

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: C. Douglas Yeager
U.S. Patent No.: 8,151,345
Issue Date: April 3, 2012
Appl. Serial No.: 12/019,318
Filing Date: January 24, 2008
Title: SELF-AUTHORIZING DEVICES

Mail Stop Patent Board

Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR *INTER PARTES* REVIEW
OF UNITED STATES PATENT NO. 8,151,345
PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	REQUIREMENTS FOR IPR	1
	A. Grounds for Standing.....	1
	B. Challenge and Relief Requested.....	1
	C. Claim Construction.....	2
	D. Level of Ordinary Skill in the Art.....	3
III.	THE '345 PATENT	3
	A. Brief Description.....	3
	B. Prosecution History.....	4
IV.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	7
	A. GROUND 1A—Huomo-Kisliakov-Linehan Renders Obvious Claim 23 .	7
	1. Uomo	8
	2. Kisliakov	10
	3. Linehan.....	10
	4. Uomo-Kisliakov Combination	11
	a) Uomo and Kisliakov are Analogous Art to the '345 Patent	11
	b) A POSITA would have been Motivated to Combine Uomo and Kisliakov	12
	c) A POSITA would have Reasonably Expected Success when Combining Uomo and Kisliakov	16
	5. Uomo-Kisliakov-Linehan Combination.....	17
	a) Linehan is Analogous Art to the '345 Patent.....	17
	b) A POSITA would have been Motivated to Combine Uomo- Kisliakov-Linehan.....	17
	c) A POSITA would have Reasonably Expected Success when Combining Uomo-Kisliakov-Linehan	20
	6. Analysis	21
	B. GROUND 1B—Huomo-Kisliakov-Linehan-Peart Renders Obvious Claims 24-25	37
	1. Peart.....	37
	2. Uomo-Kisliakov-Linehan-Peart Combination.....	38
	a) Peart is Analogous Art to the '345 Patent.....	38

b)	A POSITA would have been Motivated to Combine Huomo-Kisliakov-Linehan-Peart	39
c)	A POSITA would have Reasonably Expected Success when Combining Huomo-Kisliakov-Linehan-Peart	41
3.	Analysis	41
C.	GROUND 2—Ryan-Kisliakov-Peart Renders Obvious Claims 23-25 ..	43
1.	Ryan.....	43
2.	Ryan-Kisliakov Combination.....	44
a)	Ryan is Analogous Art to the '345 Patent.....	44
b)	A POSITA would have been Motivated to Combine Ryan and Kisliakov	44
c)	A POSITA would have Reasonably Expected Success when Combining Ryan and Kisliakov.....	46
3.	Ryan-Kisliakov-Peart Combination	47
a)	A POSITA would have been Motivated to Combine Ryan-Kisliakov-Peart	47
b)	A POSITA would have Reasonably Expected Success when Combining Ryan-Kisliakov-Peart.....	48
4.	Analysis	48
D.	GROUND 3A – Ryan-Hulbert Renders Obvious Claims 11-12.....	66
1.	Hulbert.....	66
2.	Ryan-Hulbert Combination	68
a)	Hulbert is Analogous Art to the '345 Patent.....	68
b)	A POSITA would have been Motivated to Combine Ryan-Hulbert	69
c)	A POSITA would have Reasonably Expected Success when Combining Ryan-Hulbert.....	71
3.	Analysis	71
E.	GROUND 3B – Ryan-Hulbert-Peart Renders Obvious Claims 13-22 ..	79
1.	Ryan-Hulbert-Peart Combination	79
2.	Analysis	79
F.	GROUND 3C – Ryan-Hulbert-Peart-Kisliakov Renders Obvious Claims 1-10 ..	82
1.	Ryan-Hulbert-Peart-Kisliakov Combination	82
2.	Analysis	82
V.	CONCLUSION AND FEES	85

VI.	MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1).....	85
A.	Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1).....	85
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2).....	86
C.	Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3).....	86
D.	Service Information	86

LIST OF EXHIBITS

EX1001	U.S. Patent No. 8,151,345 to Yeager (“the ’345 Patent”)
EX1002	Excerpts from the Prosecution History of the ‘345 Patent (“the Prosecution History”)
EX1003	Declaration and Curriculum Vitae of Dr. Patrick Traynor
EX1004	U.S. Patent No. 8,538,332 to Huomo et al. (“Huomo”)
EX1005	RESERVED
EX1006	U.S. Patent No. 7,213,766 to Ryan et al. (“Ryan”)
EX1007	U.S. Patent No. 7,103,575 to Linehan (“Linehan”)
EX1008	U.S. Patent No. 8,001,054 to Peart et al. (“Peart”)
EX1009	International Pub. No. WO2001096990A2 to Abbott et al. (“Abbott”)
EX1010	U.S. Patent Appl. Pub. No. US2003/0212896A1 to Kisliakov (“Kisliakov”)
EX1011	U.S. Patent Appl. Pub. No. 2009/0187687 to Hulbert et al. (“Hulbert”)
EX1012	ISO/IEC 7816-4 Second edition (2005). Available at https://www.freecalypso.org/pub/GSM/ISO7816/ISO_7816-4_2005.pdf
EX1013-1029	RESERVED
EX1030	Complaint for Patent Infringement, <i>Mobility IP Holdings, Inc. v. Apple Inc.</i> , No. 7:26-cv-00075 (W.D. Tex. Mar. 4, 2026)

- EX1031 Complaint for Patent Infringement, *Mobility IP Holdings, Inc. v. Samsung Electronics Co, Ltd. and Samsung Electronics America, Inc.*, No. 2:26-cv-157 (E.D. Tex. Feb. 27, 2026)
- EX1032 Stipulation by Apple
- EX1033 Stipulation by Samsung
- EX1034 Combined Civil and Criminal Federal Court Management Statistics (Jun. 30, 2026) | United States Courts, available at: https://www.uscourts.gov/sites/default/files/document/fcms_na_distprofile0630.2026.pdf

LISTING OF CHALLENGED CLAIMS

Claim 1	
[1pre]	A token comprising:
[1.1]	a mounting structure having a communication connector configured to connect to a computer terminal;
[1.2]	a secure element affixed to the mounting structure, the secure element comprising a data file,
[1.3]	a secure element reader affixed to the mounting structure and configured to interrogate the secure element by executing file system functions comprising a command to select a payment card application according to ISO 7816-4 and to generate file information from the secure element data file; and
[1.4]	a communications controller affixed to the mounting structure and configured to receive the file information from the secure element reader and to convert at least a portion of the file information into transaction information and to transmit the transaction information to the computer terminal through the communications connector, wherein the communication connector is a Universal Serial Bus (USB) connector and the communications controller is configured as a Human Interface Device (HID) class USB-device and the communications controller is configured to provide the transaction information in a format that auto-populates a form field defined by an application running on the computer terminal.
Claim 2	
[2]	The token of claim 1 wherein the communications controller is configured to provide the transaction information in a prescribed cadence for an application running on the computer terminal.
Claim 3	
[3]	The token of claim 1 wherein the secure element data file comprises financial authorization data and the communications controller is configured to extract at least a portion of the financial authorization data and is configured to encrypt the at least a portion of the financial data and to transmit the encrypted financial authorization data for transmission as transaction information to the computer terminal through the communications connector.

Claim 4	
[4]	The token of claim 1 wherein: the secure element data file comprises financial authorization data and the controller is configured to extract at least a portion of the financial authorization data and is configured to encrypt the at least a portion of the financial data and to transmit the encrypted financial authorization data for transmission as transaction information to the computer terminal using the USB connector.
Claim 5	
[5]	The token of claim 4 wherein: the communications controller is configured to provide the transaction information in a prescribed cadence for the application running on the computer terminal.
Claim 6	
[6]	The token of claim 1 wherein the transaction information comprises an encrypted unpredictable number constructed as a hash of a timestamp.
Claim 7	
[7]	The token of claim 1 wherein the transaction information comprises an encryption constructed from a timestamp and a transaction counter.
Claim 8	
[8]	The token of claim 1 wherein the secure element reader is configured to await a startup instruction comprising an unpredictable number originating from the computer terminal prior to interrogating the secure element.
Claim 9	
[9pre]	A token comprising:
[9.1]	a mounting structure having a communication connector configured to connect to a computer terminal;
[9.2]	a secure element affixed to the mounting structure, the secure element comprising a data file,
[9.3]	a secure element reader affixed to the mounting structure and configured to interrogate the secure element by executing file system

	functions comprising a command to select a payment card application according to ISO 7816-4 and to generate file information from the secure element data file; and
[9.4]	a communications controller affixed to the mounting structure and configured to receive the file information from the secure element reader and to convert at least a portion of the file information into transaction information and to transmit the transaction information to the computer terminal through the communications connector; wherein
[9.5]	the secure element data file comprises financial authorization data and the communications controller is configured to extract at least a portion of the financial authorization data and is configured to encrypt the at least a portion of the financial data and to transmit the encrypted financial authorization data for transmission as transaction information to the computer terminal through the communications connector, and wherein
[9.6]	the communications controller is configured to provide the transaction information in a format that auto-populates a form field defined by an application running on the computer terminal.
Claim 10	
[10]	The token of claim 9 wherein the communications controller is configured to provide the transaction information in a prescribed cadence for an application running on the computer terminal.
Claim 11	
[11pre]	A token comprising:
[11.1]	a mounting structure having a Universal Serial Bus (USB) connector configured to connect to a computer terminal;
[11.2]	a secure element affixed to the mounting structure, the secure element comprising a data file,
[11.3]	a communications controller affixed to the mounting structure and configured as a Human Interface Device (HID) class USB-device and configured to extract information from the secure element data file and to convert at least a portion of the data file into transaction information and to transmit the transaction information to the computer terminal through the USB connector as keyboard emulation and wherein the communications controller is configured to provide the transaction information in a format that auto-populates

	a form field defined by an application running on the computer terminal.
Claim 12	
[12]	The token of claim 11 wherein the communications controller is configured to provide the transaction information in a prescribed cadence for an application running on the computer terminal.
Claim 13	
[13]	The token of claim 11 wherein the secure element data file comprises financial authorization data and the communications controller is configured to extract at least a portion of the financial authorization data and is configured to encrypt the at least a portion of the financial data and to transmit the encrypted financial authorization data for transmission as transaction information to the computer terminal through the USB connector.
Claim 14	
[14]	The token of claim 11 wherein the transaction information comprises an encrypted unpredictable number constructed as a hash of a timestamp.
Claim 15	
[15]	The token of claim 11 wherein the transaction information comprises an encryption constructed from a timestamp and a transaction counter.
Claim 16	
[16]	The token of claim 11 wherein the secure element reader is configured to await a startup instruction comprising an unpredictable number originating from the computer terminal prior to interrogating the secure element.
Claim 17	
[17pre]	A token comprising:
[17.1]	a mounting structure having a Universal Serial Bus (USB) connector configured to connect to a computer terminal;
[17.2]	a secure element affixed to the mounting structure, the secure element comprising a data file; and

[17.3]	a communications controller affixed to the mounting structure and configured as a Human Interface Device (HID) class USB-device and configured to extract information from the secure element data file and to convert at least a portion of the data file into transaction information and to transmit the transaction information to the computer terminal through the USB connector as keyboard emulation; wherein
[17.4]	the secure element data file comprises financial authorization data and the communications controller is configured to extract at least a portion of the financial authorization data and is configured to encrypt the at least a portion of the financial data and to transmit the encrypted financial authorization data for transmission as transaction information to the computer terminal through the USB connector; and wherein
[17.5]	the communications controller is configured to provide the transaction information in a format that auto-populates a form field defined by an application running on the computer terminal.
Claim 18	
[18]	The token of claim 17 wherein the communications controller is configured to provide the transaction information in a prescribed cadence for an application running on the computer terminal.
Claim 19	
[19pre]	A token comprising:
[19.1]	a mounting structure having a communication connector configured to connect to a computer terminal;
[19.2]	a secure element affixed to the mounting structure, the secure element comprising a data file comprising financial authorization data,
[19.3]	a communications controller affixed to the mounting structure and configured to extract at least a portion of the financial authorization data from the secure element data file and configured to encrypt the at least a portion of the financial data and to transmit the encrypted financial authorization data as transaction information comprising an encrypted unpredictable number constructed as a hash of a timestamp to the computer terminal using the communication connector, wherein the communications controller is configured to provide the transaction information in a format that auto-populates a

	form field defined by an application running on the computer terminal.
Claim 20	
[20]	The token of claim 19 wherein the communications controller is configured to provide the transaction information in a prescribed cadence for an application running on the computer terminal.
Claim 21	
[21]	The token of claim 19 wherein the transaction information comprises an encryption constructed from the hash of the timestamp and a transaction counter.
Claim 22	
[22]	The token of claim 19 wherein the secure element reader is configured to await a startup instruction comprising an unpredictable number originating from the computer terminal prior to interrogating the secure element.
Claim 23	
[23pre]	A cellular network adapter for a cellular network device configured with a cellular network application interface comprising;
[23.1]	a secure element comprising a data file;
[23.2]	a secure element reader in the cellular network adapter configured to interrogate the secure element by executing file system functions according to ISO 7816-4 and to generate file information from the secure element data file;
[23.3]	a near field communications controller bridge chip to convert the file information to an RF data signal for an external reader; and
[23.4]	a communications controller configured to receive the file information from the secure element reader and to convert at least a portion of the file information into transaction authorization information and to transmit the transaction authorization information from the cellular network device over a wireless network through the cellular network application interface, wherein the wireless network comprises a cellular network and
[23.5]	the secure element reader in the cellular network adapter is configured to await a startup instruction comprising an unpredictable number originating over the cellular wireless network prior to interrogating the secure element.

Claim 24	
[24]	The cellular network adapter of claim 23 wherein the transaction authorization information comprises an encrypted unpredictable number constructed as a hash of a timestamp.
Claim 25	
[25]	The cellular network adapter of claim 23 wherein the transaction authorization information comprises an encryption constructed from a timestamp and a transaction counter.

I. INTRODUCTION

Apple Inc. (“Apple”) and Samsung Electronics Co., Ltd. (“Samsung”) (collectively, “Petitioners”) petition for IPR of claims 1-25 (“Challenged Claims”) of U.S. Patent No. 8,151,345 (“’345 Patent”).

II. REQUIREMENTS FOR IPR

A. Grounds for Standing

Petitioners certify the ’345 Patent is available for IPR, and Petitioners are not barred or estopped.

B. Challenge and Relief Requested

Petitioners request IPR on the grounds below, supported by testimony of Dr. Traynor (EX1003).

Ground	Claim(s)	35 U.S.C. §103
1A	23	Huomo-Kisliakov-Linehan
1B	24-25	Huomo-Kisliakov-Linehan-Peart
2	23-25	Ryan-Kisliakov-Peart
3A	11-12	Ryan-Hulbert
3B	13-22	Ryan-Hulbert-Peart
3C	1-10	Ryan-Hulbert-Peart-Kisliakov

The ’345 Patent’s earliest claimed priority date is January 25, 2007. For purpose of this proceeding and without conceding its propriety, Petitioners treat

this as the Critical Date. EX1003, ¶45.

Reference	Filed	Published/Issued	§102 Provision
Huomo (EX1004)	12/15/2006	9/17/2013	§102(e)
Hulbert (EX1011)	1/05/2007	7/23/2009	§102(e)
Ryan (EX1006)	11/16/2004	5/08/2007	§102(e)
Linehan (EX1007)	8/31/2000	9/5/2006	§102(a)
Peart (EX1008)	1/04/2006	8/16/2011	§102(e)
Kisliakov (EX1010)	12/18/2002	11/13/2003	§102(b)

C. Claim Construction

All claim terms should be construed according to the *Phillips* standard. *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005); 37 C.F.R. §42.100.

The instant Petition demonstrates obviousness of the Challenged Claims consistent with Petitioner Apple's district court constructions (reproduced below):¹

¹ The parties have not yet exchanged terms for construction in the district court action that Patent Owner initiated against Petitioner Samsung in E.D. Texas.

Claim Term	Construction
“transaction information”/ “transaction authorization information” (All claims)	information used to process a transaction that includes at least bank account information specific to a card holder

Petitioners respectfully submit that no other claim terms need be construed to resolve issues of controversy in the present Petition. *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011); EX1003, ¶¶44-45. Petitioners reserve the right to respond to any constructions offered by Patent Owner or adopted by the Board.

D. Level of Ordinary Skill in the Art

A person of ordinary skill in the art (“POSITA”) relating to the subject matter of the ’345 Patent as of January 25, 2007 would have had (1) at least a bachelor’s degree in computer science, computer engineering, or a related field, and (2) at least two years of industry experience including researching or developing software related to secure communication systems/networks. EX1003, ¶¶25-27. Additional education could substitute for professional experience, and professional experience for education. *Id.*

III. THE ’345 PATENT

A. Brief Description

The ’345 Patent relates to “tokens or cellular network devices that contain

secure element microchips.” EX1001, 1:18-23. The ’345 Patent acknowledges that in some prior payment technologies, “a microchip referred to as a ‘Secure Element’ (SE) is embedded into the... device that may be used for making payments,” and in “order to extract information from the SE, an interrogator, also referred to... as a ‘reader’, is required to interact electrically with the SE.”

EX1001, 1:27-33. The ’345 Patent contends that because “readers are not typically part of most PCs, it is very beneficial to place the reader functionality on the card device.” EX1001, 4:8-15. The ’345 Patent therefore describes embodiments “incorporating a reader on a card device or within a cellular network adapter to extract and deliver banking track data that were generally not previously possible because of the inability to extract information from the SE or from a magnetic stripe at a computer terminal without a reader or to extract information from an SE in a cellular network adapter without a reader.” EX1001, 4:51-57. The ’345 Patent describes “configurations of a ‘Reader On Card’ (ROC)... wherein the card device or cellular network adapter contains both an SE and SE reader functionality.” EX1001, 5:13-18, 7:5-12, 7:27-29; EX1003, ¶47.

B. Prosecution History

In two Office Actions, the Examiner rejected various claims as obvious based on Ryan in view of Lu and Somers. EX1002, 125-141, 187-295. In doing so, the Examiner asserted that Ryan discloses *a secure element reader...*

configured to interrogate the secure element by executing file system functions according to ISO-7816-4, stating “e.g., translation module; see Fig. 3A, 300 and Fig. 3B, 324, and col. 20, lines 38-58; It is noted that a data in a data file could be transferred to smart card fob via ISO 7816-x interface.” EX1002, 128-129, 190. The Examiner further mapped Ryan’s FIG. 1C’s translation module 144 (citing col. 18, lines 12-22) to the recited *a communications controller*. EX1002, 129, 191. In the Office Actions, the Examiner also cited Hulbert, stating “[i]t is well-known to a person in the art how to translate data into a USB HID keycodes (see Hulbert et al. (US PG-Pub. 2009/0187,687 A1), Fig. 3, paragraphs 41, 131-147).” EX1002, 136, 198. However, in the conclusions, the Examiner noted that Hulbert was “not relied upon.” EX1002, 140, 202; EX1003, ¶¶48-49.

