but does not contain *a request for digital credential data. Rather PDOL gets processing information*³. The following demonstrates with specificity what PDOL contains:

¹ Ex. 2010 (<https://mstcompany.net/blog/acquiring-emv-transaction-flow-part-4-pdol-and-contactless-cards-characteristic-features-of-qvsdc-and-quics>)

² Ex. 2011 (<https://mstcompany.net/blog/acquiring-emv-transaction-flow-part-3-get-processing-options-with-and-without-pdol>)

³ Ex. 2010 (<https://mstcompany.net/blog/acquiring-emv-transaction-flow-part-4-pdol-and-contactless-cards-characteristic-features-of-qvsdc-and-quics>)

Term: 831236A0400000000000140036D3EC3906430643 (Get Processing Options)

Cla: 80 — **command class**

Ins: A8 — **instruction code**

P1: 00

P2: 00

Lc: 14

Data: 831236A0400000000000140036D3EC3906430643 — **data field with tag 83 containing concatenation («addition») of values in the same order as they are listed up in the PDOL element of the command to SELECT RESPONSE.** Let us look into them in the same order as they are set out in the example:

Tag 9F66: Terminal Transaction Qualifiers: 36A04000. **In this object, the terminal «tells» about the card and its functionality, namely:**

- Byte 1 bit 8 = 0 Contactless magnetic stripe not supported — **the contactless interface in the magnetic stripe emulation mode is not supported.**
- Byte 1 bit 7 = 0 RFU — **reserved for future use.**
- Byte 1 bit 6 = 1 Contactless qVSDC supported — **the contactless interface in the chip (qVSDC — Quick Visa Smart Debit Credit) emulation mode is supported**
- Byte 1 bit 5 = 1 Contact VSDC supported — **the interface of the contact chip is supported.** This bit is needed for the card to be able to send the command to Switch Interface upon occurrence of certain events, i.e., to suggest the use of the contact chip (see below).
- Byte 1 bit 4 = 0 Reader is Online Capable — **the device has the online authorization capability.**
- Byte 1 bit 3 = 1 Online PIN supported — **«Online PIN» CVM method is supported.**
- Byte 1 bit 2 = 1 Signature supported — **«Signature» CVM method is supported.**
- Byte 1 bit 1 = 0 Offline Data Authentication(ODA) for Online Authorizations not supported — **ODA is not supported.**

- Byte 2 bit 8 = 1 Online cryptogram required — **online transaction cryptogram verification by the issuer is required.**
- Byte 2 bit 7 = 0 CVM not required — cardholder verification is not required. That bit is dynamic and to be introduced depending on the transaction amount and terminal limits. In our case, the transaction amount is small (see below), which is why bit = 0.
- Byte 2 bit 6 = 1 (Contact Chip) Offline PIN supported — **«Offline PIN» CVM method for the contact chip is supported.**
- Byte 2 bit 5 - 1 = 0 RFU — **: bytes 5 to 1 are reserved for future use.**
- Byte 3 bit 8 = 0 Issuer Update Processing not supported — **the capability to transmit the issuer scripts to the card is not supported.**
- Byte 3 bit 7 = 1 Mobile functionality supported (Consumer Device CVM) — **the cardholder verification on the mobile device (password, graphic key, print, etc.) is supported.**

The rest of the bits of the 3rd byte and all bits of the 4th byte are currently reserved for future use.

Tag 9F02: Transaction Amount: 000000001400 — **amount of the transaction. 14.00 rubles.**

Tag 9F37: Unpredictable Number: 36D3EC39 — **random number.**

Tag 5F2A: Transaction Currency Code: 0643 — **code of the transaction currency, rubles.**

Tag 9F1A: Terminal Country Code: 0643 — **country of the terminal, Russian Federation.**

30. Exhibit 1028 also describes the PDOL, and also describes the reader requesting the PDOL from the card. Section 4.3.1 of exhibit 1028 provides details on the PDOL processing. The data sent back from the reader to the card includes various tags. Tag 9535 is described in the following tables from exhibit 1028:

Table 4-1: Terminal Type – EMV Tag '9F35'

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
		0	1					Financial Institution
		1	0					Merchant
		1	1					Cardholder
					0	0	1	Attended – Online Only
					0	1	0	Attended – Offline with Online Capability
					0	1	1	Attended – Offline Only
					1	0	0	Unattended – Online Only
					1	0	1	Unattended – Offline with Online Capability
					1	1	0	Unattended – Offline Only

Table 4-2: Kernel 4 Reader Capabilities – Tag '9F6D'

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0			0				Contactless – Mag-Stripe Version 1.0
0	1			0				Contactless – Mag-Stripe Version 2.0.1
1	0			0				Contactless – EMV and Mag-Stripe Version 2.0.1

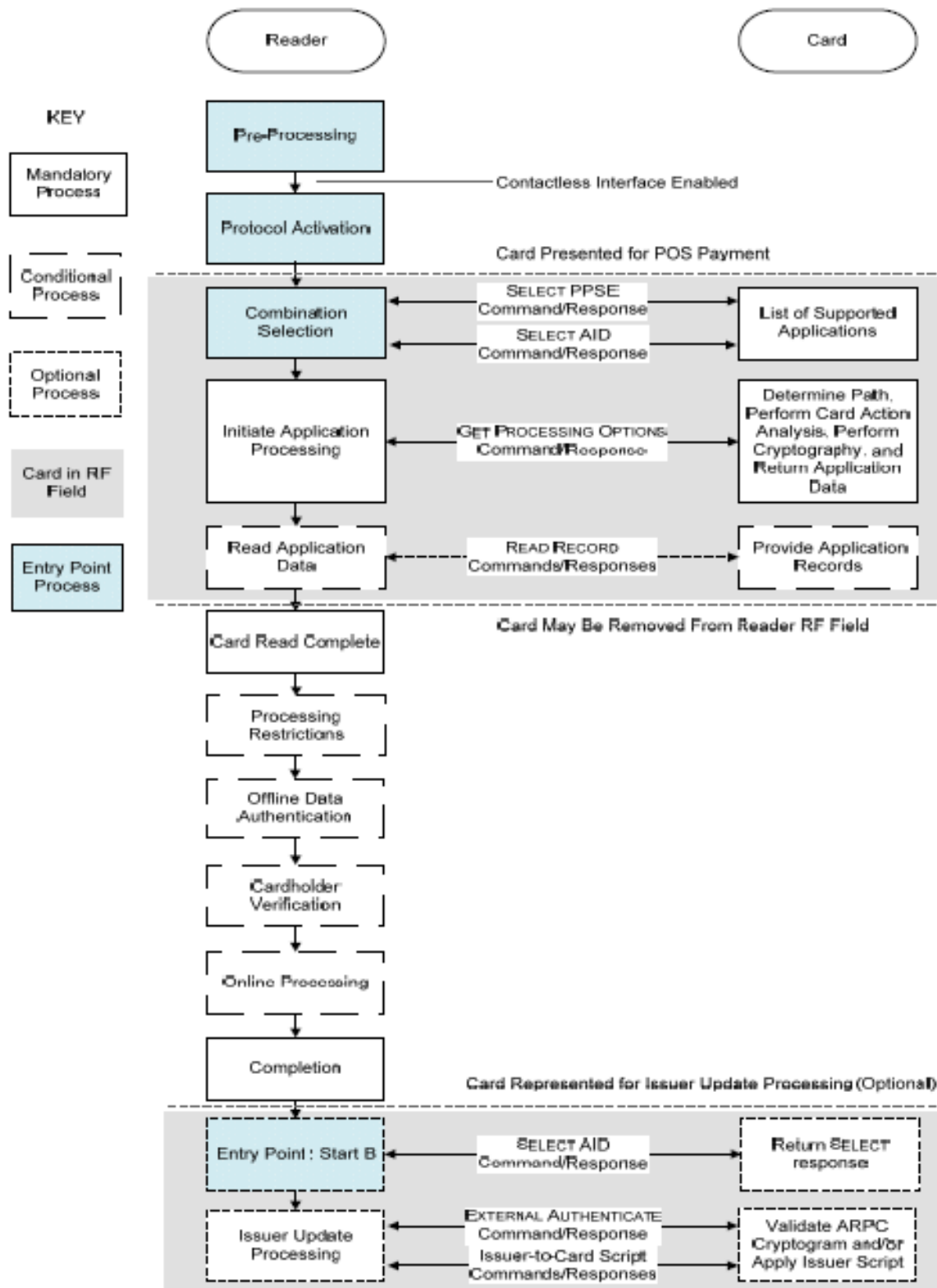
Note: Bits 6 and 5 and Bits 3 to 1 are reserved and must be set to zero. In *Terminal Type – Modified*, these bits will correspond to the values defined in EMV *Terminal Type*, Tag '9F35'.

Table 4-3: Terminal Type – Modified

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
		0	1					Financial Institution
		1	0					Merchant
		1	1					Cardholder
					0	0	1	Attended – Online Only
					0	1	0	Attended – Offline with Online Capability
					0	1	1	Attended – Offline Only
					1	0	0	Unattended – Online Only
					1	0	1	Unattended – Offline with Online Capability
					1	1	0	Unattended – Offline Only
0	0			0				Contactless – Mag-Stripe Version 1.0
0	1			0				Contactless – Mag-Stripe Version 2.0
1	0			0				Contactless – EMV and Mag-Stripe 2.0

31. Exhibit 1027 figure 2.1 demonstrates a transaction flow:

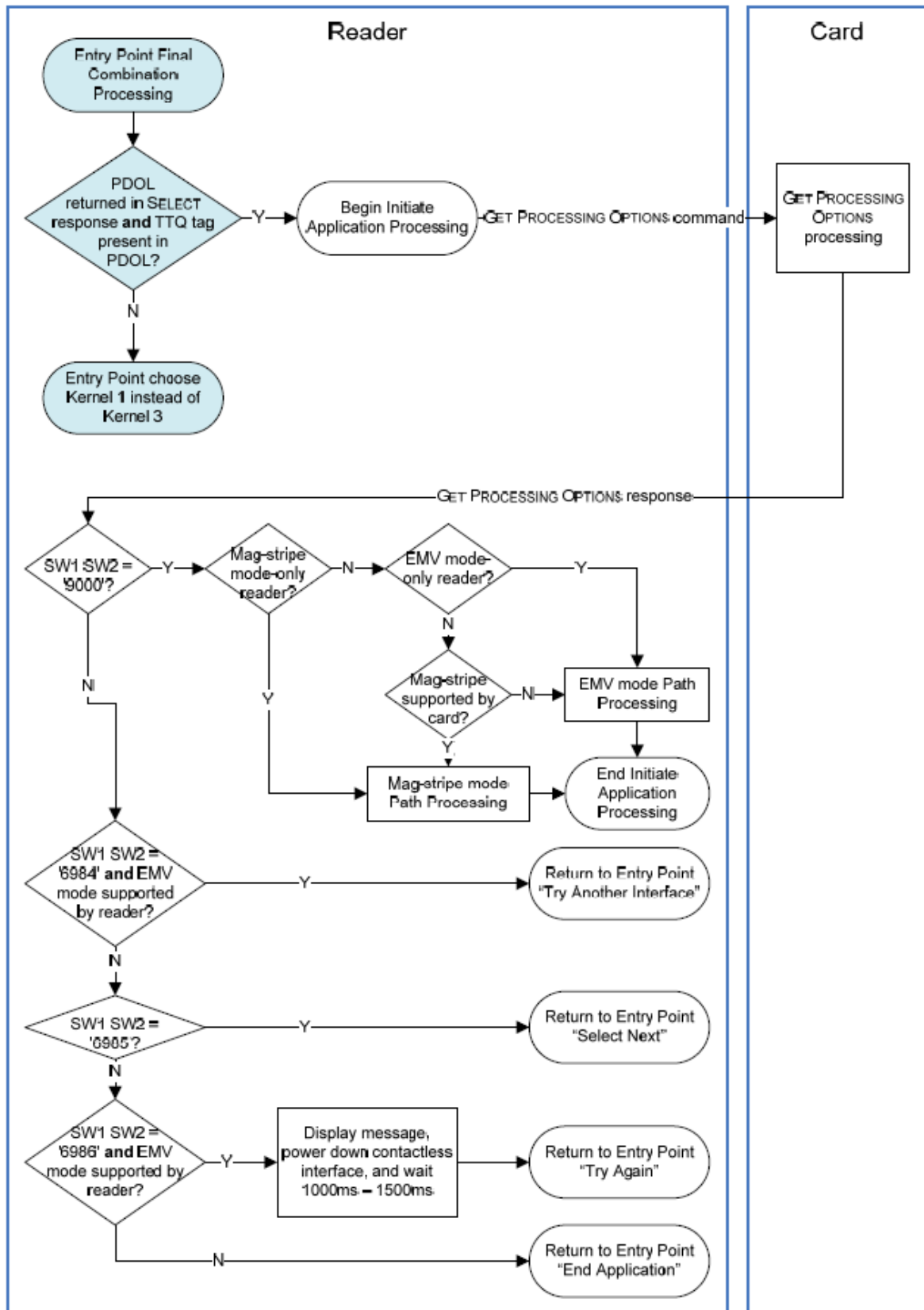
Figure 2-1: Sample Transaction Flow



Note: Processing as defined by the shaded shapes is performed by Entry Point.

32. Note: PPPSE is Proximity Payment System Environment; AID is application identifier.
33. Figure 2-1 shows the reader initiating the process, and the only items sent from the card are responses to Get Processing Options including application data, card action analysis, and performing cryptography.
34. Figure 5-1 shows the application processing initiation:

Figure 5-1: Initiate Application Processing (Reader)



35. This figure depicts the entire process initiated by the reader, and the card only sends a Get Processing Options response.

36. The EMV standards also define a number of acronyms that will be used in this declaration:

- AAC Application Authentication Cryptogram
- APDU Application Protocol Data Unit
- ARC Authorization Response Code
- ARPC Authorization Response Cryptogram
- ARQC Authorization Request Cryptogram
- ATC Application Transaction Counter
- C-APDU Command Application Protocol Data Unit
- CDOL Card Risk Management Data Object List
- CV Cryptogram Version
- DOL Data Object List
- IBAN International Bank Account Number
- PAN Primary Account Number
- PIN Personal Identification Number
- R-APDU Response Application Protocol Data Unit
- SW1 Status Byte One
- SW2 Status Byte Two

- TVR Terminal Verification Results
- TC Transaction Certificate

i. EMV Standard adoption

37. Bankrate.com states “Major credit card issuers asked that most U.S. businesses that accept credit cards move toward an EMV-compliant credit card point of sale (POS) system by Oct. 1, 2015 (for fuel retailers, the EMV liability deadline was April 2021).”⁴ This is moving towards EMV compliance by 2015 and a deadline of 2021. Even at that time, a company need not implement all of the EMV standard, but rather a minimal subset⁵.

