

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: C. Douglas Yeager
U.S. Patent No.: 8,548,924
Issue Date: October 1, 2013
Appl. Serial No.: 13/403,141
Filing Date: February 23, 2012
Title: SELF-AUTHORIZING TOKEN

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. 8,548,924
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 '924 PATENT	4
	A. Brief Description.....	4
	B. Prosecution History.....	4
IV.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	5
	A. GROUND 1A – Huomo-Smets Renders Obvious Claims 1-71 and 76-87	
		5
	1. Huomo	5
	2. Smets	7
	3. Huomo-Smets Combination.....	9
	a) Huomo and Smets are Analogous Art to the '924 Patent	9
	b) A POSITA would have been Motivated to Combine Huomo and Smets	9
	c) A POSITA would have Reasonably Expected Success when Combining Huomo and Smets	13
	4. Analysis	13
	a) First Mapping	14
	b) Second Mapping.....	16
	a) First Mapping	18
	b) Second Mapping.....	19
	a) First Mapping	21
	b) Second Mapping.....	22
	a) First Mapping	22
	b) Second Mapping.....	25
	a) First Mapping	29
	b) Second Mapping.....	30

a)	First Mapping	33
b)	Second Mapping.....	34
a)	First Mapping	36
b)	Second Mapping.....	37
a)	First Mapping	44
b)	Second Mapping.....	44
a)	First Mapping	45
b)	Second Mapping.....	45
B.	GROUND 1B – Huomo-Smets-Kisliakov Renders Obvious Claims 1-71, 76-87	45
1.	Kisliakov	45
2.	Huomo-Smets-Kisliakov Combination.....	46
c)	Kisliakov is Analogous Art to the '924 Patent.....	46
d)	A POSITA would have been Motivated to Combine Huomo-Smets-Kisliakov	46
e)	A POSITA would have Reasonably Expected Success when Combining Huomo-Smets and Kisliakov	48
3.	Analysis	48
C.	GROUND 2A – Ryan-Abbott Renders Obvious Claims 1-2, 4, 6-8, 22-23, 25, 27-29, 31-32, 34, 36-38, 52-53, 55-58, 60-61, 63-64, 66-77, 79-82, and 84-86	50
1.	Ryan.....	50
2.	Abbott.....	51
3.	Ryan-Abbott Combination	52
a)	Ryan and Abbott are Analogous Art to the '924 Patent	52
b)	A POSITA would have been Motivated to Combine Ryan and Abbott	53
c)	A POSITA would have Reasonably Expected Success	56
4.	Analysis	57
D.	GROUND 2B – Ryan-Abbott-Peart Renders Obvious Claims 3, 5, 9-13, 16-19, 21, 24, 26, 30, 33, 35, 39-43, 46-49, 51, 54, 59, 62, 78, and 87	75
1.	Peart.....	75
2.	Ryan-Abbott-Peart Combination.....	75
a)	Peart is Analogous Art to the '924 Patent.....	75

b)	A POSITA would have been Motivated to Combine Ryan-Abbott-Peart	76
c)	A POSITA would have Reasonably Expected Success	78
3.	Analysis	78
E.	GROUND 2C – Ryan-Abbott-Smets Renders Obvious Claims 65, and 83	80
1.	Ryan-Abbott-Smets Combination	80
2.	Analysis	84
F.	GROUND 2D – Ryan-Abbott-Peart-Smets Renders Obvious Claims 15, 20, 45, 50.....	85
1.	Analysis	85
	Claims 15, 20, 45, 50	85
G.	GROUND 2E/2F – Ryan-Abbott-Smets-Kisliakov Renders Obvious Claims 2, 23, 32, 53, 61, 80 / Ryan-Abbott-Peart-Smets-Kisliakov Renders Obvious Claims 11, 41	85
1.	Combination	85
2.	Analysis	86
V.	CONCLUSION AND FEES	86
VI.	MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1).....	86
A.	Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1).....	87
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2)	87
C.	Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3).....	87
D.	Service Information	87

LIST OF EXHIBITS

EX1001	U.S. Patent No. 8,548,924 (“’924 Patent”)
EX1002	Excerpts from the Prosecution History of the ’924 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	U.S. Patent Appl. Pub. No. 2006/0022033 to Smets et al. (“Smets”)
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. 2003/0212896A1 to Kisliakov (“Kisliakov”)
EX1011	RESERVED
EX1012	ISO/IEC 7816-4 Second edition (2005). Available at https://www.freecalypso.org/pub/GSM/ISO7816/ISO_7816-4_2005.pdf
EX1013	U.S. Patent Appl. Pub. No. 2009/0119516 to Tanabiki et al. (“Tanabiki”)
EX1014	U.S. Patent Appl. Pub. No. 2004/0139021 to Reed et al. (“Reed”)

EX1015	U.S. Patent Appl. Pub. No. 2008/0073426 to Koh et al. (“Koh”)
EX1016	ISO/IEC 14443-4 First edition (2001). Available at: http://www.emutag.com/iso/14443-4.pdf
EX1017	U.S. Patent Appl. Pub. No. 2005/0212690 to Nishikawa (“Nishikawa”)
EX1018	U.S. Patent Appl. Pub. No. 2006/0255160 to Winkler (“Winkler”)
EX1019 – 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, <i>Mobility IP Holdings, Inc. v. Samsung Electronics Co, Ltd. and Samsung Electronics America, Inc.</i> , 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	
[1.pre]	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 interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging a plurality of transaction data communications only between the secure element and the secure element interrogator; and
[1.4]	a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information as a single data communication to the computer terminal through the communications connector.
Claim 2	
[2]	The token of claim 1 wherein the plurality of transaction data communications comprises communications formatted according to ISO 7816-4.
Claim 3	
[3]	The token of claim 1 wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.
Claim 4	
[4]	The token of claim 1 wherein the secure element interrogator exchanges the plurality of transaction data communications with the secure element only within libraries or memory space residing on the mounting structure.

Claim 5	
[5]	The token of claim 1 wherein the secure element comprises a payment card application and the single data communication to the computer terminal comprises track data.
Claim 6	
[6]	The token of claim 1 wherein communications to and from the secure element consist of communications from and to a secure element reader.
Claim 7	
[7]	The token of claim 1 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.
Claim 8	
[8.1]	The token of claim 1 wherein: the secure element comprises an executable application; and
[8.2]	the secure element interrogator is configured to interrogate the executable application to acquire the transaction information from the data file.
Claim 9	
[9.1]	The token of claim 1 wherein: the secure element comprises a payment card application;
[9.2]	the secure element interrogator is configured to interrogate the payment card application; and
[9.3]	the transaction information comprises card-present data.
Claim 10	
[10.pre]	A token comprising:
[10.1]	a mounting structure having a communication connector configured to connect to a computer terminal;
[10.2]	a secure element affixed to the mounting structure, the secure element comprising a payment card application and a data file;
[10.3]	a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging a plurality of

	transaction data communications only between the secure element and the secure element interrogator; and
[10.4]	a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information as track data to the computer terminal through the communications connector.
Claim 11	
[11]	The token of claim 10 wherein the plurality of transaction data communications comprises communications formatted according to ISO 7816-4.
Claim 12	
[12]	The token of claim 10 wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.
Claim 13	
[13]	The token of claim 10 wherein the secure element interrogator exchanges the plurality of transaction data communications with the secure element only within libraries or memory space residing on the mounting structure.
Claim 14	
[14]	The token of claim 10 wherein the communications controller creates a random unpredictable number and sends it to the secure element.
Claim 15	
[15]	The token of claim 10 wherein the transaction information comprises a dynamic card verification code.
Claim 16	
[16]	The token of claim 10 wherein communications to and from the secure element consist of communications from and to a secure element reader.
Claim 17	
[17]	The token of claim 10 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.

Claim 18	
[18]	The token of claim 10 wherein the secure element comprises a plurality of payment card applications from different card associations and the secure element interrogator interrogates one of the payment card applications.
Claim 19	
[19.1]	The token of claim 10 wherein: the payment card application comprises an executable payment card application; and
[19.2]	the secure element interrogator is configured to interrogate the executable payment card application to acquire the transaction information from the data file.
Claim 20	
[20]	The token of claim 19 wherein the executable payment card application includes an application level protocol for authentication of the secure element.
Claim 21	
[21]	The token of claim 10 wherein the transaction information comprises card-present data.
Claim 22	
[22.pre]	A token comprising:
[22.1]	a mounting structure having a communication connector configured to connect to a computer terminal;
[22.2]	a secure element affixed to the mounting structure, the secure element comprising a data file,
[22.3]	a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging a plurality of transaction data communications only between the secure element and the secure element interrogator; and
[22.4]	a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information to the computer terminal through the communications connector.

Claim 23	
[23]	The token of claim 22 wherein the plurality of transaction data communications comprises communications formatted according to ISO 7816-4.
Claim 24	
[24]	The token of claim 22 wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.
Claim 25	
[25]	The token of claim 22 wherein the secure element interrogator exchanges the plurality of transaction data communications with the secure element only within libraries or memory space residing on the mounting structure.
Claim 26	
[26]	The token of claim 22 wherein the secure element comprises a payment card application and the transaction information comprises track data.
Claim 27	
[27]	The token of claim 22 wherein communications to and from the secure element consist of communications from and to a secure element reader.
Claim 28	
[28]	The token of claim 22 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.
Claim 29	
[29.1]	The token of claim 22 wherein: the secure element comprises an executable application; and
[29.2]	the secure element interrogator is configured to interrogate the executable application to acquire the transaction information from the data file.

Claim 30	
[30.1]	The token of claim 22 wherein: the secure element comprises a payment card application;
[30.2]	the secure element interrogator is configured to interrogate the payment card application; and
[30.3]	the transaction information comprises card-present data.
Claim 31	
[31.pre]	A token comprising:
[31.1]	a mounting structure having a communication connector configured to connect to a computer terminal;
[31.2]	a secure element affixed to the mounting structure, the secure element comprising a data file,
[31.3]	a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging at least one transaction data communication only between the secure element and the secure element interrogator; and
[31.4]	a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information as a single data communication to the computer terminal through the communications connector.
Claim 32	
[32]	The token of claim 31 wherein the at least one transaction data communication comprises communications formatted according to ISO 7816-4.
Claim 33	
[33]	The token of claim 31 wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.
Claim 34	
[34]	The token of claim 31 wherein the secure element interrogator exchanges the at least one transaction data communication with the secure element only within libraries or memory space residing on the mounting structure.

Claim 35	
[35]	The token of claim 31 wherein the secure element comprises a payment card application and the single data communication to the computer terminal comprises track data.
Claim 36	
[36]	The token of claim 31 wherein communications to and from the secure element consist of communications from and to a secure element reader.
Claim 37	
[37]	The token of claim 31 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.
Claim 38	
[38.1]	The token of claim 31 wherein: the secure element comprises an executable application; and
[38.2]	the secure element interrogator is configured to interrogate the executable application to acquire the transaction information from the data file.
Claim 39	
[39.1]	The token of claim 31 wherein: the secure element comprises a payment card application;
[39.2]	the secure element interrogator is configured to interrogate the payment card application; and
[39.3]	the transaction information comprises card-present data.
Claim 40	
[40.pre]	A token comprising:
[40.1]	a mounting structure having a communication connector configured to connect to a computer terminal;
[40.2]	a secure element affixed to the mounting structure, the secure element comprising a payment card application and a data file;
[40.3]	a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging at least one transaction

	data communication only between the secure element and the secure element interrogator; and
[40.4]	a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information as track data to the computer terminal through the communications connector.
Claim 41	
[41]	The token of claim 40 wherein the at least one transaction data communication comprises communications formatted according to ISO 7816-4.
Claim 42	
[42]	The token of claim 40 wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.
Claim 43	
[43]	The token of claim 40 wherein the secure element interrogator exchanges the at least one transaction data communication with the secure element only within libraries or memory space residing on the mounting structure.
Claim 44	
[44]	The token of claim 40 wherein the communications controller creates a random unpredictable number and sends it to the secure element.
Claim 45	
[45]	The token of claim 40 wherein the transaction information comprises a dynamic card verification code.
Claim 46	
[46]	The token of claim 40 wherein communications to and from the secure element consist of communications from and to a secure element reader.
Claim 47	
[47]	The token of claim 40 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.

Claim 48	
[48]	The token of claim 40 wherein the secure element comprises a plurality of payment card applications from different card associations and the secure element interrogator interrogates one of the payment card applications.
Claim 49	
[49.1]	The token of claim 40 wherein: the payment card application comprises an executable payment card application; and
[49.2]	the secure element interrogator is configured to interrogate the executable payment card application to acquire the transaction information from the data file.
Claim 50	
[50]	The token of claim 49 wherein the executable payment card application includes an application level protocol for authentication of the secure element.
Claim 51	
[51]	The token of claim 40 wherein the transaction information comprises card-present data.
Claim 52	
[52.pre]	A token comprising:
[52.1]	a mounting structure having a communication connector configured to connect to a computer terminal;
[52.2]	a secure element affixed to the mounting structure, the secure element comprising a data file,
[52.3]	a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging at least one transaction data communications only between the secure element and the secure element interrogator; and
[52.4]	a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information to the computer terminal through the communications connector.

Claim 53	
[53]	The token of claim 52 wherein the at least one transaction data communication comprises communications formatted according to ISO 7816-4.
Claim 54	
[54]	The token of claim 52 wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.
Claim 55	
[55]	The token of claim 52 wherein the secure element interrogator exchanges the at least one transaction data communication with the secure element only within libraries or memory space residing on the mounting structure.
Claim 56	
[56]	The token of claim 52 wherein communications to and from the secure element consist of communications from and to a secure element reader.
Claim 57	
[57]	The token of claim 52 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.
Claim 58	
[58.1]	The token of claim 52 wherein: the secure element comprises an executable application; and
[58.2]	the secure element interrogator is configured to interrogate the executable application to acquire the transaction information from the data file.
Claim 59	
[59.1]	The token of claim 52 wherein: the secure element comprises a payment card application;
[59.2]	the secure element interrogator is configured to interrogate the payment card application; and
[59.3]	the transaction information comprises card-present data.

Claim 60	
[60.pre]	A token for transmitting a communications data package to a host device, the token comprising:
[60.1]	a mounting structure;
[60.2]	a secure element affixed to the mounting structure, the secure element including a data file containing transaction information;
[60.3]	a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire the transaction information from the data file by exchanging at least one transaction data communication between the secure element and the secure element interrogator and to generate the communications data package based on the transaction information; and
[60.4]	a communications controller affixed to the mounting structure and configured to receive the communications data package from the secure element interrogator and to transmit the communications data package to the host device.
Claim 61	
[61]	The token of claim 60 wherein the at least one transaction data communication comprises a plurality of transaction data communications between the secure element and the secure element interrogator, the plurality of transaction data communications being formatted according to ISO 7816-4.
Claim 62	
[62]	The token of claim 60 wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.
Claim 63	
[63]	The token of claim 60 wherein the secure element interrogator exchanges the at least one transaction data communication with the secure element occurs only within libraries or memory space residing on the mounting structure.
Claim 64	
[64]	The token of claim 60 wherein all communications to and from the secure element consist of communications from and to a secure element reader.

Claim 65	
[65]	The token of claim 60 wherein the secure element comprises a microprocessor and the transaction information comprises a dynamic card verification code calculated from an unpredictable number by the microprocessor.
Claim 66	
[66]	The token of claim 60 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.
Claim 67	
[67]	The token of claim 60 wherein the secure element comprises a plurality of payment card applications from different card associations and the secure element interrogator interrogates one of the payment card applications.
Claim 68	
[68]	The token of claim 60 wherein the host device comprises a cellular network device and the cellular network device comprises the secure element, the interrogator and the communications controller.
Claim 69	
[69]	The token of claim 60 wherein the host device comprises a cellular network device and the cellular network device comprises the secure element, the interrogator and the communications controller and the host device has the physical form of a mobile phone or a PDA.
Claim 70	
[70]	The token of claim 60 wherein the mounting structure comprises a substrate.
Claim 71	
[71]	The token of claim 60 wherein the mounting structure comprises a packaging case.
Claim 72	
[72]	The token of claim 60 wherein the token has the physical form of a payment card.

Claim 73	
[73]	The token of claim 60 wherein the token has the physical form of a fob.
Claim 74	
[74]	The token of claim 60 wherein the token has the physical form of a cartridge.
Claim 75	
[75]	The token of claim 60 wherein the token has the physical form of a dongle.
Claim 76	
[76]	The token of claim 60 wherein the token has the physical form of a secure digital (SD) chip.
Claim 77	
[77]	The token of claim 60 wherein the host device comprises a cellular network device and the cellular network device is configured to transmit the data communications package over a wireless network.
Claim 78	
[78.1]	The token of claim 60 wherein: the secure element comprises a payment card application;
[78.2]	the secure element interrogator is configured to interrogate the payment card application; and
[78.3]	the transaction information comprises card-present data.
Claim 79	
[79.pre]	A cellular network device comprising:
[79.1]	a mounting structure;
[79.2]	a secure element affixed to the mounting structure, the secure element including a data file containing transaction information; and
[79.3]	a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire the transaction information from the data file by exchanging at least one transaction data communication between the secure element and the secure element interrogator and to generate a communications data package based on the transaction information.