In response to the first Office Action, the Applicant argued that “Ryan only refers to ‘ISO 7816’ and there is no indication that Ryan even recognizes that ISO 7816 contains a large number of subsections,” and that “a ‘smart card reader’ is not equivalent to a ‘a secure element reader... configured to interrogate the secure element by executing file system functions according to ISO 7816-4,” citing Brian Charles Murray Declaration. EX1002, 163-164 (emphasizing “**The distinction provided by providing a secure element reader for executing file system functions according to ISO-7816-4 is a hypertechnical distinction, but it is of great importance.**”) (emphasis in original), 177-179. The Applicant also

amended claim 1 by adding “[executing file system functions] comprising a command to select a payment card application” to further distinguish over the prior art. EX1002, 155, 161. The Applicant additionally responded to the Examiner’s reference to Hulbert, asserting that “the Examiner has failed to establish that ‘how to translate data into USB HID keycodes’ is a fact of notorious character,” criticizing the Examiner’s use of official notice for the limitation specifying that “the communications controller is configured to provide the transaction information in a format that auto-populates a form field defined by an application running on the computer terminal,” and noting the Examiner’s statement that Hulbert was not relied upon. EX1002, 169-170; EX1003, ¶50.

In response to the second Office Action, the Applicant simply amended the claims. Claim 1 was amended by adding the allowable subject matter from claim 5 relating to a USB communication connector a HID class communications controller, and transaction information in a format that auto-populates a form field.” EX1002, 207-208, 155-156, 189. Claim 30 (issued as claim 23) was amended by adding the allowable subject matter from claim 33 relating to the wireless network comprises a cellular network and the secure element reader in the cellular network adapter is configured to await a startup instruction comprising an unpredictable number originating over the cellular wireless network prior to interrogating the secure element. EX1002, 212, 160, 189; EX1003, ¶51.

Allowance followed with an “examiner’s statement of reasons for allowance” that “the prior arts of record do not teach nor suggest, either alone or in combination... the communications controller is configured to provide the transaction information in a format that auto-populates a form field defined by an application running on the computer terminal” (e.g., claims 1, 9, 11, 17, 19) and “the secure element reader in the cellular network adapter is configured to await a startup instruction comprising an unpredictable number originating over the cellular wireless network prior to interrogating the secure element” (e.g., claim 23). EX1002, 232-233 (emphasis in original); EX1003, ¶52.

As demonstrated by Ground 1A-3C below, however, the claims never should have been allowed. *Infra*, §IV. Critically, Ryan and Hulbert of record, as well as other pertinent prior art never presented to the Examiner during examination, plainly disclose what the Examiner mistakenly believed to be missing from the prior art. EX1003, ¶53. The ’345 Patent is ripe for review.

IV. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. GROUND 1A—Huomo-Kisliakov-Linehan Renders Obvious Claim 23

1. Uomo²

Uomo describes an NFC (Near Field Communication) enabled communication device having a “secure element 30” that stores transaction data, transaction applications, and encryption algorithm and keys, a “controller 20” that receives data from the secure element 30 through an interface that is “in compliance with ISO 7816,” and an “NFC communicator 15” for transmission of the transaction data to another (recipient) device via an NFC link. EX1004, Abstract, 2:35-67, 3:20-40, 5:24-40, 6:23-41, 7:19-67, FIGS. 1 (reproduced below), 2, 10; EX1003, ¶54.

² General descriptions provided for this and other references and combinations are incorporated into each subsection and mapping of the claims that includes citations to these references.

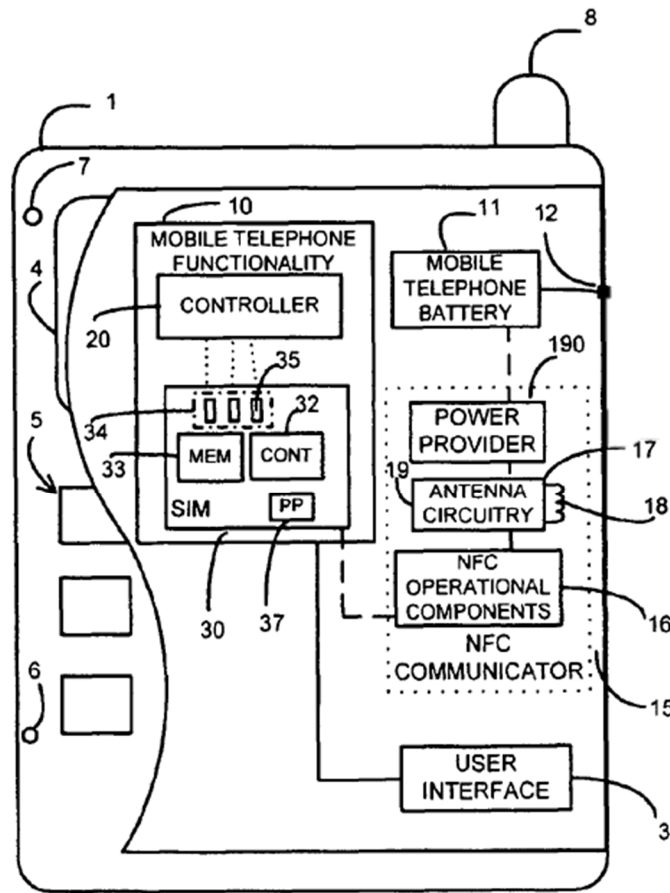


FIG. 1

EX1004, FIG. 1

Huomo's secure element 30 (e.g., "SIM," "USIM") having "memory store 33" is "programmed with or programmable with an operating system and one or more applications platforms applications so as to be capable of encrypting transaction data and storing encrypted transaction data (for example, purchase data) in accordance with that applications platform." EX1004, Abstract, 7:19-67, 3:58-67, 7:65-8:41, 10:35-12:57 (details of "memory 33"). Application areas of Huomo include "the financial transaction area which involves payment for

products such as goods and services.” EX1004, 1:56-60; EX1003, ¶55.

2. Kisliakov

Like Huomo and the ’345 Patent, Kisliakov describes systems in which secure data is stored in a secure element (e.g., smart card) and communicated through a reader to a host, e.g., to enable transactions such as payments. EX1010, Abstract, [0002]-[0003], [0095], [0101], [0243]-[0245], [0264], [0219], [0234]; EX1003, ¶56.

Kisliakov expressly describes (1) the “International Standards Organisation (ISO)/International Electrotechnical Commission (IEC) 7816-4 Standards,” which “describe a file system designed for smart cards, together with commands that can be used to interface with the file system,” and (2) communications (commands and responses) between the secure element (e.g., smart card or CPU card 100B) and the secure element reader (e.g., reader 300) as using “Application Protocol Data Unit (APDU)” format, “as described in the ‘ISO/IEC 7816-4 Standards.” EX1010, [0001], [0006], [0086], [0272]-[0286], [0338]-[0349], [0323]-[0335], [0343], [0354], [0241]-[0245]; EX1003, ¶57.

3. Linehan

Linehan relates to “enabling use of smart cards by consumer devices for Internet commerce... by integrating an existing ‘Integrated Circuit Card Specification for Application Payment Systems’ standard (commonly known as the

‘EMV’ standard) with an augmented Four-Party Credit/Debit Payment Protocol.”

EX1007, 1:8-17. In Linehan, consumers “make purchases (and to perform other types of on-line financial transactions) over the Internet using a smart card which is processed by a smart card reader attached to a consumer computing device.”

EX1007, 5:44-62. Like Uomo, Linehan’s consumer computing device can be a cellular phone. *Id.* “The consumer computing device in use provide[s] an interface for using a smart card, as defined by the EMV Standard.” EX1007, 6:15-17.

Linehan further describes a “Four-Party Credit/Debit Payment Protocol” or “4-party protocol” where the “authorization process is performed between a consumer (using his or her credit or debit card and a consumer device such as a personal computer, or ‘PC’) and the bank that issued the consumer’s card.” EX1007, 1:56-2:2; EX1003, ¶58.

4. Uomo-Kisliakov Combination

a) Uomo and Kisliakov are Analogous Art to the ’345 Patent

Huomo and Kisliakov are analogous art to the ’345 Patent, which is generally directed to “the field of devices configured to authorize transactions using secure element microchips.” EX1001, 1:18-24; cl. 1 (“A token”); *supra*, §IV.A.1-2 (Huomo and Kisliakov); EX1003, ¶59. In addition to being in the same field of endeavor, Uomo and Kisliakov are reasonably pertinent to the problems the ’345 Patent purports to solve. *See, e.g.*, EX1001, 1:39-45 (“what are needed

therefore are devices and methods that adapt the enhanced security and fraud prevention techniques used in smartcard systems for use in internet-based transactions.”), 4:8-24, 4:29-35, 4:36-50, 4:51-60, 4:61-5:12, 5:18-27 (encrypting track data “to securely transport the data packet over a public network”), 5:50-56; 10:50-56, 9:24-30, 17:22-44, 18:34-48, 19:40-42; *supra*, §IV.A.1-2.

b) A POSITA would have been Motivated to Combine Huomo and Kisliakov

Huomo discloses that the secure element is coupled to the controller 20 of the mobile telephone through a “coupling interface 34 comprising one or more coupling elements 35” “to enable communication of data between the controller and the secure element” “in compliance with ISO 7816.” EX1004, 6:23-28, 7:47-52, 8:5-34, 20:48-54, 21:11-14. Based on Huomo’s express disclosure of an ISO 7816 interface between the secure element and controller, a POSITA would have found it obvious that the secure element includes a file system accessed using commands configured in accordance with ISO 7816-4. EX1003, ¶60.

Kisliakov provides express examples of ISO 7816 file system and compliant commands, providing implementation details of the 7816 communication described by Huomo. EX1003, ¶61. Specifically, Kisliakov addresses ISO 7816-4 standards, which “describe a file system designed for smart cards, together with commands that can be used to interface with the file system.” EX1010, [0006].

Kisliakov specifies the message format, stating that “[a]ll commands issued to the CPU card 100B by the reader 300 are in an ‘Application Protocol Data Unit (APDU)’ format as described in the ‘ISO/IEC 7816-4 Standards, Part 4.’” EX1010, [0268]. Kisliakov specifies the commands themselves, describing a SELECT FILE command that “is configured as an application protocol data unit” and “is a subset of the specification for such a command as outlined in the ISO 7816-4 standards,” and a READ BINARY command “according to the ISO 7816-4 standard” that is “executed to read data from a currently selected elementary file stored in the storage means 276.” EX1010, [0323], [0414]. Kisliakov also describes the storage those commands address, explaining that data “can be stored in the storage means 276 as a file being one file of a file system implemented on the CPU card,” with “the user’s home address” and “the user’s credit card number” held “in separate files in the memory 276 of the card 110B.” EX1010, [0126], [0351].

Kisliakov describes the file system on the card itself (e.g., the files are in the “storage means 276” and each SELECT FILE or READ BINARY command is executed by “an application executing within the CPU 275.”). EX1010, [0323], [0326]. A POSITA would have been motivated to implement Uomo’s controller 32—which controls “transfer of data from a memory store of the secure element”—to issue those commands to memory store 33, especially because ISO 7816-4 is defined by the file system it addresses. EX1004, 7:19-52; EX1010,

[0323], [0326]; EX1003, ¶62.

Multiple predictable benefits would have motivated a POSITA to implement Huomo's secure element as an ISO 7816-4 file system and data communication between a controller and the secure element as ISO 7816-4 file system commands, in accordance with Kisliakov. EX1003, ¶63.

First, a POSITA would have combined Huomo and Kisliakov to provide reliable and robust operation by utilizing messaging in conformance with a published standard. EX1003, ¶64. For example, Huomo explicitly specifies its interfaces by standard number, including "coupling elements may, for example, be in compliance with ISO 7816" and "protocols set out in various standards such as ISO/IEC 18092, ISO/IEC 21481, ISO/IEC 14443 and ISO/IEC 15693." EX1004, 6:23-28, 7:47-52, 8:5-34, 20:48-54, 21:11-14, 9:55-59, 11:52-55, 12:13-15, 14:38-62, 18:54-56; EX1012, §§5-6. Per Kisliakov, utilizing a standard messaging protocol such as ISO 7816-4 promotes interoperability such that each deployment does not require a terminal be programmed to a particular card. EX1003, ¶64. In the Huomo-Kisliakov-Linehan combination, the reader selects the elementary file holding the cardholder's transaction data with a SELECT FILE APDU, reads its contents with a READ BINARY APDU, and receives the file's contents from the secure element's memory store, all according to a published specification any conforming card supports. EX1010, [0323], [0414]. Accordingly, the combination

predictably promotes interoperability with cards and infrastructure built to a published specification (e.g., as compared to terminal-specific programming). EX1003, ¶64.

Second, a POSITA would have been motivated to implement Kisliakov's suggestions in Huomo's system to promote file handling and control. EX1003, ¶65. For example, implementing messaging according to ISO 7816-4 would have promoted a defined addressing scheme for the secure element's storage such that distinct categories of cardholder data occupy separate files that the reader can select individually. *Id.* Kisliakov describes a SELECT FILE command carrying a "two-byte file identifier," such that "[i]f the two-byte file identifier as shown in Table 31 points to a valid file, then that file becomes an active file." EX1010, [0324]. The reader then reads that file alone, because Kisliakov's read binary process is "executed to read data from a currently selected elementary file stored in the storage means 276." EX1010, [0414]. A POSITA would have recognized that this lets a given transaction retrieve only the data that transaction needs. EX1003, ¶65. Where information such as "the user's home address" and "the user's credit card number" are in "separate files in the memory 276 of the card 110B," selecting one beneficially leaves the other unread. *Id.*; EX1010, [0351].

Third, a POSITA would have been motivated to implement Huomo's user interface in accordance with Kisliakov's teachings. EX1003, ¶66. Huomo

discusses a user interface providing “a user with capability to view data and/or applications stored on the secure element” and “to select secure element or contents within the secure element from a menu service provided by the device user interface on the mobile telephone or PDA or laptop for display in a user friendly format by a display of the device user interface.” EX1004, 20:11-29, 20:65-21:31. Kisliakov describes “a user interface... allowing a user to access a file stored on the CPU card.” EX1010, [0001]. Based on Huomo’s explicit disclosure of a user interface for accessing secure element data, a POSITA would have found it obvious and would have been motivated to look to Kisliakov for implementation details relating to user interfaces for accessing secure element data. EX1003, ¶66.

c) A POSITA would have Reasonably Expected Success when Combining Huomo and Kisliakov

The combination amounts to use of a known technique (ISO 7816-4 messaging in accordance with Kisliakov) in a known system (e.g., Huomo’s reader that uses ISO 7816 compliant messaging) to yield predictable results. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007); EX1003, ¶67. A POSITA would have had a reasonable expectation of success, especially because the combination would have been implemented primarily through routine software updates. *Id.* Kisliakov describes command formats field by field and card-side process

executed in response to each command. EX1010, [0361]-[0373]. The two references share the same hardware substrate, which a POSITA would have recognized as making the layering straightforward. EX1003, ¶67 Indeed, Huomo describes ISO 7816 compliant interfaces and its controller 32, for example, controls “transfer of data from a memory store of the secure element,” and Kisliakov's card is a CPU card whose processor likewise executes file-system commands against the “storage means” it manages. EX1004, 7:19-56; EX1010, [0268], [0326].

5. Huomo-Kisliakov-Linehan Combination

a) Linehan is Analogous Art to the '345 Patent

Linehan is analogous art to the '345 Patent, both because it is within the same field of endeavor (EX1001, 1:18-24; cl. 1, cl. 23 (“cellular network adapter”); *supra*, §IV.A.3; EX1007, 1:8-16, 6:15-17, 5:55-58) and because Linehan is reasonably pertinent to the problems the '345 Patent purports to solve. *See, e.g.*, EX1007, 1:8-16, 6:15-17, 5:55-58; EX1001, 1:39-45, 4:8-24, 4:29-35, 4:36-50, 4:51-60, 4:61-5:12, 5:18-27, 5:50-56; 10:50-56, 9:24-30, 17:22-44, 18:34-48, 19:40-42; *supra*, §IV.A.3; EX1003, ¶68.

b) A POSITA would have been Motivated to Combine Huomo-Kisliakov-Linehan

Huomo discloses that “the user may wish to use the device as a credit card and may request that VISA... or MasterCard... or some other similar credit card

company activates or loads a credit card applications platform (for example an EMV platform) onto the secure element” and provides “a banking applications platform defining payment protocols in accordance with banking standards and procedures (including credit card requirements, EMV specifications and the like).” EX1004, 16:28-33, 11:48-52. A POSITA would have found it obvious that the payment protocols for using the secure element as a credit/debit card to make purchases is in accordance with the EMV standard, especially in view of Huomo’s express disclosure of EMV platforms and specifications. EX1003, ¶69.

Linehan provides more details regarding the EMV standard for “an on-line shopping transaction” “made over the Internet” using a “consumer computing device” with a “smart card” that “includes a logic chip that contains stored information pertaining to the owner, such as the owner’s name, address, and account number; the card issuer (such as Mastercard, Visa, etc.); a Personal Identification Number (PIN); and any limitations on the cards use (such as a dollar maximum used for an individual purchase).” EX1007, 1:8-55, 2:48-67, 3:48-64, 5:44-62. Given Huomo’s explicit reference to the EMV standard, a POSITA would have naturally been motivated to look to Linehan for implementation details for using the secure element as a credit/debit card to make purchases over the Internet. EX1003, ¶70. And like Huomo and Kisliakov, Linehan also discusses ISO 7816. EX1007, 15:36-46. Multiple predictable benefits would have

motivated a POSITA to utilize implementation details of the EMV standard and 4-party protocol in Huomo-Kisliakov, in accordance with Linehan. EX1003, ¶70.

First, a POSITA would have been motivated to implement Huomo-Kisliakov to use the EMV standard and 4-party protocol as suggested by Linehan “to increase efficiency of authorizing smart card transactions for Internet on-line shopping by taking advantage of the consumer's ability to directly connect to the smart card issuer.” EX1007, 1:56-2:47. EX1007, 4:4-7; EX1003, ¶71. Linehan further explains that this “allows the consumer device to present the card authorization (as an authorization token) along with the payment message to the merchant. One advantage of sending this authorization token with the payment message is that the consumer’s account number might not be required to be sent to the merchant. This reduces the exposure of the account number and may thereby reduce the potential for theft by unscrupulous employees working at the merchant location. A further advantage is that pre-authorization considerably simplifies many aspects of the payment protocol and permits much of the consumer function to be operated remotely by the issuing bank.” EX1007, 10:4-14.

Second, a POSITA would have been motivated to implement Huomo-Kisliakov to use the 4-party protocol as suggested by Linehan for the common goal of improved interoperability across systems. EX1003, ¶72. Huomo expresses a desire for “interoperability to maintain a consistent and viable user

experience...flexibility and backwards compatibility with existing systems and devices.” EX1004, 2:16-19. Linehan explains that the 4-party protocol beneficially “allows consumers to purchase items from a consumer computing device over the Internet using smart card technology, but without requiring modification of the existing EMV standard or of existing smart cards.” EX1007, 3:48-52.