38. It was not until October 2015 the liability for in store fraud shifted to the party that was not EMV compliant⁶. The following chart shows EMV adoption in 2014⁷:

⁴ Ex. 2012 (<https://www.bankrate.com/credit-cards/business/what-is-emv-compliance-law-should-your-business-worry/>)

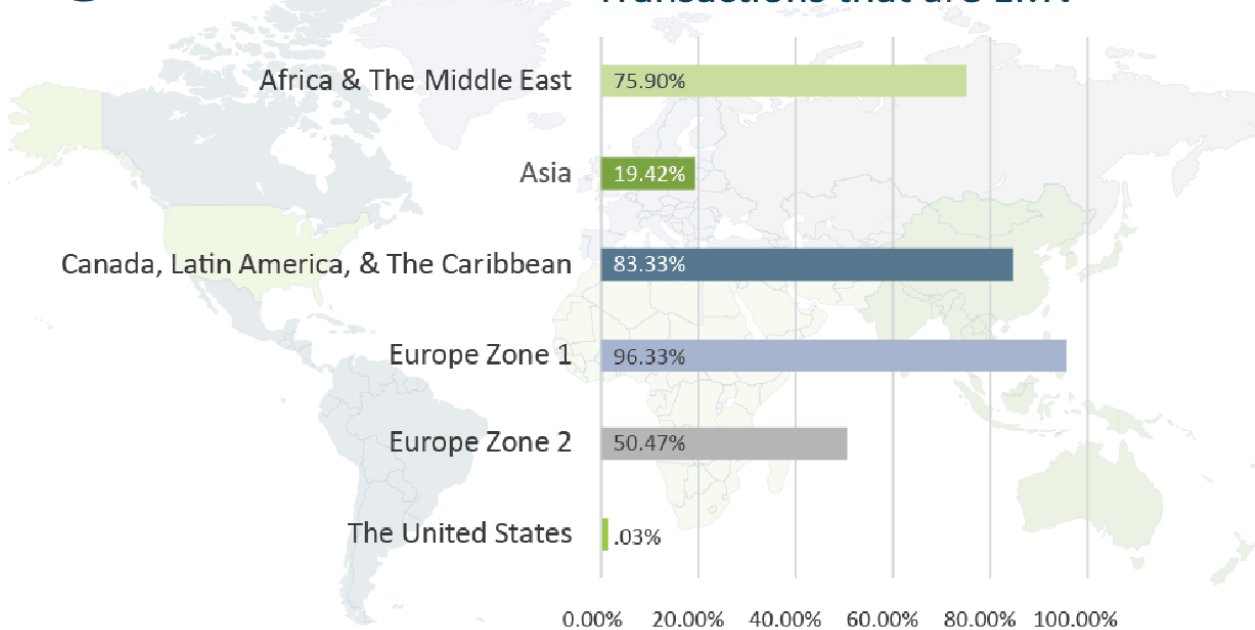
⁵ Ex. 2013 (<https://www.uspaymentsforum.org/minimum-emv-chip-card-and-terminal-requirements-u-s/>)

⁶ Ex. 2014 (<https://www.carat.fiserv.com/en-us/resources/emv-chip-card-technology/>)

⁷ Ex. 2015 (https://www.fisglobal.com/-/media/fisglobal/WorldPay/Docs/Insights/A-Guide-to-EMV-Chip-Technology.pdf?sc_lang=en)



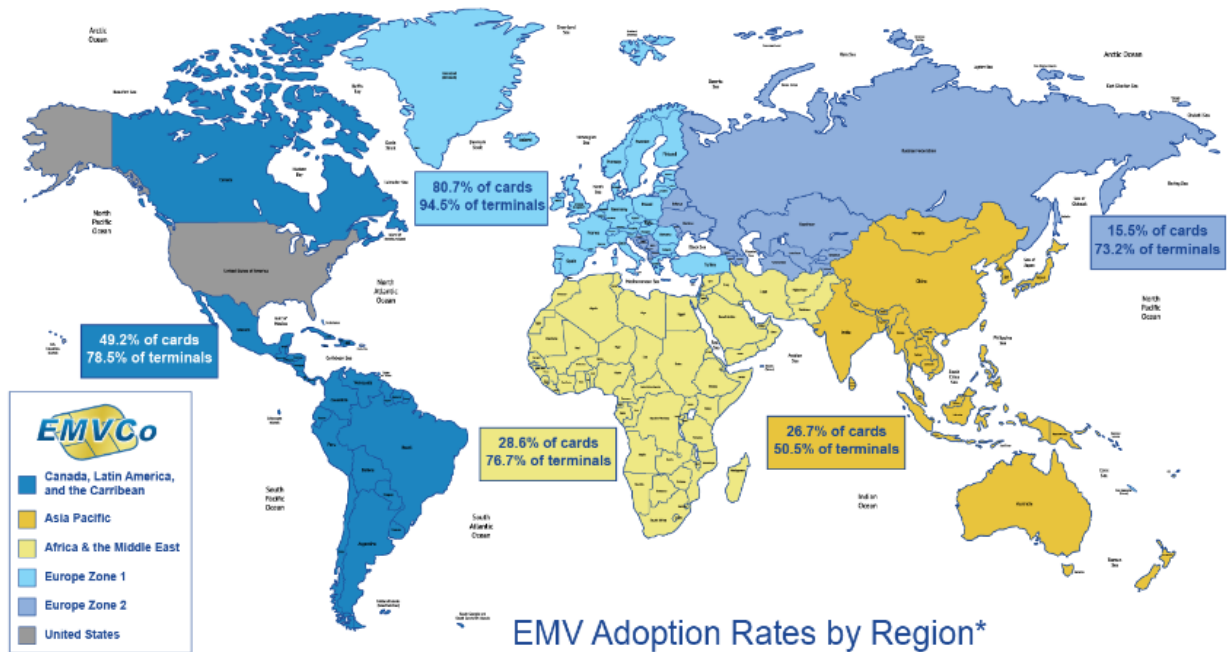
Percentage of Card-Present Transactions that are EMV



39. Even by December of 2013, adoption of EMV was far from widespread⁸:

⁸ Ex. 2016 (<https://www.smartpaymentassociation.com/liste-documents/public-resources/position-papers/121-13-12-11-wp-spa-instant-issuance-pdf/file>)

Chart 1: Worldwide EMV Adoption⁴



40. With such low adoption of EMV standards in the United States, a POSITA at the time would have considered considered alternatives. The magnetic stripe card was being widely used at the time. In fact, during the time period of 2010 to 2012 there was discussion about different types of magnetic stripe cards⁹. Documents from the time have specifications that allow for non-EMV cards “Specifications: EMV-compliant or proprietary non-EMV”¹⁰

⁹ Ex. 2017 (<https://www.alphacard.com/blog/whats-the-difference-between-hico-and-loco-magnetic-stripe-cards/>)

¹⁰ Ex. 2018 (<https://www.smartpaymentassociation.com/liste-documents/public-resources/position-papers/117-11-11-15-wp-spa-advancedpaymentwg-privatelabel-en-final-pdf/file>)

41. The Payment Card Industry Data Security Standards from 2010 state “Most environments processing EMV transactions today are hybrid environments, handling both EMV and non-EMV transactions.”¹¹ Non-EMV cards were quite common even in 2012 “Non-EMV cards work like magnetic stripe cards. This is common in the U.S. (PayPass Magstripe and VISA MSD)”¹²

42. During his deposition Dr. Fiske admitted that by 2012 the US had not yet migrated to EMV standard (Ex. 2036, “Fiske Dep.” at 49:5 - 50:4):

A. In the U.S., which in 2012 was not a country
6 that had yet migrated to EMV, the acquiring networks
7 that transport the transaction data from the terminal
8 through the acquirer card network to the issuer were
9 really only capable of transferring information in
10 what's called Track 2 data -- sometimes Track 1 data,
11 but Track 2 data. So there's actually very little
12 space available.
13 So for that reason, in contactless at that
14 time in the U.S. there were variants of contactless
15 payments for each of the brand. So American Express
16 had ExpressPay magstripe mode. Visa had legacy MSD.
17 MasterCard had PayPass Magstripe, and Discover had
18 Discover Zip. So those were the predominant

¹¹ Ex. 2019 (https://listings.pcisecuritystandards.org/documents/pci_dss_emv.pdf)

¹² Ex. 2020 (https://epordo.com/us/trends/smart_card_tech.html)

19 contactless transaction methods in the U.S.

43. I agree with Dr. Fiske that in 2012 there were multiple options for contactless payments, including at least the ones Dr. Fiske mentioned.

ii. EMV Standards Options

44. All of the EMV standard documents have the following section:

1.7.3 Terminology and Conventions

The following words are used often in this specification and have a specific meaning:

shall	Defines a product or system capability which is mandatory.
may	Defines a product or system capability which is optional or a statement which is informative only and is out of scope for this specification.
should	Defines a product or system capability which is recommended.

The following conventions apply:

45. This is common in all standards documents. Only those items denoted as ‘shall’ or mandatory are actually mandatory. Other items are optional. Furthermore, the standards documents make this point repeatedly throughout the standards. As one example, exhibit 1020 Section 8 Application Cryptogram and Issuer Authentication states “Note that the methods provided in this specification are not mandatory. Issuers may decide to adopt other methods for these functions.”

46. Dr. Fiske admitted in his deposition that this section is not mandatory, and vendors can implement cryptograms in other ways (Ex. 2035 at 60:1-61:1).

47. Another example is also found in exhibit 1020. Section A1.3 Session Key Derivation states “Note that the session key derivation method provided in Annex A1.3.1 is not mandatory. Issuers may decide to adopt another method for this function.”
48. Yet another example is also found in exhibit 1020. Section A1.4 Master Key Derivation states "Note that neither method is mandatory. Issuers may decide to adopt an alternative method for this function."
49. Yet another example is found in exhibit 1027:

5.7 Cardholder Verification

The kernel determines if a Cardholder Verification Method (CVM) is to be performed. The CVMs that may be supported for Kernel 3 are Online PIN, Consumer Device CVM, and Signature.

Note: A Consumer Device CVM is a CVM performed on, and validated by, the consumer's payment device, independent of the reader.

5.7.1 Cardholder Verification – EMV Mode Path Processing

Implementation-Mandatory: Cardholder Verification shall be implemented for EMV mode-enabled readers.

Acquirer-Merchant-Optional: The acquirer-merchant shall be able to enable and disable the supported CVMs. However, support for the Consumer Device CVM shall be enabled (TTQ byte 3 bit 7 is 1b).

The kernel shall perform the procedure defined in this section for EMV mode transactions if the Decline Required by Reader Indicator is 0.

50. Yet another example is found in exhibit 1026 section A.1.168, which states "The UDOL is the DOL that specifies the data objects to be included in the data field

of the COMPUTE CRYPTOGRAPHIC CHECKSUM command. The UDOL must at least include the Unpredictable Number (Numeric). The UDOL is not mandatory for the Card. If it is not present in the Card, then the Default UDOL is used."

51. A POSITA reviewing Exhibits 1019-1029 would readily understand that there is wide variation in the implementation disclosed in these documents.

iii. Alternatives to EMV standard

52. In 2012 there were multiple alternative contactless standards. Each is briefly described in this section.

53. MasterCard M/Chip¹³. M/Chip cards perform cryptographic functions, provide secure authentication, and protect against card fraud by making it difficult to clone cards. The technology supports both contact and contactless payment methods, offering flexibility and improved transaction speed for consumers and merchants.

54. Visa QVSDC¹⁴. Visa QVSDC (Quick Visa Smart Debit/Credit) enables fast and secure transactions using a chip embedded in payment cards. It supports dynamic data authentication, which enhances security by making it difficult to clone

¹³ Ex. 2021 (<https://www.scribd.com/doc/80222587/MChip-4-Issuer-Guide-to-Debit-and-Credit-Parameter-Management-Dec2004>)

¹⁴ Ex. 2022

(<https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://technologypartner.visa.com/Download.aspx%3Fid%3D50&ved=2ahUKEwiy-5bs2-WGAxXA18kDHau-BwkQFnoECBsQAQ&usg=AOvVaw2bZsYlVLrv42iWzfe0Nof->)

the card. QVSDC is designed for quick, tap-and-go transactions, commonly used in retail, transit, and other environments requiring fast payment processing.

55. Discover D-PAS which supports both contact and contactless transactions, providing flexibility for cardholders. The specification includes guidelines for issuers and acquirers to ensure interoperability and security across different payment environments.

III. Claim Analysis

56. In the following subsections, specific claim limitations addressed by the petitioner and Dr. Fiske are addressed.

57. I note that Dr. Fiske, in his declaration, describes the requirements for anticipation, specifically stating “I understand that a prior art reference anticipates a challenged claim, and thus renders the claim invalid, if all limitations of the claim are disclosed in that prior art reference, either explicitly or inherently (i.e., necessarily present or implied), as arranged or combined in the claim.” (Dr. Fiske declaration: 13).

58. I agree with Dr. Fiske in his description of the requirements for anticipation. As will be discussed in this declaration, there are many claim elements that are neither explicitly nor inherently in the prior art that the petitioner and Dr. Fiske rely on.

IV. Technical Background

59. There are particular technologies being used in the ‘171 patent as well as in the asserted prior art. It is therefore necessary to gain a good general understanding of that technology. Specific technologies that are relevant are discussed in the following sub-sections.

D. Claim Construction

60. Throughout my analysis I view terms using their plain and ordinary meaning to one of ordinary skill in the art.

61. The petitioner and Dr. Fiske both assert that the term R-APDU “is potentially subject to at least two alternative constructions: “one or more response application data protocol units, collectively containing the response cryptogram and an account identifier for the account” (“Construction 1”) or “one or more response application data protocol units, each of which contains both the response cryptogram and an account identifier for the account” (“Construction 2”).”

62. The ‘171 patent is explicit in that the term APDU comes from ISO 7816. Section 12.1.1 of ISO 7816 provides a detailed description of the APDU’s used:

12.1.1 Command-response pairs

An application protocol data unit is either a command APDU or a response APDU. A step in application protocol consists of transmitting a command APDU, processing it in the receiving entity and returning the response APDU. This pair of APDUs is called a command-response pair.

Illustrated by Figure 24, each command APDU defined in this document consists of

- a mandatory header of four bytes denoted CLA INS P1 P2,
- a conditional body of variable length.

Command header				Command body		
CLA	INS	P1	P2	[L _c field]	[Data field]	[L _e field]

Figure 24 — Command APDU structure

Illustrated by Figure 25, each response APDU defined in this document consists of

- a conditional body of variable length,
- a mandatory trailer of two bytes denoted SW1 SW2 and encoding the status of the receiving entity after processing the command.

Response body		Response trailer
[Data field]		SW1 SW2

Figure 25 — Response APDU structure

The values of the command header and the response trailer shall be as specified in ISO/IEC 7816-4. If the process is aborted, then the card may become unresponsive. However if a response APDU occurs, then the response body shall be absent and SW1 SW2 shall indicate an error.

12.1.2 Data fields within command-response pairs

Each command-response pair may carry a command data field and/or a response data field.

- N_c denotes the number of bytes in the command data field. If $N_c \neq 0$, then the L_c field is present for encoding N_c and the command data field consists of the subsequent N_c bytes. If $N_c = 0$, then both the L_c field and the command data field are absent.
- N_e denotes the maximum number of bytes expected in the response data field. If $N_e \neq 0$, then the L_e field is present for encoding N_e . If $N_e = 0$, then the L_e field is absent.
- N_r denotes the number of bytes in the response data field. N_r shall be from zero to N_e . If $N_r = 0$, then the response data field is absent.

In case 1, $N_c = N_r = 0$. The command APDU consists of the header; the L_c field, the command data field and the L_e field are absent. The response APDU consists of the trailer; the response data field is absent.

In case 2, $N_c = 0$ and $N_r \neq 0$. The command APDU consists of the header and the L_e field; the L_c field and the command data field are absent. The response APDU consists of the response data field and the trailer.

In case 3, $N_c \neq 0$ and $N_r = 0$. The command APDU consists of the header, the L_c field and the command data field; the L_e field is absent. The response APDU consists of the trailer; the response data field is absent.

In case 4, $N_c \neq 0$ and $N_r \neq 0$. The command APDU consists of the header, the L_c field, the command data field and the L_e field. The response APDU consists of the response data field and the trailer.

Table 12 summarizes the four possible cases of command-response pairs.

Table 12 — Data fields within command-response pairs

Case 1	No command data field	No response data field
Case 2	No command data field	Response data field
Case 3	Command data field	No response data field
Case 4	Command data field	Response data field

Figure 26 shows the four structures of command APDUs according to the previous four cases.

- A command APDU of case 1 consists of a header.
- A command APDU of case 2 consists of a header and a L_e field.
- A command APDU of case 3 consists of a header, a L_c field and a data field.
- A command APDU of case 4 consists of a header, a L_c field, a data field and a L_e field.

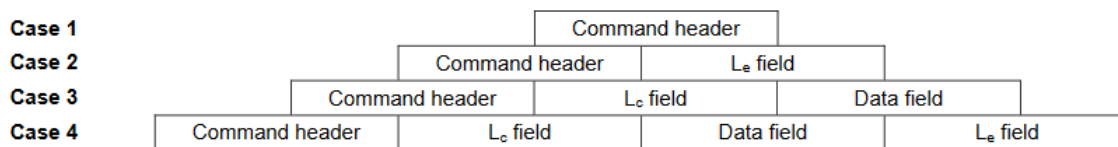


Figure 26 — The four structures of command APDUs

63. SW1-SW2 are defined as status bytes in the ISO 7816-4. The data fields possible are shown in section 6.1 of the ISO 7816-4:

6.1 SM fields and SM data objects

By definition, any command or response data field in SM format, as also the SM template (tag '7D'), is an SM field. Each SM field shall be encoded in BER-TLV (see 5.2.2) where the context-specific class (first byte from '80' to 'BF') is reserved for SM data objects. In command-response pairs, the SM format may be selected either implicitly, i.e., known before issuing the command, or explicitly, i.e., indicated by CLA (see 5.1.1).

NOTE Command chaining and / or the use of SW1 set to '61' induces sequences of commands where data fields (and consequently, data objects) may be split in smaller consecutive data fields. In such a case, when using SM format, the concatenation of all the consecutive data fields in the same direction in the same sequence is an SM field.

Table 27 shows the SM data objects specified in this document, all in the context-specific class. Some SM data objects (SM tags '82', '83', 'B0', 'B1') are recursive, i.e., the plain value field is an SM field.