Claim 80	
[80]	The token of claim 79 wherein the at least one transaction data communication comprises a plurality of transaction data communications between the secure element and the secure element interrogator, the plurality of transaction data communications being formatted according to ISO 7816-4.
Claim 81	
[81]	The token of claim 79 wherein the secure element interrogator exchanges the at least one transaction data communication with the secure element only within libraries or memory space residing on the mounting structure.
Claim 82	
[82]	The token of claim 79 wherein all communications to and from the secure element consist of communications from and to a secure element reader.
Claim 83	
[83]	The token of claim 79 wherein the secure element comprises a microprocessor and the transaction information comprises a dynamic card verification code calculated from an unpredictable number by the microprocessor.
Claim 84	
[84]	The token of claim 79 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.
Claim 85	
[85]	The token of claim 79 wherein the secure element comprises a plurality of payment card applications from different card associations and the secure element interrogator interrogates one of the payment card applications.

Claim 86	
[86]	The cellular network device of claim 79 further comprising a communications controller affixed to the mounting structure and configured for receiving the communications data package for transmission by the cellular network device over a wireless network.
Claim 87	
[87.1]	The cellular network device of claim 79 wherein: the secure element comprises a payment card application;
[87.2]	the secure element interrogator is configured to interrogate the payment card application; and
[87.3]	the communications data package comprises card-present data.

I. INTRODUCTION

Apple Inc. (“Apple”) and Samsung Electronics Co., Ltd. (“Samsung”) (collectively, “Petitioners”) petition for IPR of claims 1-87 (“Challenged Claims”) of U.S. Patent No. 8,548,924 (“the ’924 Patent”).

II. REQUIREMENTS FOR IPR

A. Grounds for Standing

Petitioners certify that the ’924 Patent is available for IPR, and that Petitioners are not barred or estopped.

B. Challenge and Relief Requested

Petitioners request IPR of the Challenged Claims, supported by the testimony of Dr. Traynor (EX1003).

Ground	Claims	35 U.S.C. §103
1A	1-71, 76-87	Huomo-Smets
1B	1-71, 76-87	Huomo-Smets-Kisliakov
2A	1-2, 4, 6-8, 22-23, 25, 27-29, 31-32, 34, 36-38, 52-53, 55-58, 60-61, 63-64, 66-77, 79-82, 84-86	Ryan-Abbott
2B	3, 5, 9-13, 16-19, 21, 24, 26, 30, 33, 35, 39-43, 46-49, 51, 54, 59, 62, 78, 87	Ryan-Abbott-Peart
2C	65, 83	Ryan-Abbott-Smets

Ground	Claims	35 U.S.C. §103
2D	15, 20, 45, 50	Ryan-Abbott-Peart-Smets
2E/2F	2, 11, 23, 32, 41, 53, 61, 80	Ryan-Abbott-Smets-Kisliakov/ Ryan-Abbott-Peart-Smets-Kisliakov

The '924 Patent's earliest claimed priority date is January 25, 2007. For purpose of this proceeding alone and without conceding its propriety, Petitioners treat this as the Critical Date. EX1003, ¶¶45.

Reference	Filed	Published/Issued	§102 Provision(s)
Huomo (EX1004)	12/15/2006	9/17/2013	§102(e)
Smets (EX1005)	7/15/2005	2/2/2006	§102(a)
Ryan (EX1006)	11/16/2004	5/8/2007	§102(e)
Abbott (EX1009)	6/15/2001	12/20/2001	§102(b)
Peart (EX1008)	1/4/2006	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

Claim Term	Construction
"transaction 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 '924 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

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.

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 '924 PATENT

A. Brief Description

The '924 Patent relates to “the field of devices configured to authorize transactions using secure element microchips,” such as “tokens that contain secure element microchips and are configured to authorize financial transactions over the internet.” EX1001, 1:24-28. A “token” is described as any of several form factors—“fobs, cartridges, or dongles, or form factors that resemble removable digital memory media such as secure digital (SD) chips”—and “[e]ach token has a mounting structure such as substrate (for card devices) or a packaging case (for fobs, cartridges, and dongles or SD chips).” EX1001, 4:15-21. In some embodiments the secure element is provisioned with information about a particular payment card holder account. EX1001, Abstract; EX1003, ¶¶47-49.

B. Prosecution History

The '141 application was filed with 31 claims, which were rejected based on Ryan (US7,213,766; EX1006), Gold (US2005/0231467), and Somers (US2007/0262138). EX1002, 53-58, 205-215. In response to the rejection, the applicant argued that the prior art “fails to disclose or suggest a secure element and

an interrogator affixed to the same mounting structure.” EX1002, 258. For several dependent claims, the applicant relied on a Declaration for ISO 7816-4 features not recited in the independent claims. EX1002, 259-260; 262-266. In a Notice of Allowability, the examiner’s statement of reasons for allowance recited the “prior arts of record and further search does not teach/suggest... ‘a secure element affixed to the mounting structure...; a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element...’.” EX1002, 334; EX1003, ¶¶50-52.

IV. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. GROUND 1A – Huomo-Smets Renders Obvious Claims 1-71 and 76-87

1. Huomo²

Huomo 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

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.

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, ¶¶53-54.

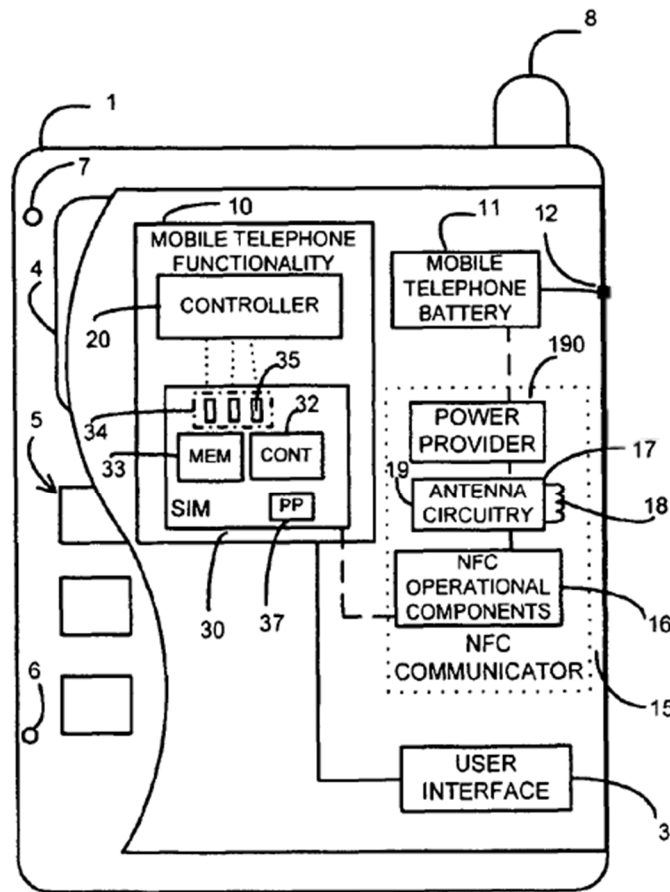


FIG. 1

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

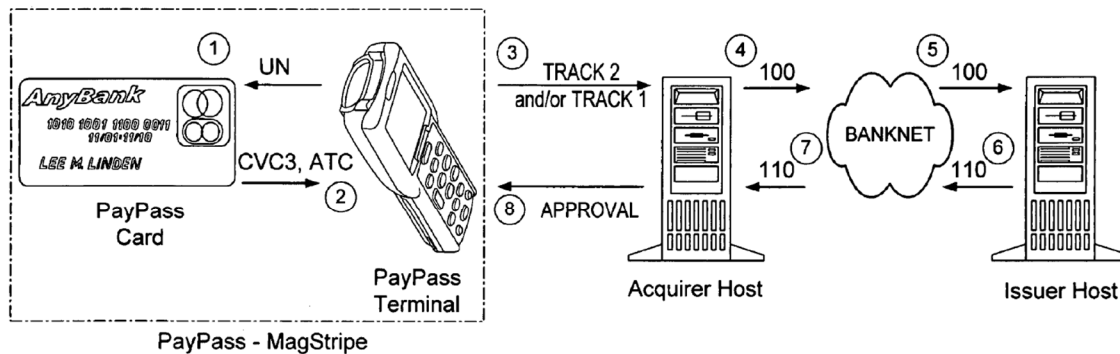
transaction data and storing encrypted transaction data (for example, purchase data) in accordance with that applications platform.” EX1004, Abstract (“secure element (30; 31) . . . to provide secure data storage for transaction data”), 7:19-67, 3:58-67, 7:65-8:41, 10:35-12:57 (details of “memory 33”); EX1003, ¶55.

Application areas of Huomo include “the financial transaction area which involves payment for products such as goods and services.” EX1004, 1:56-60.

2. Smets

Like Huomo and the '924 Patent, Smets describes transaction systems in which secure transaction data is stored in a secure element and communicated through a reader to a host to enable transactions. EX1003, ¶¶56; EX1005, Abstract, [0002], [0005], [0009]-[0010], [0025]-[0026]. In more detail, Smets describes formatting and communicating “proximity card transaction data” stored on “a payment card 1” (e.g., “PayPass Card” that is “consistent with the ISO 14443 Standard”) to “a reader terminal 2” then to a host, by embedding such transaction data within standardized magnetic stripe track formats (e.g., “Track 1,” “Track 2,” and “Track 3” data), “for processing magnetic stripe card transactions” consistent with ISO 7811. *See e.g.*, EX1005, Abstract, [0004]-[0008], [0013], [0025], [0026], [0037]-[0039], FIG. 5 (reproduced below). Through such formatting, proximity payment card implementations are made “compatible with existing standardized magnetic stripe payment card transaction processes.” EX1005, [0011]-[0012];

EX1012, §§5-6.



EX1005, FIG. 5

Smets describes application-level (e.g., “a ‘PayPass-MagStripe’ application”) dynamic authentication for improved security, through “generation of a dynamic authentication value or number (CVC3)” from “an unpredictable number (UN),” and optionally “the card’s application transaction counter (ATC),” using “a secret encryption key” stored on the payment card, such that the value of the CVC3 “changes with each transaction” and “the unauthorized person cannot use that CVC3 number...for the next or any other transactions.” EX1005, [0010], [0014], [0024]-[0025], [0026], [0037]-[0039], FIG. 5; EX1003, ¶57.

The computed dynamic CVC3, optionally along with the transaction counter (ATC) and/or the unpredictable number (UN), is integrated in Track data (e.g., a discretionary data field of Track 2) and communicated to the host for authorization of the transaction. EX1005, Abstract, [0014], [0026], [0029]-[0031], [0035],

[0037]-[0038]; EX1003, ¶58.

3. Huomo-Smets Combination

a) Huomo and Smets are Analogous Art to the '924 Patent

Huomo and Smets are analogous art to the '924 Patent, which is generally directed to “the field of devices configured to authorize transactions using secure element microchips.” EX1001, 1:24-28; cl. 1 (“A token”); *supra*, §§IV.A.1-2 (Huomo and Smets); EX1003, ¶59. Huomo and Smets are also reasonably pertinent to the problems the '924 Patent purports to solve. *See, e.g.*, EX1001, 1:44-50 (“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.”), 4:52-67, 5:5-11, 5:12-26, 5:27-36, 5:37-55, 5:61-6:3 (encrypting track data “in order to securely transport the data packet over a public network”), 6:26-32; 10:4-10, 11:31-37, 18:7-29, 19:19-33, 20:25-27; *supra*, §IV.A (Huomo and Smets).

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

Huomo already provides an NFC communication platform for transmitting transaction data stored in a secure element, e.g., a proximity payment card compatible with ISO/IEC 14443. *Supra*, §IV.A.1; *see e.g.*, EX1004, Title, Abstract, 3:44-55 (“a secure element, for example a SIM card, USIM card, WIM card, SWIM card, SD card, SMC card or other form of secure element, is operable

to transfer data from its memory or data store to an external near field RF communicator through an NFC communicator....in accordance with or compatible with ISO/IEC 14443”), FIGS. 1-2. Smets provides a known technique to structure proximity transaction data stored in a payment card, including a dynamic authentication code (e.g., CVC3), so that its implementation is compatible with existing magnetic stripe infrastructure and processes, e.g., compatible with both ISO/IEC 14443 for contactless proximity payment card transactions and ISO 7811 for magnetic stripe card transactions. *Supra*, §IV.A.2; *see e.g.*, EX1005, Abstract, [0010], [0011]-[0014], [0025], [0026]; EX1003, ¶60.

A POSITA would have been motivated to incorporate Smets’s teaching of backward-compatible data formatting for integrating proximity payment data, including the dynamic authentication code (e.g., CVC3), into Huomo’s proximity (e.g., NFC based) payment card system. EX1005, [0011]-[0013]. Multiple considerations would have led a POSITA to implement this combination. EX1003, ¶61.

First, a POSITA would have incorporated Smets’s backward-compatible formatting of proximity transaction data including a dynamic CVC3 into Huomo’s proximity transaction system, to promote the ability of the combination’s contactless transactions (both following the same ISO 14443 standard) to be processed using existing magnetic stripe infrastructure of the legacy payment

networks, a known commercial advantage and common goal expressed in Huomo and Smets. *See e.g.*, EX1004, Title, Abstract, 2:18-19 (desire for “flexibility and backwards compatibility with existing systems and devices”), 3:44-55; EX1005, Abstract, [0010]-[0011] (“backwards compatible), [0025]; EX1003, ¶62.

Second, a POSITA would have incorporated Smets’s teaching into Huomo’s system, because it would provide enhanced security through dynamic authentication. EX1003, ¶63. Huomo already supports encrypted storage, where the secure element stores encryption “keys” and “encryption software or an encryption algorithm to ensure secure storage of data relating to a transaction such as, for example, a financial transaction or transactions.” EX1004, 3:59-62, 5:26-52, 7:19-31, 8:25-41, 11:28-35. Huomo also strongly emphasizes that the secure transaction data in the secure element is kept isolated and not visible (or not required to be understood) by the host or NFC communicator. EX1004, 1:64-2:24 (“the secure data is made secure (for example a manner of encryption) is not known to and is not relevant to the NFC communicator... the NFC communicator does not need to be a secure or trusted device, only the secure element and the device that decrypts communicated secure data need to be trusted devices...the NFC communicator communicates the secured data to a near field RF communicator without any knowledge of these features of the secure element.”). Smets’s use of dynamic authentication value (e.g., CVC3) (along with the UN and

transaction counter) adds dynamic authentication specific to each transaction and protection against fraud and replay attacks. EX1005, [0010], [0014], [0026].

Third, a POSITA would have been motivated to incorporate Smets's teaching into Huomo's system for the common goal of improved interoperability across vendors and systems. EX1003, ¶64; EX1004, 2:16-19 (desire for "interoperability to maintain a consistent and viable user experience...flexibility and backwards compatibility with existing systems and devices"); EX1005, [0011]. Smets identifies that inconsistent vendor and issuer usage of the magnetic-stripe discretionary data fields can cause the space available for the CVC3 to "vary from card to card," which "makes it difficult to standardize use of the space for storing proximity card function related data (e.g., CVC3)." EX1005, [0011]. Smets addresses with an "issuer or vendor-specific bitmap" that "identifies available unused space in the discretionary data fields" in which the dynamic authentication codes, unpredictable numbers, and transaction counter are placed, allowing each issuer to define how much space is available and exactly where data may go without changing terminals or networks, while "[c]ard behavior is independent of vendor usage of the discretionary data fields." EX1005, [0014], [0015], [0026], [0033].

Additionally, a POSITA would have found it obvious that the Huomo-Smets combination uses the same type of ISO 7816-4 commands and responses (APDUs)

for a plurality of transaction data communications between the secure element (e.g., payment card) and the reader in a single interrogation session to acquire Track data for transactions, as Huomo's secure element and reader interface is explicitly "in compliance with ISO 7816," and Smets provides the details of command-layer command-response pairs defined by ISO 7816-4. EX1003, ¶65; *supra*, §IV.A.1-2; EX1004, 7:51-52; EX1005, [0036]-[0039], FIG. 6.

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

The combination amounts to use of a known technique (e.g., Smets's teaching of proximity data structure) in a known system (e.g., Huomo) to yield predictable results. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007); EX1003, ¶66. A POSITA would have had a reasonable expectation of success, especially because the combination would have been implemented primarily through routine software updates. *Id.* Smets specifies how to structure proximity transaction data stored in a payment card, including a dynamic authentication code (e.g., CVC3). *Id.* Huomo describes an interface expressly "in compliance with ISO 7816," and Smets provides details of command-layer command-response pairs defined by ISO 7816-4. EX1004, 7:51-52; EX1005, [0036]-[0039], FIG. 6.

4. Analysis

Huomo-Smets renders obvious the claims in multiple manners. The

following analysis presents two mappings, each of which render the claims obvious. EX1003, ¶¶67-70, 75, 81, 90.