Third, a POSITA would have been motivated to combine Huomo-Kisliakov with Linehan to provide additional ISO 7816 features such as the ISO 7816 Based Card Numbers and the Domain Name System (DNS). EX1007, 15:36-46; EX1003, ¶73. Doing so would allow the user device to use an account number to look up the Uniform Resource Locator (URL) or network address of the issuing bank in order to transmit authorization messages to the bank. *Id.*

c) A POSITA would have Reasonably Expected Success when Combining Huomo-Kisliakov-Linehan

Ultimately, the combination amounts to use of a known technique (EMV standard with a 4-party protocol in accordance with Linehan) in a known system (e.g., Huomo-Kisliakov’s secure element including EMV platforms) to yield predictable results. *KSR*, 550 U.S. at 417 (2007); EX1003, ¶74. A POSITA would have had a reasonable expectation of success, especially because the combination would have been implemented primarily through routine software updates. *Id.*

The references share the same hardware substrate, which a POSITA would have recognized as making the layering straightforward. *Id.* Indeed, Huomo-Kisliakov's secure element includes EMV platforms for secure elements to be used as credit/debit cards for transactions over the Internet, and Linehan's smart card is used as a credit/debit card to make purchases over the Internet. EX1004, 16:28-33, 11:48-52, 6:10-18; EX1007, 1:8-55, 2:48-67, 3:48-64, 5:44-62.

6. Analysis

Claim 23

[23.pre]

Huomo describes a device 1 that is “a mobile telephone” (*cellular network device*) including “mobile telephone functionality 10” (*cellular network adapter*) “comprising the controller 20... for controlling operation of the mobile telephone” and a “SIM (Subscriber Identity Module) or USIM (Universal Subscriber Identity Module)” that “will carry the usual user and operational data required by the mobile telephone user to operate the mobile telephone,” as shown in FIG. 1 below. EX1004, 7:65-8:15, 15:60-16:13; EX1003, ¶75.

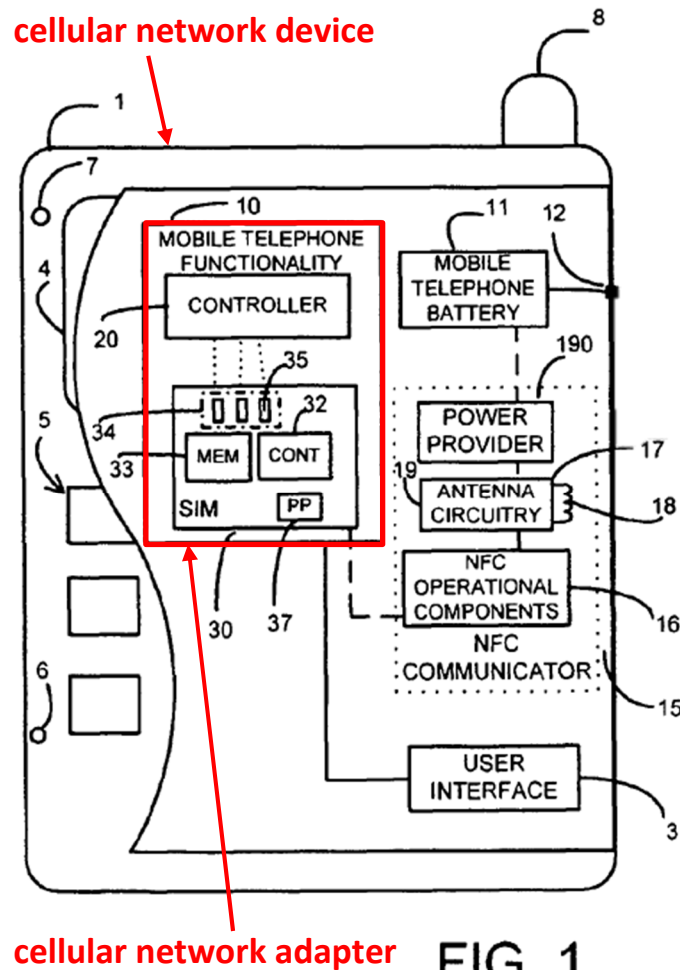


FIG. 1

EX1004, FIG. 1³

Huomo discloses that a secure element 30 provided by the SIM is programmed with “applications platforms to enable the secure element to load a corresponding application to enable a transaction to be effected... which requires communication of secure data.” EX1004, 5:41-48. In Huomo, “an applications platform may be provided as a JAVA (Registered Trade Mark of Sun

³ Annotations and color added to figures unless otherwise noted.

Microsystems)-enabled applet.” EX1004, 13:16-22. The mobile telephone is “able to communicate secure data, via the mobile telecommunications network 1010.” EX1004, 15:13-36, 7:19-25. Huomo describes communicating “data, for example transaction or product data via the Internet,” “via the mobile telecommunications system in... the device[] 1.” EX1004, 5:41-6:18, 13:1-44. Huomo also provides a “communications device” “comprising a mobile telecommunications communicator configured to communicate via a mobile telecommunications network.” EX1004, 27:25-28; EX1003, ¶76.

A POSITA would have understood or found it obvious that Huomo’s “mobile telecommunications communicator” of the mobile phone (*cellular network device*) provides a *cellular network application interface* for the JAVA-enabled applet applications platforms to communicate data via the Internet via the cellular network. EX1003, ¶77; EX1004, 5:41-6:18, 13:1-44; EX1001, 6:58-60. A POSITA would have understood that the mobile telecommunications communicator (*cellular network application interface*) is included in the “mobile telephone functionality 10” (*cellular network adapter*) because the communicator provides the mobile telephone with functionality “to communicate via a mobile telecommunications network.” EX1004, 27:25-28; EX1003, ¶77.

[23.1]

As discussed above in [23.pre], Huomo describes a “secure element 30”

provided by the SIM of the mobile telephone functionality 10 (*cellular network adapter*) of the mobile telephone (*cellular network device*). EX1004, 7:65-8:1, 3:1-19, 3:44-55, 8:6-15, 15:62-16:13. Huomo uses the term “secure element” to mean “any element which is capable of being used to hold secure encrypted information and/or data.” EX1004, 25:41-44. Huomo discloses that the secure element 30 includes “a data or memory store (MEM) 33.” EX1004, 7:31-46. Huomo discloses that the memory store 33 of the secure element provides “transaction data storage” for “transaction data” including “payment data” for “a financial product such as a credit or debit card.” EX1004, 10:35-11:7, 2:44-46, 3:63-4:15, 25:51-62; EX1003, ¶78.

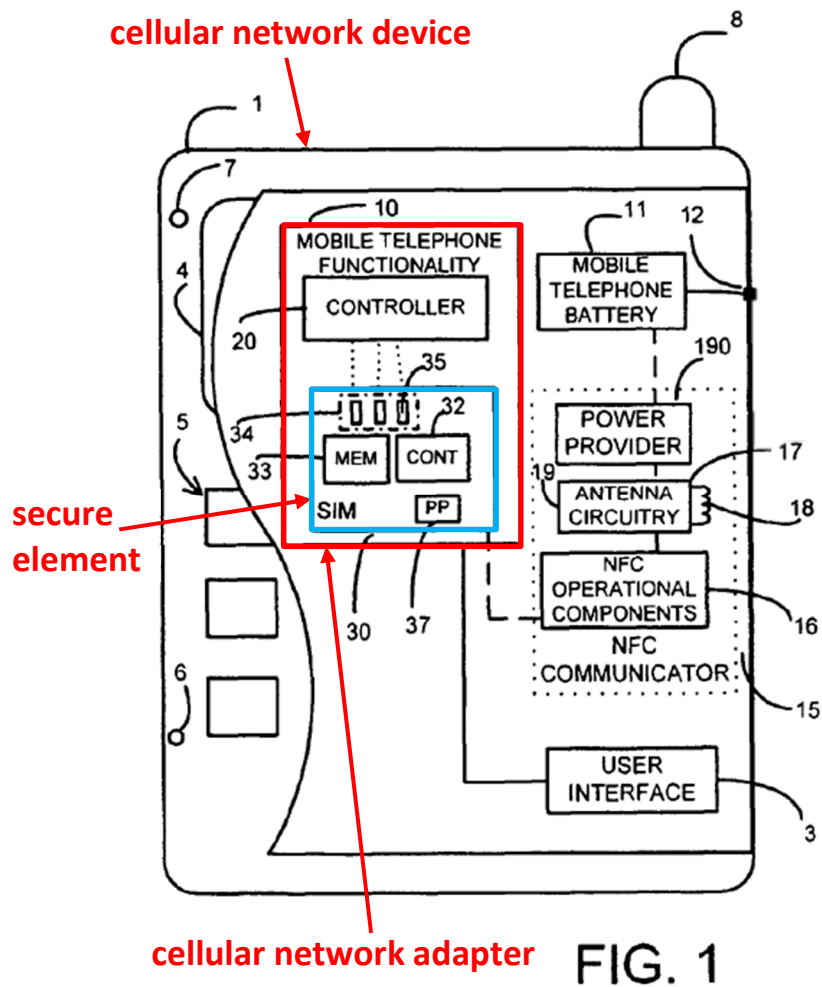


FIG. 1

EX1004, FIG. 1

A POSITA would have found it obvious that memory store 33 of the secure element stores transaction/payment data for each financial product (credit/debit card number) in one or more data files based on Kisliakov's teachings. EX1003, ¶79. Similar to Huomo, Kisliakov describes a type of "smart card," referred to as a "CPU card," that includes "an on-board memory chip, for storing data (e.g. a personal identification number) associated with the card" (*secure element*). EX1010, [0002]-[0003], [0086]. In Kisliakov, a CPU card can be "configured for

use with an electronic banking application.” EX1010, [0236]. Kisliakov discloses that for the CPU card, “data... can be stored in the storage means 276 as a file being one file of a file system implemented on the CPU card.” EX1010, [0126]. Kisliakov’s CPU card stores “the user’s home address” and “the user’s credit card number” “in separate files in the memory 276 of the card 110B.” EX1010, [0351]. In the combined system, the file holding the cardholder’s credit/debit card number provides a *data file*. EX1010, [0126], [0351]; EX1003, ¶79.

[23.2]

Huomo discloses that the mobile telephone functionality 10 (*cellular network adapter*) has a *secure element reader* including “a controller (CONT) 32... which controls the functionality of the secure element in accordance with its operating systems and the installed applications platform or platforms.” EX1004, 7:31-46; EX1003, ¶80. Huomo describes that the controller 32 (*secure element reader*)⁴ “controls the functionality of the secure element” including “decrypting

⁴ That the controller 32 is provided within Huomo’s secure element 30 is consistent with the ’345 Patent, which recites that the interrogator “may be physically

encrypted data” stored in the memory store and “transfer of data from a memory store of the secure element,” which would involve *interrogating the secure element* (memory store 33 of secure element 30) and generating information from the secure element data. EX1004, 7:19-52, 8:25-42, 2:47-49, 5:41-61, 24:55-60; EX1003, ¶80. As discussed above in [23.1], the Huomo-Kisliakov-Linehan combination teaches that the secure element, through its memory store 33, stores transaction/payment data for each financial product (credit/debit card number) in one or more data files and therefore teaches that the controller 32 (*secure element reader*) *generates file information* (including credit/debit card number) *from the secure element data file* to transfer the data from the memory store 33. *Id.*

incorporated into the secure element” and that in a “‘Reader On Card’ (ROC) device the interrogator and SE are integrated together on the same medium, device or circuit.” EX1001, 6:65-7:29; EX1003, ¶80.

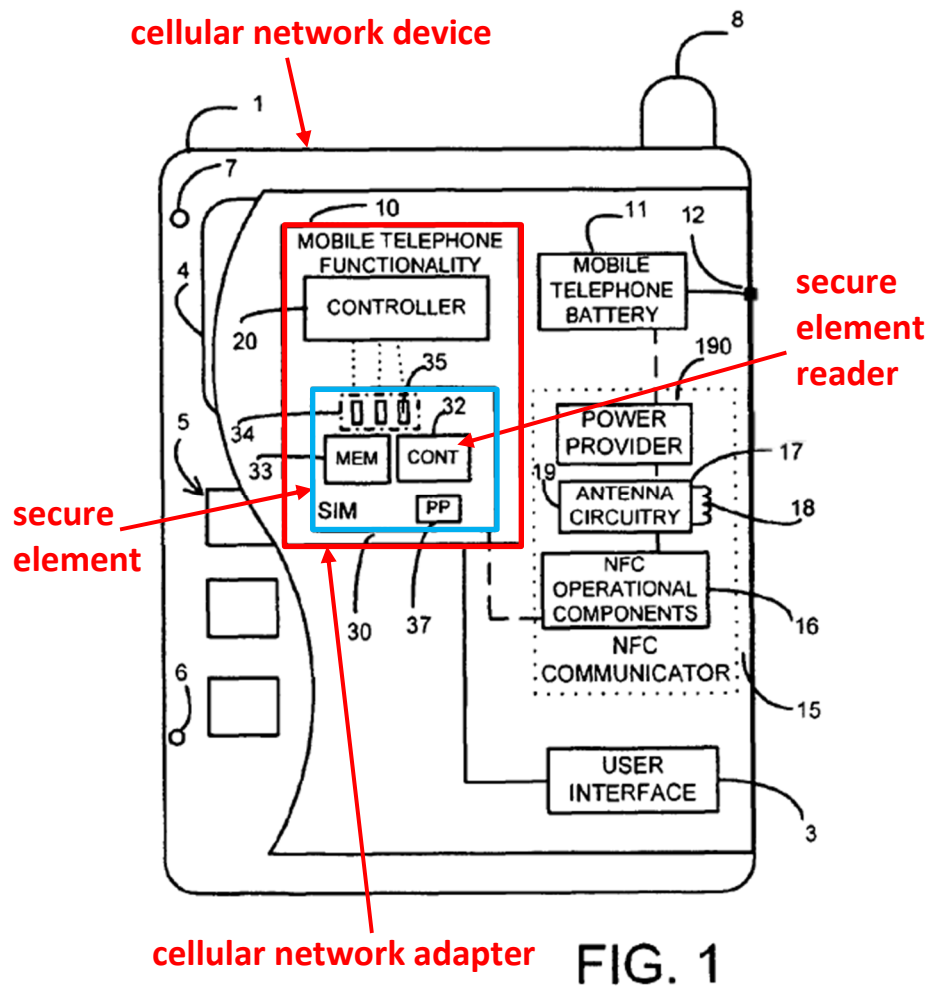


FIG. 1

EX1004, FIG. 1

In the combined system, the controller 32 (*secure element reader*) interrogates the secure element by executing file system functions according to ISO 7816-4 based on Kisliakov's teachings. EX1003, ¶81. Kisliakov discloses that ISO 7816-4 standards "describe a file system designed for smart cards, together with commands that can be used to interface with the file system." EX1010, [0006]. Kisliakov describes that all "commands issued to the CPU card 100B by the reader 300 are in an 'Application Protocol Data Unit (APDU)' format

as described in the ‘ISO/IEC 7816-4 Standards...’.” EX1010, [0268]. To “select a file stored in the storage means 276,” the reader “sends a SELECT FILE command” to an “application executing within the CPU 275.” EX1010, [0323]. To “read from a selected elementary file stored in the storage means 276,” the reader sends “a READ BINARY command” to an “application executing within the CPU 275.” EX1010, [0326]. In the Huomo-Kisliakov-Linehan combination, a POSITA would have found it obvious that the controller 32 (*secure element reader*) executes “a SELECT FILE command” and/or “a READ BINARY command” (*file system functions according to ISO 7816-4*) to select and/or read from the data file stored in the memory store 33 (*interrogate the secure element*). EX1010, [0323], [0326]; EX1003, ¶81.

In the Huomo-Kisliakov-Linehan combination, the data returned to the controller 32 (*secure element reader*) in response to the above commands including the cardholder’s credit/debit card number (e.g., and associated payment data) is read out of the selected file, and provides the recited *file information* generated *from the secure element data file*. EX1003, ¶82. Linehan provides further details confirming that the data read out of the card in an EMV transaction includes “the primary account number,” which is read “from the card” before an authorization message is built. EX1007, 15:28-35, 17:27-33. Linehan discloses that the smart card generates “an authorization request (AR)” that “comprises a

card account number for the transaction, an amount of the transaction, a date of the transaction, and a serial number of the smart card” for transmitting to the consumer device. EX1007, 4:41-45, 11:48-51, 12:8-12, 19:30-42, 21:24-30, 24:22-27.

[23.3]

Huomo describes that the mobile telephone (*cellular network device*) includes “an NFC communicator 15 to communicate data stored by the secure element 30... to another near field RF communicator... by modulating the H (magnetic) field of an RF signal.” EX1004, 5:24-38. The NFC communicator 15 includes “NFC operational components 16 for... generation, modulation and demodulation of an RF signal” (*RF data signal*). EX1004, 6:55-7:3, 9:18-38. The NFC operational components 16 includes “a controller 40..., for example, a microprocessor” (*NFC controller bridge chip*) “to control overall operation of the NFC communicator.” EX1004, 9:1-12, FIG. 3. Huomo further teaches an NFC communicator “combined with” a secure element and the “combined NFC communicator/secure element... may be inserted into... a mobile telephone.” EX1004, 25:63-26:7. A POSITA would have understood the combined NFC communicator/secure element/SIM would be included in the mobile telephone functionality 10 (*cellular network adapter*). EX1003, ¶83.