Table 27 — SM data objects

Tag	Value
'80', '81'	Plain value not encoded in BER-TLV
'82', '83'	Cryptogram (plain value encoded in BER-TLV and including SM data objects, i.e., an SM field)
'84', '85'	Cryptogram (plain value encoded in BER-TLV, but not including SM data objects)
'86', '87'	Padding-content indicator byte followed by cryptogram (plain value not encoded in BER-TLV)
'89'	Command header (CLA INS P1 P2, four bytes)
'8E'	Cryptographic checksum (at least four bytes)
'90', '91'	Hash-code
'92', '93'	Certificate (data not encoded in BER-TLV)
'94', '95'	Security environment identifier (SEID byte)
'96', '97'	One or two bytes encoding N_s in the unsecured command-response pair (possibly empty)
'99'	Processing status (SW1-SW2, two bytes; possibly empty)
'9A', '9B'	Input data element for the computation of a digital signature (the value field is signed)
'9C', '9D'	Public key
'9E'	Digital signature
'A0', 'A1'	Input template for the computation of a hash-code (the template is hashed)
'A2'	Input template for the verification of a cryptographic checksum (the template is included)
'A4', 'A5'	Control reference template for authentication (AT)
'A6', 'A7'	Control reference template for key agreement (KAT)
'A8'	Input template for the verification of a digital signature (the template is signed)
'AA', 'AB'	Control reference template for hash-code (HT)
'AC', 'AD'	Input template for the computation of a digital signature (the concatenated value fields are signed)
'AE', 'AF'	Input template for the verification of a certificate (the concatenated value fields are certified)
'B0', 'B1'	Plain value encoded in BER-TLV and including SM data objects, i.e., an SM field
'B2', 'B3'	Plain value encoded in BER-TLV, but not including SM data objects
'B4', 'B5'	Control reference template for cryptographic checksum (CCT)
'B6', 'B7'	Control reference template for digital signature (DST)
'B8', 'B9'	Control reference template for confidentiality (CT)
'BA', 'BB'	Response descriptor template
'BC', 'BD'	Input template for the computation of a digital signature (the template is signed)
'BE'	Input template for the verification of a certificate (the template is certified)

— In this context, ISO/IEC JTC 1/SC 17 reserves any other data object of the context-specific class (first byte from '80' to 'BF').

64. Section 5.1 of ISO/IEC 7816-4 shows the command-response pairs:

5.1 Command-response pairs

Table 1 shows a command-response pair, namely a command APDU followed by a response APDU in the opposite direction (see ISO/IEC 7816-3). There shall be no interleaving of command-response pairs across the interface, i.e., the response APDU shall be received before initiating another command-response pair.

Table 1 — Command-response pair

Field	Description	Number of bytes
Command header	Class byte denoted CLA	1
	Instruction byte denoted INS	1
	Parameter bytes denoted P1-P2	2
L _c field	Absent for encoding N _c = 0, present for encoding N _c > 0	0, 1 or 3
Command data field	Absent if N _c = 0, present as a string of N _c bytes if N _c > 0	N _c
L _e field	Absent for encoding N _e = 0, present for encoding N _e > 0	0, 1, 2 or 3
Response data field	Absent if N _r = 0, present as a string of N _r bytes if N _r > 0	N _r (at most N _e)
Response trailer	Status bytes denoted SW1-SW2	2

In any command-response pair comprising both L_c and L_e fields (see ISO/IEC 7816-3), short and extended length fields shall not be combined: either both of them are short, or both of them are extended.

If the card explicitly states its capability of handling “extended L_c and L_e fields” (see Table 88, third software function table) in the historical bytes (see 8.1.1) or in EF.ATR (see 8.2.1.1), then the card handles short and extended length fields. Otherwise (default value), the card handles only short length fields.

N_c denotes the number of bytes in the command data field. The L_c field encodes N_c.

- If the L_c field is absent, then N_c is zero.
- A short L_c field consists of one byte not set to '00'.
 - From '01' to 'FF', the byte encodes N_c from one to 255.
- An extended L_c field consists of three bytes: one byte set to '00' followed by two bytes not set to '0000'.
 - From '0001' to 'FFFF', the two bytes encode N_c from one to 65 535.

N_e denotes the maximum number of bytes expected in the response data field. The L_e field encodes N_e.

- If the L_e field is absent, then N_e is zero.

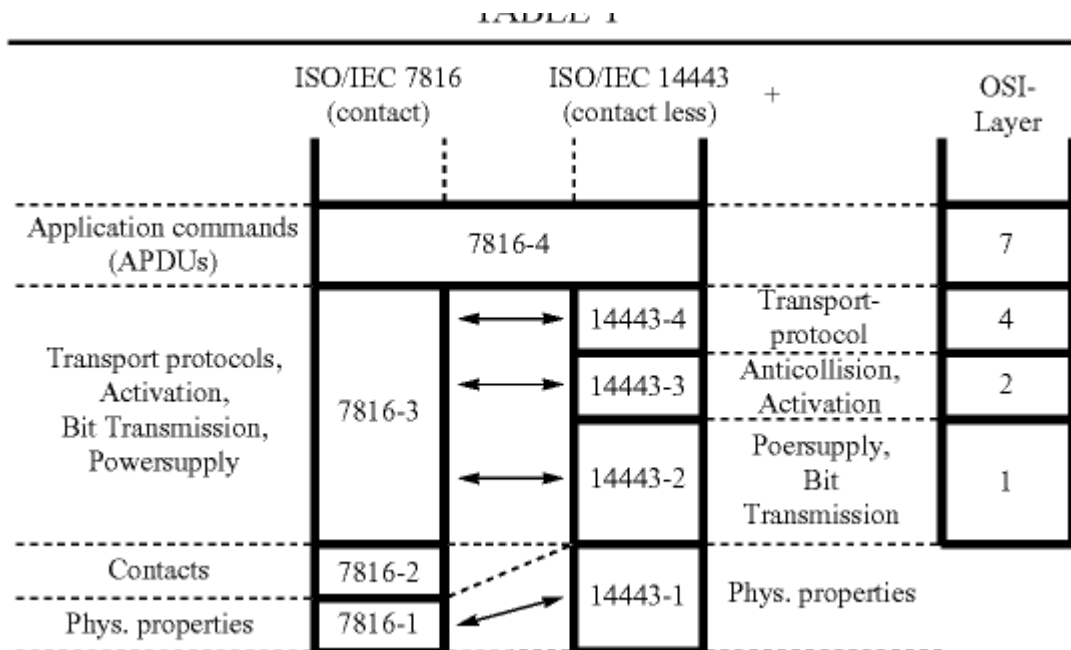
- A short L_c field consists of one byte not set to '00'.
 - From '01' to 'FF', the byte encodes N_c from one to 255.
- An extended L_c field consists of three bytes: one byte set to '00' followed by two bytes not set to '0000'.
 - From '0001' to 'FFFF', the two bytes encode N_c from one to 65 535.

N_e denotes the maximum number of bytes expected in the response data field. The L_e field encodes N_e .

- If the L_e field is absent, then N_e is zero.
- A short L_e field consists of one byte with any value.
 - From '01' to 'FF', the byte encodes N_e from one to 255.
 - If the byte is set to '00', then N_e is 256.
- An extended L_e field consists of either three bytes (one byte set to '00' followed by two bytes with any value) if the L_c field is absent, or two bytes (with any value) if an extended L_c field is present.
 - From '0001' to 'FFFF', the two bytes encode N_e from one to 65 535.
 - If the two bytes are set to '0000', then N_e is 65 536.

N_r denotes the number of bytes in the response data field. N_r shall be less than or equal to N_e . Therefore in any command-response pair, the absence of L_e field is the standard way for receiving no response data field. If the L_e field contains only bytes set to '00', then N_e is maximum, i.e., within the limit of 256 for a short L_e field, or 65 536 for an extended L_e field, all the available bytes should be returned.

65. Furthermore, table 1 of the '171 patent explains the communication involving APDU's.



66. Furthermore, the '171 patent states "The APDU section of the 7816-4 specification describes two forms of APDU communications abbreviated as C-

APDU (“command APDU”) and R-APDU (“response APDU”). “Commands” are sometimes referred to as “queries” because they originate from an “interrogator,” which has a querying connotation.” (‘171 6:47-53).

67. Figure 3 of the ‘171 “describes example transactions at the ISO/IEC 7816-4 Application Protocol Data Unit (APDU) protocol level between a reader and a card. The transaction processing depicted in FIG. 3 is representative of the MASTERCARD PAYPASS Mag Stripe application card specification v. 3.3. The notation “>CARD” denotes commands to the card and the notation “CARD>” denotes responses from the card. “(‘171 7:15-22)

```

9 {
  UN:      3
  UN:      00 00 08 99
  ATC:     00 5E
  CVC3TRACK1: 2 LEAST SIGNIFICANT BYTES OF
              DES3(KDCVC3) [77 80 00 00 08 99 00 5E]
  CVC3TRACK1: FB C7
  CVC3TRACK2: 2 LEAST SIGNIFICANT BYTES OF
              DES3(KDCVC3) [99 D3 00 00 08 99 00 5E]
  CVC3TRACK2: B8 92

  • SELECT PPSE COMMAND
10 {
    >CARD: 00 A4 04 00 0E 32 50 41 59 2E 53 59 53 2E 44 44
          46 30 31 00
    CARD>: 6F 23 84 0E 32 50 41 59 2E 53 59 53 2E 44 44 46
          30 31 A5 11 BF 0C 0E 61 0C 4F 07 A0 00 00 00 04
          10 10 87 C1 01 90 00

  • SELECT AID COMMAND
11 {
    >CARD: 00 A4 04 00 07 A0 00 00 00 04 10 10 00
    CARD>: 6F 17 84 07 A0 00 00 00 04 10 10 A5 0C 50 0A 4D
          61 73 74 65 72 43 61 72 64 90 00

  • GET PROCESSING OPTIONS COMMAND
12 {
    >CARD: 80 A8 00 00 02 83 00 00
    CARD>: 77 0A 82 02 00 00 94 04 08 01 01 00 90 00

  • READ RECORD COMMAND
13 {
    >CARD: 00 B2 01 0C 00
    CARD>: 70 7F 9F 6C 02 00 01 56 3E 42 35 34 31 33 31 32
          33 34 35 36 37 38 34 38 30 30 5E 53 55 50 50 4C
          49 45 44 2F 4E 4F 54 5E 30 39 30 36 31 30 31 33
          33 30 30 30 33 33 33 30 30 30 32 32 32 32 32 30
          30 30 31 31 31 31 30 9F 64 01 03 9F 62 06 00 00
          00 38 00 00 9F 63 06 00 00 00 00 E0 E0 9F 65 02
          00 0E 9F 66 02 0E 70 9F 6B 13 54 13 12 34 56 78
          48 00 D0 90 61 01 90 00 99 00 00 00 0F 9F 67 01
          03 90 00

  • COMPUTE CRYPTOGRAPHIC CHECKSUM COMMAND
14 {
    >CARD: 80 2A 8E 80 04 00 00 08 99 00
    CARD>: 77 0F 9F 61 02 B8 92 9F 60 02 FB C7 9F 36 02 00
          5E 90 00

```

FIG. 3

68. A POSITA would readily understand what is meant by R-APDU. Table 27 in Section 6.1 of ISO 7816-4 describes what data may be part of the data sent in an R-APDU.

E. General Comments

69. During Dr. Fiske's deposition he made the statement that a hash cannot be a cryptogram (Fiske Dep. at 29:20 – 30:3).

20 Q. Would a person of skill in the art understand
21 that MD5 is an algorithm available to generate a
22 cryptogram?

23 A. They would not -- I would not accept that
24 definition, and I don't believe a person of skill in
25 the art in 2012 would accept that definition.

1 Q. Why not?

2 A. Because the MD5 algorithm is a hash
3 algorithm, and it doesn't use a key.

70. This is incorrect. First, exhibit 1019 *EMV 4.2 Book 1* section 3 *Definitions* defines a cryptogram as a "Result of a cryptographic operation". There is no requirement for a key. Exhibit 1020 Annex B *Approved Cryptographic Algorithms* section B3 *Hashing Algorithms* specifically lists hashing algorithms as approved cryptographic algorithms.

71. More importantly, Dr. Fiske's opinion is contrary to the way the term "cryptogram" used in the '171 patent: "As used herein the term 'cryptogram' refers to encrypted data that may or may not be able to be un-encrypted. Encrypted data that cannot be un-encrypted is many times called a 'hash.' A cryptogram is typically

calculated from a series of input data that comprises some data and a cryptographic key, where the cryptographic key is used to encrypt some data.” (‘171 25:36-43)

72. The ‘171 patent explicitly states that a cryptogram can be data that may or may not be unencrypted, and further specifically names a ‘hash’ for data that cannot be un-encrypted. The ‘171 does state that cryptograms are typically calculated using a cryptographic key, but a POSITA would note the word ‘typically’ as something generally found, and not a requirement.

73. Neither the ‘171 patent nor the EMV standards support Dr. Fiske’s opinions that hash algorithms such as SHA-1 cannot produce cryptograms.

F. Collinge

iv. General Overview of Collinge

74. Collinge discloses a processing device generating a card profile that is associated with a payment account. That card profile at least includes payment credentials corresponding to the payment account and a profile identifier. That profile is provisioned to a mobile device (Collinge: 0007).

75. Collinge discloses that a mobile device sends a key request that includes at least a PIN number and the profile identifier to a processing device (Collinge 0007).

76. Collinge discloses that the processing device generates a single use key that includes at least the profile identifier, application transaction counter, and a generating key. That generating key is used to generate a payment cryptogram that

is valid for a single transaction. The single use key is transmitted to the mobile device by a transmitting device (Collinge 00007).

77. Collinge discloses a session key unpredictable number KS_{UN} and a cloud unpredictable number UN_{CLOUD} . Collinge also uses a dynamic card validation code key KD_{cvc3} . An encrypted payload including at least the dynamic card validation code keys (KD_{cvc3}), KS_{UN} , and application transaction counter to the mobile device by a transmitting device. The mobile device uses the encrypted payload to generate a dynamic card validation code for use in financial transactions. The transmitting device also transmits at least the KS_{UN} , UN_{CLOUD} , and application transaction counter to an issuer for use in validating the generated dynamic card validation code used in transactions (Collinge 00009).

78. Collinge also makes use of a UN_{CLOUD} . “At stage 19 b, the issuer processing server 308 may validate the payment CVC3 value using at least the UN_{READER} , UN_{CLOUD} , and application transaction counter” (Collinge 0087). “In step 1710, a session key unpredictable number (KS_{UN}) may be generated by a processing device (e.g., the cloud system 302). In step 1712, a cloud unpredictable number (UN_{CLOUD}) may be generated by the processing device 302” (Collinge 0140).

79. The key points that are common across embodiments in Collinge are:

- The mobile device sends a key request that includes at least a PIN number and the profile identifier to a processing device

- A processing device generates the CAP token and that token is based on at least the authentication component and at least one additional credential.
- The processing device generates a single use key that includes at least the profile identifier, application transaction counter, and a generating key. That generating key is used to generate a payment cryptogram that is valid for a single transaction.
- The single use key is transmitted to the mobile device by a transmitting device.
- An encrypted payload including at least the dynamic card validation code keys (KDcvc3), KSun, and application transaction counter to the mobile device by a transmitting device.