Claims 60, 79

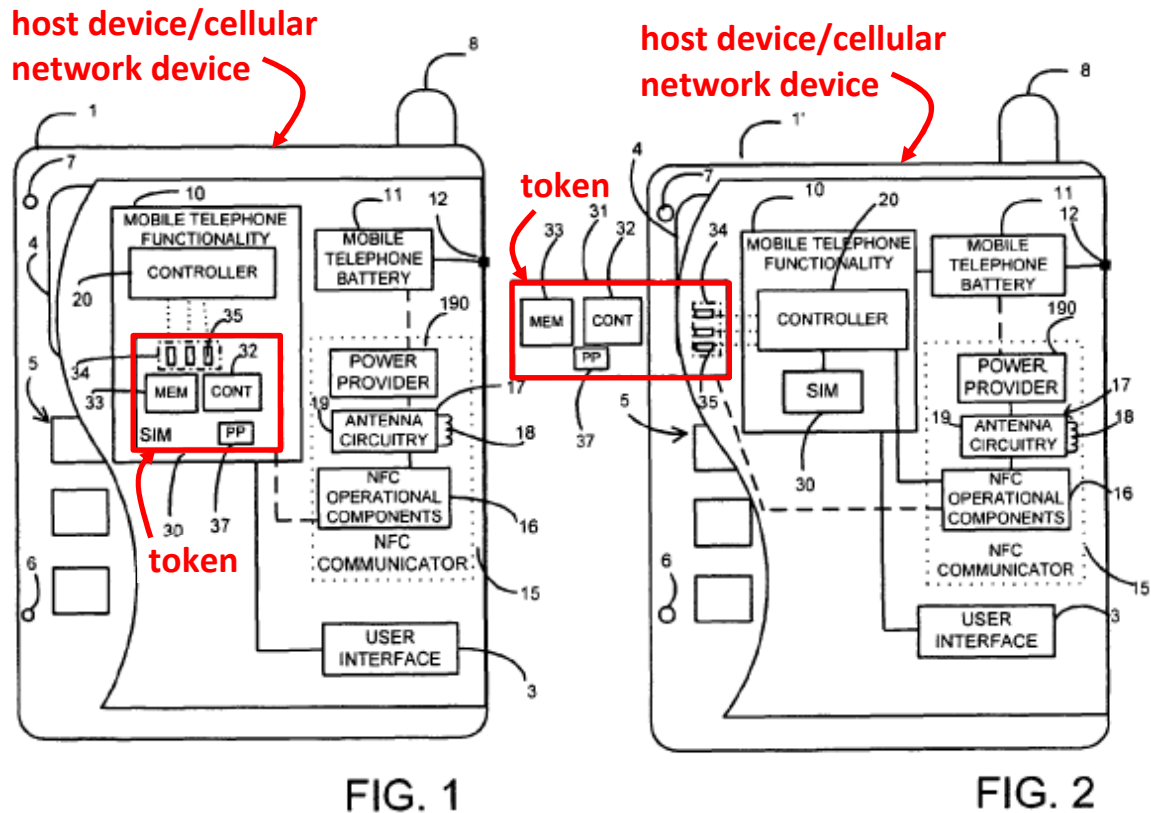
[60.pre]/[79.pre]

a) First Mapping

Huomo describes “a secure element” (SE) included in “a SIM card, SD card or other secure memory storage” (***token***). EX1004, 3:17-19, 3:44-48, 8:35-42, 15:62-66; EX1001, 4:8-21 (“smart token” and “‘token’ is used to encompass all of these form factors.”). Huomo’s SE card (***token***) is within “a larger device or host system, for example a mobile telephone, PDA, lap-top or other electrical device” (***host device/cellular network device***). EX1004, 3:56-62. In Huomo, “a mobile telephone or PDA” (***host device/cellular network device***) “is operable to receive data from the secure element” card (***token***). EX1004, 3:20-40. The ’924 Patent uses ***host device*** broadly, describing as the computer terminal that receives information from a card device or the cellular network device that receives it from a cellular network adapter—Huomo’s device 1/1’ addresses this element directly. EX1001, 4:36-40, 5:1-4, 12:54-55, 17:62-64; EX1003, ¶71.

Huomo’s FIGS. 1 and 2 show devices 1/1’ (***host device/cellular network device***) that are “mobile telephones (cellular telephones or ‘cell phones’).” EX1004, 6:35-54, 25:35-36. Each device 1/1’ (***host device/cellular network***

device) comprises a SE card (SIM 30/SD card 31) (*token*) for “secure storage of data relating to a transaction.” EX1004, 5:24-40, 7:65-8:24, 15:62-16:17, 20:42-44. The SE card (*token*) is coupled to a controller 20 of the device 1/1’ (*host device/cellular network device*) through a “coupling interface 34 comprising one or more coupling elements 35” “to enable communication of data between the controller and the secure element” card (*token*) “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 explicit disclosure of an ISO 7816 interface between the SE card and the controller 20, a POSITA would have recognized, and found obvious from Huomo’s description, that the SE card and the controller 20 exchange data using an APDU (Application Protocol Data Unit) (*communications data package*) defined in ISO 7816 (e.g., ISO 7816-4). EX1003, ¶72 (citing EX1012, 13; EX1013, [0006]; EX1014, [0016], [0030]; EX1015, [0034]).



EX1004, FIGS. 1, 2

b) Second Mapping

Huomo's devices 1/1' (*cellular network device*) each includes a *token* with a SE 30/31. EX1004, 5:24-6:22, FIGS. 1, 2; EX1003, ¶73.

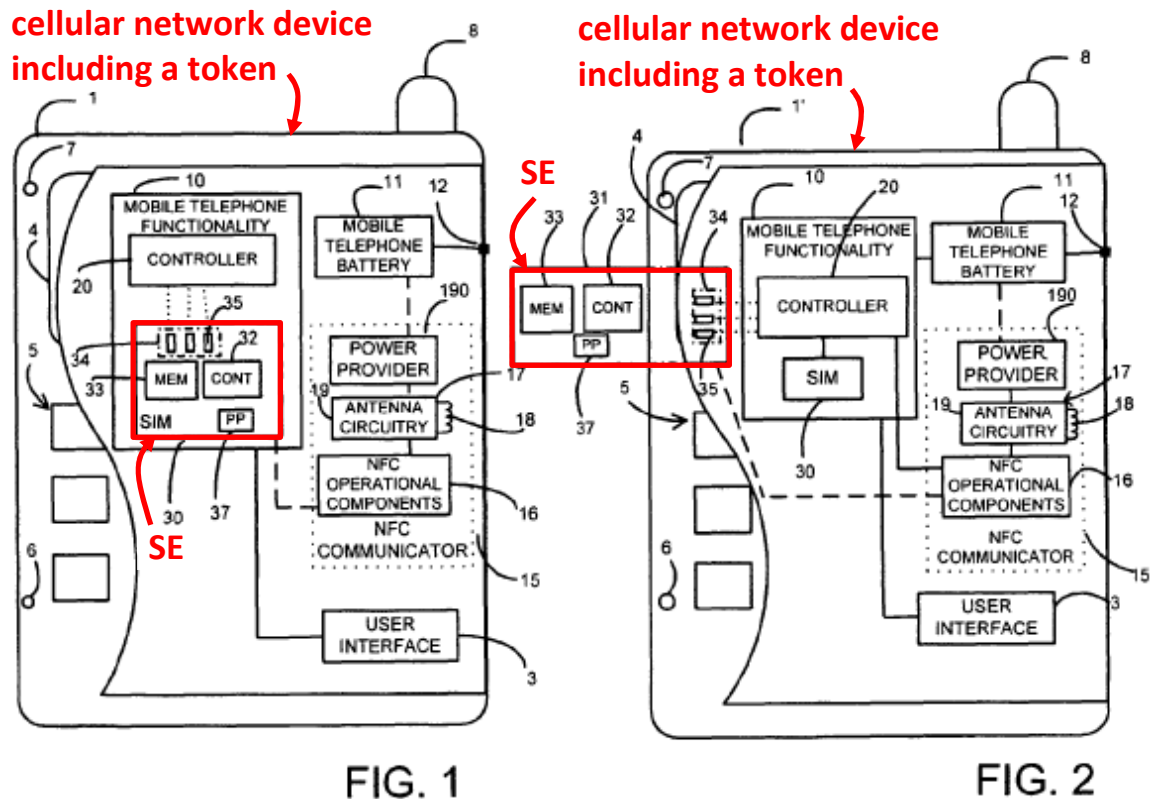


FIG. 1

FIG. 2

EX1004, FIGS. 1, 2

The **token** of Huomo's device 1/1' (**cellular network device**) also includes an NFC communicator that supplies secure data from the SE 30/31 to a near field RF communicator (**host device**) via NFC communication protocols in accordance with ISO/IEC 14443. EX1004, 1:64-3:55, 5:24-6:41, 10:19-34, 14:35-42, 15:13-16 ("device 1000 is similar to the devices 1 and 1'"), FIGS. 1-2, 13; *supra*, §IV.A.1. A POSITA would have known that the ISO/IEC 14443 protocol transfers APDUs as defined in ISO 7816-4. EX1003, ¶74 (citing EX1016, 6). Based on Huomo's explicit disclosure of the NFC communicator transmitting data to another RF communicator using an ISO/IEC 14443 protocol, a POSITA would have

recognized, and found it obvious from Huomo's description, that the NFC communicator of the *token* of device 1/1' (*cellular network device*) transmits the data using APDUs (*communications data package*) defined in ISO 7816-4 to the RF communicator (*host device*). *Id.*

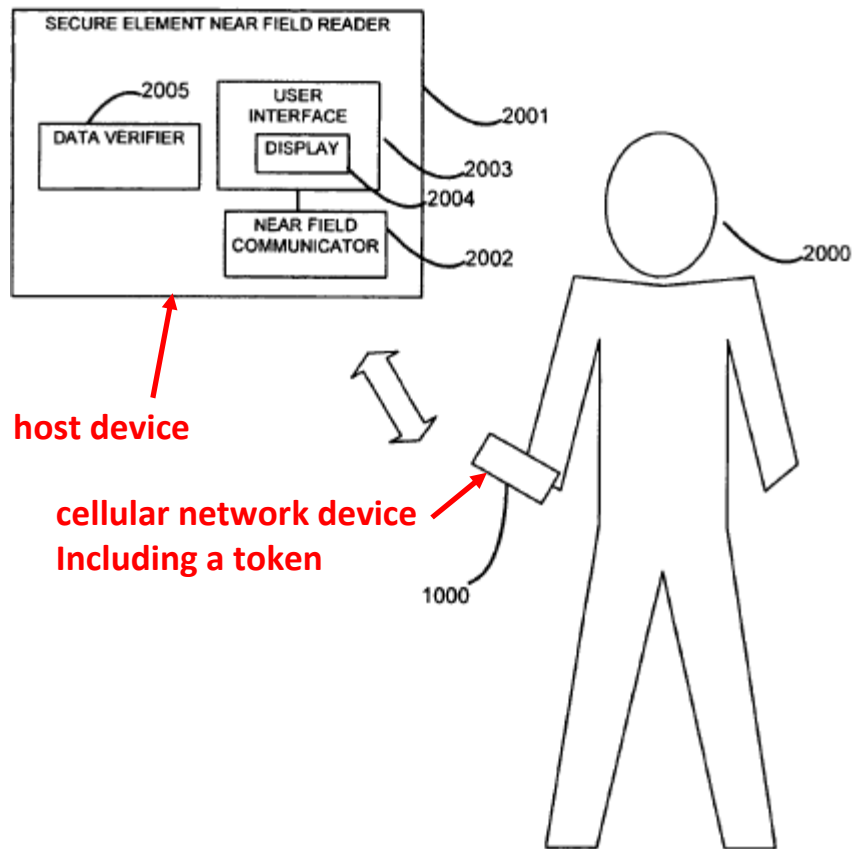


FIG. 13

EX1004, FIG. 13

[60.1]/[79.1]

a) First Mapping

Huomo's SE is in the form of "a SIM card, SD card or other secure memory

storage” (*token*). EX1004, 3:17-19, 3:44-48, 8:35-42, 15:62-66. The SE cards 30/31 “each have a controller (CONT) 32... and a data or memory store (MEM) 33... provided by an integrated circuit” (IC). EX1004, 7:19-46. A POSITA would have recognized, and found obvious from Huomo’s description, that the SIM card includes an IC chip mounted on a substrate (*mounting structure*). EX1017, [0013], [0145], FIG. 1; EX1003, ¶76. A POSITA would have also recognized, and found obvious, from Huomo’s description, that a SD card includes chips mounted to a printed circuit board and integrated in a plastic cover (*mounting structure*). EX1018, [0002]; EX1003, ¶76. Based on Huomo’s express disclosure of the SE in the form of a SIM card or SD card, a POSITA would have understood and found it obvious that the device 1/1’ (*cellular network device*) includes the SE card (*token*) that includes a substrate or a printed circuit board in a plastic cover (*mounting structure*). *Id.*

b) Second Mapping

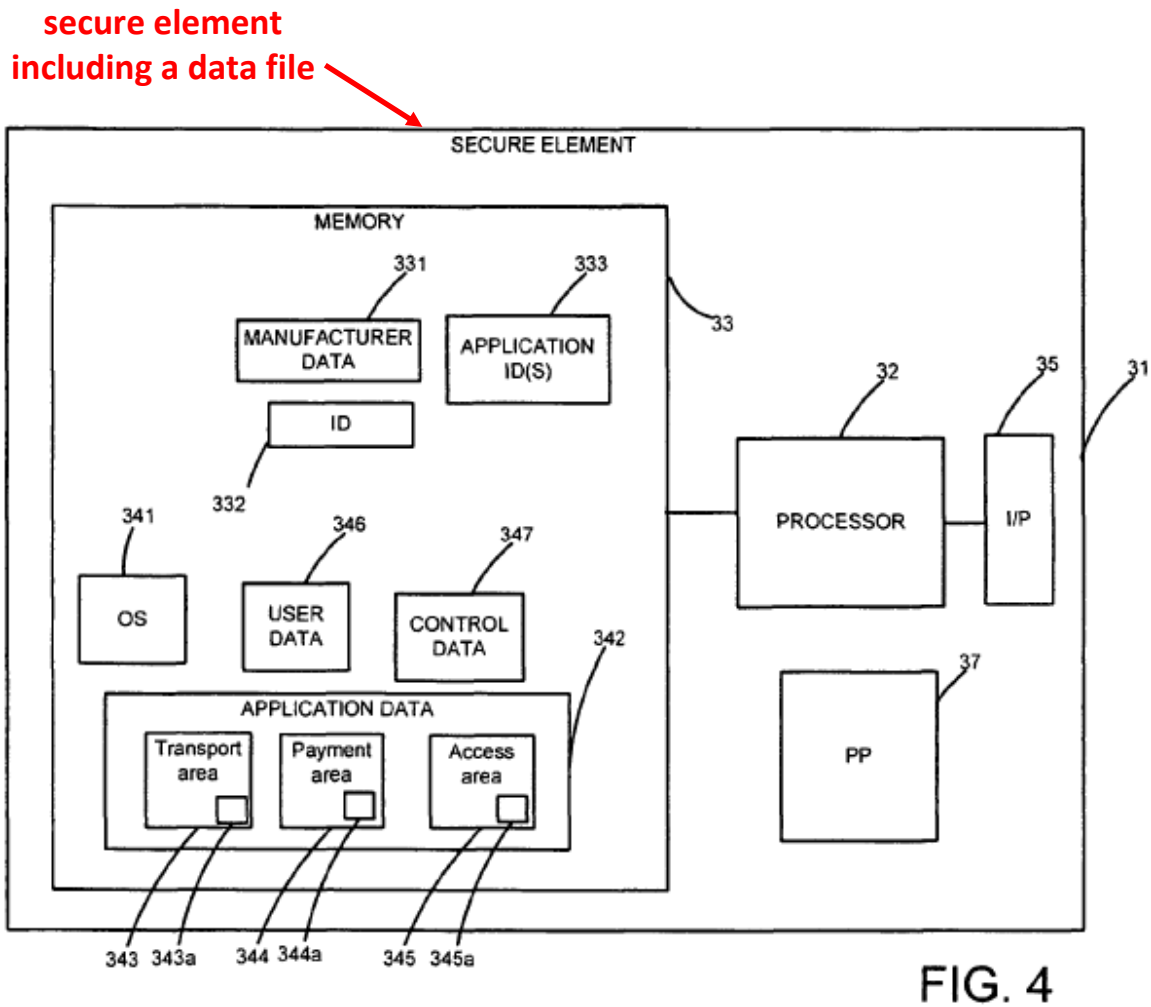
Huomo’s device 1/1’ (*cellular network device*) “may be provided wholly or partially as an integrated circuit or collection of integrated circuits.” EX1004, 5:21-23, 7:31-38. Huomo’s “NFC communicator” (e.g., “NFC communicator 15” of FIG. 3) “may be implemented as an integrated circuit connected to any peripherals and an antenna,” e.g., “implemented on a PCB board.” EX1004, 24:4-17. A POSITA would have found it obvious from Huomo’s description that the

ICs in Huomo's *token* are affixed to a *mounting structure* such as a PCB board in the device's housing, advantageously effectuating Huomo's stated objectives and implementation. EX1003, ¶77.