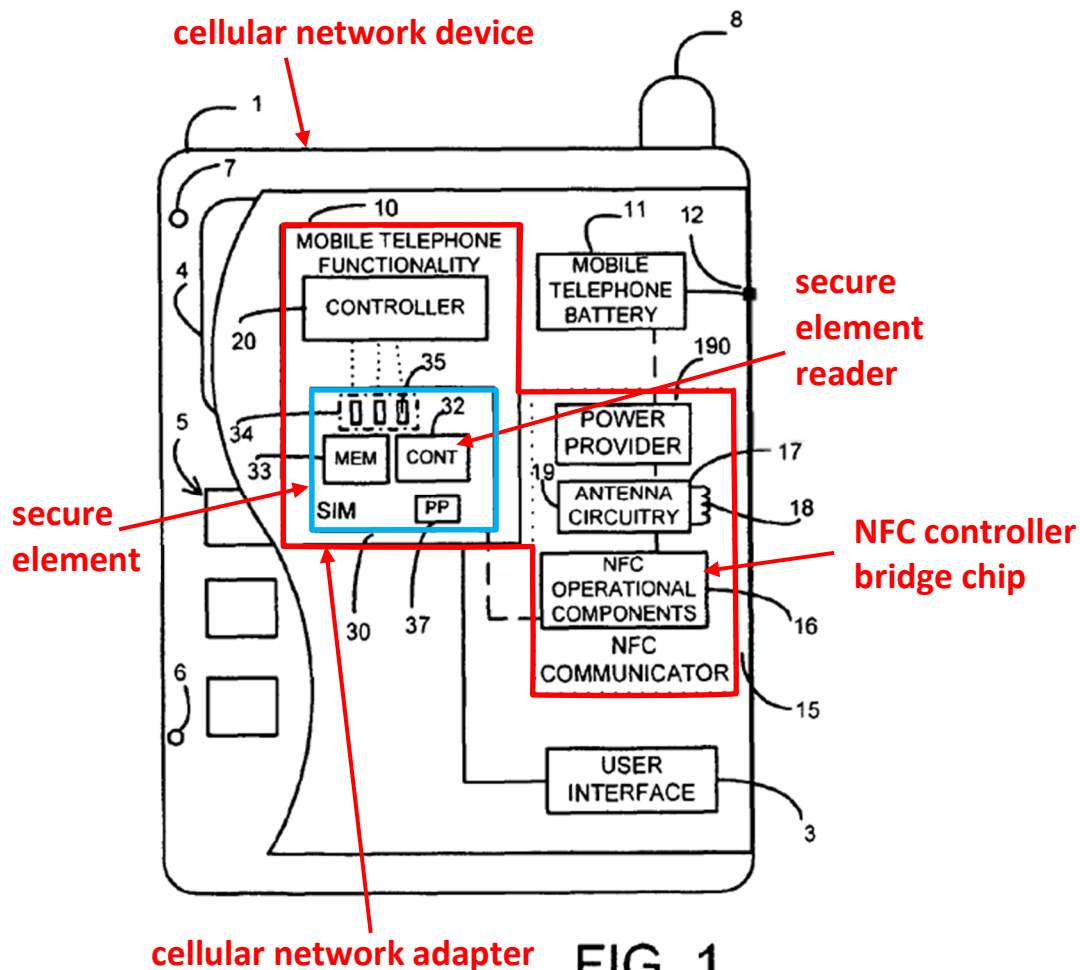


FIG. 1

EX1004, FIG. 1

Huomo’s “NFC communicator 15 is... operable to enable data communication between the secure element 30... and another near field RF communicator external to the device via the NFC communicator 15.” EX1004, 10:22-26, 15:37-59. For example, transaction data (credit/debit card number) may be “read from the secure element and communicated by the NFC communicator 15 to another near field RF communicator” (*external reader*). EX1004, 10:26-34. As discussed above in [23.2], Huomo-Kisliakov-Linehan combination teaches that the

controller 32 (*secure element reader*) generates an authorization request including the credit/debit card number (*file information*) from the secure element data file for transmitting to another reader such as Huomo's NFC communicator 15.

EX1003, ¶84. The controller 40 of the NFC communicator 15 (*NFC controller bridge chip*) would receive the authorization request including the credit/debit card number (*file information*) and convert the file information to an RF data signal for another near field RF communicator (*external reader*). *Id.*; EX1004, 5:24-38, 6:55-7:3, 9:1-38, 10:22-34, 15:37-59; EX1001, 18:46-50.

[23.4]

Huomo describes that the mobile telephone functionality 10 (*cellular network adaptor*) of the mobile telephone (*cellular network device*) includes “a controller 20” (*communications controller*) “to communicate data with the secure element 30.” EX1004, 5:52-56, 6:23-28, 10:10-14. As discussed above in [23.pre], Huomo also teaches that the mobile telephone functionality 10 (*cellular network adaptor*) of the mobile telephone (*cellular network device*) includes “a mobile telecommunications communicator” (*cellular network application interface*) “configured to communicate via a mobile telecommunications network” (*wireless network comprises a cellular network*). EX1004, 27:25-28; EX1003, ¶85.

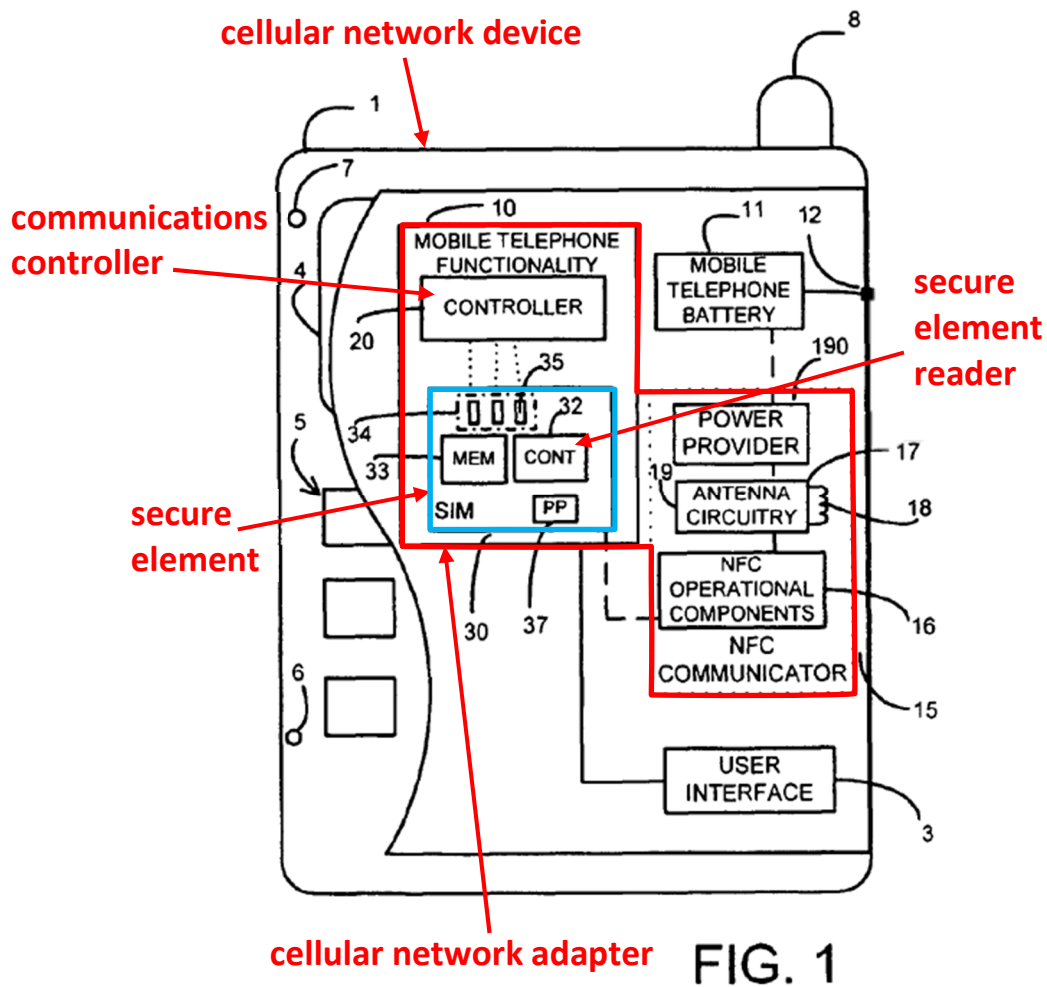


FIG. 1

EX1004, FIG. 1

Huomo discloses that the mobile telephone (*cellular network device*) is “able to communicate secure data, via the mobile telecommunications network 1010” (*wireless network comprises a cellular network*) “with one or more service providers, as shown a mobile telecommunications service provider 1003 and a transaction service provider 1004.” EX1004, 15:13-36, 7:19-25. Huomo discloses that a transaction can involve “payment authorisation.” EX1004, 11:59-61. A POSITA would have found it obvious that controller 20 (*communications*

controller) of the mobile telephone (*cellular network device*) receives data from controller 32 (*secure element reader*), converts the data into information for “payment authorisation” (*transaction authorization information*), and transmits the “payment authorisation” from the mobile telephone (*cellular network device*) over a mobile telecommunications network 1010 (*wireless network comprises a cellular network*) through the “mobile telecommunications communicator” (*cellular network application interface*). EX1003, ¶86.

As discussed above in [23.2], Huomo-Kisliakov-Linehan combination teaches that the controller 32 (*secure element reader*) generates an authorization request including the credit/debit card number (*file information*) from the secure element data file for transmitting to another reader such as Huomo’s controller 20 (*communications controller*). EX1003, ¶87. Controller 20 (*communications controller*) would receive the authorization request including the credit/debit card number (*file information*) from controller 32 (*secure element reader*) and transmit a “payment authorisation” (*transaction authorization information*) from the mobile telephone (*cellular network device*) over the mobile telephone communications network (*wireless network comprises a cellular network*) through the mobile telecommunications communicator (*cellular network application interface*) to a transaction service provider 1004. *Id.*

Linehan provides further details on converting at least a portion of the

authorization request (AR) including the credit/debit card number (*file information*) into transaction authorization information, and the content of the transaction authorization information. EX1003, ¶88. Linehan discloses that the smart card generates “an authorization request (AR)” that “comprises a card account number for the transaction, an amount of the transaction, a date of the transaction, and a serial number of the smart card.” EX1007, 4:41-45, 11:48-51, 12:8-12, 19:30-42, 21:24-30, 24:22-27. Linehan discloses converting the AR with the credit/debit card number (*file information*) into an “authenticated authorization request message” including the credit/debit card number (*transaction authorization information*) “by augmenting the received payment initiation message with the AR” which includes a credit/debit card number for the transaction, and “cryptographically authenticat[ing]” the message “with keyed Message Authentication Codes (MACs),” and then sending “the authenticated authorization request message” including the credit/debit card number (*transaction authorization information*) “directly from the consumer device to the issuer.” EX1007, 4:38-49, 11:34-42, 14:8-14, 15:50-67, 18:21-24, 19:20-42, 21:31-38, 24:28-34, 26:5-14, FIG. 6 (610), FIG. 7 (710). The credit/debit card number is linked to an issuing bank and a bank account, is used to route messages to the issuing bank, and therefore is bank account information. EX1003, ¶88 (citing EX1007, 15:40-46). Linehan further discloses that if “on-line PIN processing is

used,” the “consumer PC includes [an] encrypted PIN in the 4-party authorization request [message] transmitted to the issuing bank.” EX1007, 14:63-65, 20:6-11, 20:20-25, 22:64-67, 23:6-12, 25:14-18, 25:26-32. In the Huomo-Kisliakov-Linehan combination, the controller 20 (*communications controller*) of the mobile telephone (*cellular network device*) converts at least a portion of the authorization request (AR) including the credit/debit card number (*file information*) into an authenticated authorization request message including the credit/debit card number (*transaction authorization information*) and transmits the authenticated authorization request message (*transaction authorization information*) from the mobile telephone (*cellular network device*) over a wireless network through the mobile telecommunications communicator (*cellular network application interface*) to a transaction service provider 1004. EX1003, ¶88.

[23.5]

Linehan discloses that “initiating a transaction with a merchant using a smart card which is accessible directly from a consumer device” includes the consumer device receiving from the merchant an “initiation message” that includes “a transaction amount, a time stamp, a random nonce, and data required by the smart card.” EX1007, 4:27-37, 12:27-48, 15:12-27, 1:43-46, 18:57-67, 22:3-11, 23:56-61. In Linehan, a “random nonce is a random number generated for the purpose of uniquely identifying this transaction.” EX1007, 12:48-50. “Receipt of the wallet

initiation message... causes the consumer's browser (or equivalent software) to start the consumer's wallet (or equivalent) program.” EX1007, 12:59-61, 15:28-35, 18:57-67. “The wallet initiates the EMV application, and reads the application data—including the primary account number—from the card.” EX1007, 15:28-35, 17:27-33. “If the card performs Dynamic Data Authentication, the wallet preferably uses the random nonce from the wallet initiation message as the Unpredictable Number.” EX1007, 15:56-59, 10:50-56. In the Huomo-Kisliakov-Linehan combination, a POSITA would have found it obvious that the controller 32 (*secure element reader*) in the mobile telephone functionality 10 (*cellular network adapter*) is configured to wait for receipt of an initiation message (*await a startup instruction*) comprising a random nonce (*unpredictable number*) from the controller 20 of the mobile telephone (*cellular network device*) originating over the cellular wireless network prior to interrogating the memory store 33 (*secure element*). EX1003, ¶89.

B. GROUND 1B—Huomo-Kisliakov-Linehan-Peart Renders Obvious Claims 24-25

1. Peart

Peart discloses a system and method for securing transaction information using a seeded cryptographic algorithm (e.g., a “standard triple Data Encryption Standard (DES) operation”) in which variable data is hashed to derive a seed and a

final “unpredictable number (UN)” is generated and used by a transaction device (102) in encrypting and authenticating transaction data. EX1008, Title, Abstract, 1:34-38, 2:63-3:15, 5:3-34, 6:24-61, FIGS. 2-3 & 5; EX1003, ¶90. The seed value itself is “computed by subjecting variable data to a Secure Hashing Algorithm,” such as SHA. EX1008, Abstract, 6:24-61, 6:29-40, 9:19-10:2, FIGS. 3, 4.

The final “unpredictable number” is integrated into the encrypted transaction information (“a cryptogram”), sent in an authorization message and later validated by a verifying entity (e.g., “an ‘acquirer’ or account issuer”), which confirms that the unpredictable number and cryptogram correspond to expected values, thereby establishing transaction authenticity. EX1008, 2:21-30, 5:4-8, 5:41-51, 6:7-7:10, 9:19-10:2, FIG. 3. FIG. 4. Peart’s seeded cryptographic algorithm for securing transaction information is described in technology-agnostic terms and expressly applied to “any environment wherein security of a transaction is required.” EX1008, Title, Abstract, 5:4-54, 7:22-30, 8:21-35, FIG. 1; EX1003, ¶91.

2. Huomo-Kisliakov-Linehan-Peart Combination

a) Peart is Analogous Art to the ’345 Patent

Peart is analogous art to the ’345 Patent, both because it is within the same field of endeavor (EX1001, 1:18-24; *supra*, §IV.B.1; EX1008, 5:35-54, cl. 1), and because Peart is reasonably pertinent to the problems the ’345 Patent purports to solve. *See, e.g.*, EX1001, 1:27-45; EX1008 5:1-34; EX1003, ¶92.

b) A POSITA would have been Motivated to Combine Huomo-Kisliakov-Linehan-Peart

Peart addresses the problem of securing transaction information during generation and transmission by introducing a seeded cryptographic algorithm for producing an “unpredictable number” produced from “variable data” such as “a counter” and “the time of the transaction.” EX1008, Abstract, 2:21-3:15. Peart describes the cryptographic algorithm as beneficial for “any environment wherein security of a transaction is required.” *Id.*; EX1008, 7:22-30; EX1003, ¶93.

A POSITA would have found it obvious to incorporate Peart’s teachings of a cryptographic algorithm for securing transaction information into the Huomo-Kisliakov-Linehan system for enhanced secure transaction data transmission. EX1003, ¶94 (citing EX1008, 5:1-19; EX1004, 5:64-67, 10:32-34, 11:28-33, 15:25-36, 23:64-67; *see also* EX1006, 1:45, 2:3-9, 2:66-67, 10:35-12:39, 22:24-41, 24:60-61; EX1009, 2:9-11, 5:1-13, 8:11-14). In the combined system, an authorization request message would include an encrypted unpredictable number constructed as a hash of a timestamp and an encrypted UN together with other information constructed from a timestamp and a transaction counter, in accordance with Peart. *Id.*

Multiple considerations would have led a POSITA to implement this combination. EX1003, ¶95.

First, a POSITA would have been motivated to incorporate Peart's teachings of a cryptographic algorithm into Huomo-Kisliakov-Linehan, because this would provide a self-contained cryptographic mechanism suitable for protecting transaction data before it leaves a secure processing environment. EX1003, ¶96 (citing EX1006, 1:45, 2:3-9, 2:66-67, 10:35-12:39, 22:24-41, 24:60-61). Executing a cryptographic algorithm within Huomo-Kisliakov-Linehan's mobile telephone would help prevent exposure of transaction information to external interfaces. *Id.*

Second, a POSITA would have been motivated to incorporate Peart's teachings into Huomo-Kisliakov-Linehan for transaction uniqueness and protection against replay attacks. EX1003, ¶97. As Peart teaches that an unpredictable number is derived from transaction-specific variable data (e.g., "a transaction counter" or "time of the transaction") and processed through encryption, such incorporation in the Huomo-Kisliakov-Linehan-Peart combination would support replay-attack protection independent of the external communication channel. EX1008, Abstract, 2:66-67, 5:35-41, 6:29-40, FIG. 3.

Third, a POSITA would have been motivated to incorporate Peart's teachings regarding a cryptographic algorithm into Huomo-Kisliakov-Linehan, because the use of a seed derived from variable data and a repeatable cryptographic process (per Peart) allows a verifying/authorizing entity (e.g., "an 'acquirer' or

account issuer”) to reproduce or validate expected outputs, providing robust validation independent of the client environment. *See e.g.*, EX1008, Abstract, 2:21-30, 4:3-7, 5:1-54, FIG. 4; EX1003, ¶98.