80. Figure 7 from Collinge is a high-level diagram in accordance with exemplary embodiments:

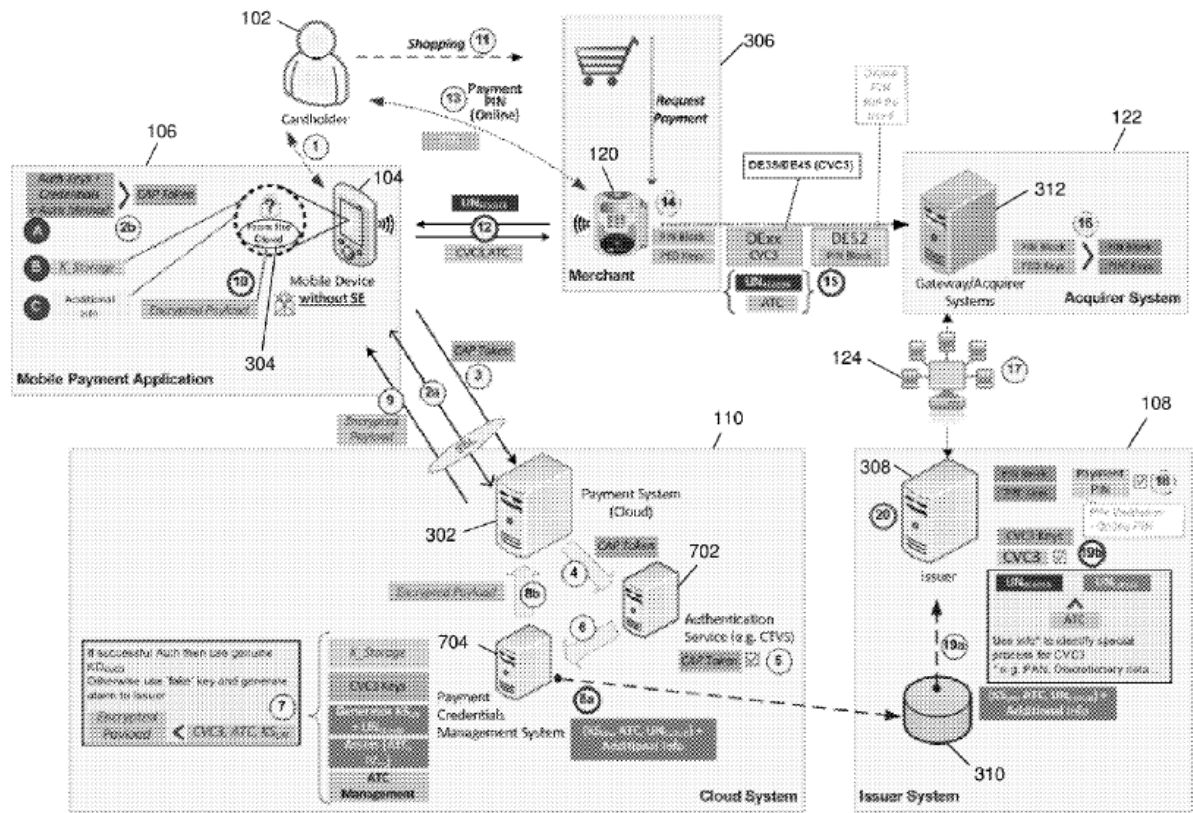


FIG. 7

81. Figure 9 is a flow diagram illustrating a method for the initialization of a mobile application program on the mobile device of the system of FIG. 1 in accordance with exemplary embodiments:

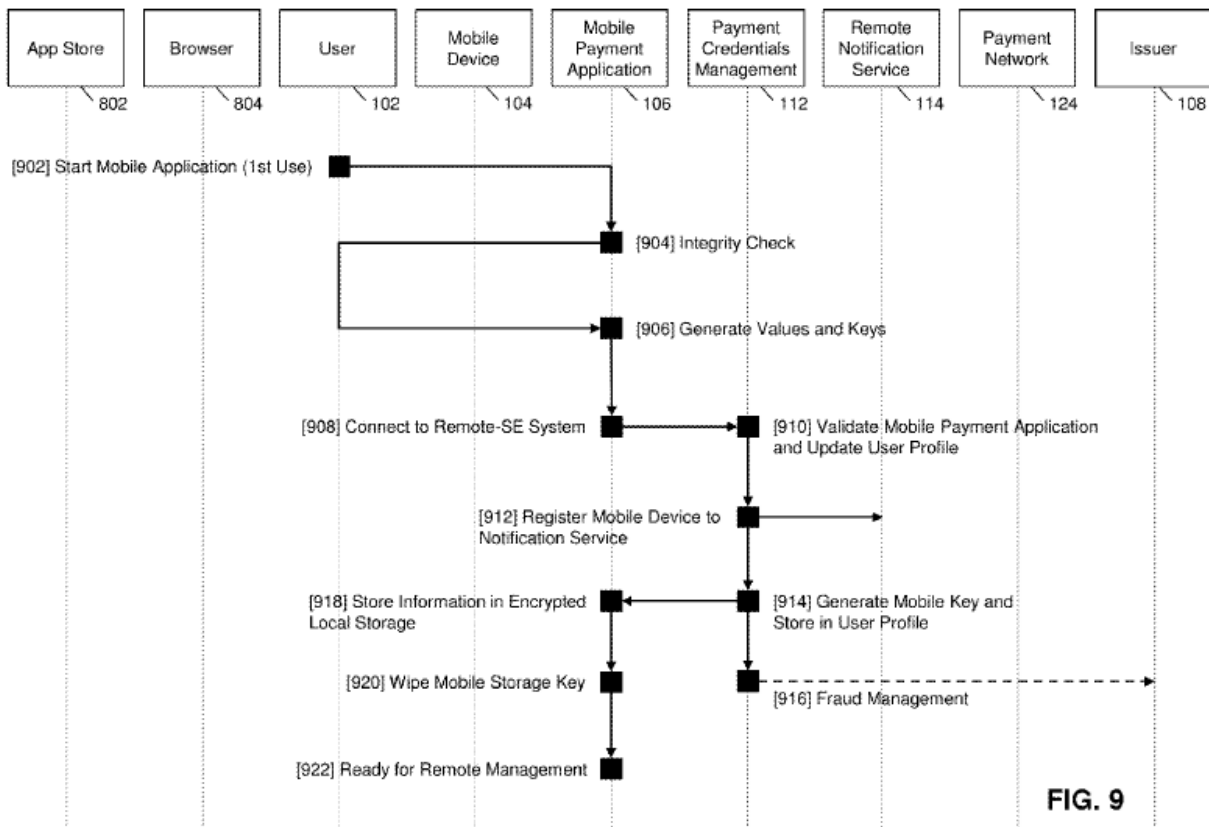


FIG. 9

82. It should also be noted that Collinge never mentions EMV nor ISO 7816. Dr. Fiske erroneously claims in his deposition that Collinge does reference “EMV.” (EX2035 at 64:6-20). Throughout the petition, Dr. Fiske’s declaration, and Dr. Fiske’s deposition, the EMV Specification is used to supply limitations that simply are not disclosed in Collinge. Even two years after Collinge, EMV adoption in the United States was at 0.03%. Because of its low adoption rate and the prevalence of many other payment transaction standards, a POSITA would not considered have considered the EMV Specifications as “standard practice” and would not have found it obvious to implement Collinge according to EMV standards.

83. In the following section, specific claim elements that the petitioner and Dr. Fiske assert are anticipated or rendered obvious by Collinge are addressed.

- v. **Claim [1.A-3]: “... configured to [1] 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”**

84. The petitioner and Dr. Fiske point to transmitting a CAP token to the remote-SE system for this claim limitation, asserting that because the sending of the CAP token will *eventually* be following by data being sent, therefore the CAP token is a “request” for said data. Dr. Fiske states “...which causes the remote-SE system to generate and return payment credentials in an encrypted payload after verification of CAP token, id. at [0082]- [0083], [0085]. A POSA would understand that sending of CAP token initiates, and thus constitutes a request for server to return payment credentials.” Ex [1006] ¶ 87. I disagree.

85. This is a misunderstanding of what Collinge teaches. A POSITA would readily understand that the CAP token in Collinge has one purpose, to validate the device (Collinge 9; 10; 13;14). Claim 53 of Collinge also makes this clear, stating “a processing device configured to generate a chip authentication program (CAP) token, wherein the CAP token is based on at least the authentication component and the at least one additional credential;” The CAP token is not a request for any data.

86. In fact, paragraph 82 of Collinge states “In stage 3, the mobile payment application 106 may transmit the generated CAP token to the remote-SE system 100. At stage 4, the CAP token may be forward to a CAP token validation service (CTVS) 702. At stage 5, the CTVS 702 may validate the CAP token using methods apparent to persons having skill in the relevant art. At stage 7, the results of the validation may be sent to the payment credentials management system 704. In some embodiments, the payment credentials management system 704 may be operated by or on behalf of the issuer 108.” According to Collinge, if anything can be said to trigger the process in paragraph 85, it is the processes in paragraph 84, which Dr. Fiske ignores.

87. Paragraph 84 of Collinge states “At stage 8a, the payment credentials management system 704 may perform a synchronization process with the issuer 108. The synchronization process may include defining rules for the validity of the values generated by the mobile payment application 106 for conducting a payment transaction. In one embodiment, the process may include transmitting at least the KS application transaction counter, and UN, to the issuer 108 for storage in the issuer database 310.” (Collinge, 84)

88. This describes a process where the mobile payment application *may* transmit the generated CAP token to the remote-SE system in stage 3 (Collinge 82) then after numerous other steps, in stage 9, the encrypted payload *may* be sent to the mobile

payment application. The CAP token sent in stage 3 has one purpose, which is to validate the mobile application. It is not a request for *a corresponding digital credential*.

89. The results of that validation are then sent to the payment credentials management system 704. After that, the cloud system and the issuer take a number of steps including synchronizing the payment credentials management system 704 with the issuer 108; transmitting the K_{UN} application transaction counter and UN_{CLOUD} to the issuer 108 for storage in a database. At least some of these steps are simply between the cloud system and the issuer and don't even involve the mobile device application.

90. A POSITA would recognize that the CAP token is for authentication, it is not a request for any data at all, much less *a corresponding digital credential*, as recited by the claim.

91. I next note that paragraph 83 of Collinge, which is cited by Dr. Fiske, simply states "At stage 7, the payment credentials management system, 704 may generate an encrypted payload. As part of the encrypted payload, the payment credentials management system 705 may generate a session key unpredictable number (K_{UN}), a cloud unpredictable number (UN_{CLOUD}) and may identify and/or store a plurality of dynamic card validation (CVC3) keys and the K_{storage})." A POSITA would readily understand first that each of these steps *may* occur, not *will* occur. Secondly, a

POSITA would also understand that stage 7 is not being executed due to any request. Nothing in Collinge teaches or even suggests a request. The occurrence of action B temporally after action A does not in any way teach that action A was a *request for* action B, and a POSITA reading Collinge would not understand it this way.

92. The petitioner and Dr. Fiske then state “Moreover, Collinge discloses that the credentials may be provisioned via a ‘pull request from the mobile device.’ Ex [1009], cl. 19.” Exhibit 1009 is not Collinge, but rather a provisional patent application that preceded Collinge. The subject matter relied upon in Exhibit 1009 regarding a “pull request from the mobile device” was not carried forward in Collinge, and a POSITA would not have understood Collinge to disclose any pull request from the mobile device. (Exhibit 1011).

93. In his declaration, Dr. Fiske states “To the extent Collinge does not explicitly disclose that the application would request a first set of data from the remote computer system, in light of the fact that such data is retrieved from a remote system, a POSA would have found it obvious to configure the mobile application to request it as that was one of a finite number of predictable ways to retrieve data.” (Ex. 1006, ¶ 88). I first note that Dr. Fiske appears to be asserting that since data is eventually sent from a remote system to the mobile device application, that data *must* have been retrieved by the mobile application. That is faulty reasoning. I first note that the claim limitation recites a “request ... data associated with the account,” which a

POSITA would understand is a different process from “retrieves data associated with the account.” As an analogy I may *request* food be delivered to my home, if I go and get the food myself, I have *retrieved* it. Retrieving and requesting are not synonymous.

94. A POSITA would easily understand that there are many ways the data could arrive at the mobile device application that do not involve was. A few options that would be readily apparent to a POSITA are explained here:

- a) A remote system can simply send data at a certain point in its processing without any request from the mobile device application (as Collinge actually does).
- b) A second option would be that the remote system could send such data over a wireless network that is not separate from the first communication channel in response to a request.
- c) A third option would be the remote system sending data over a wireless network that is not separate from the first communication channel at a predetermined point in the processing, rather than in response to a request.
- d) A fourth possibility would be the digital credential to be sent from the payment processing service to the point-of-sale device in response to a request, directly rather than to the mobile device application.

95. The preceding are simply examples of other ways in which data could arrive at the mobile device application. This list is not meant to be exhaustive.

96. I also disagree with Dr. Fiske that a POSITA would have been motivated to modify Collinge to include a “request” for data associated with the account in order to avoid “a waste of bandwidth and resources.” Ex. 1006 ¶ 88 Dr. Fiske has not shown that Collinge’s method of provisioning data to the mobile device operates to “push information regardless of the status of the user device,” and a POSITA would not understand Collinge’s disclosed approach to be a waste of bandwidth or resources.

97. Dr. Fiske further states “To the extent Collinge does not explicitly disclose that the application would ‘request’ a first set of data from the remote computer system, in light of the fact that such data is retrieved from a remote system, a POSA would have found it obvious to configure the mobile application to request it as that was one of a finite number of predictable ways to retrieve data.” This is incorrect for multiple reasons. First, as Dr. Fiske appears to admit, a POSITA would have been aware of many other ways to request information, a few exemplary options are given here:

- a) Information could be requested via the first communication channel.
- b) The digital credential could be pre-stored on the device thus there would be no need to request it from a remote computer system.

c) The POS could request the credential from the remote computer system.

98. Each of these alternatives would have alleviated the “waste of bandwidth and resources” concern that Dr. Fiske identifies associated with a “push” from the issuer and are also able to effectively limit the number of keys on the mobile device.

99. For at least the reasons discussed in this section, a POSITA would readily understand that Collinge teaches a process that is quite different from the ‘171 patent and cannot anticipate nor render obvious this claim limitation.

vi. **Claim [1.A-4]: “...[2] 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”**

100. The petitioner asserts “Collinge discloses that ‘the mobile device 104 may ... transmit a generated payment cryptogram and payment credentials to a point-of-sale terminal 120 ... via near field communication (NFC).’ Ex [1011], [0043], [0085]; see also supra § X.A.1.c (1.A-2); Ex [1009], [0061] (Table 1, Step 15), [0044], [0056], [0068].” Pet. at 41. Petitioner further asserts that “[t]he application does not access a permanent cryptographic key issued for the digital credential because the CVC3 cryptogram is generated using a single use key, ‘session key’ (K_{SUN}). Ex [1011], [0043], [0050], [0070], [0077], [0085], [0136], [0145], Fig. 16; see also Ex [1009], [0056], [0068], [0071], [0075], cl. 1.” Pet. at 41.

101. Dr. Fiske then asserts “A POSA would also have found it obvious to implement Collinge in the manner described above because using a ‘Session Key’ generated from ATC (hence unique to each transaction and non-permanent) to generate a cryptogram in a transaction was a standardized operation in secure payment transactions, and thus entailed applying a known technique (changing cryptographic key) to yield predictable results (improved resistance to security attacks).” Ex. 1006 ¶ 91. I disagree. Dr. Fiske relies on exhibit 1020 section 8.1.2.2. Section 8 Application Cryptogram and Issuer Authentication states “Note that the methods provided in this specification are not mandatory. Issuers may decide to adopt other methods for these functions.” As a result, a POSITA would recognize that implementing a session key according to Exhibit 1020 was not required to comply with EMV standards. I disagree that this optional technique for generating a cryptogram was “a standardized operation.” A POSITA would have been aware of many other techniques, as I explain further in reference to claim 6.

102. Dr. Fiske admitted in his deposition that this section is not mandatory, and vendors can implement cryptograms in other ways (Ex. 2035 at 60:1-61:1). Indeed, during his deposition, Dr. Fiske admitted that there are items in Collinge that are not EMV standard (Ex. 2035 at 42:5-6).

103. Furthermore, during his deposition Dr. Fiske admitted that by 2012 the US had not yet migrated to EMV standard (Ex. 2035 at 49:5 - 50:4). This further

demonstrates that implementing Collinge in accordance with EMV standards would not have been obvious.

104. Furthermore, as was discussed in section II.C.i of this declaration, even as late as 2014 EMV adoption in the United States was at 0.03%. This further demonstrates that implementing Collinge in accordance with EMV standards would not have been obvious. Quite clearly a great many persons of ordinary skill in the art were implementing credit card processing solutions that were not EMV compliant.

105. For at least the reasons discussed in this section, a POSITA would readily understand that Collinge does not anticipate nor render obvious this claim limitation.

vii. Claim [1.B]: “requesting by the application, from the remote computer system, over the wireless network, a first set of data associated with the account;”

106. For this claim limitation the petitioner simply refers to 1.A-3 and then states “POSA would also have found it obvious to configure the mobile application to make a request, either together with transmitting a CAP token or separately (e.g., before transmission), for purposes of efficiency and resources, as explained in [1.A-3].” Pet. at 42. I disagree that configuring Collinge’s mobile application to make a request would improve efficiency or conserve resources. Indeed, Petitioner has identified no weakness in the process disclosed in Collinge in this regard, and a POSITA would not have understood Collinge’s disclosed process to be deficient in this way.

107. As was discussed in reference to petitioners 1.A-3, the CAP token is simply used for authentication. It is not a request for any data, much less a first set of data associated with the account.

108. Furthermore, in reference to other claims, the petitioner and Dr. Fiske point to exhibit 26 to the petition. Exhibit 26 has the word 'request' 348 times. None of which involve the mobile device or mobile device application making any request. The specifics of exhibit 26 are discussed in more detail in relevant claims, however, what is relevant to the current claim limitation is that the EMV standard itself describes a method of performing these transactions **without** the mobile device or mobile device application generating a request. While the petitioner and Dr. Fiske assert it would have been obvious to a POSITA to configure Collinge to have a mobile device application generate such a request, the fact that industry standards accomplish the same goals without the mobile device application generating any request, refutes that assertion.

109. For at least the reasons discussed in this section, a POSITA would readily understand that Collinge does not anticipate nor render obvious this claim limitation.

viii. **Claim 1.C “receiving by the application, from the remote computer system, over the wireless network, 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;”**

110. I note that Petitioner does not cite to the declaration of Dr. Fiske in support of this limitation, other than for its contention (last paragraph of its [1.C] section) relating to APDUs.

111. The petitioner asserts that KS_{UN} is a “first non-permanent cryptographic key” that is unique to each transaction and “associated with the account.” Pet. 43. I disagree that Collinge’s session key (KS_{UN}) is “associated with the account.”