~~[60.2]/[79.2]~~

Huomo uses the term "secure element" to describe an "element which is capable of being used to hold secure encrypted information and/or data." EX1004, 25:41-44. Huomo's devices 1/1' each comprises a SE in the form of a card (SIM 30/SD card 31) that provides "secure storage of data relating to a transaction." EX1004, 2:25-46, 3:63-4:24, 5:24-40, 7:65-8:24, 15:62-16:17, 20:42-44. The SE cards 30/31 "each have a controller (CONT) 32... and a data or memory store (MEM) 33... provided by an integrated circuit" (IC). EX1004, 7:19-46. Huomo's 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" (*transaction information*). EX1004, 10:35-11:7, 2:44-46, 3:63-4:15, 25:51-62. 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, ¶78 (citing EX1007, 15:40-46). A POSITA would have found it obvious that the SE for storing transaction data comprises *a data file containing transaction information* in its memory store 33 based on Smets's teachings. *Id.*; EX1004, 7:19-67, 10:35-12:57 (describing "memory store 33 in

greater detail”), FIGS. 1-2. For example, Smets discloses “file control information” and that “data... are included in record 1 of the file,” confirming that the SE stores information in data files in the combined system. EX1005, [0037]; EX1003, ¶78.



EX1004, FIG. 4

a) First Mapping

A POSITA would have understood and found it obvious, based on Huomo’s description, that the controller 32 and memory store 33 of the SE card 30/31 are

affixed to the substrate or printed circuit board in the plastic cover (*mounting structure*). EX1003, ¶79; EX1004, 7:19-46 (The SE cards 30/31 (*token*) “each have a controller (CONT) 32... and a data or memory store (MEM) 33... provided by an integrated circuit” (IC)); *see also*, EX1004, 3:17-19, 3:44-48, 8:35-42, 15:62-66; EX1017, [0013], [0145], FIG. 1; EX1018, [0002].

b) Second Mapping

Huomo’s “secure element 30” (e.g., “SIM”) of device 1 is an “integrated circuit.” EX1004, Abstract, 5:24-52, 7:19-67, FIG. 1; *supra*, §IV.A.1. As discussed in [60.1], a POSITA would have found it obvious from Huomo’s description that the ICs in Huomo’s token are affixed to the *mounting structure* such as a PCB board in the device’s housing, advantageously effectuating Huomo’s stated objectives and implementation. EX1003, ¶80.

[60.3]/[79.3]

a) First Mapping

Huomo’s SE cards 30/31 (*token*) each have a *secure element interrogator* 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. The controller 32 (*secure element interrogator*) and memory store 33 of the SE card 30/31 are affixed to the substrate or printed circuit board in the plastic cover (*mounting structure*). EX1003, ¶82;

EX1017, [0013], [0145], FIG. 1; EX1018, [0002]; *see also, supra*, [60.1] (citing EX1004, 3:17-19, 3:44-48, 8:35-42, 15:62-66).

Huomo's controller 32 (*secure element interrogator*)³ "controls the functionality of the secure element" including "decrypting 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). EX1004, 7:19-52, 8:25-42, 2:47-49, 5:41-61, 24:55-60 ("processor of the secure element will control transmission of data from the secure element"); EX1003, ¶¶83-84. As discussed above in [60.2], the Huomo-Smets 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 interrogator*) *acquires the transaction information* (including credit/debit card

³ That the controller 32 is provided within Huomo's secure element 30 is consistent with the '924 Patent, which recites that the interrogator "may be physically 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, 7:43-8:3; EX1003, ¶84.

number) *from the secure element data file* to transfer the data from the memory store 33. EX1003, ¶85. For this example, as discussed above in [60.pre], the SE card controller 32 sends the transaction data to the host device controller (e.g. Huomo's controller 20) by generating an APDU (Application Protocol Data Unit) (*generating the communications data package*) defined in ISO 7816-4 *based on the transaction information* (including credit/debit card number). *Id.*

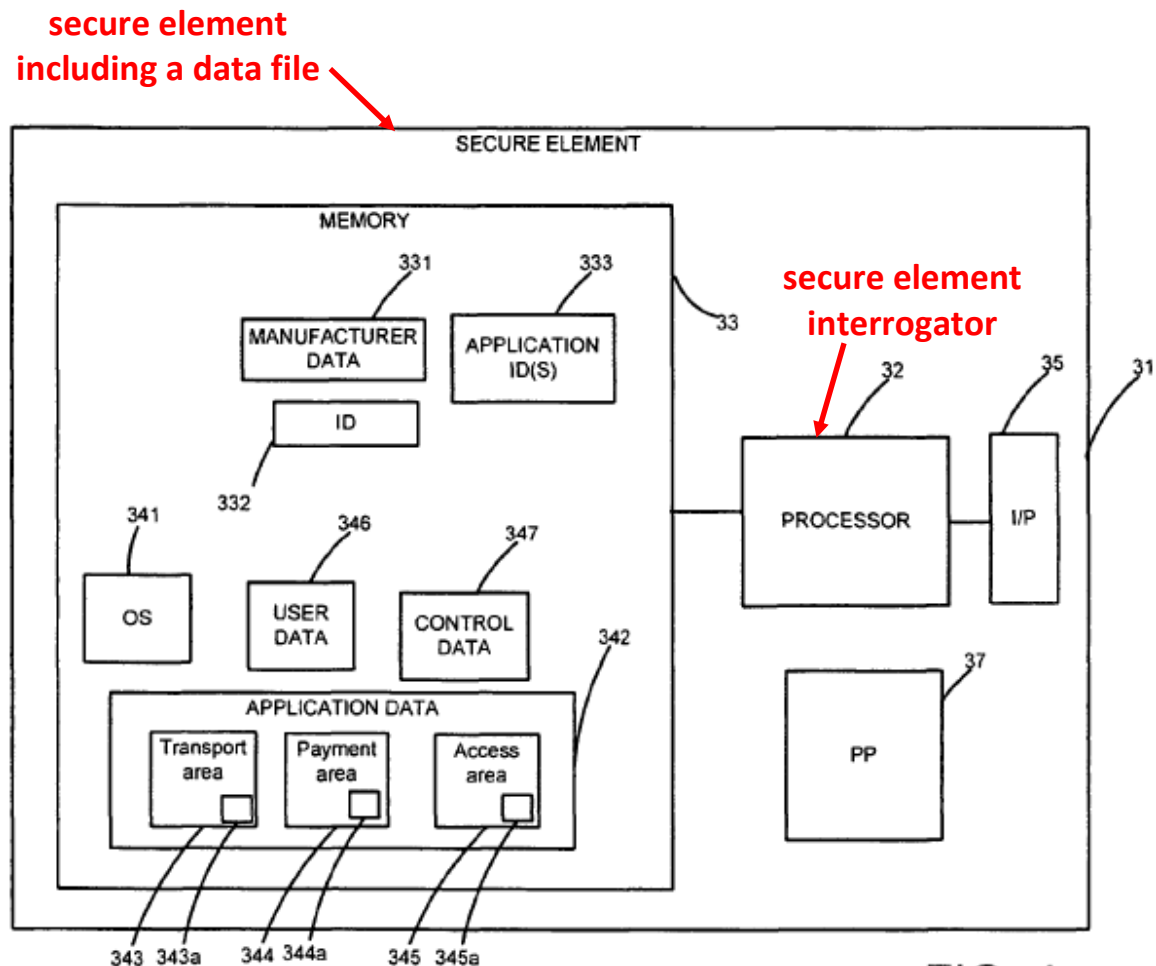
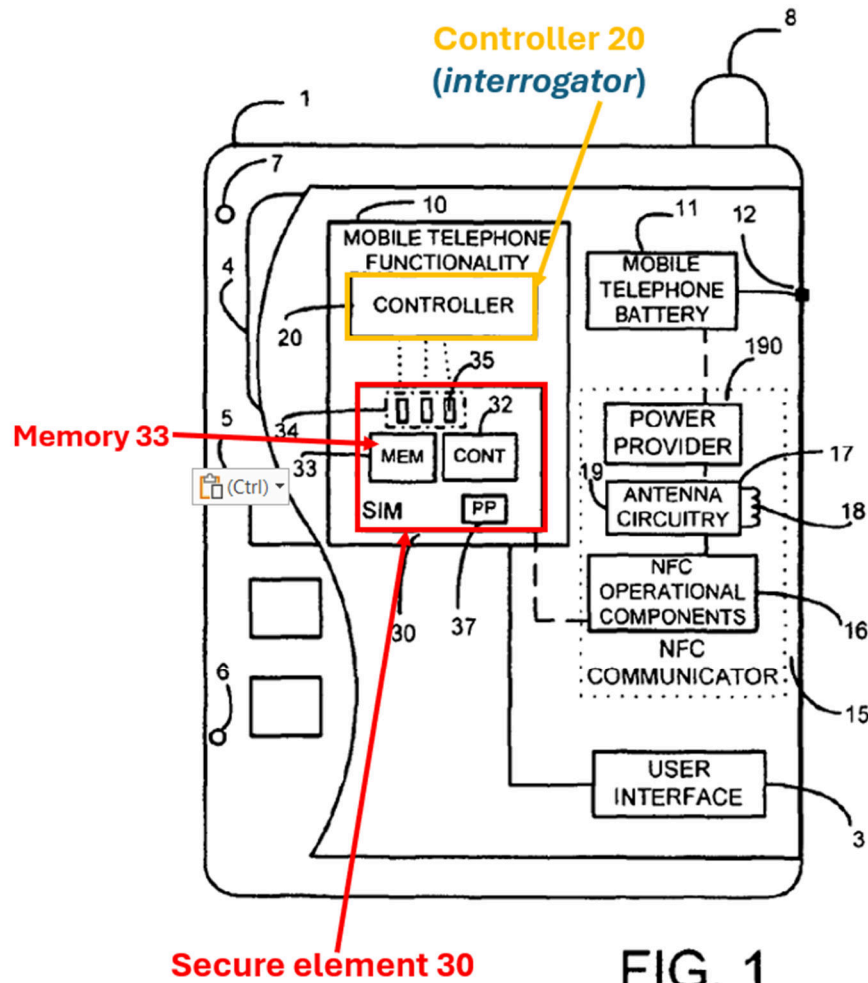


FIG. 4

EX1004, FIG. 4

b) Second Mapping

Huomo's *token* includes the secure element 30/31 coupled to "a controller 20" (*secure element interrogator*) of the device 1/1' (*cellular network device*) to "enable communication of data between the controller and the secure element 30," and the controller 20 is coupled to the NFC communicator 15 to "enable communication of data between the controller 20 and the NFC communicator 15." EX1004, 6:23-28, FIGS. 1-2. Given that the device "may be provided wholly or partially as an integrated circuit or collection of integrated circuits," a POSITA would have found it obvious from Huomo's description that the "controller 20" is also provided as integrated circuit(s), e.g., on a PCB board of the device housing (*affixed to the mounting structure*). EX1004, 5:22-23, 7:31-38, 24:4-17; *supra*, §IV.A.4, Element [60.1]; EX1003, ¶86.



EX1004, FIG. 1

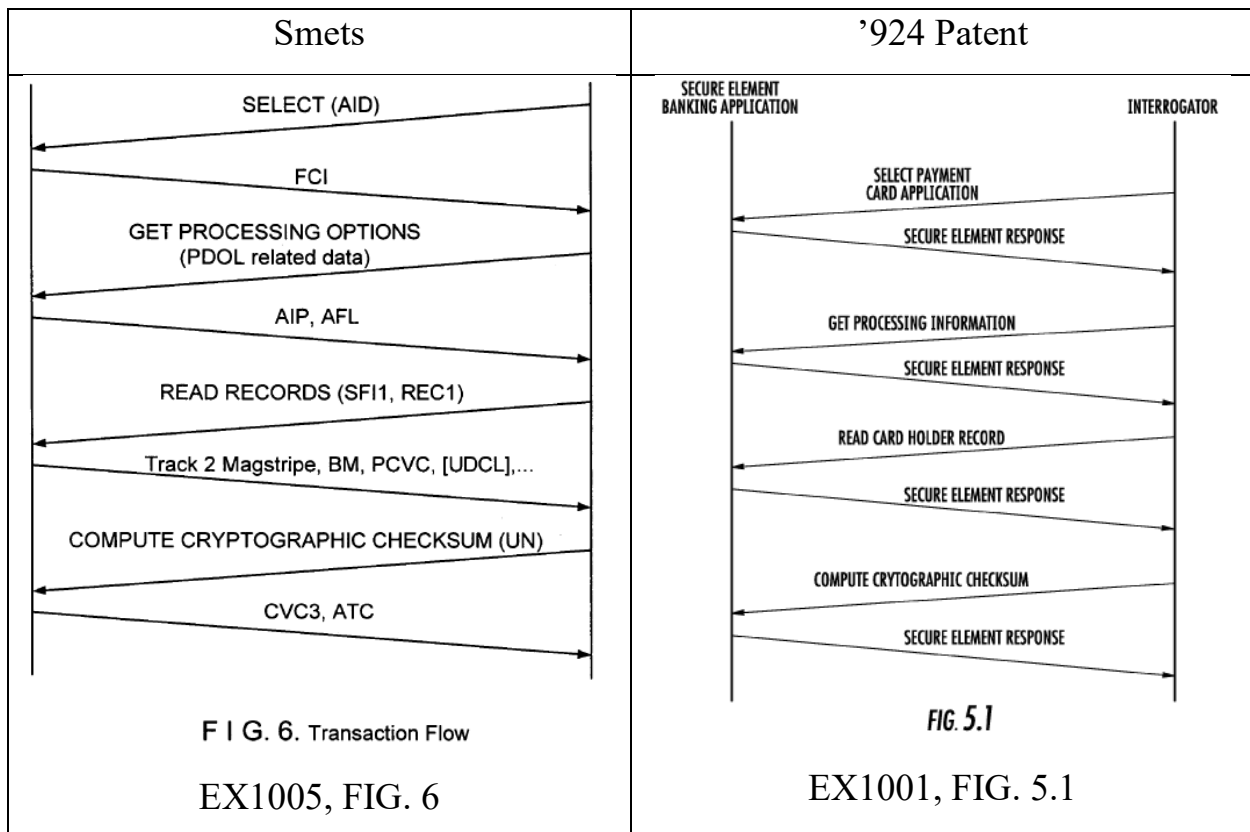
The controller 20 (*secure element interrogator*) “communicate[s] data with the secure element” through an interface that is “in compliance with ISO 7816.” EX1004, 5:52-56, 6:23-28, 7:47-52, 10:10-14; *supra*, §IV.A.1; EX1003, ¶87. A POSITA would have found it obvious that the controller 20 is *configured to interrogate the secure element* using the communication capability to communicate data with the secure element. *Id.*

As discussed above in [60.2], the Huomo-Smets 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 20 (*secure element interrogator*) *acquires the transaction information* (including bank account information, e.g., credit/debit card number) *from the secure element data file* to acquire the data from the memory store 33. EX1003, ¶88. For this example, the controller 20 generates an APDU (Application Protocol Data Unit) (*generates the communications data package*) defined in ISO 7816-4 *based on the transaction information* (including credit/debit card number) and sends the APDU to the NFC communicator of device 1/1', which then transmits the APDU to the RF communicator (*host device*). *Id.*

For both the first and second mappings, in the Huomo-Smets combination, as discussed above, the secure element and the interrogator *exchange transaction data communications* in a single interrogation session to acquire the transaction/payment data including bank account information, e.g., credit/debit card number (*transaction information*), in accordance with Huomo and Smets. *Supra*, §IV.A.3; EX1004, 7:19-52; EX1005, [0036]-[0039], FIG. 6 (below). Smets's FIG. 6 illustrates "the interactions and communications between a proximity payment card and a terminal during the conduct of an electronic transaction" (*exchange of transaction data communications*). EX1005, [0022],

[0036]-[0037]. In Smets, the terminal is a reader/interrogator. EX1005, [0008] (“reader/terminal”), [0026] (“reader terminal”); EX1003, ¶89. A POSITA would have found it obvious to implement the *exchange of transaction data communications* between the secure element and the interrogator (either controller 32 or controller 20) based on Smets’s teachings. *Id.*; *supra*, §IV.A.3. Smets’s description of the exchange of transaction data communications aligns with the ’924 Patent’s description of the “interaction and data exchange between the interrogator chip and... the SE” as shown in the ’924 Patent’s FIG. 5.1 (below). EX1001, 12:7-10.



[60.4]

a) First Mapping

Huomo's NFC communicator can be "combined with a removable secure element" and the secure element provides a data store for the NFC communicator. EX1004, 25:63-26:7. A POSITA would have understood and found it obvious based on Huomo's description that the controller 32, memory store 33, coupling interface 34 comprising one or more coupling elements 35, and NFC communicator of the SE card 30/31 are affixed to the substrate or printed circuit board in the plastic cover (*mounting structure*). EX1003, ¶91; EX1017, [0013], [0145], FIG. 1; EX1018, [0002]. Huomo discloses that "where the NFC communicator has a direct link to the secure element, then relevant data may be transferred directly from the secure element to the NFC communicator," and "there may be no direct link between any host processor and the secure element and... the NFC communicator controller... will control transmission of data from the secure element" such that "communication between the secure element... and the mobile telephone functionality 10 is via the NFC communicator." EX1004, 24:50-60, 15:17-19. For this example, the NFC communicator controller (e.g., NFC operational components 16 including controller 40) (*communications controller*) receives the APDU (*communications data package*) from the secure element controller (*interrogator*) and transmits the APDU (*communications data package*) to the host device controller 20 through the coupling elements 35. EX1003, ¶91.