*c) A POSITA would have Reasonably Expected Success when
Combining Huomo-Kisliakov-Linehan-Peart*

A POSITA would have expected a high likelihood of success in implementing the combination, because incorporating Peart’s teachings into Huomo-Kisliakov-Linehan is technically straightforward. EX1008, Abstract; EX1003, ¶99. Peart’s teachings regarding a cryptographic algorithm are readily executed within Huomo-Kisliakov-Linehan’s mobile telephone before any transaction information is exposed to external interface. *Id.*

3. Analysis

Claims 24 and 25

[24]/[25]

In the Huomo-Kisliakov-Linehan combination as discussed in [23.5], the controller 32 (*secure element reader*) in the mobile telephone functionality 10 (*cellular network adapter*) is configured to wait for receipt of an initiation message (*await a startup instruction*) comprising a random nonce (*unpredictable number*) from the controller 20 of the mobile telephone (*cellular network device*) originating over the cellular wireless network prior to interrogating the memory store 33 (*secure element*). EX1003, ¶100. In the Huomo-Kisliakov-Linehan

combination as discussed in [23.4], the controller 20 (*communications controller*) of the mobile telephone (*cellular network device*) converts at least a portion of the authorization request (AR) including the credit/debit card number (*file information*) into an authorization request message including the credit/debit card number (*transaction authorization information*) by augmenting the received initiation message (*startup instruction*) comprising the random nonce (*unpredictable number*) with the AR (*file information*). *Id.*

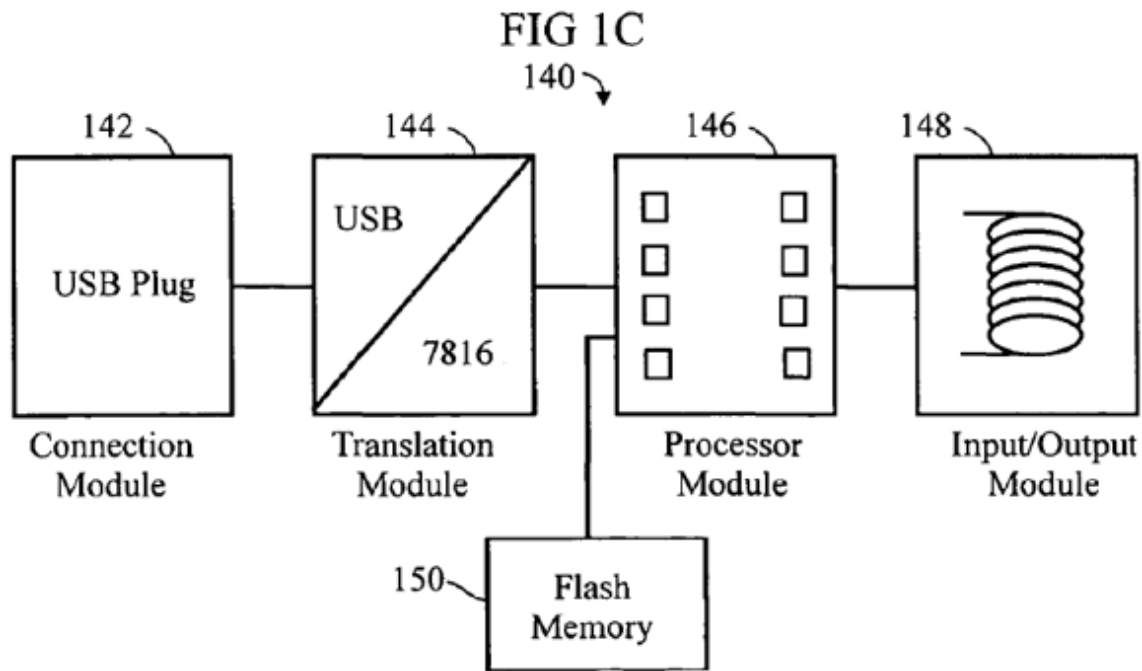
Peart provides further details regarding transaction authorization information comprising an encrypted unpredictable number constructed from a hash of a timestamp or comprising an encryption constructed from a timestamp and a transaction counter. EX1003, ¶100. Peart discloses performing “a secure hashing algorithm on the variable data,” which includes “the time of the transaction” (*timestamp*), to generate “a counter value” that is used “in a pseudo number generator to generate the unpredictable number using a Data Encryption Standard.” EX1008, 6:31-7:10. In Peart, an “RFID reader 104 sends a UN to transaction device 102 at, for example, the start of a payment transaction.” EX1008, 5:35-38. “Transaction device 102 *encrypts the UN* together with other information (a *transaction counter* and a user identifier) using a secret key and sends the transaction to RFID reader 104.” EX1008, 5:38-41. In the Huomo-Kisliakov-Linehan-Peart combination, the authorization request message (*transaction*

authorization information) comprises an encrypted unpredictable number constructed as a hash of a timestamp and an encrypted UN together with other information (*encryption*) constructed from a timestamp and a transaction counter, in accordance with Peart. EX1003, ¶100.

C. GROUND 2—Ryan-Kisliakov-Peart Renders Obvious Claims 23-25

1. Ryan

Ryan describes a “compact personal token apparatus” (e.g., “smart fob”) that bridges the “virtual world of the Internet” and “real world transactions.” *See e.g.*, EX1006, Title, Abstract, 2:7-9, 1:45, 2:31-40, 3:18-23, 5:13-30, 12:58-67, 15:52-55, 29:20-22; EX1003, ¶102. Figure 1C illustrates Ryan’s core modular architecture, comprising four modules—connection module 142 (e.g., USB plug), translation module 144, processor module 146, and input/output (I/O) module 148—arranged in a pipeline and provided on the same mounting structure of token 140. EX1006, 17:35-18:54, FIG. 1A; *see also id.*, 19:24-40, FIG. 1C (the same architecture is extended with flash memory 150, in a “Secure Digital (SD) card format, and including SIM card,” which stores application data and transaction values); EX1003, ¶¶103-107.



2. Ryan-Kisliakov Combination

a) Ryan is Analogous Art to the '345 Patent

Ryan is analogous art to the '345 Patent, both because it is within the same field of endeavor (EX1001, 1:18-24; cl. 1 (“A token”); *supra*, IV.C.1) and because Ryan is reasonably pertinent to the problems the '345 Patent purports to solve.

See, e.g., EX1001, 1:39-45, 4:8-24, 4:29-35, 4:36-50, 4:51-60, 4:61-5:12, 5:18-27, 5:50-56; 10:50-56, 9:24-30, 17:22-44, 18:34-48, 19:40-42; *infra*, IV.C.4; EX1003, ¶108; *see also, supra*, §III.B (application of Ryan by Examiner).

b) A POSITA would have been Motivated to Combine Ryan and Kisliakov

Ryan describes its processor module 106 is “a smartcard processor”

implemented as a dual-interface chip that interfaces “from ISO 7816 (contact interface) to either or both of ISO 14443 and 15693 (contactless interfaces).” EX1006, 18:30-38; *see also, id.*, 18:12-17 (“(moving signals) from USB (the exemplary interface with the computer) to a smart card interface format, such as ISO 7816, and vice-versa.”). Ryan describes the exchanges as “ISO 7816 compliant messages,” and describes the card as functioning both as a smart card and “as a smart card reader (with contacts for reading/writing smart cards).” EX1006, 14:28-39, 20:50-58; *infra*, [23.pre]; EX1003, ¶109.

Ryan expressly identifies the ISO 7816 standard and identifies an example translation component (e.g., “Philips TDA8030 USB/7816”). EX1006, 18:12-17. Ryan repeatedly specifies its interfaces by standard number, including “a standard-compliant smart card contact interface complying to ISO 7816” and an “RFID-contactless interface according to ISO 14443 and ISO 15693.” EX1006, 37:39-40, 14:21-27. In the Ryan-Kisliakov combination, the reader, for example, selects the elementary file holding the cardholder’s transaction data with a SELECT FILE APDU, reads its contents with a READ BINARY APDU, and receives the file’s contents from the secure element's storage, all according to a published specification any conforming card supports. EX1010, [0323], [0414]; EX1003, ¶110. Ryan already has flash memory 150 and EEPROM “powered and addressed by the processor module,” with “memory management for the device ... handled

by a crypto controller operating system” in the dual interface chip; Kisliakov provides express implementation details of the ISO 7816-4 file-system form that addressing takes, and confirms organization of the stored cardholder data in separately selectable elementary files. EX1006, 19:24-30, 19:31-40; EX1010, [0126], [0351]; EX1003, ¶110. For similar reasons discussed above in §IV.A.4, a POSITA would have been motivated to implement Ryan using ISO 7816-4 file system commands, in accordance with Kisliakov. *Id.*

c) A POSITA would have Reasonably Expected Success when Combining Ryan and Kisliakov

The combination amounts to use of a known technique (ISO 7816-4 messaging in accordance with Kisliakov) in a known system (e.g., Ryan’s reader that uses ISO 7816 compliant messaging) to yield predictable results. *KSR*, 550 U.S. at 417; EX1003, ¶111. A POSITA would have had a reasonable expectation of success, especially because the combination would have been implemented primarily through routine software updates. *Id.* Kisliakov describes command formats field by field and card-side process executed in response to each command. EX1010, [0361]-[0373]. Ryan describes communicating over an “ISO 7816 compliant interface” and describes flash memory 50 and EEPROM “powered and addressed by the processor module,” and Kisliakov’s card is a CPU card whose processor likewise executes file-system commands against storage means it

manages. EX1006, 14:28-39, 19:24-30; EX1010, [0268], [0326].

3. Ryan-Kisliakov-Peart Combination

a) A POSITA would have been Motivated to Combine Ryan-Kisliakov-Peart

Ryan already describes transaction environments centered on smart-card-class processing and secure storage, including expressly describing “secret cryptographic keys,” “cryptography” applications, and a “crypto controller...capable of encrypting and decrypting data to be stored in internal or external memory” on its smart token. *See e.g.*, EX1006, 1:29-30, 1:45, 2:3-9, 2:66-67, 10:35-12:39, 19:24-40, 22:24-41, 24:24-26, 24:60-61, 32:23-31; EX1003, ¶112.

Peart addresses the same problem through a seeded cryptographic algorithm producing an “unpredictable number” from “variable data” such as “a counter” and “the time of the transaction,” beneficial for “any environment wherein security of a transaction is required.” *Supra*, §IV.B.1; EX1008, Abstract, 2:21-3:15, 7:22-30; EX1003, ¶113.

A POSITA would have found it obvious to use Peart’s suggestions of a cryptographic algorithm for securing transaction information in the Ryan-Kisliakov system, to promote enhanced secure transaction data transmission, consistent with the express desires of Ryan. EX1006, 1:45, 2:3-9, 2:66-67, 10:35-

12:39, 22:24-41, 24:60-61; EX1003, ¶114. Doing so also furthers Ryan’s secure transaction model and mitigates risks in exposing transaction flows to general-purpose host environments, also mitigating potential security risks at the host interface level. *Id.* For similar reasons discussed above in §IV.B.2, multiple considerations would have led a POSITA to implement this combination. *Id.*

*b) A POSITA would have Reasonably Expected Success when
Combining Ryan-Kisliakov-Peart*

Availing Ryan-Abbott of Peart’s suggestions would have been technically straightforward to a POSITA. EX1003, ¶115. Ryan describes cryptographic computation and secure storage, and Peart specifies a concrete method for generating transaction-specific cryptographic values derived from variable data such as counters and other transaction parameters. *Id.* Peart’s use of standard primitives, e.g., secure hashing and “a data encryption standard operation” aligns with Ryan’s smart-card-class processor environment. EX1006, 4:15-22; EX1008, Abstract. Peart’s teachings can be executed within Ryan-Kisliakov before any transaction information is exposed to external interface. EX1003, ¶115.

4. Analysis

Claim 23

[23.pre]

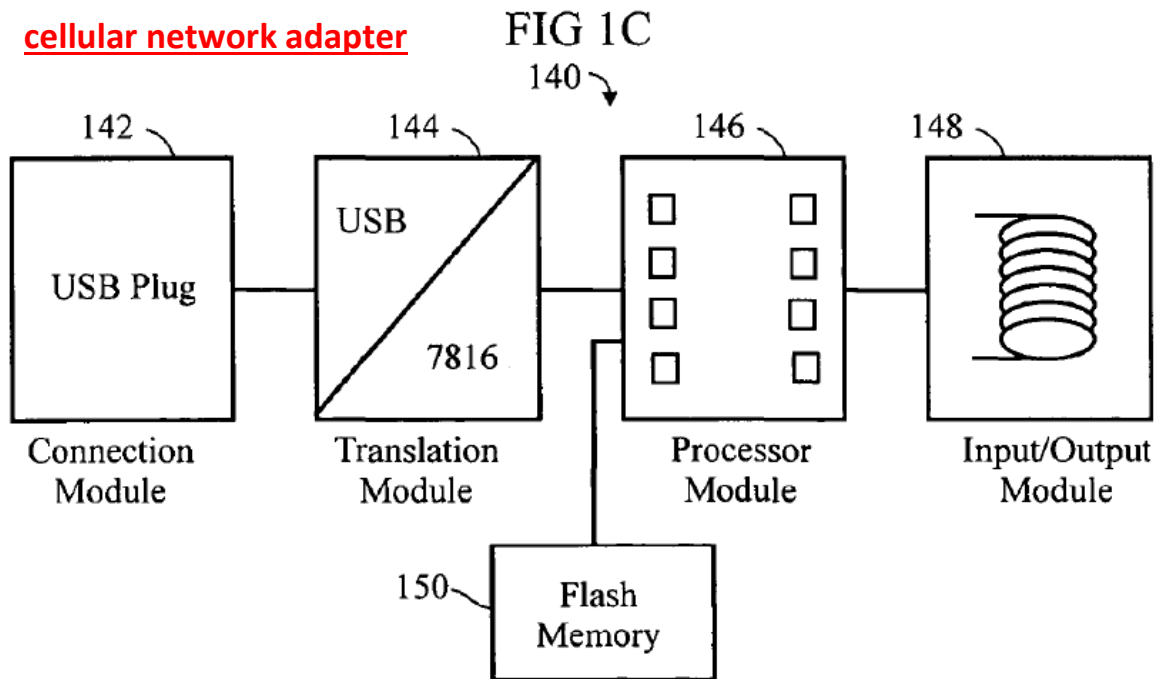
Ryan describes a token which can be connected to “internet capable devices such as[] cell phones” (*cellular network device*) “and interfaced with the virtual

world of the Internet.” EX1006, 13:23-29. Ryan describes the form that token takes when intended for a phone, explaining that “the apparatus of the present invention can be embodied in a format (form factor) such as that of an SD (secure digital) card which can be plugged into any device having an appropriate interface for inserting an SD card, such as a laptop, palmtop, cell phone.” EX1006, 16:4-10. For “an Internet capable mobile phone, a SIM card or SD card format may be preferable.” EX1006, 21:23-31, 15:11-20, 17:47-57, 18:18-22, 19:31-40, 29:6-23. Ryan explains that a SIM card is “inscribed with a customer’s information and designed to be inserted into any mobile telephone” and “contains a user’s GSM mobile account information,” and “SIM card phones work by GSM technology.” EX1006, 10:56-63. Ryan’s token in that form and supplying it with the secure element, reader and transaction capability provides a *cellular network adapter*. EX1003, ¶116.

Ryan describes the token includes “an antenna and tamper-resistant area which can be inserted into handsets for performing” e-commerce and other applications. EX1006, 32:54-63. Although not recited by the plain language of claim 23, Ryan’s token provides an adapter that adds capability to a handset, explaining that “the compact personal token apparatus (or equivalent) may remain in the apparatus capable of interacting with the personal token (e.g., cell phone, PDA), when the personal token device communicates contactlessly in the real

world,” and “[i]t does not necessarily have to be removed from the host device.”

EX1006, 13:39-44; EX1003, ¶117.



EX1006, FIG. 1C

Ryan describes a “handset” (*cellular network device*) that the token is located in. EX1006, 32:54-63. Ryan describes the token connecting to that host through its own connection module, describing the “[t]he apparatus may further comprise a connection module, connecting the personal token apparatus to a host device such as PC, PDA, smart cellular phone or similar device, either directly or with the help of a standard reader device such as a memory card reader.” EX1006, 15:29-33; EX1003, ¶118.

The combination includes a *cellular network application interface*. The ’345 Patent describes that interface as “a baseband input/output port for a web

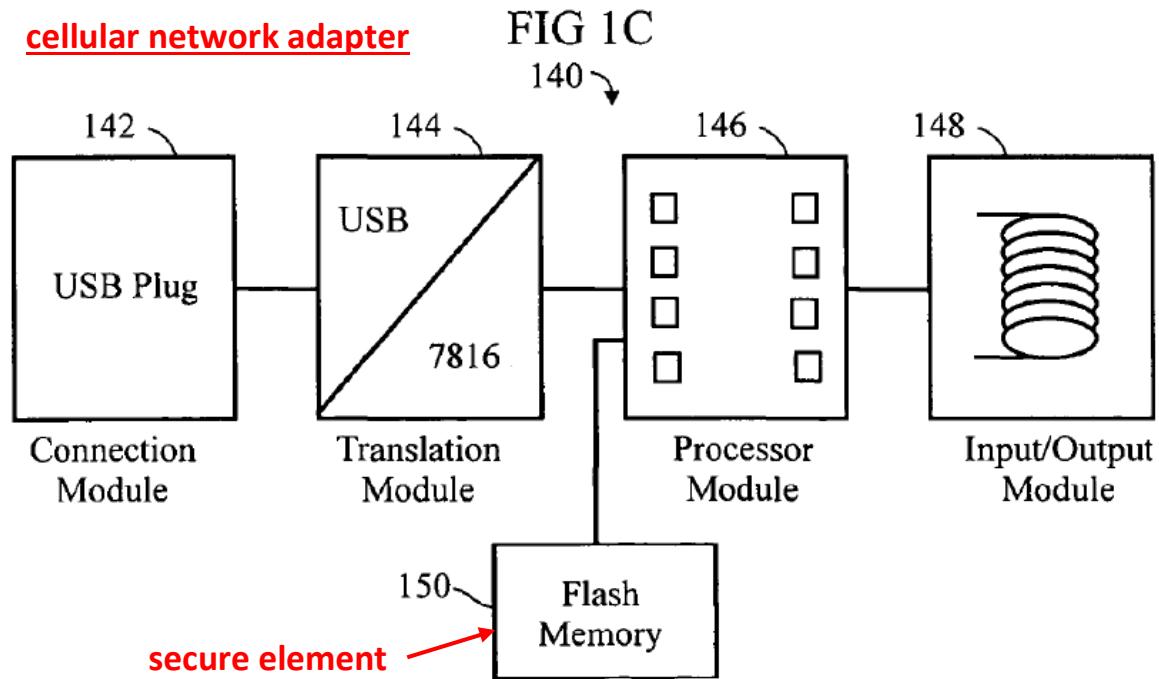
browser running on the cellular network device.” EX1001, 6:58-60. Similarly, Ryan describes the network as cellular, describing “GSM/GPRS.” EX1006, 7:65-67. Ryan describes the data path such a network provides, indicating that “GPRS enabled networks offer ‘always-on’, higher capacity, Internet-based content and packet-based data services.” EX1006, 8:3-9. Ryan describes the token connected to such a handset and reaching the Internet through it, explaining that the apparatus “can be by means of standard-compliant interfaces” connected to “internet capable devices such as; cell phones.” EX1006, 13:23-38. A POSITA would have understood a browser running on such a handset to reach the network through the handset’s own interface. EX1003, ¶119. Indeed, Ryan describes GPRS as enabling “Internet browsing” on the mobile phone network itself, for example. EX1006, 8:3-9.

[23.1]

Ryan’s token (*cellular network adapter*) includes “a flash memory device 150,” which “may be any suitable device including, but not limited to, Secure Digital (SD) card format, and including SIM card” (*secure element*) EX1006, 19:24-40, 15:21-25, 17:35-45, FIGS. 1A, 1C. In the FIG. 1C embodiment, “a flash memory device 150 can be included, with a storage capacity of 1 to 4 megabytes (or more) for the purpose of running applications.” EX1006, 19:31-36; *see also* EX1006, 4:34-47, FIGS. 1A, 1C. Ryan describes that a “flash memory chip” is

“managed by a 32 bit micro-controller.” EX1006, 3:9-13. Based on Ryan’s explicit disclosure of a flash memory chip with its own micro-controller, a POSITA would have found it obvious that the flash memory 150 includes and is managed by a micro-controller, providing a *secure element*. EX1003, ¶120.

Ryan discloses that the token “is capable of loading and storing information from the Internet... to its flash memory” and “could be used to store files... and make payment for services.” EX1006, 17:10-15, 22:14-16; *see also* EX1010, [0126]; EX1003, ¶121. Ryan’s token can include a “tamper-resistance area... for performing various of the e-commerce and other applications.” EX1006, 32:54-63. Additionally, “credit card details can be encrypted and stored in the smart fob,” which would reside in one or more data files (*data file*) of the flash memory or EEPROM. EX1006, 24:24-26, 17:10-15, 22:14-16; EX1003, ¶122.