112. Petitioner provides three reasons to support its contention. First, Petitioner says “it is generated in response to an account-specific request.” Pet. 43. This is not evidence of KS_{UN} being associated with an account. Indeed, as Dr. Fiske admitted during his deposition, a POSITA would not understand that a piece of data is “associated with the account” when data is sent as part of an account-specific request and that data cannot be used to determine which account it relates to. Ex. 2035 at 84:19-86:11. I agree. A POSITA would be aware of many data items that could be sent and/or generated as part of an account-specific interaction—for example, a timestamp or packet header information—that would not be associated with an account. A POSITA would also understand that KS_{UN} , which is an unpredictable number, cannot be used to determine any of the account information, such as the

PAN. Ex. 1011 at 9, 10, 13, 83. A POSITA would readily understand that Collinge's session key is associated with a given session, *not an account*. Should the user perform another transaction using Collinge's system, even just a few minutes later, another Session Key will be generated.

113. Collinge's disclosures as to the session key unpredictable number appear to be consistent with how "session keys" would have been understood in the art:

- a) "A session key is a one-use-only key for both encryption and decryption. *A session key is randomly generated so that unauthorized users can't access or guess it.* It is used to encrypt and protect the communication between two users, a user and a computer, or two computers. One session key can only be used once, which is excellent for protection as attackers won't be able to find it after the fact and use it to crack future communications. "¹⁵(Emphasis added)
- b) "A relatively short-lived symmetric key (a cryptographic key negotiated by the client and the server based on a shared secret). A session key's lifespan is bounded by the session to which it is associated. A session key has to be strong enough to withstand cryptanalysis for the lifespan of the session."¹⁶

¹⁵ Ex. 2023 (<https://nordvpn.com/cybersecurity/glossary/session-key>)

¹⁶ Ex. 2024 (https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-nrpc/b5e7d25a-40b2-41c8-9611-98f53358af66)

- c) “A key such as K that is used for a single communication session is called a session key.”¹⁷

114. Second, Petitioner says that KS_{UN} is “associated with the account” because it uses the account specific ATC in its generation. A POSITA reading Collinge would not understand that the ATC is used to generate KS_{UN} . The ATC is only mentioned once in Collinge, where it indicates that the single use key may include an application transaction counter and a generating key (i.e., KS_{UN}). Ex. 1011 ¶50. A POSITA would not understand that Collinge’s disclosure of “a single use key [that] may include an application transaction counter (ATC) and a generating key” indicates or suggests that the generating key is itself generated using the ATC. *Id.*

115. The petitioner asserts that it is well known in the art to use C-APDU and R-APDU for communication. Pet. 43. It should first be noted that the term APDU does not appear in Collinge, and a POSITA would not understand Collinge to disclose or suggest communications using APDUs. I understand that a Petitioner may not rely on non-prior art disclosures to fill gaps in the prior art, which is what the petitioner appears to be doing here. Dr. Fiske states “it would be obvious to implement Collinge in this way to ensure interoperability with EMV standardized devices” (Ex. 1006 ¶95). However, as has been discussed in this declaration previously, there were

¹⁷ Ferguson, Niels; Schneier, Bruce; Kohno, Tadayoshi. Cryptography Engineering: Design Principles and Practical Applications (p. 100). Wiley. Kindle Edition.

alternatives to EMV, and at the time of invention of the '171 patent, EMV standards were not widely adopted in the United States. Therefore, a POSITA would have recognized many alternatives to EMV, which was by no means widely implemented. I also note that the petitioner has provided no explanation of any deficiencies in Collinge that would be solved by the use of APDUs. In my opinion, a POSITA would not have recognized that the use of APDUs, as claimed, presented a particular advantage over other available techniques for communicating data between devices in Collinge.

116. In his deposition, Dr. Fiske asserted that Collinge would need to use ADPU's due to ISO 7816 (Ex. 2035 at 87:2-16). I disagree. It should be noted that Collinge never mentions ADPU's, nor does Collinge ever mention ISO 7816. Ex. 1011.

117. For at least the reasons discussed in this section, a POSITA would readily understand that Collinge does not anticipate nor render obvious this claim limitation.

ix. Claim [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”

118. Dr. Fiske contends that Collinge's “payment CVC3 value” is a “response cryptogram” that is generated using KSUN, which he contends is the local cryptographic key. Ex. 1006 ¶ 102. As to the limitation “wherein the response cryptogram does not include the local cryptographic key,” Dr. Fiske does not cite to

any disclosure in Collinge to support this. EX1006 ¶ 103 (citing EX1034 at 17-18; EX1039). Indeed, as Dr. Fiske acknowledged, Collinge does not disclose how the CVC3 value is calculated. Ex. 2035 at 105:2-5. Instead of pointing to any disclosure in Collinge, Dr. Fiske relies on Exhibit 1034 and Exhibit 1039, which I understand have not been asserted as a prior art patents or printed publications.

119. Dr. Fiske appears to contend that Exhibit 1034 is relevant based on its disclosure of “message authentication code (MAC) generation” (Ex. 1006 ¶ 103), yet he offers no explanation as to how a MAC is relevant to the generation of a payment CVC3 value in Collinge. The cited portions of Exhibit 1034 say nothing of a CVC3 value, and Collinge never mentions a message authentication code or MAC, let alone equate the payment CVC3 value to a MAC.

120. Finally, Dr. Fiske cites to Exhibit 1039 with its only explanation coming in a parenthetical stating “showing single-use key is not present in the MAC/cryptogram.” *Id.* Once again, he points to no disclosure in Exhibit 1039 of a CVC3 value or Collinge’s KS_{UN}. And he cites to the entirety of Exhibit 1039, which is 20 pages in length, but does not identify any particular portions that are relevant.

121. Based on my review of Exhibit 1039, a POSITA would not have understood that it demonstrates or suggests how Collinge’s CVC3 would be generated. Without knowing how the CVC3 in Collinge is generated, a POSITA would be unable to conclude that the CVC3 “does not include the cryptographic key.”

122. Petitioner’s generalized statement that “[u]sing a single-use key ... to generate a cryptogram results in a cryptogram that does not include the single-use key” is incorrect. There are numerous ways to generate a cryptogram using a cryptographic key, including techniques that would include the generating key in the cryptogram. Dr. Fiske’s citation to Exhibits 1009, 1034, and 1039 do not change this, and, as explained above, are not indicative of how Collinge operates. Ex. 1006 ¶103.

- x. **Claim [1.E-3] “responding to the at least one POS command communication...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;”**

123. Petitioner offers two potential constructions of this limitation but fails to show unpatentability under either construction. Under the **first construction**, Petitioner says the limitation would include “one or more APDUs collectively containing the response cryptogram and an account identifier for the account.” Pet. 49. Dr. Fiske contends that this would be satisfied by “Collinge’s reference to the Paypass card specification in the provisional application.” Ex. 1006 ¶108 (citing EX1009 [0003], [0029]-[0032]). Dr. Fiske cites only to the Collinge Provisional application. But there is no disclosure in Collinge itself of a Paypass card specification. Ex. 1011.

124. Furthermore, even if disclosure in the Collinge Provisional of “Paypass” were considered as a prior art disclosure, Dr. Fiske has not shown that “Paypass” would indicate to a POSITA that one should look to Exhibit 1026 for the implementation details of “Paypass.” Exhibit 1026 includes the word “PayPass” only once, in Figure 3.1 (Ex. 1026, 78), which is part of a section titled “Implementation Options.” *Id.* A POSITA would not understand this to indicate that a “Mastercard interrogation” is being implemented. Furthermore, Exhibit 1026 states that “[a]n implementation option allows the vendor to select whether the software behind the option will be implemented in a particular installation.” *Id.*, 31. Accordingly, a POSITA would recognize the implementations Petitioner relies on in Exhibit 1026 as a “Mastercard interrogation” (Pet. 55) are not mandatory for EMV compliance and may not be implemented in a particular installation. Dr. Fiske does not provide any explanation as to why a POSITA would be motivated to choose this optional implementation strategy over other available options. Accordingly, I disagree that Dr. Fiske has shown this limitation would be obvious under Construction 1.

125. Petitioner further contends that “because a POSA reading Collinge will understand its disclosure as compatible with EMV transactions ... it would have been obvious to a POSA to implement Collinge to carry out EMV transactions.” Pet. 50. But Collinge never mentions EMV transactions, and Petitioner’s only support for its contention that Collinge’s disclosures would be compatible with EMV comes

from (1) the Collinge provisional's disclosure of PayPass and (2) reference to "CVC3" and "application cryptogram" in paragraph 50 of Collinge. The Paypass disclosures in Collinge's provisional are not carried forward into Collinge. In addition, Dr. Fiske does not how "CVC3" and "application cryptogram" would inform a POSITA that Collinge is compatible with **any** EMV transactions, let alone the "EMV mode contactless Visa transaction." In fact, at his deposition, he admitted that a POSITA would not have understood "CVC3" to refer to an EMV mode transaction, but instead to a Magstripe transaction. In addition, at the time of the invention of the '171 patent, a POSITA would not have understood "CVC3" or "application cryptogram" as necessarily indicating an "EMV mode Visa transaction." A cryptogram is simply the output of a cryptographic algorithm. In his deposition Dr. Fiske stated "A cryptogram is the result of a cryptographic calculation." (Ex. 2035 at 27:18-19). I agree with Dr. Fiske on this issue. Furthermore, an application cryptogram is simply a cryptogram being used by an application. This in no way suggests to a POSITA an "EMV mode Visa transaction."

126. Under Petitioner's proposed **second construction**, this limitation could refer to "one or more APDUs, each of which contains *both* the response cryptogram and an account identifier for the account." Pet. 50. Dr. Fiske contends that an EMV mode Visa transaction would satisfy this claim element. Ex. 1006 ¶109. However, as explained above, Petitioner provides no explanation as to how "CVC3" and

“application cryptogram” would inform a POSITA that Collinge is compatible with **any** EMV transactions, let alone the “EMV mode contactless Visa transaction” Petitioner relies upon. Accordingly, Dr. Fiske has not shown that a POSITA would have found this limitation obvious based on Collinge under Petitioner’s Construction 2.

127. For at least the reasons discussed in this section, a POSITA would readily understand that Collinge does not anticipate nor render obvious this claim limitation.

xi. Claims 4 and 20: “wherein the interrogation conforms to a card specification...”

128. Dr. Fiske does not identify any disclosure in the “Mastercard Paypass or EMV Specifications” that the Collinge system is compliant with. Ex. 1006 ¶¶117-118. In fact, I see no reference at all to the details of any “Mastercard Paypass” specification. I therefore disagree that Collinge discloses or renders obvious “the interrogation conforms to **a card specification**, the set of inputs is **specified by the card specification**,” or that “the at least one device response is formulated according to **the card specification**” as claim 4 recites. As a POSITA would recognize, card specifications often provide only a loose framework for transactions and often leave many implementation details to the issuer’s discretion. Dr. Fiske provides no explanation as to why a POSITA would be motivated to modify Collinge or that such modifications would result in Collinge’s system performing the recited steps.

129. For at least the reasons discussed in this section, a POSITA would readily understand that Collinge does not anticipate nor render obvious this claim limitation.

xii. Claims 6 and 22: "The method of claim 1, 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"

130. For this claim the petitioner and Dr. Fiske simply state it is common knowledge to use 3DES as a symmetric algorithm in financial applications. I agree with this point, however, using an algorithm to encrypt data in financial applications is not the same as using an algorithm to generate a cryptogram.

131. I further note that a cryptogram can be generated with a hash algorithm (including MD5, SHA1, SHA2, SHA3, RIPEMD, HAVAL, Whirlpool, Skein, GOST, BLAKE, etc.), or an HMAC. One need not use a MAC with any symmetric algorithm (DES, 3DES, AES, Blowfish, McGuffin, IDEA, MARS, etc.) in order to generate a cryptogram. And in fact, there are numerous variations of MAC including AMAC (ANSI Retail MAC); PMAC (A parallelizable Message Authentication Code); UMAC (universal message authentication code); KMAC (Keccak Message Authentication Code). Using a DES based MAC is only one of a wide array of options, many of which are either more efficient and/or more secure than DES. Therefore, it would not have been obvious to a POSA to use DES to encrypt inputs to create a cryptogram.

132. A POSITA would understand any cryptography algorithm could be used to fulfill the requirements of a cryptogram. Credit card processing can also be done with Advanced Encryption Standard (AES)¹⁸¹⁹, an in fact any secure symmetric cipher could be used including Serpent²⁰²¹, and Blowfish²². It should also be noted that other algorithms are indeed used in banking and finance “In addition to AES and 3DES, other symmetric encryption algorithms are used by banks, such as Blowfish, Twofish, and Serpent. These algorithms offer different levels of security and performance, allowing banks to choose the one that best suits their needs.”²³

133. I note that during his deposition Dr. Fiske stated he was unfamiliar with the Serpent, IDEA, MARS, or Camelia algorithms (Ex. 2035 at 33:21-34:21). MARS, Serpent, and Idea are all discussed in the introductory cryptography textbook “Understanding Cryptography: A Textbook for Students and Practitioners”²⁴ published in 2010. These algorithms are also discussed in the 2006 book “An Introduction to Cryptography”²⁵. The Serpent protocol was one of the finalists for the AES project, alongside Rijndael, and was created to be applied to financial

¹⁸ Ex. 2025 (<https://www.visa.com.au/content/dam/VCOM/global/support-legal/documents/bulletin-encryption-best-practices.pdf>)

¹⁹ Ex. 2026 (https://sec.cloudapps.cisco.com/security/center/resources/next_generation_cryptography)

²⁰ Ex. 2027 (<https://www.cl.cam.ac.uk/~rja14/Papers/serpent.pdf>)

²¹ Ex. 2028 (https://www.cl.cam.ac.uk/~rja14/Papers/serpent_card_final.pdf)

²² Ex. 2029 (<https://fastercapital.com/topics/encryption-techniques-for-financial-transactions.html/1>)

²³ Ex. 2030 (<https://www.newsoftwares.net/blog/how-do-banks-encrypt-data/>)

²⁴ Paar, Christof; Pelzl, Jan. Understanding Cryptography: A Textbook for Students and Practitioners (Kindle Locations 135-136). Apress - A. Kindle Edition.

²⁵ Mollin, Richard A... An Introduction to Cryptography (Discrete Mathematics and Its Applications). CRC Press. Kindle Edition.

transactions²⁶. These are well known cryptographic algorithms that are found in introductory books and courses on cryptography. It is rather surprising that Dr. Fiske is unfamiliar with them.

134. Dr. Fiske also stated he was unfamiliar with the terms AMAC, PMAC, and UMAC (Ex. 2035 at 35:16-36-2). ANSI Retail MAC, this actually has been used in banking²⁷. A parallelizable MAC (Message Authentication Code) is a type of cryptographic algorithm designed to enable efficient computation by allowing the processing of multiple parts of a message simultaneously. This parallel processing capability makes these MACs particularly suitable for high-performance environments and applications where low latency and high throughput are critical. A universal hashing, or UMAC, is a type of message authentication code (MAC) calculated choosing a hash function from a class of hash functions according to some secret (random) process and applying it to the message. Dr. Fiske appears unfamiliar with basic cryptography.

135. For at least the reasons discussed in this section, a POSITA would readily understand that Collinge does not anticipate nor render obvious this claim limitation.

²⁶ Ex. 2027 (<https://www.cl.cam.ac.uk/~rja14/Papers/serpent.pdf>)

²⁷ Ex. 2031
(<https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report/%40%40download/fullReport&ved=2ahUKEwiynsvmveWGAXVbOkQIHRJDCEAQFnoECBIQAQ&usg=AOvVaw3grzkdAsLGwgTUzppZioN7>)

xiii. Claim 8

136. For claim 8, all subsections, the petitioner and Dr. Fiske simply refer back to claim 1. This ignores the fact that claim 8, while dependent upon claim 1, adds additional requirements. Claim 8 begins with “The method of claim 1, further comprising, at the remote computer system :”

137. By ignoring the differences between claim 8 and claim 1, and simply referring back to claim 1, the petitioner and Dr. Fiske have not even attempted to show that Collinge anticipates or renders obvious these claim limitations. However, I will perform a more thorough analysis.

xiv. Claim 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; and”

138. For this claim limitation the petition simply states “See §§ X.A.1.d, X.A.1.f, X.A.1.g, X.A.1.i(3) ([1.A-3], [1.B], [1.C], [1.E-3].” None of these prior sections show that Collinge discloses or renders obvious the limitation “at the remote computer system ... sending the first non-permanent cryptographic key and the account identifier to the mobile device.”

139. As was discussed previously in this declaration, the petitioner, and Dr. Fiske point to KS_{UN}, which simply is not associated with the account, but rather is associated with a specific session.