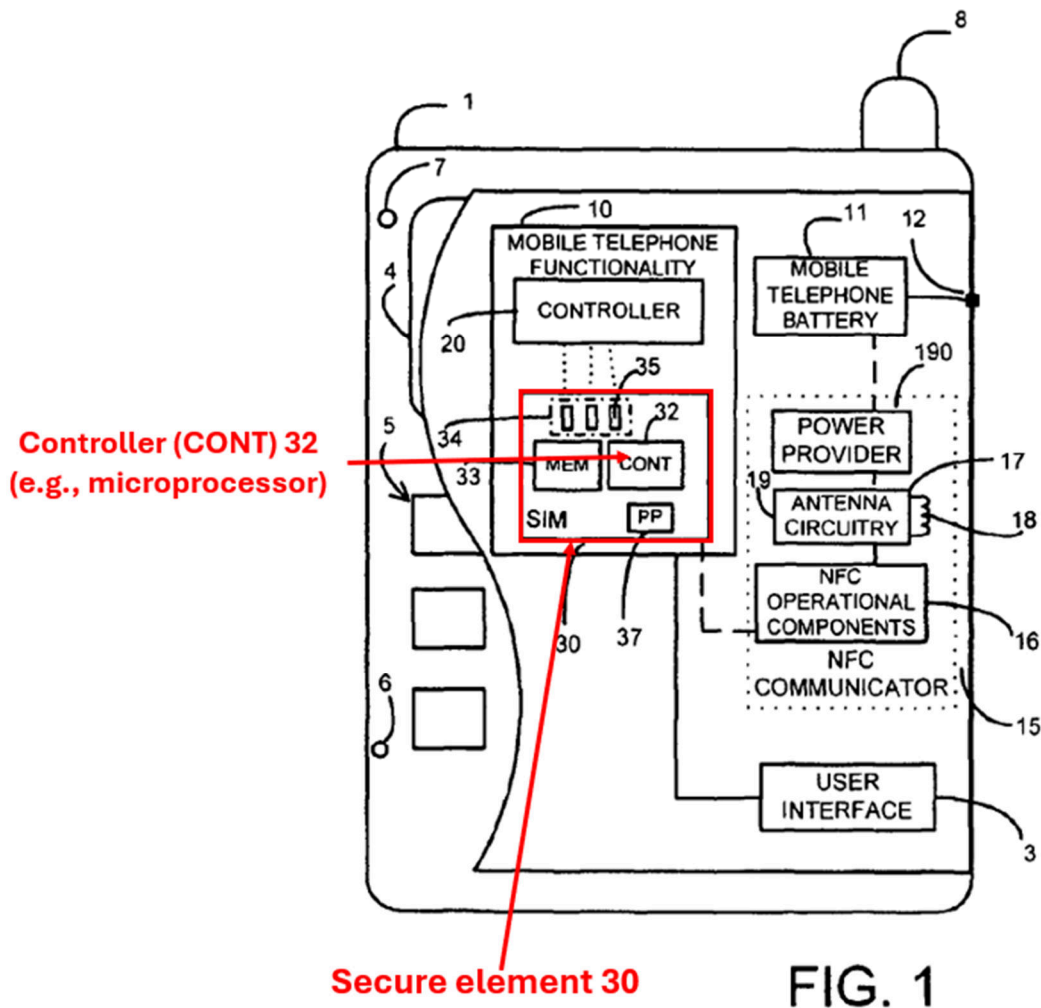
b) Second Mapping

In Huomo, the **communications controller** (e.g., operational components 16 and controller 40 of NFC communicator 15) of the **token** provided by the integrated circuit(s) affixed to a PCB board in the device housing (**affixed to the mounting structure**) receives the APDU (**communications data package**) from controller 20 (**secure element interrogator**) and transmits the APDU (**communications data package**) to “an external near field RF communicator” (**host device**) through the NFC connection. *Supra*, §IV.A.1, 4, Elements [60.1]-[60.3]; EX1004, Abstract, 2:47-67, 3:20-40, 5:22-40, 6:23-41, 13:50-55, 20:11-12, 23:42-45, 24:4-17, 25:11-16, 25:35-40, FIGS. 1-2, claims 11-12; EX1003, ¶92.

Claims 65, 83

Under both mappings, the Huomo-Smets combination structures its transaction data stored in the secure element 30, including a dynamic authentication code (e.g., CVC3) (**dynamic card verification code**) computed from the **unpredictable number** (UN), in accordance with Smets, for compatibility with existing magnetic stripe infrastructure and enhanced security through dynamic authentication. *Supra*, §§IV.A.2-4; EX1005, [0010], [0014], [0024]-[0026], [0037]-[0039], FIG. 5; EX1003, ¶93. Huomo’s secure element 30/31 has its own “controller (CONT) 32 (which may be a microprocessor, microcontroller or state machine, for example) which controls the functionality of the secure element in

accordance with its operating systems and the installed applications platform or platforms...provided by an integrated circuit.” EX1004, 7:31-38, FIG. 1 (below).



EX1004, FIG. 1 (annotated)

In the combined system, the “controller (CONT) 32” (*microprocessor*) of the secure element 30/31 uses application-level (e.g., “a ‘PayPass-MagStripe’ application”) dynamic authentication to calculate the dynamic CVC3 (*dynamic card verification code*), from the UN and optionally “the card’s application transaction counter (ATC),” using a secret encryption key stored on the secure

element, in accordance with Smets. *Supra*, §IV.A.2-3; EX1005, [0010] (“A security solution, which may be utilized in PayPass, is based on generation of a dynamic authentication value or number (CVC3). The dynamic authentication value changes with each transaction.”), [0014], [0024]-[0025] (“The PayPass implementation provides a ‘Pay Pass-Mag Stripe’ application, which can process transactions based on proximity cards and magnetic stripe cards. (See FIG. 5). The PayPass-Mag Stripe application is an extension of the currently available magnetic-stripe applications for debit and credit payments.”), [0026] (“payment card 1 computes a CVC3 number based on a portion of the UN and transmits the computed CVC3 number to terminal. Payment card 1 may use a secret encryption key stored on the card for computing the CVC3 number. Alternatively, payment card 1 may be personalized at the card issuer option to compute the CVC3 number based on a portion of the UN and on the card’s application transaction counter (ATC).”), [0037]-[0039]; EX1003, ¶94.

Claims 77, 86

As discussed above, the combination’s device 1/1’ in one example is a mobile telephone (cellular telephone or cell phone) (*cellular network device*) configured to “communicate secure data, via the mobile telecommunications network” or the NFC connection (*transmit the data communications package over a wireless network*). EX1004, 6:35-41 (“In the examples shown in FIGS. 1

and 2 the devices 1 and 1' are mobile telephones (cellular telephones or 'cell phones'), although the device may be any suitable portable (user-carryable) user device having mobile communications such as a for example a portable computing device, for example a PDA or laptop having mobile communications facilities"), 15:25-35 ("devices...communicate secure data, via the mobile telecommunications network"), FIGS. 1-2; *supra*, §IV.A.4, Elements [60.pre], [60.4]. For Claim 86, the **communications controller** — operational components 16 and controller 40 of NFC communicator 15, provided by integrated circuit(s) on the mounting structure — receives the communications data package from the interrogator for that transmission. *Supra*, Elements [60.1], [60.4]; EX1003, ¶95.

Claims 1, 10, 22, 31, 40, 52

[1.pre]/[10.pre]/[22.pre]/[31.pre]/[40.pre]/[52.pre]

Supra, [60.pre]. EX1003, ¶96.

[1.1]/[10.1]/[22.1]/[31.1]/[40.1]/[52.1]

Supra, [60.1]. EX1003, ¶97.

a) First Mapping

Huomo's SE card (**token**) connects to a controller 20 of the device 1/1', which may be a laptop, (**computer terminal**) through a "coupling interface 34 comprising one or more coupling elements 35 which may be electrical contact elements" (**communication connector**) "to enable communication of data between

the controller and the secure element” card (*token*) “in compliance with ISO 7816.” EX1004, 3:33-40, 6:23-41, 7:47-52, 8:5-34, 20:48-54, 21:11-14. Based on Huomo’s express disclosure of the SE in the form of a SIM card or SD card, a POSITA would have understood and found it obvious that the SE card (*token*) includes a substrate or a printed circuit board in a plastic cover (*mounting structure*) with contact terminals (*communication connector*) to connect to the device 1/1’ (*computer terminal*). EX1003, ¶98.

b) Second Mapping

Huomo’s NFC communicator “communicate[s] data stored by the secure element 30 [of sending device 1/1’]... to another near field RF communicator” of “another device” (recipient device) through a near field radio frequency (“RF”) connection/link (*communication connector*). *Supra*, §IV.A.1; EX1004, Abstract, 2:3-7, 2:47-67, 3:20-26, 5:24-40, 6:23-28, 17:64-18:24 (reader 2001), FIGS. 1-2. A POSITA would have understood that the near field reader 2001 is a *computer terminal*. EX1003, ¶99.

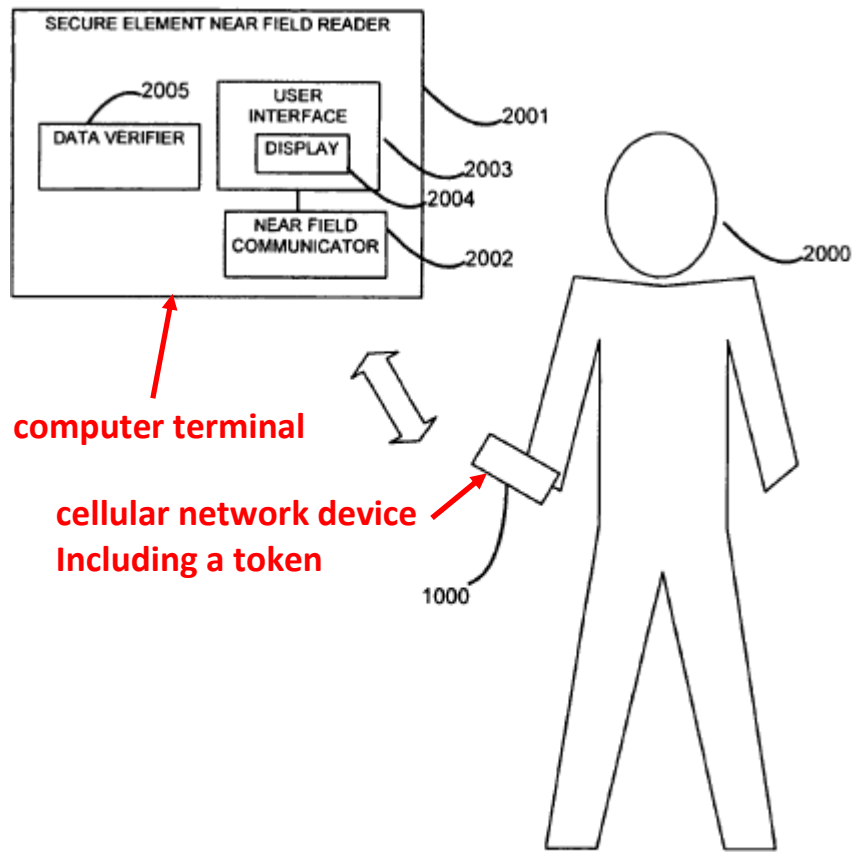


FIG. 13

EX1004, FIG. 13

[1.2]/[10.2]/[22.2]/[31.2]/[40.2]/[52.2]

Supra, [60.2]. EX1003, ¶100.

[10.2]/[40.2]

Supra, §IV.A.4, Element [1.2]. EX1003, ¶101. The SE 30/31 “is configured to be programmed or is already programmed with an operating system and one or more applications platforms to enable the secure element to load a corresponding application to enable a transaction to be effected such as at least one

of payment” (*payment card application*) for products and/or services. EX1004, 5:41-6:22. Huomo explains that “[t]he types of transactions that can be handled by the device 1 or 1’ are determined by the applications platform or platforms loaded onto the secure element 30 or 31.” *Id.*; *see also id.*; 11:28-52, 16:18-33; EX1005, [0025], [0036]-[0037].

[1.3]/[10.3]/[22.3]/[31.3]/[40.3]/[52.3]

Supra, [60.3]. EX1003, ¶102. The exchange between the secure element and the secure element interrogator takes place within the SE between memory store 33 and controller 32. *Id.*; EX1004, 7:19-52; *see also* 6:23-28; 7:47-52. A POSITA would have understood and found obvious from Huomo’s description that the transaction data communications acquiring the transaction/payment data including the credit/debit card number (*transaction information*) to pass only between those two components alone, especially as Huomo describes no other participant on that link. EX1004, 6:23-28, 7:47-52, FIG. 1; EX1003, ¶102.

[1.4]/[10.4]/[22.4]/[31.4]/[40.4]/[52.4]

Supra, [60.4]. EX1003, ¶103.

a) First Mapping

Huomo’s NFC communicator controller (*communications controller*) receives the APDU (*data*) from the secure element controller (*interrogator*) and transmits the APDU with the transaction/payment data including the credit/debit

card number (*transaction information*) to the device 1/1' (*computer terminal*) controller through the coupling elements 35 (*communication connector*).

EX1003, ¶104.

b) Second Mapping

Huomo's "NFC communicator 15" (*communications controller*) receives the APDU (*data*) from controller 20 (*secure element interrogator*) and transmits the APDU with the transaction/payment data including a credit/debit card number (*transaction information*) to "an external near field RF communicator" (*computer terminal*) through the NFC connection (*communications connector*). *Supra*, §§IV.A.1, 4, *infra*, [1.1]; Elements [60.1]-[60.3]; EX1004, Abstract, 2:47-67, 3:20-40, 5:22-40, 6:23-41, 13:50-55, 20:11-12, 23:42-45, 24:4-17, 25:11-16, 25:35-40, FIGS. 1-2, claims 11-12; EX1003, ¶105.

For both mappings, because the exchange of transaction data communications between secure element and the *interrogator* for acquiring transaction information from the secure element during a single interrogation session occur only between the secure element and the interrogator, it would have been obvious that the output transaction information transmitted by the communications controller to the computer terminal is *a single data communication*. *Supra*, §IV.A.4, Element [1.3]. Even if Huomo alone did not make this obvious, Huomo-Smets makes it explicit, where at the end of an

interrogation to acquire transaction information, the transaction information is transmitted to the computer terminal as **Track data** via “a standardized message” (**a single data communication**). *Supra*, §IV.A.2-4, Element [1.3]; EX1005, Abstract, [0014], [0026] (“terminal 2 packages or formats the ATC, UN, and the CVC3 number in a discretionary data field according to these rules.”), [0029]-[0031], [0035], [0036]-[0039], FIG. 6; EX1003, ¶106.

Claims 2, 11, 23, 32, 41, 53, 61, 80

As discussed above, the Huomo-Smets combination provides ISO 7816-4 command-layer commands and responses (APDUs), e.g., “GET PROCESSING OPTIONS,” “READ RECORD,” “COMPUTE CRYPTOGRAPHIC CHECKSUM,” for a plurality of transaction data communications between the secure element and the secure element interrogator in a single interrogation session to acquire Track data for transactions. *Supra*, §IV.A.1-4, Element [1.3]; EX1004, 7:51-52; EX1005, [0036]-[0039], FIG. 6; EX1003, ¶107.

Claims 3, 12, 24, 33, 42, 54, 62

Huomo’s secure element 30/31 already stores an **encryption algorithm** and an **encryption key** (e.g., “a private key or keys” of a “a public-private key encryption system”) to encrypt transaction data. *Supra*, §IV.A.1; EX1004, 3:58-62, 5:26-52, 7:19-65, 8:25-34, 11:28-34, 15:33-36, 23:67-24:3; EX1003, ¶108.

In the Huomo-Smets combination, the secure element uses the stored

encryption key to calculate a dynamic CVC3, using the unpredictable number (UN) and an “application transaction counter (ATC)” (*transaction counter*) also stored on the secure element, in accordance with Smets. *Supra*, §IV.A.2-3; EX1005, [0026]; *see also id.*, [0014], claims 3 and 10; EX1003, ¶109.

Claims 4, 13, 25, 34, 43, 55, 63, 81

Supra, §IV.A.3-4, Element [60.3]; EX1004, 6:23-28, 7:51-52; EX1005, [0036]-[0039], FIG. 6 (below). Under both mappings, that exchange occurs only between the combination’s *secure element* and *interrogator*, over their coupling interface, and only within libraries or memory space (e.g., “memory 33”) *residing on the mounting structure* — both components are integrated circuit(s) on the same substrate or PCB, so no transaction data communication leaves the mounting structure. EX1004, Abstract, 2:35-37, 2:47-67, 3:44-55, 5:22-23, 6:23-28, 7:31-52, 24:4-17, FIG. 1 (below); EX1005, [0036]-[0039], FIG. 6; EX1003, ¶110.