EX1006, FIG. 1C

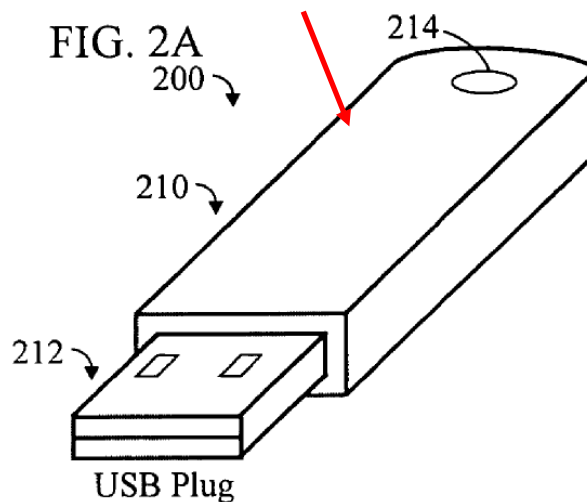
Ryan's token is "embodied in the form of a 'smart fob' apparatus... comprising a main body portion 210 housing the electronics (cf. 104,106, 108) and a USB plug 212 (cf. 102) extending from an end of the body portion 210."

EX1006, 19:45-52. Ryan's flash memory 150 as a SD/SIM card (*secure element*) is in the token (*cellular network adapter*) by, e.g., a secure mechanical engagement holding the secure element on the PCB and within the housing of the main body portion 210 of the token. EX1003, ¶123. A POSITA would have further found obvious that the flash memory is within the token with the processor module for packaging efficiency and physical connection based on Ryan's express description that the memory is powered and addressed by the processor module.

Id.; EX1006, 15:21-24; 19:31-40. Ryan describes that memory residing in the

token together with the processor module that addresses it. *Id.* Ryan explains that the token's "major components, mounted on a circuit board (PCB, not shown) and within a housing (not shown)" include "a processor module 106," and describes the FIG. 1C embodiment 140 as "based on the embodiment 100 of FIG. 1A." EX1006, 17:35-41, 19:24-30, FIGS. 1A, 1C. Ryan describes that "[t]he flash memory could be integrated into the dual interface (DI) chip itself." EX1006, claim 1, 29:35-36. A POSITA would have understood from these descriptions that the memory holding the token's stored credentials would beneficially sit within the same token housing, as the processor module that powers it and addresses it over "an 8 bit address bus," and in any event resides within the token's housing. EX1006, 15:21-24, 17:35-41, 19:31-36; EX1001, 4:15-21; EX1003, ¶123.

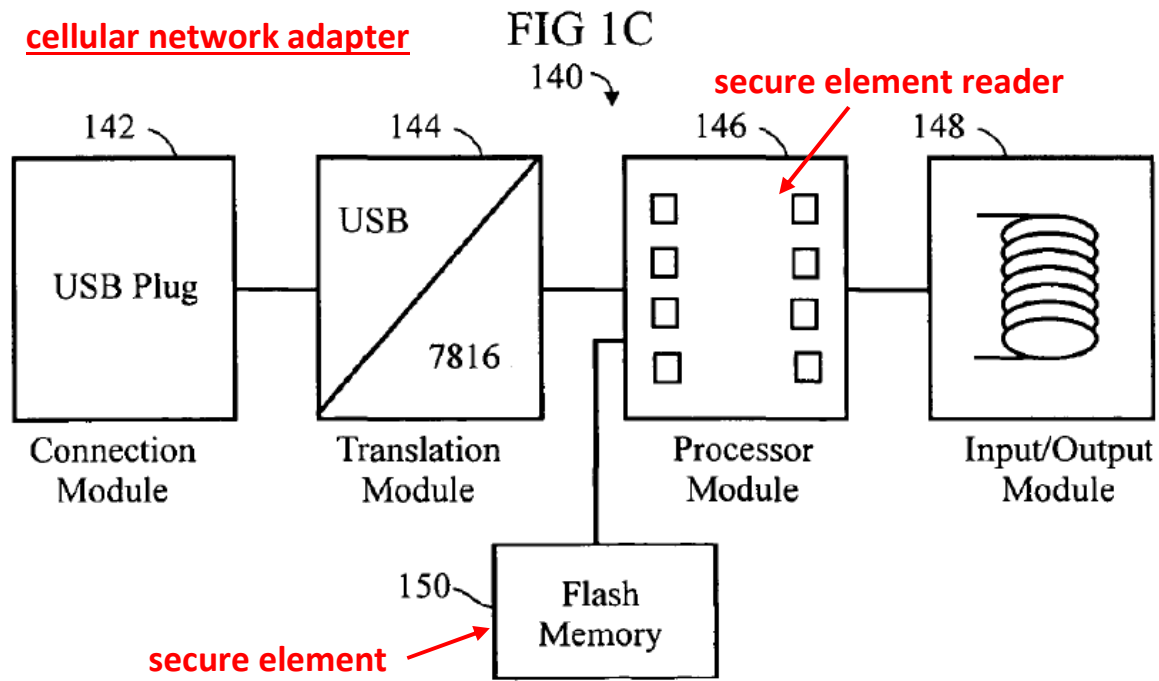
cellular network adapter with secure element



EX1006, FIG. 2A

[23.2]

Ryan's token includes a "processor module 146" (*secure element reader*), "based on the embodiment 100 of FIG. 1A" which includes a "processor module 106," and "flash memory and EEPROM device powered and addressed by the processor module." EX1006, 19:24-30, 17:35-46, 15:21-25; EX1003, ¶124. Ryan's "processor could be mounted in a SIM module" (*in the cellular network adapter*). EX1006, 18:18-22. Ryan discloses that the processor module 106/146 "is for controlling operation of the compact personal token... and is preferably capable of operating as a dual-interface (DI) chip." EX1006, 18:30-38. The processor module 106/146 is for "preparing messages to be sent by the contactless and/or wireless interfaces and interpreting messages received via the interface(s)." EX1006, 15:40-43.



EX1006, FIG. 1C

The processor module 106/146 “can be directly programmed by a software running on the host system using the interface processor without the need for an external contact based dual interface read/write device,” and “information from the web” can be downloaded “directly into the dual interface processor memory.”

EX1006, 14:55-65. The processor module 146 has “a crypto controller operating system” that handles the “memory management” for the flash memory device 150 and EEPROM and is “capable of encrypting and decrypting data to be stored” in the flash memory device 150 and EEPROM. EX1006, 19:31-40. For example, “credit card details can be encrypted and stored in the smart fob.” EX1006, 24:24-26. Ryan discloses that the processor module 106/146 and the output module 148 “is sufficient for conducting real world, contactless transactions, in the manner of a smart card.” EX1006, 20:7-10. For example, the “smart fob can be used as a payment device for retail purchase” and “personalised like a conventional credit/debit card for electronic payment.” EX1006, 24:9-18, 31:5-7 (“store a credit card and/or debit card on the fob to pay for the purchase.”), 31:39-40. A POSITA would have understood, or found it obvious, that the processor encrypting and decrypting credit/debit card data stored in the flash memory 150 for conducting an electronic payment transaction through the wireless and/or contactless interface would involve *interrogating the secure element* (flash memory 150) and

“preparing messages to be sent by the contactless and/or wireless interfaces”

(*generating file information*) from the secure element data file containing the credit/debit card information. *Id.*; EX1006, 15:40-43; EX1003, ¶125.

Ryan discloses that the processor 106/146 “may be mounted in a dual interface card complying to... a 7816 compliant SIM module” and has “an ISO 7816 compliant interface communicating through [an] interface module with the host processing device.” EX1006, 15:11-20, 14:35-37, 18:30-38. A POSITA would have understood that a processor (*secure element reader*) in an ISO 7816 compliant SIM module having an ISO 7816 compliant interface executes file system functions according to ISO 7816-4 and would have found it obvious to use such a processor to interrogate the flash memory 150 or EEPROM of the *secure element*. EX1003, ¶126.

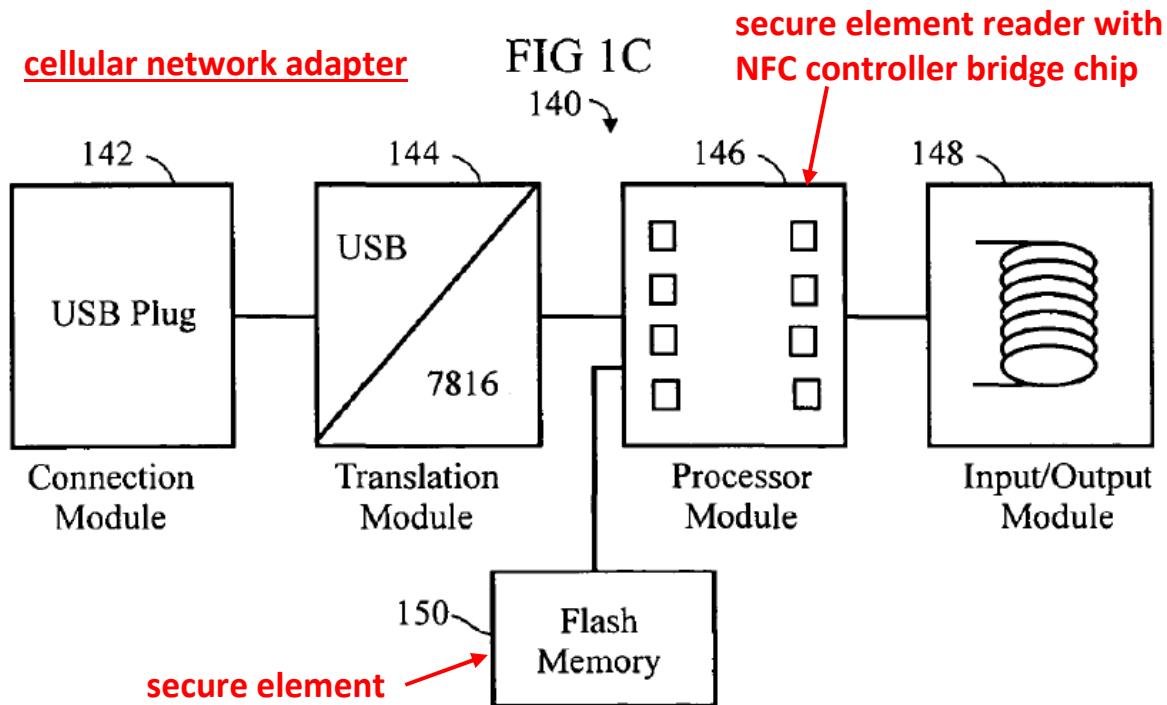
Even if not disclosed by Ryan, in the combined system, a POSITA would have found it obvious to implement the processor module 146 (*secure element reader*) to execute file system functions according to ISO 7816-4 and to use such a processor to interrogate the flash memory 150 of the *secure element*, in accordance with Kisliakov’s teachings. *Supra*, §IV.C.2; EX1003, ¶127.

In describing the processor module addressing the memory, Ryan renders obvious the use of a device that is capable of such interrogation, and configuration of that device as distinct of the structures that are subject of its interrogation

(*secure element reader*). EX1003, ¶128. As such, Ryan additionally renders obvious [23.1] and [23.2] in this manner, even if the processor module and memory together are considered to provide the secure element. *Id.*

[23.3]

Ryan describes that the processor module 106/146 is a dual interface chip having contact and contactless interfaces for “interfacing from ISO 7816 (contact interface) to either or both of ISO 14443 and 15693 (contactless interfaces)” and therefore also functions as a *near field communications controller bridge chip*. EX1006, 18:30-38; EX1003, ¶129. Ryan expressly describes an NFC interface. EX1006, cl. 5, 9:35-46.



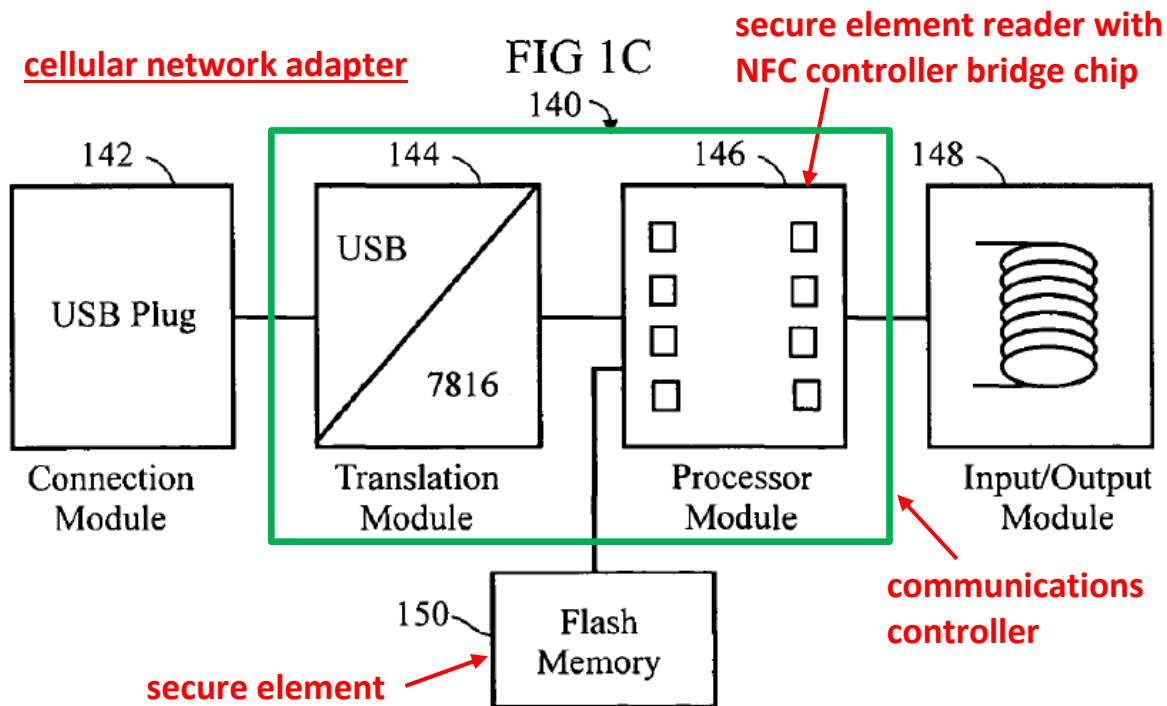
EX1006, FIG. 1C

Ryan describes the chip serves *to convert the file information to an RF data signal for an external reader*. EX1003, ¶130. “[T]he processor module prepares messages to be sent by the contactless and wireless interfaces, and interprets messages received via the contactless and wireless interfaces.” EX1006, cl. 43. Ryan identifies the RF hardware that carries the prepared message (*file information*), indicating that “[t]he output module 108 comprises an RF antenna and a modulator,” a module Ryan describes as “a transceiver module adapted to transmit as well as receive data.” EX1006, 18:39-52. Ryan confirms that stored data reaches that path, explaining that “information exchanged and stored can be accessed in the real world application via its contactless interface.” EX1006, 17:6-26.

As described above, the combined device reads the cardholder’s data from the secure element’s file as ISO 7816-4 file information (*see* [23.2], *supra*), and the chip (e.g., dual interface chip) prepares that information as a message (*file information*) the modulator and RF antenna radiate to the merchant’s reader. EX1003, ¶131. That chip *converts the file information to an RF data signal for an external reader*. *Id.* Indeed, Ryan describes it as the “processor module prepares messages to be sent by the contactless and wireless interfaces.” EX1006, cl. 43, 18:30-38.

[23.4]

Ryan describes Ryan's processor module 106/146 provides the *secure element reader* described in [23.2], and that chip, together with the coupled translation module 104/144, performs the *communications controller* capabilities. See §II.C; see [23.2], *supra*; EX1006, FIGS. 1A, 1C; EX1003, ¶132. Ryan describes the translation module as a controller, explaining that "[a] micro-controller such as an 8 bit micro-controller (ST7 FSCR1E4M1) can be used as an interface translator chip (104) between the USB connection 102 and the processor module 106." EX1006, 18:12-22. And Ryan describes the processor module as the device's controlling component, indicating that "[t]he processor module 106 is for controlling operation of the compact personal token apparatus ('device') of the present invention and is preferably capable of operating as a dual-interface (DI) chip." EX1006, 18:12-38. Ryan describes the two as interchangeable in this respect, teaching that "the processor module (e.g., 106 or 126) could include (incorporate) the translation module (e.g., 104 or 124) within the processor module itself, thus enabling an even more cost effective solution, enabling using a single chip approach for some, or even all of the embodiments discussed herein." EX1006, 19:15-24, FIG. 1B. Based on Ryan's explicit disclosure, it would have been obvious to integrate the processor module and translation module into a single *communications controller*. EX1003, ¶132.



EX1006, FIG. 1C

Ryan describes translation module receiving secure element data over the ISO 7816 link, explaining that it “is for going (moving signals) from USB (the exemplary interface with the computer) to a smart card interface format, such as ISO 7816, and vice-versa.” EX1006, 18:12-15; *see* [23.2], *supra*. In the combined device, the message (*file information*) generated from a credit card number read out of the selected elementary file (*data file*) passes from the reader capability to the controller capability (e.g., across the coupling Ryan shows between translation module 104/144 and processor module 106/146 or within a single merged chip). *See* §II.C; EX1006, 18:12-22, FIGS. 1A, 1C; EX1010, [0326], [0351]; EX1003, ¶133.

Ryan describes the cryptographic capability residing in that same chip set.

EX1003, ¶134. “The memory management for the device may be handled by a crypto controller operating system with an 8 bit address bus in the dual interface (DI) chip,” and that “[a] crypto controller is a processor chip capable of encrypting and decrypting data to be stored in internal or external memory.” EX1006, 19:31-40. In the combined device, the controller capability encrypts the credit card number together with the unpredictable number and transaction counter into a cryptogram the account issuer validates (*transaction authorization information*). EX1006, 19:31-40; EX1008, 5:35-41; EX1003, ¶134; *supra*, §IV.C.3. The credit/debit card number is linked to an issuing bank and a bank account, is used to route messages to the issuing bank, and provides bank account information. EX1003, ¶134 (citing EX1007, 15:40-46).

Peart supplies the cryptographic construction the combined device applies, explaining that “RFID reader 104 sends a UN to transaction device 102 at, for example, the start of a payment transaction,” and “[t]ransaction device 102 encrypts the UN together with other information (a transaction counter and a user identifier) using a secret key and sends the transaction to RFID reader 104.” EX1008, 5:35-41; *supra*, §IV.C.3; EX1003, ¶135. Peart describes the result as issuer-verifiable, teaching that where the issuer’s checks succeed, “the transaction is known to have been generated by a transaction device issued by issuer 112 and

that it has not been tampered with.” EX1008, 5:49-51.