140. In § X.A.1.d (limitation [1.A-3]), Petitioner identifies the PAN as the claimed *account identifier*. Pet. 49-50; Fisk Dep. 22:8-14. Petitioner further contends that transmission of a CAP token “causes the remote-SE system to generate and return payment credentials in an encrypted payload.” Pet. 38-39 (citing EX1011, [0082]-[0083], [0085]). Petitioner says that payment credentials management system 704 generates the encrypted payload, which “may include at least one CVC3 key, the KS_{UN}, and the application transaction counter.” *Id.* But a CVC3 key, KS_{UN}, and the application transaction counter are not account identifiers, and they are not the PAN. Paragraph [0085] of Collinge says “the encrypted payload may be transmitted to the cloud system 302 for transmitting to the mobile device,” but makes no mention of the encrypted payload including the PAN.

141. Section § X.A.1.f of the Petition (limitation [1.B]) 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. Pet. 42. In § X.A.1.g (limitation [1.C]), 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. In § X.A.1.i(3) (limitation [1.E-3]), Petitioner contends that the **mobile device** sends payment credential data, which a POSA would understand to include generated cryptogram and “other common payment credential information” such as the PAN. Pet. 48-49. This 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.

142. Thus, the only discussion of anything sent **from** the remote-SE to the mobile device is the “encrypted payload,” which does not include the PAN.

143. For at least the reasons discussed in this section, a POSITA would readily understand that Collinge does not anticipate nor render obvious this claim limitation.

xv. **Claim 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 non-permanent cryptographic key and the account identifier to the mobile device over the wireless network.”**

144. For this claim limitation the petition simply states “See §§ X.A.1.j ([1.F]-[1.G]).” Pet. 57. Petitioner’s discussion of limitations [1.F] and [1.G], however, not present any argument or evidence of the steps performed “at the remote computer system and after the interrogation,” as recited in limitation [8.B].

145. Dr. Fiske says that “the new KS_{UN} for a subsequent transaction would be **requested** subsequent to a prior transaction.” Ex. 1006 ¶111 (emphasis added). But this request would be a request by the application. This does not show that the remote-SE generates a new KS_{UN} value after an interrogation. And, as a POSITA would recognize, KS_{UN} values need not be generated after an interrogation. They could readily be generated prior to interrogation, and they need not be generated by the remote computer system. Therefore, I disagree that this limitation is disclosed by

Collinge. I note that Dr. Fiske has not presented any argument that limitation [8.B] would have been obvious.

146. For at least the reasons discussed in this section, a POSITA would readily understand that Collinge does not anticipate nor render obvious this claim limitation.

xvi. **Claims [10.A]/[27.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;”**

147. I note the preamble of claim 10 recites “at the remote computer system.” Accordingly, I understand that each of the steps recited in claim 10 is performed at the remote computer system. I also note that claim 10 depends from claim 1, which introduces the “remote computer system” in in the limitation “at a mobile device, executing an application ... configured to request, **from a remote computer system** ... data associated with the account.”

148. In Dr. Fiske’s analysis of claim 1, he identifies “remote-SE system 110” as the “remote computer system.” Ex. 1006 ¶87. Dr. Fiske also confirmed during his deposition that “remote-SE system 110,” as shown, for example in Collinge’s Figure 7, is what he identifies as the claimed remote computer system.” Ex. 2035 at 74:15-75:9. Dr. Fiske identifies the same alleged “remote computer system” in its analysis of limitation [1.C], which recites “receiving by the application, from the remote

“[t]he merchant point-of-sale terminal 120 may transmit the received payment information ... to the **acquirer processing server 312** of the acquirer 122.” Thus, it is “acquirer processing server 312,” which is not part of “remote-SE 110” that Dr. Fiske relies on to perform the recited “receiving an authorization request” step.

150. Although I see no disclosure in either the Petition or Dr. Fiske’s declaration that the claimed “remote computer system” would include some kind of aggregation of the various distinct systems disclosed in Collinge, I also note that a POSITA would **not** have understood Collinge as disclosing a single “remote computer system” that combines, for example, “Cloud System 110,” “Issuer System 108,” “Payment Network 124,” and “Acquirer System 122” (or any combination thereof). *See, e.g.*, Ex. 1011 at Fig. 7. Rather, a POSITA would understand based on Collinge, that each of these items is (one or more) separate systems that operates independently from the others. For example, Collinge repeatedly describes communications between various systems. Ex. 1011 ¶ 45 (“acquirer 122 may submit an authorization request for payment transaction to a payment network 124”); 56 (“payment network 124 may forward relevant information to the issuer 108”); 56 (“issuer processing servier 308 may authenticate the dynamic card validation code ... received from the cloud system 302”); *see also* Ex. 1011 at Fig. 14 and associated descriptions (illustrating and describing the flow of information between Acquirer, Payment Network, and Issuer).

151. For limitation [10.B], which recites “at the remote computer system ... determining a current non-permanent cryptographic key,” Dr. Fiske alleges that “Collinge discloses that ‘the **issuer processing server 308** may validate the payment CVC3.’” Pet. 59 (emphasis added). As is evident from, for example, Figure 7 of Collinge, “issuer processing server 308” is also not part of “remote-SE 110.”

For at least the reasons discussed in this section, a POSITA would readily understand that Collinge does not anticipate nor render obvious this claim limitation

xvii. **Claim 10 B “determining a current non-permanent cryptographic key associated with the account using the account identifier,”**

152. Dr. Fiske has not shown that limitation [10.B] is disclosed by Collinge because he does not demonstrate the step of “**determining a current non-permanent cryptographic key ... using the account identifier.**” Dr. Fiske says that issuer processing server 308 retrieves (and thus “determines”) the UN_{CLOUD} and KS_{UN} (i.e., the alleged “**cryptographic key**”) values that were used to generate the CVC3 value. Ex. 1011 ¶ 132. But he ignores that limitation [10.B] also recites the determination is done “**using the account identifier.**” Dr. Fiske does not show that issuer processing server 308 determines KS_{UN} using the PAN (i.e., the alleged “**account identifier**”). Indeed, EX1009, which Dr. Fiske relies on, states in step 19a that the “ATC provided in the Payment Transaction” is “used to retrieve UN_{CLOUD} and KS_{UN} values.” EX1009, 23. For this reason, Dr. Fiske has not shown that limitation [10.B] is disclosed or rendered obvious by Collinge.

xviii. Claim 10 C “calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account ”

153. Petitioner appears to contend that Collinge’s Payment Credentials Management System “calculate[es] a calculated cryptogram,” but it has provided no evidence of that. Pet. 59. Petitioner cites to paragraph [0087] of Collinge, but that paragraph makes no mention of “Payment Credentials Management System” or any step of “generating” a cryptogram. EX1011, [0087]. Petitioner also cites to paragraph [0061] of EX1009, which states “Payment Credentials Management System to generate the CVC3 value.” As a POSITA would readily understand, this disclosure in the Collinge Provisional is not carried forward into Collinge. As Dr. Fiske acknowledged, the disclosure in Collinge by itself resulted in “maximum confusion,” so he had to look to the Collinge Provisional. Ex. 2035 at 97:22-98:24. Even if statements in the Collinge Provisional could be used here, Payment Credentials Management System in Collinge (*see, e.g.*, element 704 in Figure 7) is separate from issuer processing server 308, and Petitioner presents no evidence or argument that these distinct components are part of the same remote computer system. A POSITA would understand that they are not.

xix. Claim 15 “The method of claim 1, wherein the application is configured to generate the response cryptogram according to a card specification,”

154. Dr. Fiske presents no analysis of this claim, instead referring to “Claims 4 and 20.” Ex. 1006 ¶141. His arguments as to claim 15 fail for the same reasons as described above as to claim 4. In addition, his analysis of claim 4 does not show that “generat[ion] of the response cryptogram [is] according to a card specification.” He says only that “card specifications were well known in the art and a POSA would have been motivated to make their systems compliant with such specifications.” Ex. 1006 ¶ 118. This allegation, even if true, does not demonstrate that it would have been obvious that “the application is configured to generate the response cryptogram according to a card specification.” Dr. Fiske has not shown that either the Mastercard Paypass or EMV Specifications specify how a response cryptogram is generated. Therefore, he has not shown that conducting a transaction in compliance with either specification involves generating a response cryptogram according to the card specification. Also, as 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. Ex. 2035 at 61:1-62:1.

xx. Claim 16 “The method of claim 1, wherein the first and second non-permanent cryptographic key are associated with an issuer master key,”

155. Petitioner has not shown that Collinge discloses this limitation. First, Petitioner alleges that KS_{UN} (i.e., the alleged “cryptogram”) is “generated using an

intermediate key (using KD_{UN}) which itself is generated from an issuer master key IMK .” Pet. 62. However, as a POSITA would recognize, Collinge does not specify how KS_{UN} is generated. Petitioner cites to paragraph [0083] of Collinge, but that paragraph says that “[m]ethods and systems for the generation of unpredictable numbers will be apparent to persons having skilled [sic] in the relevant art,” and does not mention an “intermediate key,” “ KD_{UN} ,” or the “issuer master key” that Petitioner says are used to generate KS_{UN} . EX1011, [0083]. These additional keys are not described in Collinge, as Petitioner appears to acknowledge. Pet. 62. Petitioner identifies them only in the Collinge Provisional, but the disclosure there was not carried forward into Collinge. Dr. Fiske acknowledged that he could not identify any disclosure in Collinge showing how Collinge’s session key is derived. Ex. 2035 at 78:18-79:7. He also affirmed that Collinge itself lacks the detail for him to understand how KS_{UN} is derived and that he needed to refer to the Collinge Provisional to understand its derivation. Ex. 2035 at 78:25-79:7; *see also id.* at 103:10-16.

156. Dr. Fiske also opines that claim 16 would have been obvious. Ex. 1006 ¶ 143. I disagree. He says that “using issuer master keys to generate card-specific and transaction specific keys for generating cryptograms was well-known” and cites to Exhibit 1020 for its alleged disclosure of “derivation of Session Key from ICC Master Key generated from issuer master key.” Ex. 1006 ¶143. But, as Dr. Fiske

confirmed, Collinge does not follow the “mechanism [] in EMV” for generating session keys. Ex. 2035 at 77:12-78:17. In addition, as Dr. Fiske also acknowledged, EMV does not mandate any technique for generating session keys. *Id.*, 62:21-25; EX1020, 142 (Appendix A1.3). Dr. Fiske provided no argument as to why a POSITA would choose to generate session keys in Collinge using an issuer master key. Dr. Fiske’s assertion that using an issuer master key to generate a session key was “well-known” is unsupported. A POSITA would have understood that there were many ways to generate Collinge’s session keys, and Dr. Fiske provides no explanation of why a POSITA would have chosen to use an issuer master key instead of a different technique. He also has not shown that a POSITA would have had an expectation of success in doing so. Ex. 1006 ¶ 143.

xxi. Claim 17 F “receive by the application, from the remote computer system, over the wireless network, the first set of data associated with the account,”

157. For this claim limitation the petitioner and Dr. Fiske merely state “see 1.c.”

158. As was stated in reference to 1.C, the KS_{UN} is not generated in response to a request (See III.C.i). Furthermore, the ATC is not account specific. Rather it is a counter for the application. While generating the KS_{UN} does use the KD_{UN} , nothing in the KD_{UN} is account specific according to exhibit 1009. Furthermore, the KS_{UN} is not data associated with the account.

159. For at least the reasons discussed in this section, a POSITA would readily understand that Collinge does not anticipate nor render obvious this claim limitation.

xxii. Claim 17 H-1 “wherein the at least one POS command communication comprises a request for digital credential data, the request for digital credential data including a cryptogram request”

160. For this claim limitation the petitioner and Dr. Fiske only refer to 1.E-1. Claim 1.E-1 states “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;”

161. This was addressed in reference to claim 1.E-1, but that discussion is repeated here.

162. The petitioner and Dr. Fiske state “Because the POS terminal generates an unpredictable number for the mobile device to generate the cryptogram (CVC3), and the mobile device generates CVC3 in response to that communication from the POS terminal as part of a ‘standard payment transaction process,’ a POSA would understand the communication from the POS terminal containing the unpredictable number is a command or request for the mobile device to generate the cryptogram. Ex [1006] ¶ 99; Ex [1009] ¶¶ [0061] (Stage 11-20), [0063].” Pet. at 45.

163. As with previous claim limitations, the petitioner and Dr. Fiske fail to point to any actual request, but instead assume that if action B follows at some time later than action A, then action A must be a request. A POSITA would understand that this is not a request, but rather some action happens later in time, after a number of other steps. I further note that the petitioner and Dr. Fiske rely primarily on Exhibit 1009, the Collinge provisional patent application, specifically relying on language that is not in Collinge, for the “request” claim limitation. The only citations to Collinge relate to the generated CVC3 and say nothing about any request. Accordingly, a POSITA would understand that Collinge does not disclose or suggest limitation 1.E-1.

164. The petitioner and Dr. Fiske point to exhibit 1026 which is the *Contactless Specifications for Payment Systems Book C-2 Kernel 2 Specification*. Exhibit 1026 has the word “request” hundreds of times, but I have not seen any instance involving a mobile device or mobile device application making any request. To the contrary, for example, Exhibit 1026 uses the term request in the following ways:

- a) The terminal sends the online authorization request to the issuer"
(Exhibit 1026 table 2-1).
- b) "Provide data needed for a transaction in progress and indicate to the Reader to continue processing the transaction or request additional data from the Reader" (Exhibit 1026 table 2-3)

- c) "It allows the Kernel to send tagged data to and request data from the Terminal through the DEK Signal." (Exhibit 1026 table 3-1)
- d) "Then the Kernel requests the Card to generate a cryptogram, which is then included in the Data Record." (Exhibit 1026: 3.4.1)
- e) "the Kernel continues with the following steps:....requesting the Card to return a CVC3 cryptogram, calculated over Unpredictable Number (Numeric)." (Exhibit 1026:3.4.2)

165. A POSITA would readily understand that Exhibit 1026 does not disclose any request to or from a mobile device or a mobile device application.

166. The petitioner and Dr. Fiske also point to exhibit 1027 to the petition, which is titled *Contactless Specifications for Payment Systems Book C-3 Kernel 3 Specification*. This exhibit does not mention a mobile device or mobile device application.

167. Nothing in the references cited by the petitioner or Dr. Fiske shows a mobile device, mobile device application, or card requesting *a digital credential data to authorize a transaction against the account* as required by this claim limitation.

168. For at least the reasons discussed in this section, a POSITA would readily understand that Collinge does not anticipate nor render obvious this claim limitation.

xxiii. Claim 17.H-2

169. For this claim limitation, the petitioner and Dr. Fiske simply state “Collinge discloses this limitation as the CVC3 is generated using KS_{UN} stored on the mobile device, as shown in [1.D] and [1.E-2].”

170. Claim 17.H-2 is “access the local cryptographic key associated with the account;”

171. As has been discussed in detail in this declaration, KS_{UN} is not data associated with the account.

172. For at least the reasons discussed in this section, a POSITA would readily understand that Collinge does not anticipate nor render obvious this claim limitation.

xxiv. Claim 17.I subsequent to the interrogation, request from the remote computer system, over the wireless network, a second set of data associated with the account;

173. For this claim limitation, the petitioner and Dr. Fiske merely refer to claim 1.F. In the petition, the petitioner and Dr. Fiske combine 1.F and 1.G. This was discussed in this declaration regarding claim 1.F, but that discussion is repeated here.

174. For this limitation the petitioner and Dr. Fiske state “In other words, the “second set of data” in a given transaction may correspond to the “first set of data” [1.A-3] of a subsequent transaction.” The only basis they provide for this is Dr. Fiske’s declaration which simply repeats the exact phrasing in the petition. There is

no basis for the petitioner nor Dr. Fiske's opinion that the second set of data is just the first set of data of a subsequent transaction.

175. In fact, the claim language belies this opinion "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; 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; 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"

176. A POSITA would readily recognize that this is part of the same transaction. The first set of data is usable by the application to formulate an application protocol data unit response, then subsequent to the interrogation a second set of data is requested.

177. For at least the reasons discussed in this section, a POSITA would readily understand that Collinge does not anticipate nor render obvious this claim limitation.

xxv. Claim 17.J “receive 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 associated with the account comprising a second non-permanent cryptographic key associated with the account; and”

178. For this claim limitation, the petitioner and Dr. Fiske merely refer to claim 1.G.

179. The petitioner and Dr. Fiske’s assertions were addressed in response to claim 1.F-G and 17.I. That discussion is included here by reference.

180. For at least the reasons discussed in this section, a POSITA would readily understand that Collinge does not anticipate nor render obvious this claim limitation.

xxvi. Claim 17.K “store 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.”