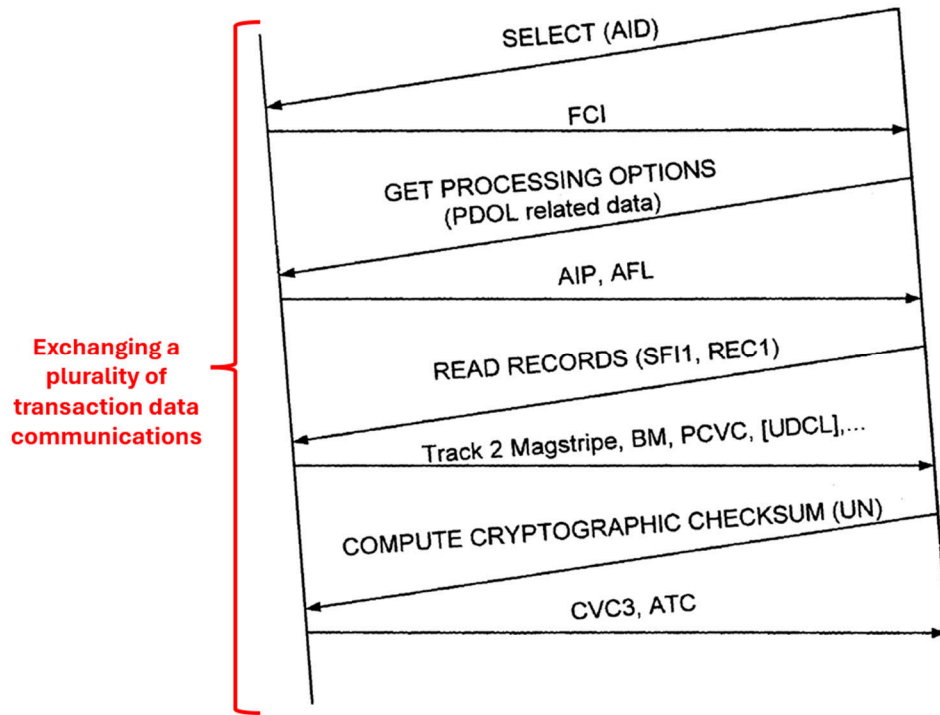


FIG. 6. Transaction Flow

EX1005, FIG. 6 (annotated)

Claims 5, 26, 35

Supra, §IV.A.4, Element [10.2] (regarding *payment card application*);
EX1004, 5:41-6:22, 11:28-52, 16:18-33; EX1005, [0025], [0036]-[0037]. EX1003,
¶111.

The combined system embeds transaction data retrieved from the secure element within standardized magnetic stripe track formats (e.g., Track 1, Track 2, and Track 3 data) (*single data communication ... comprises track data*) before transmitting to the host (*computer terminal*), for processing magnetic stripe card transactions. *Supra*, §IV.A.2-3; EX1005, Abstract, [0004]-[0008], [0011]-[0013],

[0025]-[0026], [0037]-[0039], FIG. 5; EX1003, ¶112.

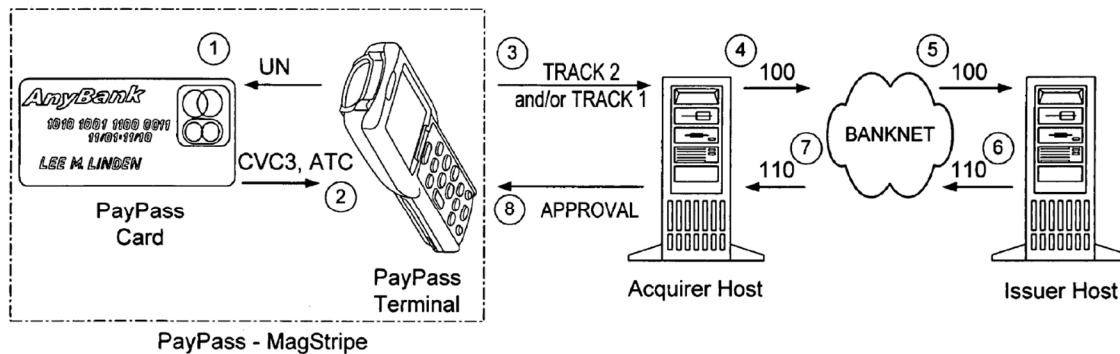


FIG. 5

EX1005, FIG. 5

Claims 6, 16, 27, 36, 46, 56, 64, 82

Supra, §IV.A.4, Element [60.3] (the secure element interrogator reading transaction information from the secure element 30 corresponds to *a secure element reader*); EX1003, ¶113.

Claims 7, 17, 28, 37, 47, 57, 66, 84

Huomo describes NFC communicator 15 comprises “a coupler 17 comprising an inductor or coil in the form of an antenna 18 and antenna circuitry 19” (antenna) that inductively couples to the antenna of another near field RF communicator to transmit and receive data. EX1004, 6:55-7:3, 8:50-53, 24:4-6, FIGS. 1-2. Huomo further describes a “load modulation” mode in which the NFC communicator responds to commands “sent to an NFC communicator from, for example, an RFID reader” (interrogated by an external reader), and a “secure

element near field reader 1007 capable of reading by near field communication transaction data from the secure element” of devices 1000-1002. EX1004, 13:50-15:2, 15:5-50 (describing FIG. 10); EX1003, ¶114.

Claims 8, 19, 29, 38, 49, 58

[8.1]/[29.1]/[38.1]/[58.1]/[19.1]/[49.1]

Huomo’s banking applications and payment applications stored in the secure element are executable payment card applications (or applets). *Supra*, §IV.A.4, Claim [5]; EX1004, 5:41-6:22, 11:28-52, 16:18-33. Huomo explains that the data stored by memory store 33 “will generally include data such as program data comprising commands and instructions of the applications platform(s) and operating system and content data such as data used by the program data, transaction data and user data.” EX1004, 10:46-51; EX1003, ¶115; *see also id.*, 13:522, 16:64-65, claim 25.

[8.2]/[19.2]/[29.2]/[38.2]/[49.2]/[58.2]

Supra, §IV.A.4, Element [1.3] and Claim [5]. EX1003, ¶116.

Claims 9, 18, 21, 30, 39, 48, 51, 59, 67, 78, 85, 87

[9.1]/[30.1]/[39.1]/[59.1]/[78.1]/[87.1]/[18.1]/[48.1]/[67.1]/[85.1]

Supra, §IV.A.4, Claim [5]. For [18.1], [48.1], [67.1], and [85.1], in the combined system, Huomo’s secure element is “programmed with an operating system and one or more applications platforms,” and “[t]he types of transactions

that can be handled by the device 1 or 1' are determined by the applications platform or platforms loaded onto the secure element 30 or 31." EX1004, 5:41-6:22. A POSITA would have found it obvious to beneficially load payment applications of different card associations on that secure element, so a single token could serve a cardholder's several cards, furthering Uomo's express objectives. EX1005, [0025]; EX1003, ¶117.

[9.2]/[30.2]/[39.2]/[59.2]/[78.2]/[87.2]/[18.2]/[48.2]/[67.2]/[85.2]

Supra, §IV.A.4, Claim [5]. EX1003, ¶118.

*[9.3]/[21]/[30.3]/[39.3]/[51]/[59.3]/[78.3]
[87.3]*

Supra, §IV.A.4, Claim [5] (track data provides *card-present data*); EX1001, 5:12-36. EX1003, ¶119.

Claims 14, 44

Smets describes its reader terminal providing "an unpredictable number (UN)" to the payment card (secure element), which then "computes a CVC3 number based on a portion of the UN and transmits the computed CVC3 number to terminal." EX1005, [0026], [0028], [0037]. In the combined system, components or computing systems in the transaction stream, other than the reader, beneficially perform the same function of generating the unpredictable number and transmitting to the secure element — for example, that the Uomo-Smets combination's NFC communicator 15 (e.g., its operational components 16 and controller 40)

(*communications controller*) creates the UN and sends it to secure element 30.

EX1003, ¶120; EX1008, 5:35-41, 7:22-30.

Claims 15, 45

Supra, Claim 65. EX1003, ¶121.

Claims 20, 50

Supra, §IV.A.4, Claim [65] (the combination’s “‘PayPass-MagStripe’ application” providing *an application level protocol* for dynamic authentication of the secure element). EX1003, ¶122.

Claims 68-69

Supra, §IV.A.4, Elements [60.pre], [79.pre] (“cellular network device,” “mobile phone”); *supra*, Element [60.2] (“secure element”), [60.3] (“interrogator”), [60.4] (“communications controller”). EX1003, ¶124.

Claim 70

a) First Mapping

A POSITA would have recognized, and found obvious from Huomo’s description, that the SIM card includes an IC chip mounted on a substrate (*mounting structure comprises a substrate*). *Supra*, §IV.A.4, Element [60.1]; *see also* EX1017, [0013], [0145], FIG. 1; EX1003, ¶125-126.

b) Second Mapping

A POSITA would have found it obvious from Huomo’s description that the ICs in Huomo’s *token* are affixed to a *mounting structure* such as a PCB board

(*substrate*). EX1003, ¶127.

Claim 71

a) First Mapping

A POSITA would have also recognized, and found obvious, from Huomo's description, that a SD card includes chips mounted to a printed circuit board and integrated in a plastic cover (*mounting structure comprises a packaging case*).

Supra, §IV.A.4, Element [60.1]; EX1018, [0002]; EX1003, ¶¶128-129.

b) Second Mapping

A POSITA would have found it obvious from Huomo's description that the ICs in Huomo's *token* are affixed to a *mounting structure* such as a PCB board in the device's housing (*a packaging case*). EX1003, ¶130.

Claim 76

Supra, Element [60.pre] (first mapping). EX1003, ¶¶123, 131.

B. GROUND 1B – Huomo-Smets-Kisliakov Renders Obvious Claims 1-71, 76-87

1. Kisliakov

Like Huomo, Smets, and the '924 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. EX1003, ¶132; EX1010, Abstract, [0002]-[0003], [0086], [0095], [0101], [0243]-[0245], [0264], [0219], [0234]. 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], [0268]; *see also id.*, [0272]-[0286], [0338]-[0349], [0323]-[0335], [0343], [0354], [0241]-[0245]; EX1003, ¶133.

2. Huomo-Smets-Kisliakov Combination

c) Kisliakov is Analogous Art to the '924 Patent

Kisliakov is analogous art, as it is both in the same field and reasonable pertinent to the problems, of the '924 Patent. EX1001, 1:24-29; 1:44-50 (“enhanced security and fraud prevention techniques”), 4:52-67, 5:5-11, 5:12-26, 5:27-36, 5:37-55, 5:61-6:3, 6:26-32; 10:4-10, 11:31-37, 18:7-29, 19:19-33, 20:25-27.cl. 1 (“A token”); *supra*, IV.B.1 (Kisliakov); EX1003, ¶134.

d) A POSITA would have been Motivated to Combine Huomo-Smets-Kisliakov

Smets already describes ISO 7816-4 type commands and responses (Application Protocol Data Units, or APDUs), e.g., “GET PROCESSING OPTIONS,” “READ RECORD,” for transaction data communications between the

payment card (or secure element) and the reader in a single interrogation session, without expressly using the term “ISO 7816-4” or “APDU.” *Supra*, §IV.A.2; EX1005, [0036]-[0039], FIG. 6. Kisliakov provides an example of conventional commands and responses expressed in the APDU format “as described in the ‘ISO/IEC 7816-4 Standards.’” EX1010, [0268]. This is also consistent with Huomo’s secure element and reader (controller 20) interface that is “in compliance with ISO 7816.” EX1004, 7:51-52, FIG. 1; EX1003, ¶135.

Multiple predictable benefits would have motivated a POSITA to implement Huomo-Smets system as an ISO 7816-4 file system and data communication between the interrogator (e.g., controller 32 or controller 20) and the secure element (e.g., its memory 33) as ISO 7816-4 file system commands, in accordance with Kisliakov. EX1003, ¶136.

First, a POSITA would have combined Huomo-Smets and Kisliakov to promote reliable and robust operation, and interoperability, by utilizing messaging in conformance with a published standard. EX1004, 7:47-52 (“in compliance with ISO 7816”); *see also* 6:23-28, 8:5-34, 20:48-54, 21:11-14, 9:55-59, 11:52-55, 12:13-15, 14:38-62, 18:54-56; EX1010, [0323], [0414]; EX1003, ¶137.

Second, a POSITA would have been motivated to implement Kisliakov’s suggestions in the Huomo-Smets system to promote file handling and control. EX1003, ¶138. For example, implementing messaging according to 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 interrogator (e.g., controller 32 or controller 20) can select individually. EX1010, [0351], [0414].

e) A POSITA would have Reasonably Expected Success when Combining Huomo-Smets 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 system that uses ISO 7816 compliant messaging) to yield predictable results. *KSR*, 550 U.S. at 417; EX1003, ¶139. A POSITA would have had a reasonable expectation of success, especially because the combination would have been implemented primarily through conventional software updates, and Huomo describes communication over an ISO 7816 compliant interface, Huomo's controller 32 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. *Id.*; EX1004, 7:47-56; EX1010, [0268].

3. Analysis

Claims 1, 10, 22, 31, 40, 52, 60, 79

Even if Huomo-Smets did not render obvious *interrogat[ing] the secure element to acquire [the] transaction information from the data file by*

exchanging at least one (or a plurality of) transaction data communication[s] [only] between the secure element and the secure element interrogator, Huomo-Smets-Kisliakov does. *Supra*, §§IV.B.1-2. In the combination, the interrogator (controller 32 (first mapping), controller 20 (second mapping)) acquires that transaction information by interrogating its memory and the interrogation involves an exchange of ISO 7816-4 APDUs—e.g., SELECT FILE and READ BINARY commands and their responses—with the secure element’s memory store 33, and with nothing else. EX1010, [0268], [0323], [0326], [0414]; EX1001, 11:33-37; EX1003, ¶140.

Claims 2, 11, 23, 32, 41, 53, 61, 80

Even if the Huomo-Smets combination did not render obvious *ISO 7816-4* type of commands and responses (APDUs) (*plurality of transaction data communications*) between the secure element and the secure element interrogator (e.g., controller 32 (first mapping), controller 20 (second mapping)), the Huomo-Smets-Kisliakov combination renders obvious such features through express disclosure. *Supra*, §§IV.B.1-2; EX1003, ¶141.

Remaining Challenged Claims

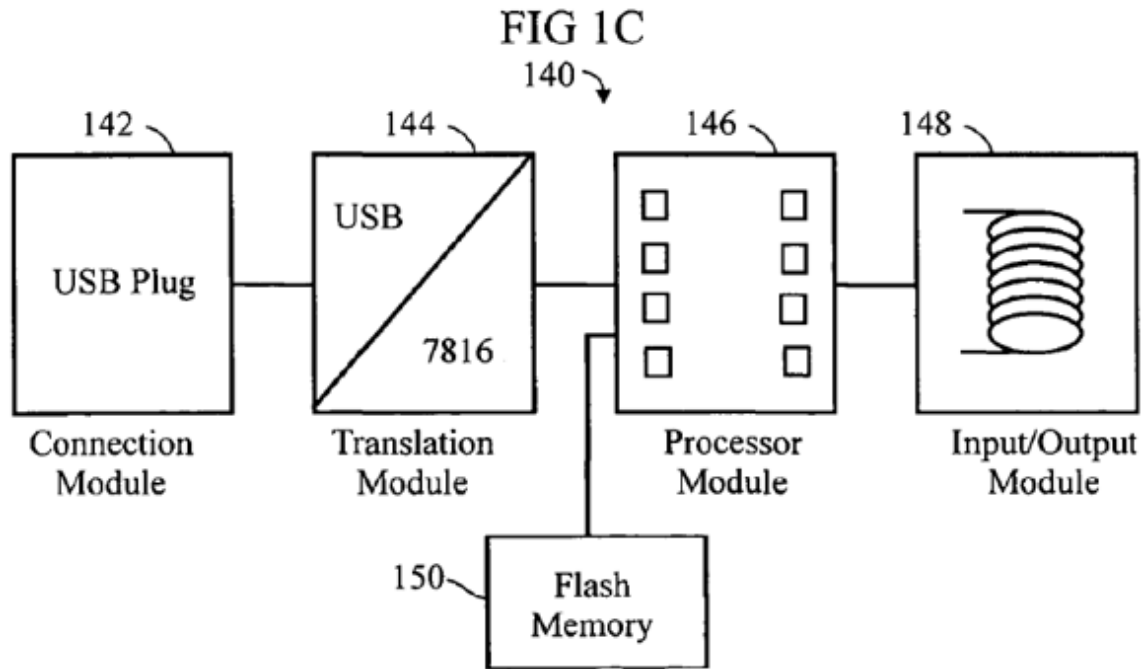
The remaining limitations of Claims 1-71 and 76-87 are met as shown in Ground 1A. *Supra*, §IV.A.4; EX1003, ¶142.

C. GROUND 2A – Ryan-Abbott Renders Obvious Claims 1-2, 4, 6-8, 22-23, 25, 27-29, 31-32, 34, 36-38, 52-53, 55-58, 60-61, 63-64, 66-77, 79-82, and 84-86

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 (“secure identification, electronic payment transaction and authentication are completed”), 1:45 (“Internet transactions”), 2:31-40, 3:18-23, 5:13-30, 12:58-67, 13:32-38, 15:52-55, 29:20-22; EX1003, ¶143.

Figure 1C illustrates Ryan’s 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—provided on the same mounting structure of token 140. EX1006, 17:35-18:54, FIG. 1A, 1C; *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, ¶¶144-148.



EX1006, FIG. 1C

2. Abbott

Like Ryan, Abbott describes a USB-compliant personal key architecture (e.g., “compact personal token (300)”) in which a translation module (e.g., “translation module 318”) resides within an interface processor positioned between a host computer and a secure smartcard processor (e.g., “smartcard processor 320”). *See e.g.*, EX1009, Title, Abstract, 9:12-10:15, claim 1 (“A compact personal token (300)...”), FIG. 3; EX1003, ¶149.