Ryan describes the translation module carrying data outbound toward the host. EX1003, ¶136. Ryan explains that the connection module “is typically for inputting data to the device from the virtual world of the Internet, via the PC or other Internet capable appliance, and in some cases the device can or needs to also output data to the PC.” EX1006, 17:59-62. Ryan also describes path to the host, explaining that “[t]he connection module 102 is for interfacing the device with a personal computer (not shown) apparatus, or other appliance capable of communicating and interacting with remote servers and networks.” EX1006, 17:47-57, FIGS. 1A, 1C. Ryan identifies that appliance as a handset, teaching that the smart SD card is one “which could also include an antenna and tamper-resistant area which can be inserted into handsets for performing various of the e-commerce and other applications mentioned above” (*cellular network device*). EX1006, 32:54-64. Ryan further teaches that the token connects to that host (e.g., handset) “either directly or with the help of a standard reader device such as a memory card reader,” such that a token in SIM or SD format inserts into the handset through the handset's own card slot. EX1006, 15:29-33, 17:47-57, 21:23-31; EX1003, ¶136.

Ryan describes the handset’s own network-facing interface, explaining that “[s]o called smart cellular phones are also Internet enabled devices allowing the user to connect to and browse the world wide web, send and receive email, and

some also incorporate the functionality of a PDA” (*cellular network application interface*). EX1006, 6:13-20, 7:65-67, 12:45-48; *see* [23.pre], *supra*. In the combined device, the translation module 104/144 of the communications controller first transmits the cryptogram with the encrypted credit card number (*transaction authorization information*) out through connection module 102/142 to the handset (*cellular network device*). EX1006, 15:29-33, 17:47-57, 32:54-64. The handset then transmits the cryptogram over the GSM/GPRS mobile phone network (*wireless network comprises a cellular network*) through the handset’s Internet-facing interface (*cellular network application interface*) for authorization. EX1006, 6:13-20, 7:65-8:9, 12:45-48, 15:40-43, 17:47-57; EX1008, 5:35-41. A POSITA would have understood, and found obvious from Ryan’s description, that the combined device sends that cryptogram over the handset’s cellular connection, especially in view of Ryan’s teaching of connection module 102 as reaching an “appliance capable of communicating and interacting with remote servers and networks.” EX1006, 17:47-57; EX1003, ¶137. Ryan’s translation module of the communications controller is configured to transmit the cryptogram (*transaction authorization information*) from the handset (*cellular network device*) over a cellular wireless network through the cellular network application interface by transmitting the cryptogram to the handset that then transmits it over a cellular wireless network through the cellular network application interface. *Id.*

[23.5]

As discussed above, Peart describes receipt of a “UN” (unpredictable number) “at...the start of a payment transaction.” EX1008, 5:1-41. A POSITA would have found it obvious that processor module (*secure element reader*) awaits the UN (*a startup instruction comprising an unpredictable number*) *prior to interrogating the secure element* based on Peart’s teachings that the UN is received at the start of a payment transaction. EX1003, ¶138.

Peart explains that the unpredictable number is “generated and/or regenerated by any one of the computing systems in the transaction stream [e.g.,] at the account issuer 112, acquirer 110, the receiver, or merchant system 132 locations.” EX1008, 7:22-30. Thus, a POSITA would have found it obvious that such unpredictable number is *originating over the cellular wireless network* when the combined device communicates with “account issuer 112, acquirer 110, the receiver, or merchant system 132 locations” over the cellular network. EX1003, ¶139; EX1008, 7:22-30.

Claim 24

[24]

In the combination, the encrypted unpredictable number is constructed as a hash of a timestamp, in accordance with Peart. *Supra*, Ground 1B, Analysis of Claim 24; EX1003, ¶140.

Claim 25

[25]

In the combination, the transaction authorization information comprises an encryption constructed from a timestamp and a transaction counter, in accordance with Peart. *Supra*, Ground 1B, Analysis of Claim 25; EX1003, ¶141.

D. GROUND 3A – Ryan-Hulbert Renders Obvious Claims 11-12

1. Hulbert

Hulbert discloses a portable USB device that operates as a “human interface device (HID)” to automatically deliver structured input to a host computer terminal (e.g., a PC) in the form of keycodes that simulate user keystrokes. EX1011, Abstract, [0019], [0039], [0042], [0073]-[0077]; EX1003, ¶¶142-143.

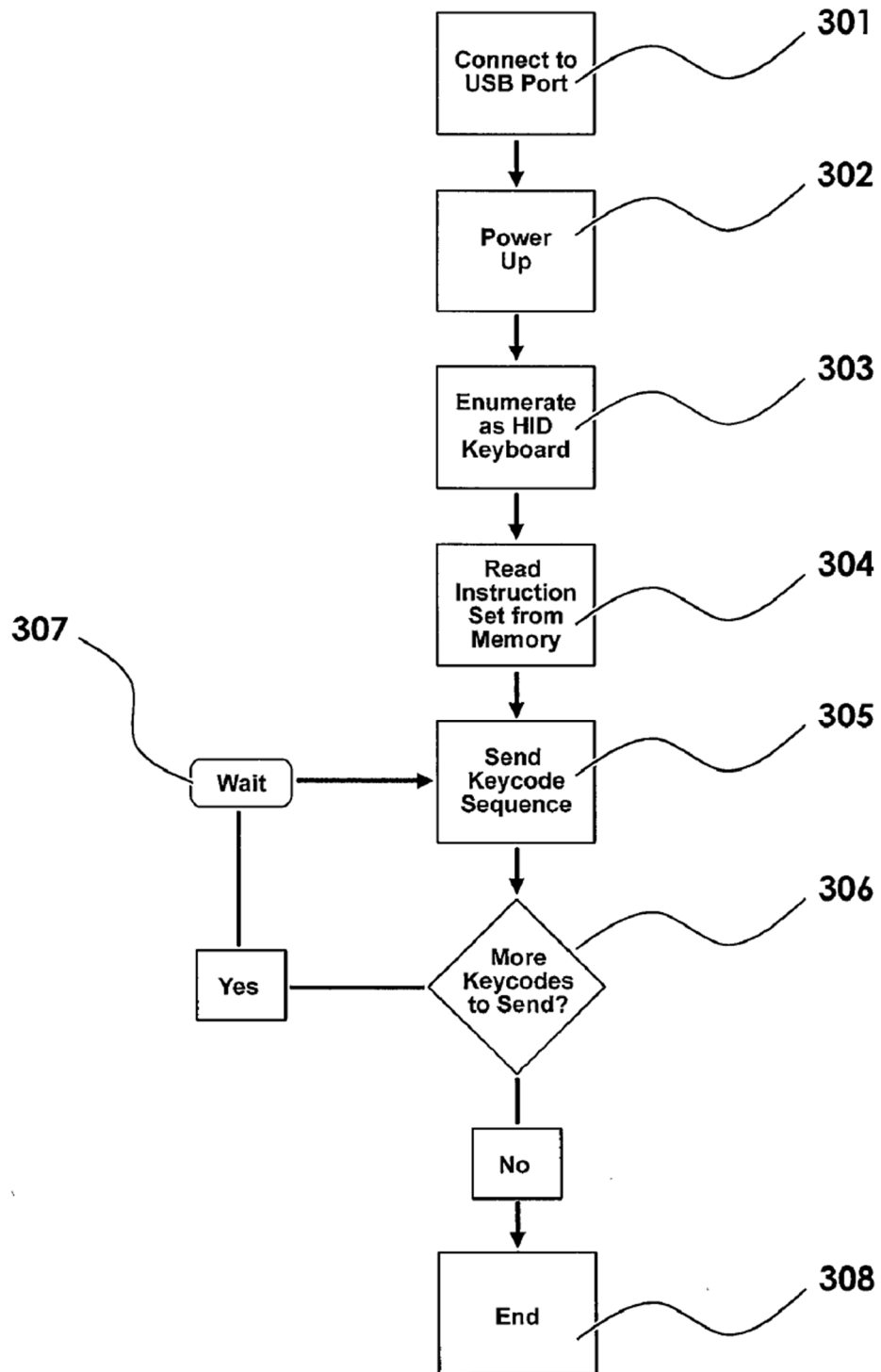


Figure 3

EX1011, FIG. 3

Hulbert explains the sequence of keycodes may perform “data-entry functions (for example, entering a text string into a field on a form),” enabling automatic population of application-defined fields through standard UI pathways. EX1011, [0041]-[0042], [0043]-[0044], [0064], [0065]; EX1003, ¶144. Hulbert describes applications involving authentication and authorization, as the device can transmit “unique data—e.g. data identifying or authenticating a user and/or the apparatus” as part of the keycode sequence, allowing it to participate directly in login and account-access workflows. EX1011, [0020], [0065], [0067], [0068]-[0077]; EX1003, ¶¶145-146.

2. Ryan-Hulbert Combination

a) Hulbert is Analogous Art to the '345 Patent

Hulbert is analogous art to the '345 Patent, both because it is within the same field of endeavor (EX1001, 1:18-24; *supra*, §IV.D.1; EX1011, [0019], [0042], [0053], [0074]-[0077]) and because Hulbert is reasonably pertinent to the problems the '345 Patent purports to solve. *See, e.g.*, EX1001, 4:8-18 (HID keyboard emulation “for inputting a form field or fields on an application running on the PC.”), 5:10-12, 8:9-24, 8:42-45 (“in a prescribed cadence”); EX1011, [0019]-[0020], [0041], [0046] (describing ID keyboard emulation into a form field); *see also* EX1011, [0064]-[0065], [0069], [0077], [0091]-[0093], *supra*, §III.B (application of Hulbert by Examiner); EX1003, ¶147.

b) A POSITA would have been Motivated to Combine Ryan-Hulbert

As discussed above, Ryan describes a multi-interface personal token (e.g., “smart fob”) that connects to a host. *Supra*, §IV.C.1; *see e.g.*, EX1006, Title, Abstract, 15:52-54, FIGS. 1A & 1C. Hulbert provides a host-interaction mechanism based on HID keyboard emulation. *Supra*, §IV.D.1; *see e.g.*, EX1011, Abstract, [0041]; EX1003, ¶148.

Hulbert describes this capability within transaction-oriented contexts involving authentication and authorization, recognizing associated security considerations. *Supra*, §IV.D.1; EX1011, [0065]-[0077]; EX1006, 28:1-7; EX1003, ¶149.

A POSITA would have found it obvious to incorporate Hulbert’s suggestions related to HID USB keyboard emulation into Ryan, e.g., Ryan’s “interface processor, communicatively coupled to the USB-compliant interface and to the smartcard processor-compliant interface,” to promote functional synergy with host-side automation of transaction data, and interoperability and portability advantages. EX1006, 4:34-47. Multiple considerations would have led a POSITA to implement this combination. EX1003, ¶150.

First, availing Ryan’s system of Hulbert’s suggestions would have predictably enhanced how Ryan interacts with host applications, especially for data

entry and transaction initiation. EX1003, ¶151. Ryan already contemplates using the token for transactions such as “e-payment and similar applications.” *See e.g.*, EX1006, Abstract, 3:24-35, 14:66-15:4, 17:15-17, 22:24-43, 23:19-24, 23:66-24:8. A POSITA would have recognized from Hulbert its benefit of promoting direct, application-agnostic control of the host UI via keystrokes, which can launch applications, input URLs, and “enter...a text string into a field on a form.” *See e.g.*, EX1011, [0041], [0064]-[0067]; EX1003, ¶151. Ryan’s token uses Hulbert’s suggestions of HID sequences to automatically populate login forms, payment fields, or transaction interfaces on any host system, without requiring installation of Ryan-specific client software, or reliance on auto-run, as Hulbert motivates HID-based input as promoting a universally compatible approach. EX1011, [0018]. Doing so furthers Ryan’s stated objective of interacting with any “host processing device...under command of an operating system.” EX1006, 4:35-38; EX1003, ¶151.

Second, incorporating Hulbert into Ryan would further enhance cross-platform compatibility, consistent with Ryan’s design philosophy of multi-interface interoperability. EX1006, Title. Hulbert’s device leverages standardized HID protocols and thus “does not require unique software or drivers,” allowing it to function with “any personal computer terminal running common Operating System software.” EX1011, [0020], [0046]. By emulating a generic

keyboard and using the “method determined by the operating system or application,” the solution facilitates use across heterogeneous platforms. EX1011, [0042] (“agreed standards for communication”), [0046]; EX1003, ¶152.

c) A POSITA would have Reasonably Expected Success when Combining Ryan-Hulbert

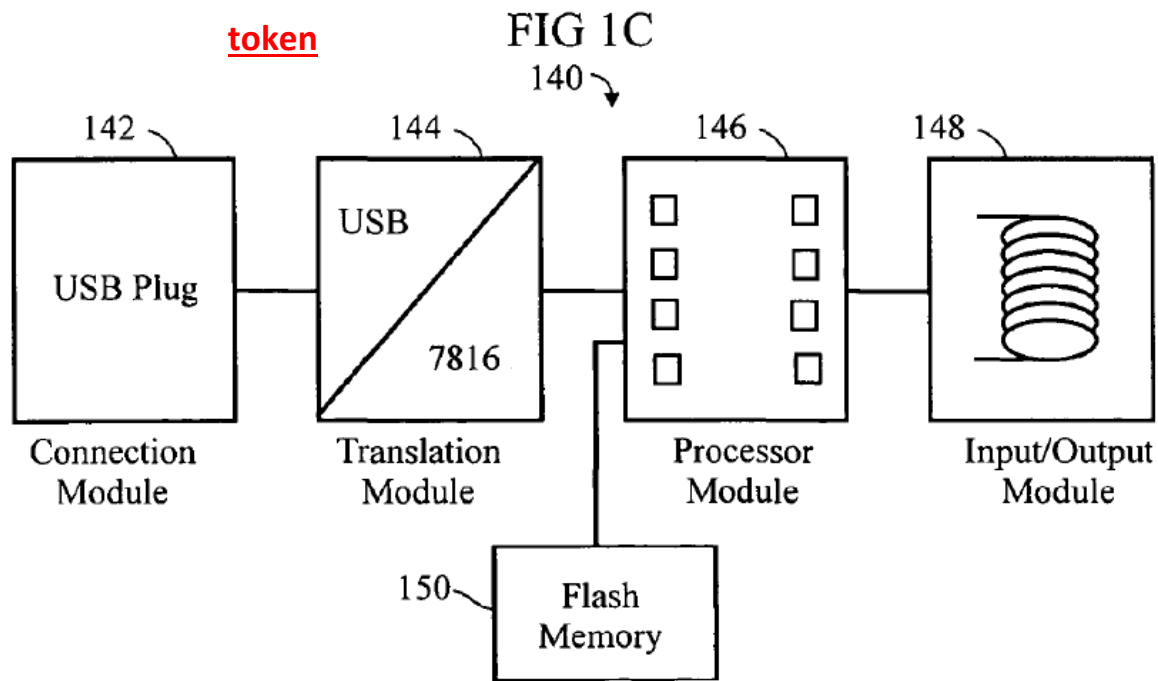
A POSITA would have expected success in implementing the combination, especially since Ryan contemplates USB-based host communication and protocol translation, architecturally compatible with Hulbert’s approach. EX1003, ¶153. Hulbert’s HID operation provides another standard USB device profile, such that the combination’s translation or connection module would handle USB HID keycode output as another standardized communication path. *Id.*

3. Analysis

Claim 11

[11.pre]

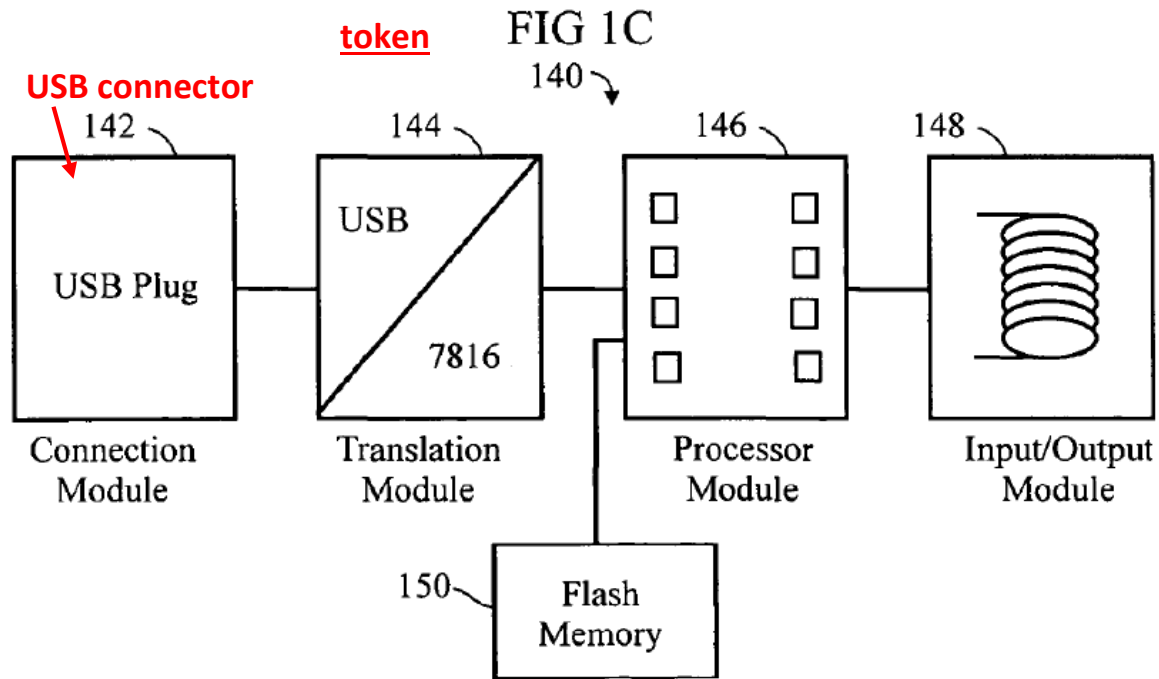
Ryan discloses a “token apparatus.” *See e.g.*, EX1006, Title, Abstract, 12:58-13:9, 15:52-16:10, 17:27-19:40, FIGS. 1A, 1C; EX1003, ¶154.