181. For this claim limitation the petitioner and Dr. Fiske merely refer to claim 1.H.

182. I incorporate my discussion in reference to claim 1.H here. As was discussed previously KS_{UN} is not associated with the account (See III.C.ii). However, there are additional issues with the petitioners reasoning on this claim limitation. Most notable is that the petitioner and Dr. Fiske already asserted that KS_{UN} is the first cryptographic key. This claim limitation requires a *second cryptographic key*. Even viewing this claim limitation in a light most favorable to the petitioner and Dr. Fiske, KS_{UN} cannot be both the first cryptographic key and a second cryptographic key. The

petitioner and Dr. Fiske simply ignore that this claim limitation is related to a second non-permanent key. Without even addressing that portion of the claim limitation they point to KS_{UN} again, without even asserting that their position is that KS_{UN} is both the first and second non-permanent key.

183. For at least the reasons discussed in this section, a POSITA would readily understand that Collinge does not anticipate nor render obvious this claim limitation.

xxvii. Claim 24 “wherein the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation.”

184. For this claim limitation the petitioner and Dr. Fisk point to claim 1F, 1G, 17I and 17J.

185. I incorporate my discussion in reference to those claim limitations here.

186. As I pointed out in reference to claim 1F, the petitioner and Dr. Fiske assert “the “second set of data” in a given transaction may correspond to the “first set of data” [1.A-3] of a subsequent transaction.” The only basis they provide for this is Dr. Fiske’s declaration which simply repeats the exact phrasing in the petition. There is no basis for the petitioner nor Dr. Fiske’s ipse dixit opinion that the second set of data is just the first set of data of a subsequent transaction.

187. In fact, the claim language belies this opinion “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; 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; 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”

188. A POSITA would readily recognize that this is part of the same transaction. The first set of data is usable by the application to formulate an application protocol data unit response, then subsequent to the interrogation a second set of data is requested.

189. For at least the reasons discussed in this section, a POSITA would readily understand that Collinge does not anticipate nor render obvious this claim limitation.

xxviii. Claim 25 “The system of claim 17, further comprising the remote computer system, the remote computer system configured to generate non permanent cryptographic keys associated with the account and send each of the non-permanent cryptographic keys and the account identifier to the mobile device over the wireless network”

190. For this claim limitation the petitioner and Dr. Fisk point to claim 8.A and 8B.

191. I incorporate my discussion in reference to those claim limitations here.

192. As was discussed previously in this declaration, the petitioner, and Dr. Fiske point to KSUN, which simply is not associated with the account, but rather is associated with a specific session.

193. As was pointed out in reference to claim 8B, the petitioner and Dr. Fiske merely point to claim [1.F]-[1.G]. As I pointed out in that section of my declaration, this claim limitation explicitly involves a second non-permanent key. Without explicitly stating such, it appears that the petitioner and Dr. Fiske are trying to use KSUN as the first non-permanent key and the second non-permanent key.

194. For at least the reasons discussed in this section, a POSITA would readily understand that Collinge does not anticipate nor render obvious this claim limitation.

G. Fiske

195. I first note that the petitioner did not even bother to put the claim language in the petition in reference to Fiske, but rather simply references ‘1.B.’ and similar references.

xxix. General overview of Fiske

196. The abstract of Fiske states “Methods , apparatus and computer software are provided for authorizing an EMV transaction between a user device and a point of sale terminal , particularly, but not exclusively , in situations where a secure element is not made available for the deployment of a payment application on the user

device.” Fiske is directed towards authorizing an EMV payment transaction between a user device and a point-of-sale terminal (1012 9:21-36).

197. The issuing bank generates a session key based on the ICC master key and provisions the payment application with that session key (1012 9:36-41). The ICC master key is a unique key that is associated with the payment application and is used to derive session keys (1012 9:59-63). That ICC Master key remains with the issuing bank (1012 10:1-8).

198. The point-of-sale terminal sends a request for an application cryptogram to the payment application (1012 9:42-46).

199. The payment application generates an application cryptogram based on the session key it received from the issuing bank (1012 9:47-48). The application cryptogram is data encrypted by the payment application using a session key (1012 9:63-67).

200. The payment application then transmits that application cryptogram to the point-of-sale terminal for verification by the issuing bank (1012 9:49-51).

201. Figure 7 of Fiske shows a message flow diagram illustrating an online authorization process according to an embodiment of Fiske (1012 11:27-29):

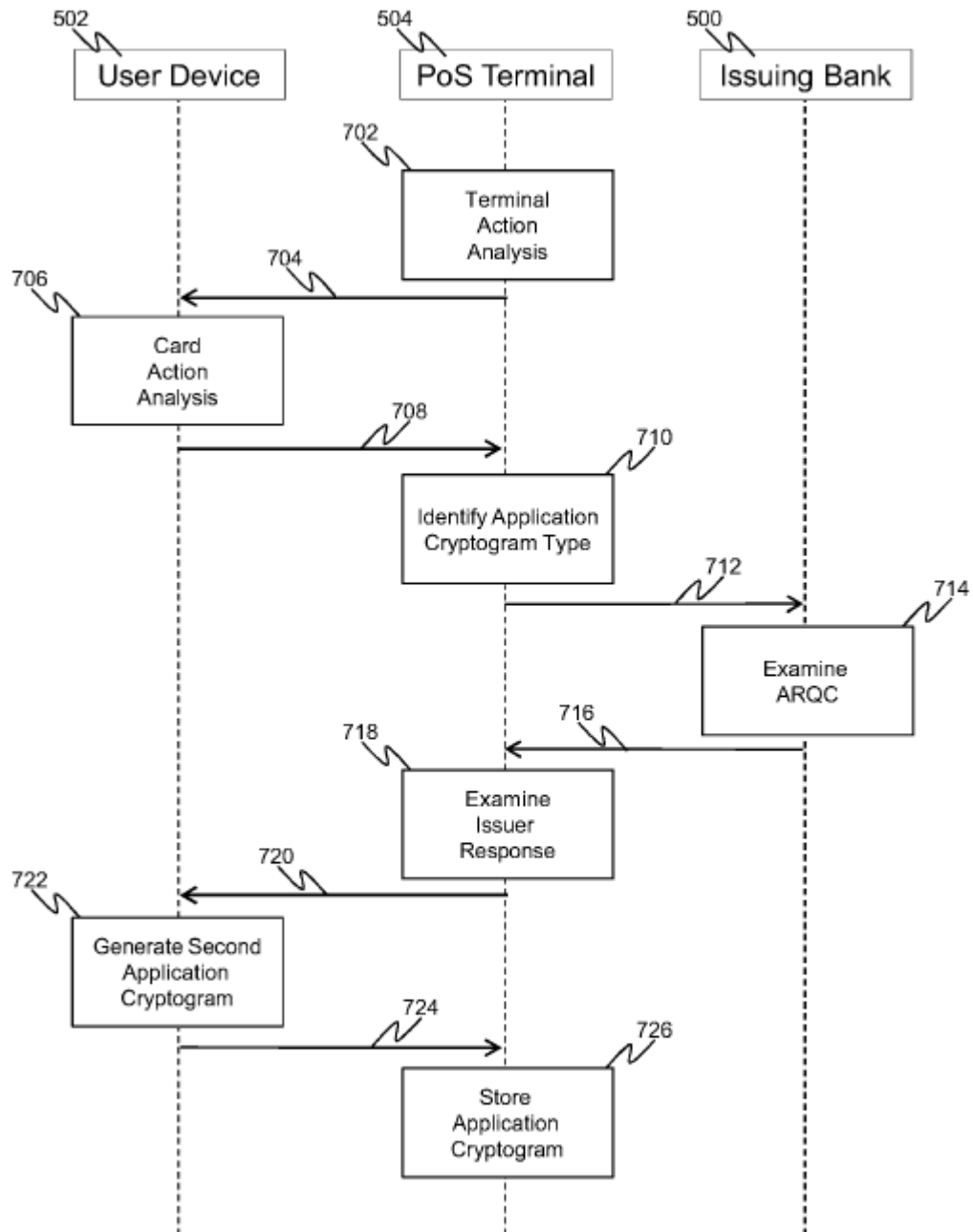


Figure 7

xxx. [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”

202. Petitioner contends that “it is well understood in the art that the Application Cryptogram would not include the ICC Session Key itself because the cryptogram is generated using the Session Key as encryption key.” Pet. 72. (citing EX1006 ¶ 181, EX1034 at 17-18, and “[Rabah]”). Dr. Fiske’s statements in paragraph 181 of his declaration merely parrot verbatim the language of the Petition. I do not agree that it was well understood in the art that Fiske’s Application Cryptogram would not include the ICC Session Key. The references that Dr. Fiske relies on do not show **how** Fiske’s Application Cryptogram is generated. For example, Dr. Fiske appears to contend that Exhibit 1034 is relevant based on its disclosure of “message authentication code (MAC) generation.” Pet. 72; Ex. 1006 ¶181. Yet Dr. Fiske ignores that the techniques for generating a MAC in the EMV Specifications are “not mandatory.” Ex. 1020 at 99. As Dr. Fiske acknowledged during deposition, a POSITA would have been familiar with many different techniques for cryptogram generation, and a payment card could be used for EMV transactions **without** adopting EMV’s disclosed methods of generating an application cryptogram. Fiske Dep. at 61:1-62:1. Accordingly, a POSITA would not understand Fiske’s disclosure

of an Application Cryptogram to disclose or imply any particular technique for generating it or any particular format/structure for the resulting cryptogram.

203. For at least the reasons discussed in this section, a POSITA would readily understand that Fiske does not anticipate nor render obvious this claim limitation.

xxxi. Claim [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;

204. Dr. Fiske states “Fiske also describes the POS terminal issuing a ‘READ RECORD’ command to the payment device to ‘read all of the transaction related data parameters’ from the device, including the primary account number (PAN), and that the mobile device would return an Application Cryptogram in response to a ‘GENERATE AC’ command. Ex[1012], 3:26-46, 2:63-67; 5:28-30, 7:30-41.” Ex. 1006 ¶182.

205. A POSITA would next note that a cryptogram is not even mentioned until 7:30-41 and that section specifically states that “If the terminal decides to approve the transaction offline, the GENERATE AC command requests a Transaction Certificate in step 308”. A cryptogram is only requested if the decision is to authorize the transaction online (in which case an Authorization Request Cryptogram is

requested) or decline the transaction (in which case an Application Authentication Cryptogram is requested). This is important because the other sections that the petitioner and Dr. Fiske cite (3:26-46, 2:63-67; 5:28-30) are part of a section describing offline authentication. In fact, 3:9-22 is a discussion of digitally signing using digital certificates. The section 3:26-46 that the petitioner cites actually states “All of the data necessary for offline data verification...” The section 5:28-30 that the petitioner and Dr. Fiske cite is part of a section explicitly describing the use of digital certificates. A POSITA would recognize that what the petitioner and Dr. Fiske cites is first, not part of the embodiment in Exhibit 1012 that Dr. Fiske relies on, and secondly is not related to cryptograms, but rather to offline authentication that uses a digital certificate rather than a cryptogram. In [1.E], Petitioner contends that command- and response-application data protocol units are well known in the art for “EMV transactions referred to by Fiske.” Pet. 71 (citing EX1037 at 46-48). However, the cited pages of Exhibit 1037 say nothing about EMV specifications. Instead, they purport to describe ICC functionality based on the standard ISO/IEC 7816. EX1037, 46. And, as Dr. Fiske acknowledges, “APDUs are not an EMV concept” and “EMV itself uses the concept from an international standard, ISO 7816.” EX2035 at 90:11-24. ISO 7816 is mentioned in the Fiske reference, but this is with respect to “**contact** ICCs [that] are powered by the PoS terminal.” EX1012, 1:45-51 (emphasis added). A POSITA would readily recognize that Fiske’s “user

device” is different from a **contact** ICC powered by the POS terminal. *See, e.g.,* EX1012 at Figure 5 (depicting “use device” 502). Petitioner provides no evidence or argument as to why a POSITA would choose—among the many available options within EMV—to implement Fiske for an “EMV mode Visa” transaction. As Dr. Fiske acknowledged, a contactless transaction could be compatible with EMV specifications **without** implementing “EMV mode” transactions. EX2035 at 59:18-25. The EMV specifications provide a general framework for an issuer’s card to interact with a POS terminal and for the POS terminal to interact with the issuer’s systems. The EMV specifications leave many implementation decisions (e.g., cryptogram generation algorithms, session key generation algorithms, EMV/magstripe mode) in the hands of the issuers. Ex. 2035 at 60:12-62:1 (“As far as EMV is concerned, all it is doing is providing a globally interoperable mechanism whereby that issuer’s card can interact with any EMV terminal and information can get through to the issuer.”).

206. Petitioner’s reliance on purported commands and responses in an “EMV mode contactless Visa transaction” ignores that those commands are inconsistent with the commands and responses disclosed in Fiske that he relies upon. In particular, Petitioner says that the mobile device responds to the “GENERATE AC” command disclosed in Fiske by returning an Application Cryptogram. Pet. 73 (citing Ex. 1012 at 3:26-46, 2:63-67, 5:28-30, 7:30-41). But the EMV specification on which

Petitioner relies to satisfy its second construction expressly states “there is no GENERATE AC command.” Ex. 1027 at 84 (Section 6.1). For at least the reasons discussed in this section, a POSITA would readily understand that Fiske does not anticipate nor render obvious this claim limitation.

- xxxii. Claims 4, 5, 20, 21: “The method of claim 1, 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.” “The method of claim 4, wherein the request for digital credential data comprises a request for a first cryptogram according to the card specification and the at least one device response communication comprises a second cryptogram, wherein the second cryptogram is the response cryptogram.**

207. I understand that the Board recognized in its Institution Decision that Fiske does not incorporate by reference the EMV Specifications (i.e., any of Exhibits 1019-1029). Dr. Fiske’s arguments as to claim 4 (and 20) and claim 5 (and 21) are premised on an assertion that the EMV Specifications are incorporated by reference in Exhibit 1012. Pet. 76-77. Accordingly, I disagree that Dr. Fiske has shown that any of claims 4 (or 20) or claim 5 (or 21) are anticipated by Exhibit 1012, because the disclosures in the EMV specifications are not part of Fiske.

208. As to obviousness, Dr. Fiske provides only his conclusion that these claims would have been obvious. Ex. 1006 ¶¶195-196. He does not explain why a POSITA would have found these claims obvious and does not cite to any evidence supporting

his conclusion. *Id.* I do not agree that he has shown that these claims would be obvious.

209. The petitioner and Dr. Fiske ignore the state of payment systems at the time of Exhibit 1012. Exhibit 1012 was filed October 4, 2013. Bankrate.com states “Major credit card issuers asked that most U.S. businesses that accept credit cards move toward an EMV-compliant credit card point of sale (POS) system by Oct. 1, 2015 (for fuel retailers, the EMV liability deadline was April 2021).”²⁸ This is moving towards EMV compliance by 2015 and a deadline of 2021. Even at that time, a company need not implement all of the EMV standard, but rather a minimal subset²⁹.

210. It was not until October 2015 the liability for in store fraud shifted to the party that was not EMV compliant^{30,31}. In fact, as late as 2015 many sources were complaining that the US was lagging in EMV adoption ““We are way behind the rest of the world,” says Deborah Baxley, principal for Capgemini Financial Services. “We need to set a date.””³²

²⁸ Ex. 2012 (<https://www.bankrate.com/credit-cards/business/what-is-emv-compliance-law-should-your-business-worry/>)

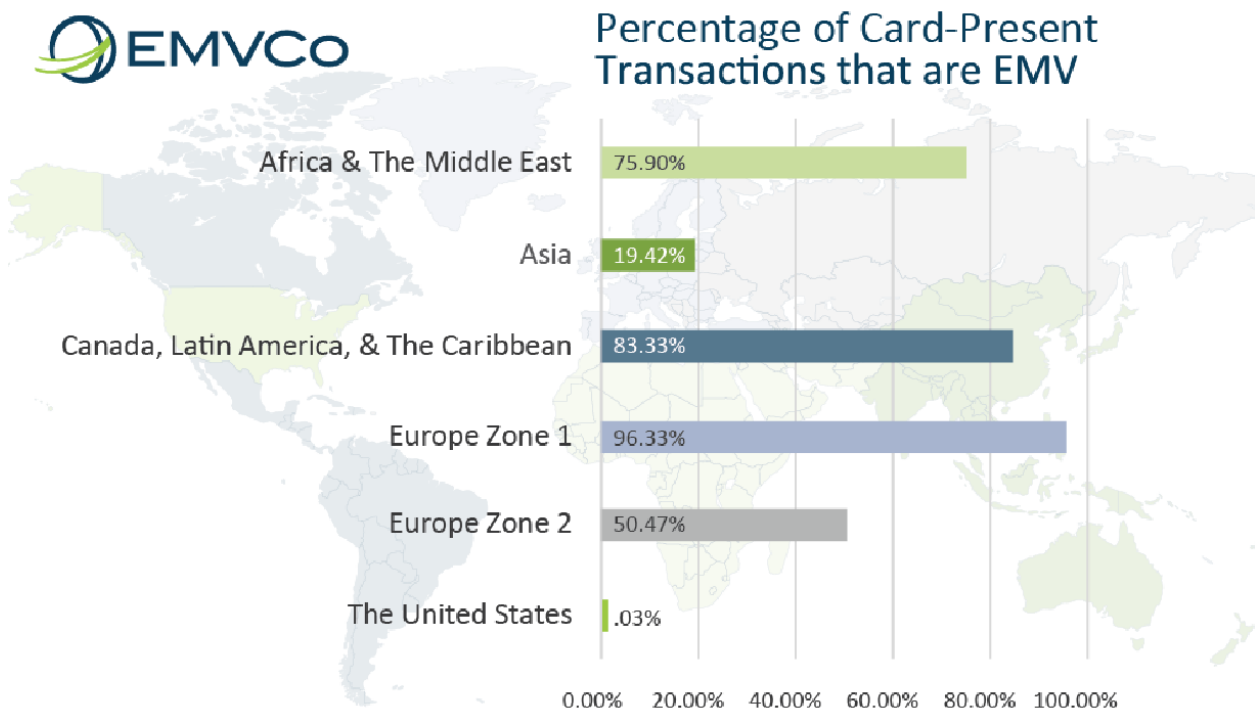
²⁹ Ex. 2013 (<https://www.uspaymentsforum.org/minimum-emv-chip-card-and-terminal-requirements-u-s/>)

³⁰ Ex. 2014 (<https://www.carat.fiserv.com/en-us/resources/emv-chip-card-technology/>)

³¹ Ex. 2032 (<https://www.globalpaymentsintegrated.com/en-us/blog/2019/03/06/the-next-big-thing-in-payment-processing-emv-contactless>)

³² Ex. 2033 (<https://www.scmagazine.com/feature/the-long-and-winding-road-emv-adoption>)

211. The following chart shows EMV adoption in 2014³³:



212. As of 2019, the shift to all EMV compliant cards was still not complete³⁴. Discover did not adopt EMV standards until September 2013³⁵. At the time exhibit 1012 was filed, much of the United States was not EMV compliant, and even compliance does not mean implementing every single aspect of the EMV standard. A POSITA would understand that a general reference to EMV in exhibit 1012, does not disclose any specific aspect of the EMV standard.