Messages originating at the host are packaged using USB conventions and transmitted to the personal key/token (300) and, upon arrival, the translation module 318 performs “unpackaging...to recover the smartcard reader command” and then translates that command into “a smartcard command within the personal

key...[which is] provided to the smartcard processor [320].” EX1009, 4:9-18, 10:17-11:7, FIGS. 3, 4B. Conversely, responses generated by the smartcard processor 320 are returned to the interface processor, translated into reader-level responses if needed, and then transmitted back to the host after being “packaged by the translation module 318” using USB framing, including the addition of USB headers and related metadata prior to transmission. EX1009, 10:17-11:11, Table II (“the translation module 318 adds a USB header to create a USB response”); EX1003, ¶150.

This bidirectional translation pipeline enables the smartcard processor 320 to operate as if it were connected to a conventional smartcard reader, while still communicating over a USB interface (326). EX1009, 11:12-13, claim 2. The packaging step ensures that smartcard-level transaction responses (e.g., command results, ATR responses, or protocol exchanges) are properly formatted for transport over the USB interface, while preserving the semantics of the underlying smartcard communication. EX1009, 10:17-11:11, 14:1-15; EX1003, ¶151.

3. Ryan-Abbott Combination

a) Ryan and Abbott are Analogous Art to the '924 Patent

Ryan and Abbott are within the same field of endeavor (EX1001, 1:24-28; cl. 1 (“A token”); *supra*, IV.C.1-2) and reasonably pertinent to the problems the '924 Patent purports to solve. *See, e.g.*, EX1001, 1:44-50, 4:52-67, 5:5-11,

5:12-26, 5:27-36, 5:37-55, 5:61-6:3, 6:26-32; 10:4-10, 11:31-37, 18:7-29, 19:19-33, 20:25-27; *infra*, IV.C.3; EX1009, 1:16-18, 2:9-11; EX1003, ¶152; *see also, supra*, §III.B (application of Ryan by Examiner).

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

Ryan already defines its translation module 104 as a protocol translation boundary between the host interface (e.g., USB) and the smartcard domain (e.g., ISO 7816), and it may be implemented as a microcontroller performing interface translation between USB and the processor module. *Supra*, §IV.C.1; EX1006, 14:31-35, 18:12-22. This bidirectional conversion role already includes parsing and constructing messages at both interfaces. EX1003, ¶153. Abbott provides an example of a translation module that performs a closely aligned function and makes express the known technique of including packaging and unpackaging of messages with USB framing (adding/removing USB header and metadata to/from smartcard response / command messages). *Supra*, §IV.C.1. Abbott explains that “messages transmitted by the smartcard processor 320...are packaged by the translation module 318” before transmission to the host. EX1009, 10:17-11:11, FIGS. 3, 4B, Table II. A POSITA would have naturally been motivated to look to Abbott for implementation details for a packaged single-message transmission. EX1003, ¶153. In the Ryan-Abbott combination, Ryan’s translation module 104 is

enhanced with Abbott's suggestions of message packaging functionality of translation module 318. *Id.*

Multiple considerations would have led a POSITA to implement this combination. EX1003, ¶154.

First, a POSITA would have been motivated to implement this combination for clean separation between transport protocol (USB) and application protocol (ISO 7816 smart-card messaging). Abbott's explicit message packaging ensures that each layer is clearly delimited. EX1006, 17:35-18:38; FIGS. 1A, 1C; EX1009, 9:12-11:16. This reduces ambiguity in message parsing on the host side and enables compatibility with existing middleware or drivers that expect USB-framed payloads, which is particularly important for transaction-oriented data exchanged with secure elements. EX1003, ¶155.

Second, a POSITA would have been motivated to implement the Ryan-Abbott combination for enhanced robustness or fault tolerance (the system works reliably even when things go wrong). EX1003, ¶156. Incorporating Abbott's message packaging functionality into Ryan's translation module introduces message headers for better error detection, improved synchronization and safer multi-message handling, such that messages do not get mixed up, errors are easier to detect, and communication stays consistent. *Id.*; EX1006, 13:58-67, 18:12-29, 27:19-20; EX1009, 4:9-18, 10:17-11:13, FIGS. 3, 4B, Table II.

Third, a POSITA would have been motivated to use Abbott’s message packaging suggestions in Ryan for improved host-side interoperability. For example, incorporating Abbott’s structured message format promotes compatibility with various host drivers and middleware through supporting standardized communication framing (e.g., USB). EX1006, Abstract (desire for capability of “exchanging information with other devices having compatible interfaces”), 14:28-37, 18:12-38; EX1009, 1:16-18 (“compatible with existing smartcard processors, drivers, and instruction sets”), 3:17-23 (desire to use with “legacy personal identification devices...mak[ing] maximum use of existing smartcard protocols, software and devices wherever possible...retain[ing] at least a limited compatibility with existing devices designed to interact with smartcards”), 4:9-18, 10:17-11:13; EX1003, ¶157.

In addition, a POSITA would have found it obvious to use Abbott’s SREM (smartcard reader emulation module) functionality in Ryan’s processor module 106/146 to explicitly emulate reader behavior as a functional enhancement. EX1003, ¶158. Abbott explains that the SREM “implements functions that emulate those of a smartcard reader, thus projecting the image of a smartcard reader to the smartcard processor 320,” and “provides all instructions and commands to the smartcard processor 320 and receives messages and responses ... according to the [smartcard] protocol.” EX1009, 10:10-16. Ryan’s translation

module 104 already performs bidirectional movement and conversion of signals between USB and smart-card formats, and may be implemented as a programmable microcontroller and even be integrated into the processor module. *Supra*, §IV.C.1; EX1006, 18:12-22. Such incorporation has the benefit of native compatibility with existing smartcard software and protocols (Abbott explicitly frames SREM as enabling reuse of legacy smartcard environments), allowing Ryan's secure processor module to interact seamlessly with standard smartcard common workflows. EX1009, 1:16-18 ("compatible with existing smartcard processors, drivers, and instruction sets"). Additional benefits include, but are not limited to, decoupling of host interfaces from processor constraints and stronger modular separation and control over secure communications, promoting interoperability and transaction reliability. EX1003, ¶158. Packaging the transaction information inside the processor module results in the data being framed before it crosses to the host-facing translation module, such that what reaches the combination's output boundary is already-structured data. *Id.*; EX1006, 19:31-40; EX1009, 10:17-11:11.

c) A POSITA would have Reasonably Expected Success

A POSITA would have expected success in implementing this combination, as Ryan already performs bidirectional conversion between USB messages and smart-card messages, adding a structured packaging layer (USB headers/metadata)

is largely an extension of its existing translation function rather than a fundamental architectural change. Moreover, Ryan explicitly contemplates the translation module may be implemented as a programmable microcontroller or even integrated into the processor module), which further supports the feasibility of adding packet-formatting logic such as USB encapsulation, in accordance with Abbott. EX1003, ¶¶159-160.

4. Analysis

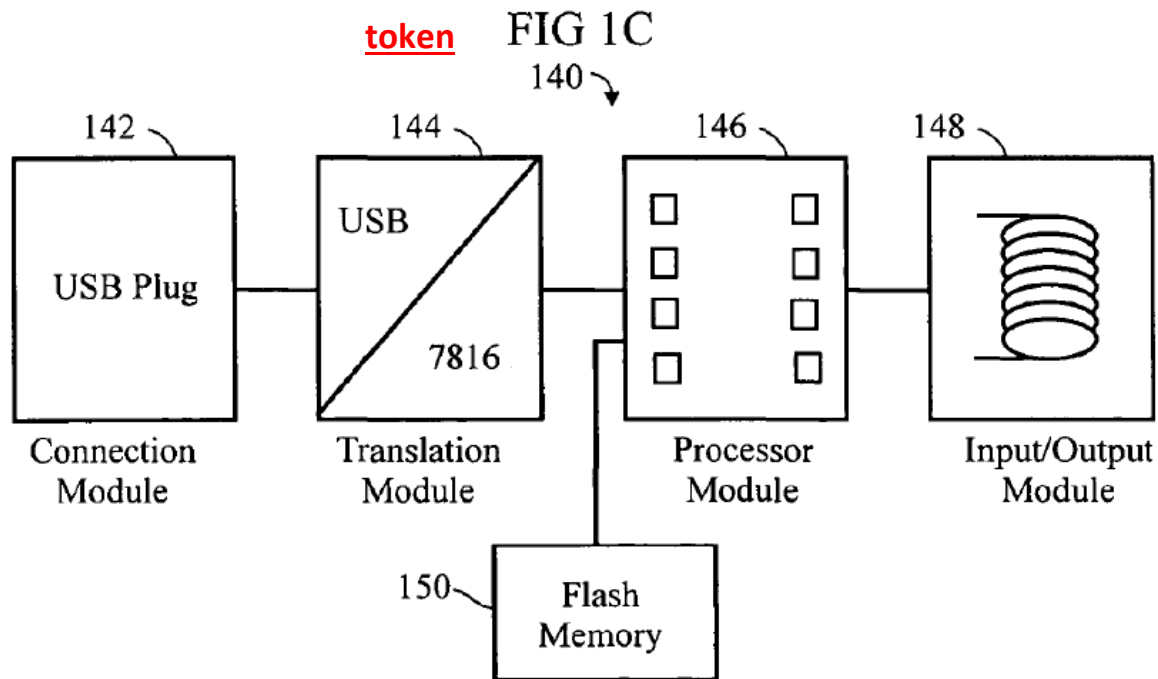
Similar to Ground 1A, elements and claims with overlapping features are addressed in groups. EX1003, ¶161.

Claims 60, 79

[60.pre]

Ryan describes a “compact personal token apparatus” (e.g., “smart fob”) that bridges the “virtual world of the Internet” and “real world transactions,” that “generally comprises a wireless interface,” and that may take “the general form factor required of the standard compliant interface such as SD and Mini SD cards, Multi Media Cards (MMC), PCMCIA Cards, etc.” *Supra*, §IV.C.1; EX1006, Title, Abstract, 2:7-9, 12:58-67, 13:32-38, 15:52-55, 29:20-22 (“[t]he device (smart fob, USB key fob) can function as a Smart Card for online-banking. This embodiment could include a SIM card.”); cf. EX1001, 1:54-56, 4:8-21. Token 140 of FIG. 1C includes 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, Abstract, 17:35-18:54, 19:24-40, FIG. 1C; EX1003, ¶162.



EX1006, FIG. 1C

Ryan's token connects to a host device. EX1003, ¶163. Ryan states that the 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. Ryan also describes "a standard-compliant interface releaseably coupleable to a host processing device, this being under the command of an operating system." EX1006, 14:28-30. Ryan explains

that information “received through the RFID-interface can be stored in the memory of the personal token and can then be provided to the host processing device via the standard interface, thus allowing a complete information exchange between the virtual world and the real world.” EX1006, 15:4-8.

In the Ryan-Abbott combination, the transaction information acquired from the processor module is transmitted to the host as a single packaged message (*a communications data package*), in accordance with Abbott’s suggestions. See §IV.C.3, *supra*; EX1009, 10:17-11:11 (“messages transmitted by the smartcard processor 320 to the host computer 102 are packaged by the translation module 318”), FIGS. 3, 4B, Table I; EX1003, ¶164.

[79.pre]

Ryan describes “cell phone,” such as “smart cellular phones,” used as “transaction device, data storage device using SD or MMC cards for that,” communicating via various wireless technology (e.g., TDMA, CDMA, GSM digital cellular system) over Internet or “mobile phone networks” (*cellular network device*). EX1006, 6:12-20, 10:3-6 (“A PDA is a handheld device that combines computing, telephone/fax, Internet and networking features. A typical PDA can function as a cellular phone”), 11:20-24 (“TDMA Short for ‘Time Division Multiple Access’, a technology for delivering digital wireless service using time-division multiplexing (TDM). TDMA works by dividing a radio

frequency into time slots and then allocating slots to multiple calls. In this way, a single frequency can support multiple, simultaneous data channels. TDMA is used by the GSM digital cellular system.”), 12:45-48 (“wireless Technology that allows a user to communicate and/or connect to the Internet or mobile phone networks without physical wires. Wi-Fi, Bluetooth®, CDMA and GSM are all examples of wireless technology.”); *infra*, Elements [60.1]-[60.4]; Claim 76; EX1003, ¶165.

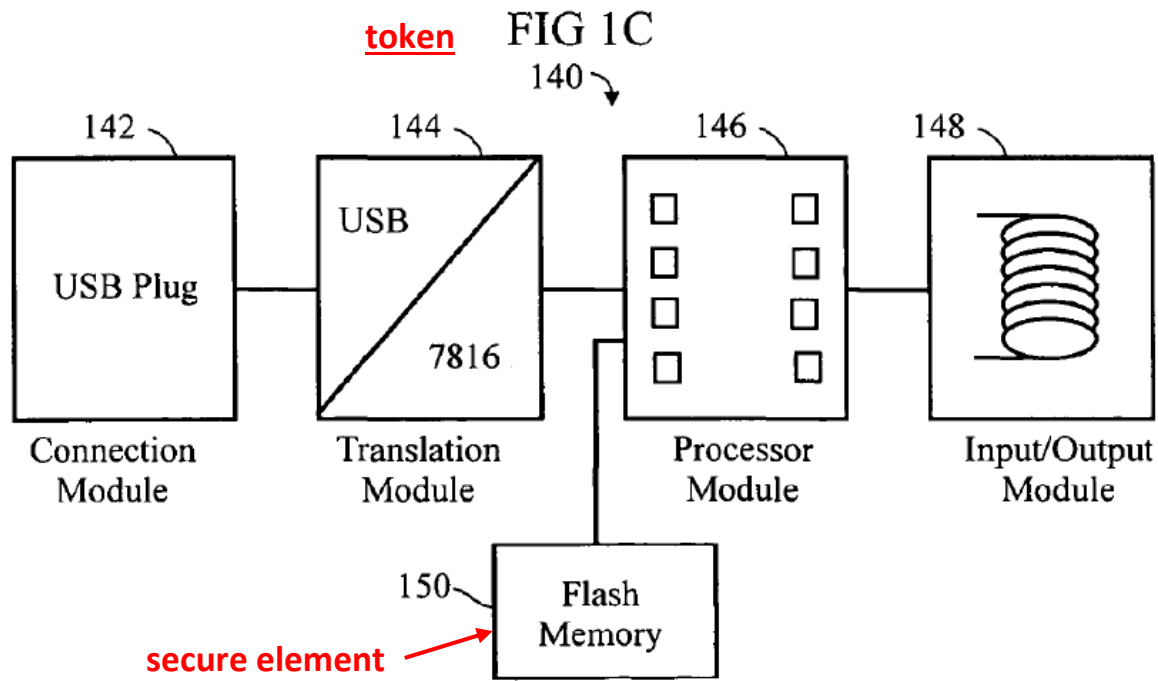
Ryan makes clear that “the compact personal token apparatus (or equivalent) may remain in the apparatus capable of interacting with the personal token (e.g., cell phone, PDA), when the personal token device communicates contactlessly in the real world. It does not necessarily have to be removed from the host device.” EX1006, 13:39-44; EX1003, ¶166.

[60.1]/[79.1]

Ryan explains that the token device’s major components are “mounted on a circuit board (PCB...)” (**mounting structure**) and “within a housing” (**mounting structure**)). EX1006, 4:34-47 (“The personal key comprises a USB-compliant interface releaseably coupleable to a host processing device operating under command of an operating system”), 17:35-57, 15:29-33 (“a connection module, connecting the personal token apparatus to a host device such as PC, PDA, smart cellular phone or similar device”), FIG. 1A; EX1003, ¶167.

[60.2]/[79.2]

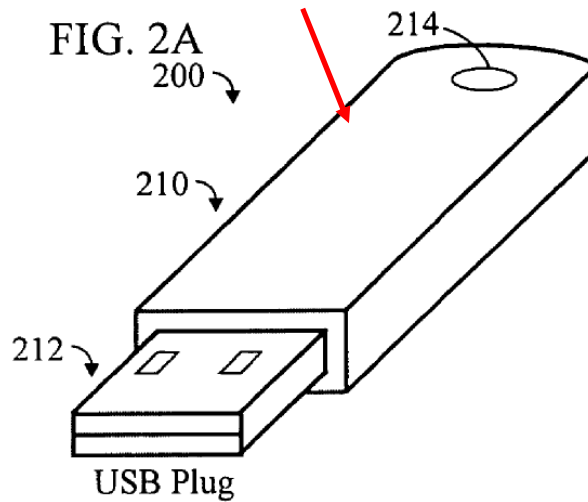
Ryan's token includes a flash memory 150. EX1006, 15:21-24. In the FIG. 1C embodiment, "a flash memory device 150 can be included, with a storage capacity of 1 to 4 megabytes (or more) for the purpose of running applications." EX1006, 19:31-36; *see also* EX1006, 4:34-47, FIGS. 1A, 1C. Ryan describes the "flash memory device may be any suitable device including, but not limited to, Secure Digital (SD) card format, and including SIM card." EX1006, 19:36-38. 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, ¶168.