EX1006, FIG. 1C

[11.1]

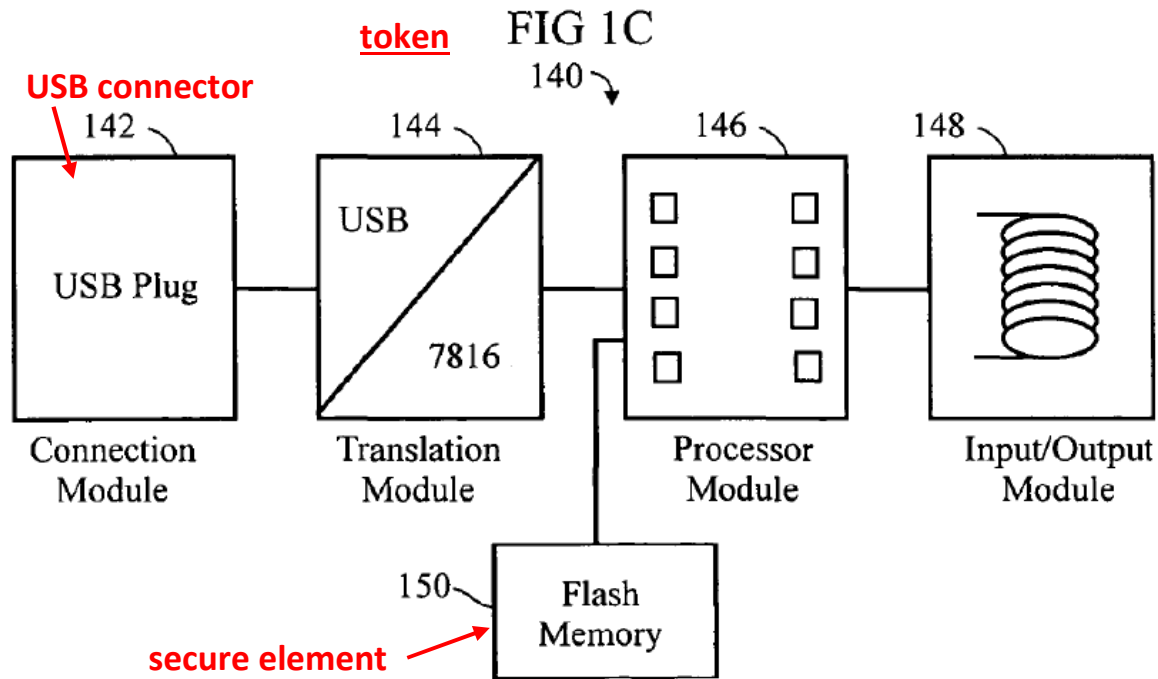
Ryan explains that the token's major components are "mounted on a circuit board (PCB...) and within a housing" (*mounting structure*), and the token has a "connection module" 102/142 (e.g., "a USB plug") (*Universal Serial Bus (USB) connector*) "for plugging directly into a personal computer (PC)" (*computer terminal*). EX1006, 4:34-47, 17:35-57, 15:29-33, FIG. 1C (reproduced below); EX1003, ¶155.



EX1006, FIG. 1C

[11.2]

Ryan describes that the secure element comprises a data file. *Supra*, Ground 2, [23.1]; EX1003, ¶156.

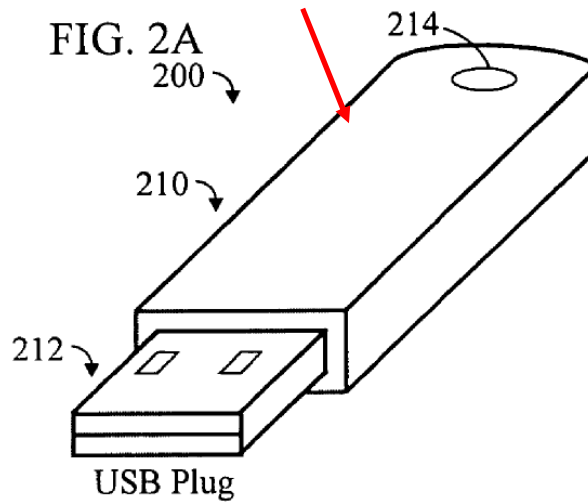


Ryan's token is "embodied in the form of a 'smart fob' apparatus... comprising a main body portion 210 housing the electronics (cf. 104,106, 108) and a USB plug 212 (cf. 102) extending from an end of the body portion 210."

EX1006, 19:45-52. Ryan's flash memory 150 as a SD/SIM card (*secure element*) is *affixed to the mounting structure* by, e.g., a secure mechanical engagement holding the secure element on the PCB and within the housing (*mounting structure* per [11.1]) of the main body portion 210 of the token. EX1003, ¶157. A POSITA would have further found obvious that the flash memory is beneficially affixed to the mounting structure with the processor module for packaging efficiency and physical connection based on Ryan's express description that the memory is powered and addressed by the processor module. EX1006, 15:21-24;

19:31-40. Ryan describes that memory residing on the token's mounting structure together with the processor module that addresses it. Ryan explains that the token's "major components, mounted on a circuit board (PCB, not shown) and within a housing (not shown)" include "a processor module 106," and describes the FIG. 1C embodiment 140 as "based on the embodiment 100 of FIG. 1A." EX1006, 17:35-41, 19:24-30, FIGS. 1A, 1C. Ryan describes that "[t]he flash memory could be integrated into the dual interface (DI) chip itself." EX1006, claim 1, 29:35-36. A POSITA would have understood from these descriptions that the memory holding the token's stored credentials would beneficially sit on the same circuit board, within the same housing, as the processor module that powers it and addresses it over "an 8 bit address bus," and in any event resides within the token's housing (*mounting structure*), which the '345 Patent describes as "a packaging case (for fobs, cartridges, and dongles or SD chips)." EX1006, 15:21-24, 17:35-41, 19:31-36; EX1001, 3:42-44; EX1003, ¶157.

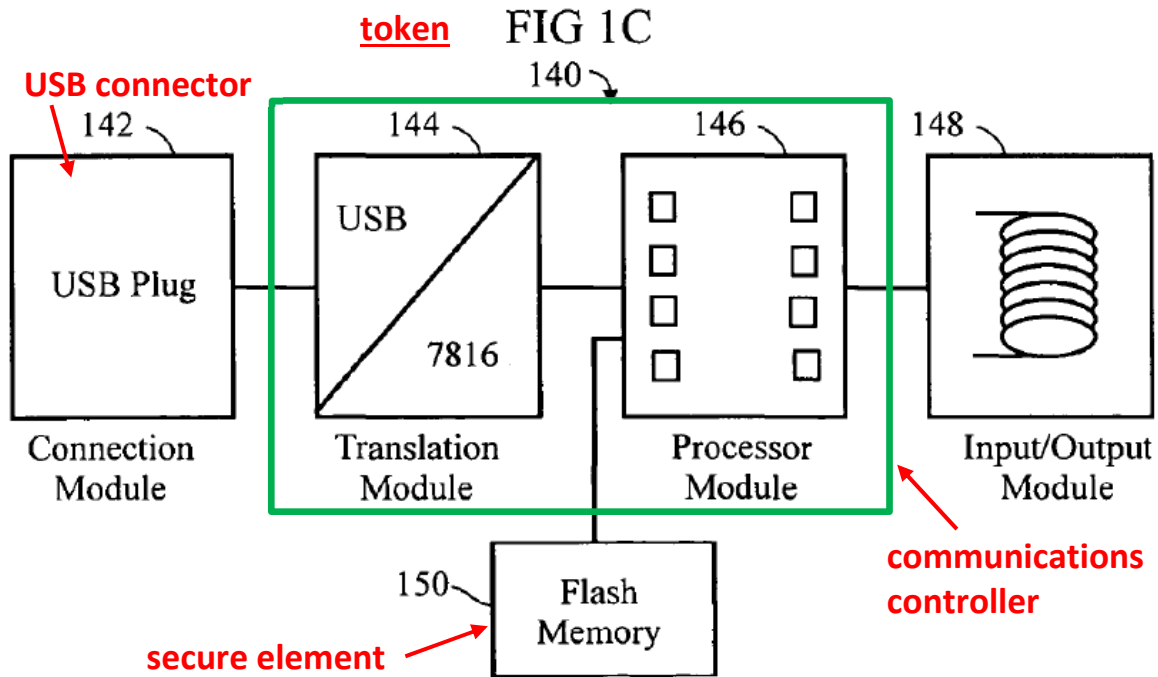
token with mounting structure on/within which
secure element is affixed



EX1006, FIG. 2A

[11.3]

Ryan's processor module 106/146 together with the coupled translation module 104/144 performs the *communications controller* capabilities. See §II.C; see Ground 2, [23.2], [23.4], *supra*; EX1006, FIGS. 1A, 1C. The processor module 106/146 and translation module 104/144 are mounted on the “circuit board” of the token housing (*mounting structure*). EX1006, 17:35-41, FIGS. 1A, 1C; EX1003, ¶158.



EX1006, FIG. 1C

As discussed above in Ground 2, [23.2], the processor module 106/146 of the *communications controller* extracts credit card information from the secure element data file. EX1003, ¶159. As discussed above in Ground 2, [23.4], the *communications controller* converts at least a portion of the data file into transaction information. *Id.*

In the Ryan-Hulbert combination, the translation module of the *communications controller* uses HID USB keyboard emulation (*configured as a Human Interface Device (HID) class USB-device*) in accordance with Hulbert, for enhanced interaction with host applications and multi-interface interoperability. *Supra*, §IV.D.2; EX1003, ¶160.

Ryan-Hulbert's *communications controller* converts the credit card information in the data file stored in the smartcard memory into *transaction information*. EX1006, 3:18-24, 28:30-37; EX1011, [0065]-[0067]; *supra*, §IV.D.2. The combination's *communications controller* then transmits such transaction information to the host computer (*computer terminal*) through the "connection module," e.g., "USB plug" (*USB connector*) as keyboard emulation, where the *communications controller* is configured to provide the transaction information *in a format that auto-populates a form field defined by an application* (e.g., Hulbert's "application 107") running on the host computer. *Supra*, §§IV.D.1-IV.D.2; EX1006, 2:61-64 ("multi-functional smart cards in applications such as... banking etc."), 11:20-24, 14:66-15:2, 28:1-7; EX1011, Abstract, [0041], [0042], [0043]-[0044], [0046], [0064], [0065]; EX1003, ¶161.

Claim 12

Hulbert describes "a first predefined sequence" (*a prescribed cadence*) of keycodes that is "determined by the operating system or application" on the host computer (*for an application running on the computer terminal*) and "recognised by the application, which would perform the associated task or process." EX1011, Abstract, [0019], [0042]-[0046], [0064], [0093]. Hulbert also describes a "second series of timed keycodes" (or "second sequence of [HID] keycodes") (*a prescribed cadence*) that is "interpreted by the Operating System as a sequence of keystrokes

that represent data entry to the application 107 in the form of a text string URL (Universal Resource Locator).” EX1011, [0065], [0093], [0136], claims 3-4; EX1003, ¶162.

Hulbert explains, “[t]he first and/or second set of keycodes (or any other set) can include unique data—e.g. data identifying or authenticating a user and/or the apparatus 102.” EX1011, [0065]. A POSITA would have found it obvious that at least one set of such “timed keycodes” in the combined system contains the *transaction information* extracted from the *secure element*, as discussed for Element [11.3] with examples. *Supra*, §§IV.D.1-IV.D.3, Element [11.3]; EX1006, 3:18-24, 28:30-37; EX1011, [0065]-[0067]; EX1003, ¶163.

E. GROUND 3B – Ryan-Hulbert-Peart Renders Obvious Claims 13-22

1. Ryan-Hulbert-Peart Combination

As discussed for the Ryan-Kisliakov-Peart Combination (Ground 2), a POSITA would have been motivated to integrate Peart’s cryptographic algorithm for securing transaction information into Ryan (and Ryan-Hulbert), for enhanced secure transaction data transmission. *Supra*, §IV.C.3; EX1003, ¶164.

2. Analysis

Claim 13

Ryan-Hulbert-Peart teaches that the secure element data file comprises financial authorization data and that the communications controller is configured to

extract at least a portion of the financial authorization data. *Supra*, Ground 2, [23.2], [23.4]. Ryan-Hulbert-Peart also teaches that the communications controller encrypts at least a portion of the financial data and transmits the encrypted financial authorization data for transmission as transaction information to the computer terminal through the USB connector. *Supra*, Ground 2, [23.4], [24], [25]; EX1003, ¶165.

Claim 14

In the combination, the encrypted unpredictable number is constructed as a hash of a timestamp, in accordance with Peart. *Supra*, Ground 1B, Analysis of Claim 24; EX1003, ¶166.

Claim 15

In the combination, the transaction information comprises an encryption constructed from a timestamp and a transaction counter, in accordance with Peart. *Supra*, Ground 1B, Analysis of [25]; EX1003, ¶167.

Claim 16

Supra, Ground 2, [23.5]. EX1003, ¶168.

Claim 17

[17.pre]

Supra, Analysis of [11.pre]. EX1003, ¶169.

[17.1]

Supra, Analysis of [11.1]. EX1003, ¶170.

[17.2]

Supra, Analysis of [11.2]. EX1003, ¶171.

[17.3]

Supra, Analysis of [11.3]. EX1003, ¶172.

[17.4]

Supra, Analysis of [13]. EX1003, ¶173.

[17.5]

Supra, Analysis of [11.3]. EX1003, ¶174.

Claim 18

Supra, Analysis of [12]. EX1003, ¶175.

Claim 19

[19.pre]

Supra, Analysis of [11.pre]. EX1003, ¶176.

[19.1]

Supra, Analysis of [11.1]. EX1003, ¶177.

[19.2]

Supra, Analysis of [11.2], [13] (financial authorization data). EX1003, ¶178.

[19.3]

Supra, Analysis of [11.3], [13], [14]. EX1003, ¶179.

Claim 20

Supra, Analysis of [12]. EX1003, ¶180.

Claim 21

Supra, Analysis of [15]; Ground 1B, Analysis of [25]. EX1003, ¶181.

Claim 22

Supra, Analysis of [16]; Ground 2, Analysis of [23.5]. EX1003, ¶182.

F. GROUND 3C – Ryan-Hulbert-Peart-Kisliakov Renders Obvious Claims 1-10

1. Ryan-Hulbert-Peart-Kisliakov Combination

Kisliakov supplies ISO 7816-4 file-system access to the secure element, which Ryan already has “powered and addressed by the processor module”. *Supra*, §IV.C.2; Ground 2, [23.2]; EX1006, 19:24-30; *see also supra*, §IV.E.1; EX1006, 14:30-35, 27:19-23, 34:66-35:3; EX1003, ¶183. Combination with Kisliakov results in communications in APDU format “as described in the ‘ISO/IEC 7816-4 Standards,’ without compromising the HID USB keyboard emulation integrated from Hulbert or the cryptographic algorithm for securing transaction information integrated from Peart, to obtain predictable benefits described above. *Supra*, IV.C.2; EX1010, [0268]; EX1003, ¶183.

2. Analysis

Claim 1

[1.pre]

Supra, Analysis of [11.pre]. EX1003, ¶184.

[1.1]

Supra, Analysis of [11.1], [19.1]. EX1003, ¶185.

[1.2]

Supra, Analysis of [11.2]. EX1003, ¶186.

[1.3]

Ryan describes a “processor module” (106/146) (*secure element reader*) mounted on the “circuit board” (*affixed to the mounting structure*), and in the combination, the processor module (*secure element reader*) is configured to interrogate the secure element by executing file system functions comprising a command to select a payment card application according to ISO 7816-4 and to generate file information from the secure element data file. *Supra*, Ground 2, [23.2]; EX1010, [0275]-[0276] (“application identifier,” “SELECT FILE command”); *see also* EX1010, [0236], [0245], [0263], [0268], [0275]-[0276], [0323]; EX1003, ¶¶187-188.

[1.4]

Ryan-Hulbert-Peart Kisliakov teaches a communications controller affixed to the mounting structure and configured as a Human Interface Device (HID) class USB-device (*supra*, [11.3]) and the communication connector is a Universal Serial Bus (USB) connector (*supra*, [11.1]). EX1003, ¶189. In the combination, the translation module of the communications controller is configured to receive the file information from the secure element reader, convert at least a portion of the

file information into transaction information, transmit the transaction information to the computer terminal through the communications connector, and to provide the transaction information in a format that auto-populates a form field defined by an application running on the computer terminal. *Supra*, [11.3]; EX1003, ¶189.

Claim 2

Supra, Analysis of [12]. EX1003, ¶190.

Claim 3

Supra, Analysis of [13]. EX1003, ¶191.

Claim 4

Supra, Analysis of [13]. EX1003, ¶192.

Claim 5

Supra, Analysis of [12]. EX1003, ¶193.

Claim 6

Supra, Analysis of [14]. EX1003, ¶194.

Claim 7

Supra, Analysis of [15]. EX1003, ¶195.

Claim 8

Supra, Analysis of [16]. EX1003, ¶196.

Claim 9

[9.pre]

Supra, Analysis of [11.pre]. EX1003, ¶197.

[9.1]

Supra, Analysis of [1.1]. EX1003, ¶198.

[9.2]

Supra, Analysis of [1.2]. EX1003, ¶199.

[9.3]

Supra, Analysis of [1.3]. EX1003, ¶200.

[9.4]

Supra, Analysis of [1.4]. EX1003, ¶201.

[9.5]

Supra, Analysis of [3]. EX1003, ¶202.

[9.6]

Supra, Analysis of [1.4]. EX1003, ¶203.

Claim 10

Supra, Analysis of [2]; EX1003, ¶204.

V. CONCLUSION AND FEES

The Challenged Claims are unpatentable. Petitioners authorize charge of fees to Deposit Account 06-1050.

VI. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1)

A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)

Apple Inc., Samsung Electronics Co., Ltd., and Samsung Electronics America, Inc. are the real parties-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The '345 Patent is the subject of civil actions *Mobility IP Holdings, Inc. v. Apple Inc.*, No. 7:26-cv-00075 (W.D. Tex. Mar. 4, 2026) and *Mobility IP Holdings, Inc. v. Samsung Electronics Co, Ltd. and Samsung Electronics America, Inc.*, No. 2:26-cv-157 (E.D. Tex. Feb. 27, 2026). Petitioners are not aware of any disclaimers, reexamination certificates, or IPR petitions addressing the '345 Patent.

C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Petitioners provide the following designation of counsel.

Lead Counsel	Backup counsel
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email: IPR50095-0309IP@fr.com	Andrew B. Patrick, Reg. No. 63,471 Kim H. Leung, Reg. No. 64,399 Craig A. Deutsch, Reg. No. 69,264 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 IPR50095-0309IP@fr.com

D. Service Information

Please address all correspondence and service to the address listed above.

Petitioners consent to electronic service by email at IPR50095-0309IP@fr.com.

Respectfully submitted,

Dated: September 18, 2026

/W. Karl Renner/

W. Karl Renner, Reg. No. 41,265
Andrew B. Patrick, Reg. No. 63,471
Kim H. Leung, Reg. No. 64,399
Craig A. Deutsch, Reg. No. 69,264
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2026-00500)

Counsel for Petitioners

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for Inter Partes Review totals 13,812 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated: September 18, 2026

/W. Karl Renner/

W. Karl Renner, Reg. No. 41,265
Andrew B. Patrick, Reg. No. 63,471
Kim H. Leung, Reg. No. 64,399
Craig A. Deutsch, Reg. No. 69,264
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Counsel for Petitioners

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) et seq. and 42.105(b), the undersigned certifies that on September 19, 2026, a complete and entire copy of this Petition for Inter Partes Review and all supporting exhibits were provided by Federal Express, to the Patent Owner, by serving the correspondence address of record as follows:

BUCHALTER
18400 VON KARMAN AVE.
SUITE 800
IRVINE, CA 92612
(949) 760-1121

/Crena Pacheco/

Crena Pacheco
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
pacheco@fr.com