³³ Ex. 2015 (https://www.fisglobal.com/-/media/fisglobal/WorldPay/Docs/Insights/A-Guide-to-EMV-Chip-Technology.pdf?sc_lang=en)

³⁴ Ex. 2034 (<https://www.thalesgroup.com/en/americas/united-states/digital-identity-and-security/emv/>)

³⁵ Ex. 2035 (<https://investorrelations.discover.com/newsroom/press-releases/press-release-details/2013/Emvco-Membership-Grows-With-Discover/>)

213. For at least the reasons discussed in this section, a POSITA would readily understand that Fiske does not anticipate nor render obvious this claim limitation.

xxxiii. **Claims 6 and 22: “The method of claim 1, 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”**

214. Exhibit 1012 makes no mention of the algorithm used to generate the Application Cryptogram. Indeed, it expressly states that “[h]ow the Session Key is used to generate the application cryptogram is specific to the payment system being implemented.” A POSITA would readily recognize that techniques for generating a MAC in the EMV specifications are “not mandatory.” EX2035 at 61:21-62:1; EX1020 at 99. Dr. Fiske’s contention that “the AC in an EMV transaction **is generated** using a 3DES algorithm,” Ex. 1006 ¶198 (emphasis added), is simply incorrect. As Dr. Fiske acknowledged, a POSITA would have been familiar with many different techniques for cryptogram generation, and a payment card could be used for EMV transactions **without** adopting EMV’s disclosed methods of generating an application cryptogram. Ex. 2035 at 29:20-30:19. Dr. Fiske provides no explanation as to why a POSITA would have chosen any particular method for encryption, such as DES, over any of the many known and available options. For example, a POSITA would have been familiar with algorithms that could be used to

generate a cryptogram, including AES, IDEA, MARS, HMAC, FIPS, AMAC, PMAC, and many others.

xxxiv. **Claim 8.A: “*The method of claim 1, further comprising, at the remote computer system: 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; and*”**

215. Dr. Fiske presents no independent analysis of limitation 8.A. Instead, he cites to his earlier discussion of limitations 1.B and 1.C. Ex. 1012 ¶ 201. I note that each of limitations 1.B and 1.C recites steps performed “by the application,” not “at the remote computer system” as recited in claim 8. Dr. Fiske’s analysis of limitations 1.B and 1.C (paragraphs 173-175) does not make any mention of an “account identifier.” Indeed, Dr. Fiske’s only discussion in these paragraphs of any information received by the user device references only “single-use payment keys, specifically, an ICC Session Key.” Ex. 1012 ¶¶173-175. For example, as to limitation 1.B, which recites “a first set of data associated with the account,” Dr. Fiske says “data associated with the account includes the single- use payment keys such as the ICC Session Key” but makes no mention of an account identifier. Ex. 1006 ¶173. In addition, as to limitation 1.C, which recites “receiving ... the first set of data associated with the account,” Dr. Fiske again identifies only the “ICC Session Key” and makes no mention of an “account identifier.” Ex. 1006 ¶174-175. Accordingly,

Dr. Fiske has not shown that the step of “at the remote computer ... sending the first non-permanent cryptographic key and the account identifier to the mobile device” is disclosed or rendered obvious by Fiske.

216. For at least the reasons discussed in this section, a POSITA would readily understand that Fiske does not anticipate nor render obvious this claim limitation.

xxxv. Claims 10 and 27 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;”

217. I note that Petitioner’s discussion of this limitation does not cite to Dr. Fiske’s declaration. Pet. 78-79. I disagree that the arguments presented in the Petition have shown that this limitation was anticipated or obvious. The petitioner refers to Ex[1012], 16:6-10, which states “In response to receiving the Application Cryptogram, the terminal identifies the type of Application Cryptogram sent by the user device in step 710 and forwards the ARQC to the issuer in step 712 for authorization of the transaction.” This disclosure says nothing about the PAN (the alleged *account identifier*) being part of any authorization request, and a POSITA would not understand this statement as disclosing or implying an “account identifier.” In addition to the quoted disclosure from Exhibit 1012, Petitioner also cites, without explanation, 7:30-60 and Figure 7 of Exhibit 1012, but these disclosures also say nothing about an authorization request that includes the PAN.

See EX1012, 7:30-60, Fig. 7. Even if a POSITA looked to the EMV Specifications to understand Fiske's ARQC—which Petitioner has not alleged a POSITA would do—he/she would find that the ARQC described in the EMV Specifications does not include the PAN. Ex. 1028 section 11.2 page 87 (“The ARQC when sent in an online authorisation request message allows the Issuer to authenticate that they actually issued the card. Each card contains a unique DES key that is used to generate the cryptogram. This key, which is known only by the card Issuer, is then used in their host systems to validate the AC received in the Authorisation Request Message.”) Accordingly, I do not agree that the petitioner has shown that this limitation is disclosed or obvious in light of Exhibit 1012. I do not see that Petitioner has even alleged that this limitation would have been obvious.

xxxvi. Claim 10 B. determining a current non-permanent cryptographic key associated with the account using the account identifier;

218. I note that Petitioner's discussion of this limitation does not cite to Dr. Fiske's declaration. Pet. 78-79. I disagree that the arguments presented in the Petition have shown that this limitation was anticipated or obvious.

219. For this claim limitation, the petitioner merely states “Fiske discloses that “[t]he issuer may identify which Session Key was used to generate the ARQC.” Pet. 79. Petitioner's analysis of this limitation ignores the recited “account identifier” used to “determin[e] a current non-permanent cryptographic key.” Petitioner makes no allegation that the alleged “account identifier” (i.e., the PAN) is used to determine

“a current non-permanent cryptographic key” (i.e., the ICC Session Key). Its single-sentence assertion as to this limitation mentions only a Session Key (i.e., the alleged “non-permanent cryptographic key”) and the ARQC (i.e., the alleged “cryptogram”). Pet. 79 (citing Ex. 1012, 17:13-14, Fig. 7). Nothing in this assertion ties the PAN (i.e., the alleged “account identifier”) to any step at the remote computer system of determining the Session Key (i.e., the alleged “non-permanent cryptographic key”). Petitioner’s citations to Ex. 1012 are also insufficient. The disclosure at 17:13-14 appears in the middle of a sentence relating to limiting the number of ICC Session Keys that may be generated, and Figure 7 shows only one step performed by the issuing bank, which is “Examine ARQC” as part of step 714. EX1012, 17:13-14, Fig. 7. A POSITA would not understand any of these disclosures as showing or implying that the PAN is used to determine a current non-permanent cryptographic key associated with the account.

220. For at least the reasons discussed in this section, a POSITA would readily understand that Fiske does not anticipate nor render obvious this claim limitation.

xxxvii. Claim 10.C calculating a calculated cryptogram using the current nonpermanent cryptographic key associated with the account;

221. I note that Petitioner’s discussion of this limitation does not cite to Dr. Fiske’s declaration. Pet. 78-79. Because Dr. Fiske’s declaration was not cited, I have not considered any analysis by him of these limitations. I disagree that the arguments presented in the Petition have shown that this limitation was anticipated or obvious.

222. Petitioner's argument for this limitation appears to contend that the ARQC (i.e., the alleged "cryptogram") **could** be calculated using the Session Key (i.e., the alleged "cryptographic key"). Pet. 79. Petitioner's assertion as to how the ARQC **could** be calculated does not show that this limitation is disclosed by Exhibit 1012. In addition, I see no analysis in the Petition as to why a POSITA **would** have calculated the ARQC using the Session Key or why a POSITA would have expected such a calculation to be a successful way to implement the payment system of Exhibit 1012.

223. For at least the reasons discussed in this section, a POSITA would readily understand that Fiske does not anticipate nor render obvious this claim limitation.

xxxviii. Claims 11 and 28, 12 and 29

224. It is first noteworthy that these claims are not identical, though the petitioner and Dr. Fiske attempt to address them en masse.

225. Claim 11 "The method of claim 10, wherein: the set of inputs comprises unpredictable data; the authorization data comprises the unpredictable data; and the calculated cryptogram is calculated using the unpredictable data"

226. Claim 12 "The method of claim 11, wherein the POS command communications comprise the unpredictable data."

227. Claim 28 “The system of claim 27, wherein: the set of inputs comprises unpredictable data; the authorization data comprises the unpredictable data; and the calculated cryptogram is calculated using the unpredictable data”

228. Claim 29 “The system of claim 28, wherein the POS command communications comprise the unpredictable data.”

229. The petitioner and Dr. Fiske begin by stating “The set of inputs, authorization data, and calculated cryptogram would comprise unpredictable data, because Fiske explicitly incorporates by reference EMV Specifications, which explicitly require that input data for generation of the response cryptogram include an “Unpredictable Number,” which is supplied by “[POS]Terminal.” Ex[1020] § 8.1.1.”

230. I am informed that the PTAB has already determined that the EMV Specifications are not incorporated by reference in Fiske/Exhibit 1012.

231. Dr. Fiske opines that EMV Specifications “**explicitly require** that input data for generation of the response cryptogram include an ‘Unpredictable Number,’ which is supplied by ‘[POS] Terminal.’” Ex[1006] ¶ 210 (emphasis added). I disagree. As Dr. Fiske acknowledged during deposition, the EMV Specifications do not mandate a particular technique for generating a cryptogram, and a POSITA would have recognized that a payment card could be used in compliance with the EMV Specifications without adopting any cryptogram generation method disclosed in the EMV Specifications. Ex. 2035 at 60:1-61:1. Thus, even if Dr. Fiske had shown

that a POSITA would have been motivated to implement Fiske in a manner compatible with the EMV Specifications, this still does not demonstrate that a POSITA would have chosen to calculate the cryptogram *using the unpredictable data*, since this step is not needed for EMV compatibility.

232. Dr. Fiske does not include any independent analysis of claim 12. Instead, he simply says “[f]or similar reasons to Claims 11 and 28, Fiske discloses this limitation.” Ex[1006] ¶ 213. Dr. Fiske does not explain what these “similar reasons” are or how they might be different from the reasons given in his analysis of claims 11 and 28. In addition, his analysis of those claims makes no mention of “the POS command communications” recited in claim 12. Ex[1006] ¶ 210-212. Dr. Fiske’s only contention as to an “unpredictable number” states that it would be included in “the authorization request,” Ex[1006] ¶ 211, which does not demonstrate that “the POS command communications comprise the unpredictable data.” Claim 11 recites “at the **remote computer system** ... receiving an authorization request to authorize the transaction **from the POS terminal**,” but the claimed POS command communications are recited in claim 1 as being received **by the mobile device** from the POS terminal. Dr. Fiske does not explain how his identification of communications between the alleged remote computer system and the POS terminal are relevant to communications between the mobile device and the POS terminal.

Accordingly, I disagree that he has shown that Fiske discloses or renders obvious any such communication.

233. For at least the reasons discussed in this section, a POSITA would readily understand that Fiske does not anticipate nor render obvious this claim limitation.

xxxix. Claims 13 and 30 “The method of claim 12, wherein the authorization data further comprises values from the transaction.”

234. Dr. Fiske does not point to anything in exhibit 1012 that actually discloses this claim limitation. Instead, he contends only that data objects necessary to reproduce the transaction claim “**usually** include information such as amount and currency code,” Ex[1006] ¶ 214, but does not explain the circumstances in which this information would be included or why a POSITA would have chosen to include this data as part of “the authorization data.” A POSITA would have recognized that, if such data were included at all, it could be included in a number of different ways as part of different messages. And Dr. Fiske’s contention that a POSITA would have “otherwise found this obvious because it is well established practice in the art” is stated with no explanation or substantive evidence. I disagree that it is well established in the art for an authorization request to comprise “the response cryptogram and the account identifier” (as recited in limitation 10.A) as well as “values from the transaction.” A POSITA would have recognized that validation of a cryptogram (e.g., using the response cryptogram) would not require any “values from the transaction” and that if “values from the transaction” were needed for a

different purpose, e.g., to determine if a payment amount is within acceptable limits, that information need not be included as part of an “authorization request” with the “response cryptogram and the account identifier,” as claimed. In fact, using the amount of the transaction, date, or time, may be the same for many different and unrelated transactions, which makes their use less effective.

235. For at least the reasons discussed in this section, a POSITA would readily understand that Fiske does not anticipate nor render obvious this claim limitation.

xl. Claims 15 and 32 “The method of claim 1, wherein the application is configured to generate the response cryptogram according to a card specification.”

236. Dr. Fiske does not include any independent analysis of claims 15 and 32. Instead, he simply says “[f]or similar reasons as stated for Claims 4 and 20, Fiske discloses this limitation.” Ex[1006] ¶ 217. Dr. Fiske does not explain what these “similar reasons” are or how they might be different from the reasons given in his analysis of claims 4 and 20. I disagree that Dr. Fiske has shown that Fiske discloses the limitations of claims 15 and 32. His analysis of claims 4 and 20 does not establish, or even attempt to establish, that “generat[ion] of the response cryptogram [is] according to a card specification.” Ex[1006] ¶ 195-196. He alleges that EMV Specifications “describe the inputs and responses by the card to be compatible with EMV transactions” and that it would have been “obvious to make the device inputs

and responses conforming to ... EMV Specifications.” *Id.* But nothing in this contention shows that conforming to, or being compatible with, EMV Specifications involves “generat[ing] the response cryptogram according to” EMV Specifications. As Dr. Fiske admitted, and as a POSITA would recognize, 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. Ex. 2035 at 61:21-62:1; Ex. 2035 at 29:20-30:19.

xli. Claim 17

237. Dr. Fiske relies extensively on his analysis of claim 1 for his opinions as to claim 17. For all the reasons previously stated as to claim 1, I disagree that Fiske discloses or renders obvious claim 17.

xlii. Claim 24 “The system of claim 17, wherein the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation.”

238. Dr. Fiske relies entirely on his analysis of claims 1 and 17 for his opinions as to claim 24. For all the reasons previously stated as to claim 1 and 17, I disagree that Fiske discloses or renders obvious claim 24.

- xliii. **Claim 25 “The system of claim 17, further comprising the remote computer system, the remote computer system configured to generate non-permanent cryptographic keys associated with the account and send each of the non-permanent cryptographic keys and the account identifier to the mobile device over the wireless network.”**

239. Dr. Fiske relies entirely on his analysis of claim 8 for his opinions as to claim 25. For all the reasons previously stated as to claim 8 (and claim 1 from which claim 8 depends), I disagree that Fiske discloses or renders obvious claim 25.

V. Conclusions

240. The petitioner and Dr. Fiske have failed to even address several claim limitations. Furthermore, as has been shown in this declaration, the asserted references (e.g., Exhibit 1009, 1011, and 1012) do not anticipate or render obvious any of the independent claims of the ‘171 patent.

241. Furthermore, as has been demonstrated in this declaration, the dependent claims are also not anticipated nor rendered obvious by the asserted prior art.



Dr. Chuck Easttom

28 June 2024
Date