EX1006, FIG. 1C

As one example, 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 [60.1]) of the main body portion 210 of the token. EX1003, ¶169. A POSITA would have further found obvious that the flash memory is beneficially affixed to the mounting structure with the processor module based 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.

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



EX1006, FIG. 2A

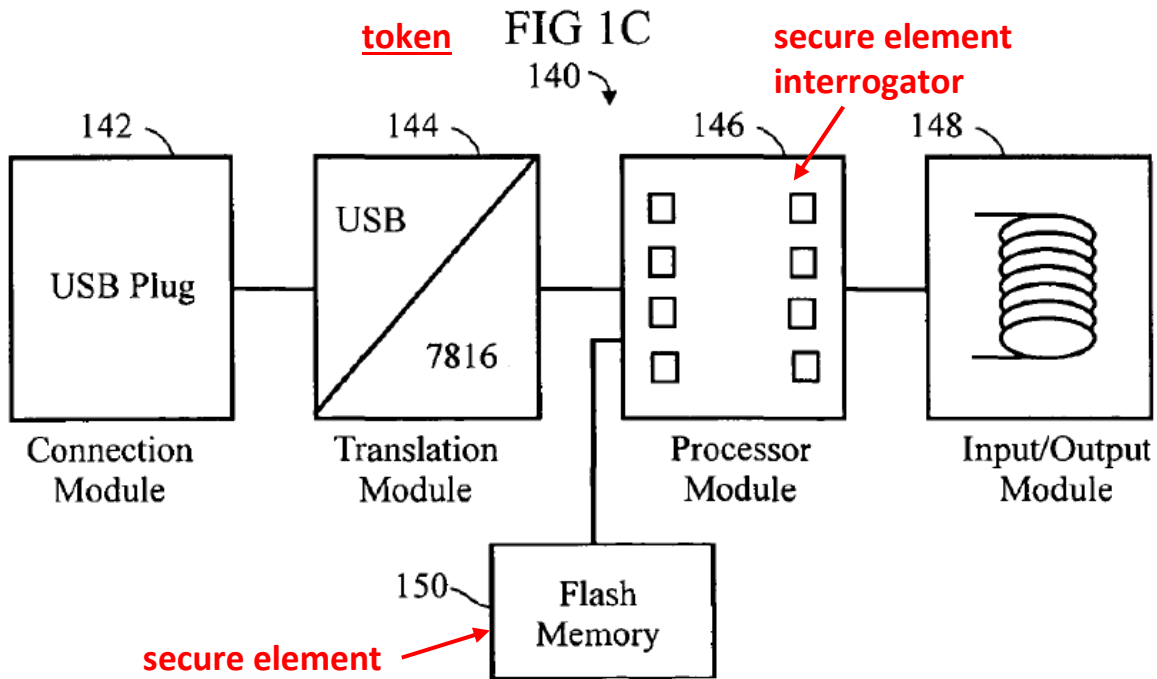
Ryan describes the transaction information stored in that memory, including that “credit card details can be encrypted and stored in the smart fob.” EX1006, 24:24-26. Ryan discloses that the processor module 106/146 and the output module 148 “is sufficient for conducting real world, contactless transactions, 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. 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, ¶170 (citing EX1007, 15:40-46). A POSITA would have understood, and

found obvious from Ryan's teachings, that credentials and stored value of this kind reside in one or more data files of the token's on-board non-volatile memory, in furtherance of Ryan's express objectives. *Id.*

Ryan repeatedly describes loading, storing, decrementing, and using stored value on the token device (e.g., "smart fob," "a SIM card, "SD card") itself, which resides in one or more data files (*a data file*) of the on-card non-volatile memory, e.g., a flash memory 150" (*secure element*). EX1003, ¶171; EX1006, claim 1, 4:21, 19:31-40, 24:24-26, 21:23-60, 23:10-14, 28:30-37, 30:52-57. Ryan describes "tamper-resistant" techniques, and that the data on the chip is encrypted and decrypted, further highlighting the module is a "secure element." EX1006, 32:54-63; EX1003, ¶172.

[60.3]/[79.3]

Ryan's processor module 106/146 provides a *secure element interrogator*. EX1006, 18:30-38, 19:24-40, FIGS. 1A, 1C; EX1003, ¶173. The processor module 106/146 is mounted on the circuit board of the token housing (*affixed to the mounting structure*). EX1006, 17:35-41, FIGS. 1A, 1C; EX1003, ¶173.



EX1006, FIG. 1C

Ryan describes the processor module 106/146 addressing the flash memory 150. EX1006, 15:21-25 (“flash memory and EEPROM device powered and addressed by the processor module.”). Ryan further explains that “[t]he 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; EX1003, ¶174.

Ryan describes the transaction information the processor module reads out from the secure element. Ryan indicates that “credit card details can be encrypted and stored in the smart fob,” (EX1006, 24:24-26), and that the memory can be used

to run applications, EX1006, 28:30-37. A POSITA would have understood that the processor module decrypting the stored credit card details (*transaction information*) for a transaction interrogates and obtains those details out of the memory holding them, especially in view of Ryan's description that the crypto controller operating system is "capable of encrypting and decrypting data to be stored in internal or external memory" (*configured to interrogate the secure element to acquire the transaction information from the data file by exchanging at least one transaction data communication between the secure element and the secure element interrogator*). EX1006, 19:31-40, 24:24-26; EX1003, ¶175.

Ryan describes the processor module generating the outbound message. Ryan explains that the processor module 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, and claims that "the processor module prepares messages to be sent by the contactless and wireless interfaces," EX1006, cl. 43. In the Ryan-Abbott combination, the processor module 106/146 packages the transaction information it reads from the memory into a single message (*communications data package based on the transaction information*) before that information passes outward, in accordance with Abbott's suggestions. *Supra*, §IV.C.3; EX1009, 10:8-16, FIGS. 3, 4B, Table II; EX1003, ¶176.

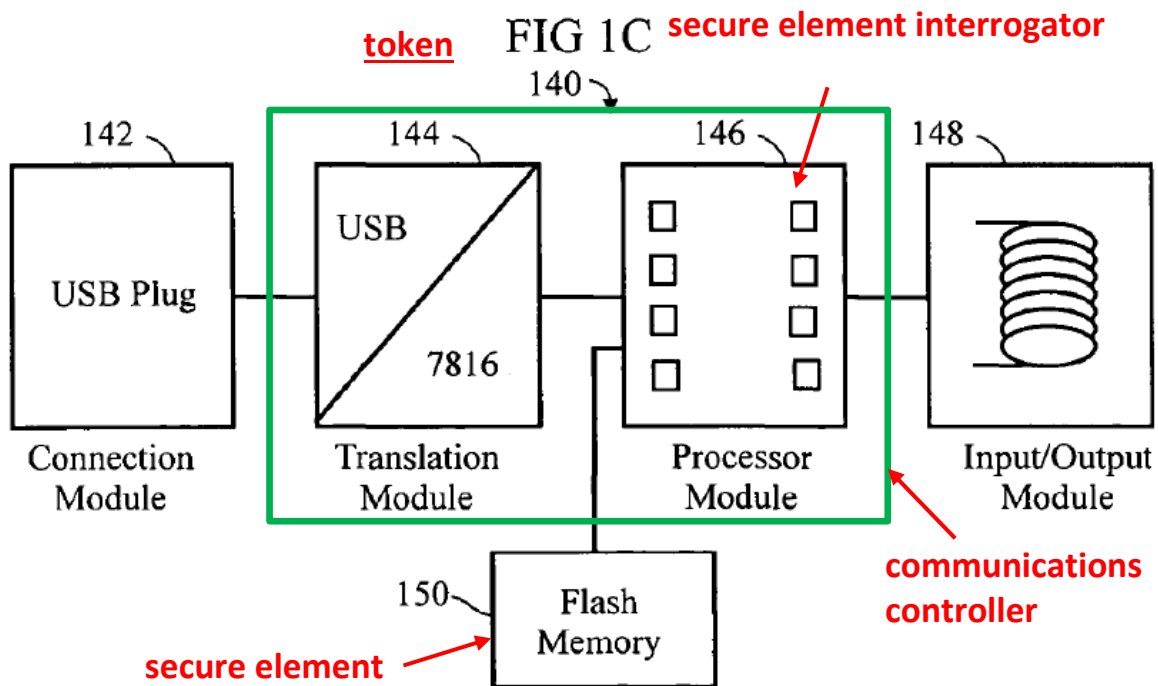
To be clear, in describing the processor module addressing the memory,

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 interrogator*). As such, Ryan additionally renders obvious [60.2] and [60.3] in this manner, even if the processor module and memory together are considered to provide the secure element. EX1003, ¶177.

[60.4]

Ryan describes Ryan's processor module 106/146 provides the *secure element interrogator* described in [60.3], and that chip, together with the coupled translation module 104/144, which is also mounted on the "circuit board" of the token housing (*affixed to the mounting structure*), performs the *communications controller* capabilities. EX1006, 4:34-47 ("the interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages"), 17:35-41, 18:12-22 ("A micro-controller such as an 8 bit micro-controller (ST7 FSCR1E4Ml) can be used as an interface translator chip (104) between the USB connection 102 and the processor module 106. (The processor could be mounted in a SIM module.)."), FIGS. 1A, 1C. Ryan explains that "[t]he translation module 104 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 also* 14:31-35

(“translation of standard-compliant contact based interface messages to ISO 7816 compliant messages and provid[es] the translation of ISO 7816 compliant messages to standard-compliant contact based interface messages.”); *see also* EX1001, 7:43-61; EX1003, ¶178.



The combination’s translation module 104/144 in the *communications controller* receives the packaged message (*communications data package*) from the processor module 106/146 (*secure element interrogator*) and transmits it to the host computer (*host device*) through the connection module 102/142. *Supra*, §IV.C.3-4, Elements [60.pre], [60.3]; EX1006, 15:29-33, 17:47-57, FIGS. 1A, 1C; EX1009, 10:17-11:11, FIGS. 3, 4B, Table II; EX1003, ¶¶179-180.

Claims 77, 86

Supra, §IV.C.4, Elements [60.4], [79.pre]. EX1003, ¶181.

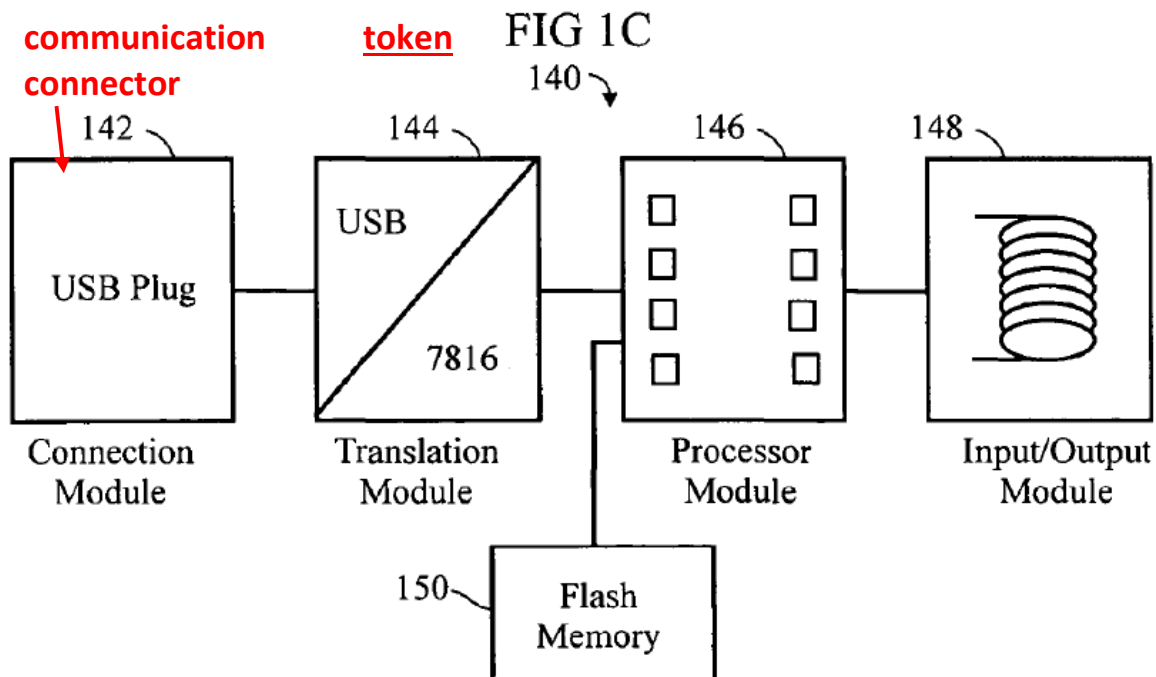
Claims 1, 22, 31, 52

[1.pre]/[22.pre]/[31.pre]/[52.pre]

Supra, §IV.C.4, [60.pre]. EX1003, ¶182.

[1.1]/[22.1]/[31.1]/[52.1]

Supra, §IV.C.4, [60.1]. EX1003, ¶183. The token device has a “connection module 142” (e.g., “a USB plug”) (*communication 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).



EX1006, FIG. 1C

[1.2]/[22.2]/[31.2]/[52.2]

Supra, §IV.C.4, [60.2]. EX1003, ¶184.

[1.3]/[22.3]/[31.3]/[52.3]

Supra, §IV.C.4, [60.3]. The data communications exchange runs between the processor module and the flash memory 150 it addresses, with no other component in between. EX1006, 15:21-25, 19:31-40, FIGS. 1A, 1C; EX1003, ¶185. A POSITA would have understood that the exchange occurs “only between” the secure element and the secure element interrogator, which takes place on that internal address bus alone, especially because Ryan describes the flash memory 150 as “powered and addressed by the processor module” and describes no other participant on that link. *Id.*; EX1006, 15:21-25.

[1.4]/[22.4]/[31.4]/[52.4]

Supra, §IV.C.4, [60.4]. EX1003, ¶186. The combination’s translation module 104/144 in the ***communications controller*** receives the packaged message from the processor module 106/146 (***secure element interrogator***) and transmits it to the host computer (***computer terminal***) through the connection module 102/142 (***communications connector***) as a ***single data communication***. *Supra*, §IV.C.3-4, Elements [60.pre], [60.3]; EX1006, 15:29-33, 17:47-57, FIGS. 1A, 1C; EX1009, 10:17-11:11, FIGS. 3, 4B, Table II.

Claims 2, 23, 32, 53, 61, 80

Ryan describes the processor module that addresses that memory as

equipped for ISO 7816 contact operation. EX1006, 18:30-38, 13:58-61; *see also*, 2:18-60, 4:34-47, 18:12-38. A POSITA would have found obvious from Ryan's description, that the processor module 106/146 and that memory exchange the transaction data communications using APDUs defined in ISO 7816-4 (*communications formatted according to ISO 7816-4*), and—for Claims 2, 23, 61, and 80, which recite a plurality of transaction data communications—that acquiring the transaction information from the secure element's data file comprises more than a single command-and-response pair, especially where the file holding that information is selected before its contents are read. EX1006, 15:21-25, 19:31-40, 24:24-26, 28:30-37; EX1003, ¶187 (citing EX1013, [0006]; EX1014, [0016], [0030]; EX1015, [0034]).

Claims 4, 25, 34, 55, 63, 81

Ryan's processor module 106/146 and the flash memory 150 it addresses are mounted on the circuit board of the token housing (*mounting structure*). EX1006, 17:35-41, FIGS. 1A, 1C; *supra*, [60.2]. The exchange of transaction data communications occurs only between the memory and interrogator, through their coupling interface, all residing on the same device housing, e.g., by integrated circuit(s) on a PCB board in the device (*mounting structure*). EX1003, ¶188

Claims 6, 27, 36, 56, 64, 82

Supra, §IV.C.4, Element [60.3] (the secure element interrogator reading

transaction information from the secure element corresponds to *a secure element reader*). EX1003, ¶189.

Claims 7, 28, 37, 57, 66, 84

Ryan describes the output module comprising “an RF antenna,” the smart card processor “communicating through an RFID-contactless interface and connected to an inductive antenna,” and “an antenna coil in the device that enables the contactless part of a separate contactless smart card to communicate with contactless readers.” EX1006, 18:39-40, 19:4-5, 19:61-20:2, 14:28-39, 29:23-26, 32:43-47; EX1003, ¶190.

Claims 8, 29, 38, 58

[8.1]/[29.1]/[38.1]/[58.1]

Ryan describes its memory (*secure element*) is used “for user authentication . . . and to run applications,” such as “e-payment and similar applications” (*executable application*), and describes the flash memory as included for “running applications.” EX1006, 14:66-15:2, 28:30-37; *see also id.*, 2:61-64, 11:20-24, 15:21-25, 19:31-40, 24:12-13, 24:25-26, 28:1-7, FIGS. 1-3; EX1003, ¶192.

[8.2]/[29.2]/[38.2]/[58.2]

Supra, §IV.C.4, Element [1.3]. EX1003, ¶193.

Claims 67, 85

[67.1]/[85.1]

A POSITA would have found it obvious, in view of Ryan’s express

description above, to load payment applications of different card associations on that secure element, so a single token beneficially serves a cardholder's several cards. *Supra*, §IV.C.4, Claim [8]; EX1003, ¶194.

~~[67.2]/[85.2]~~

Supra, §IV.C.4, Element [1.3], Claim [8]; EX1003, ¶195.

Claims 68, 69

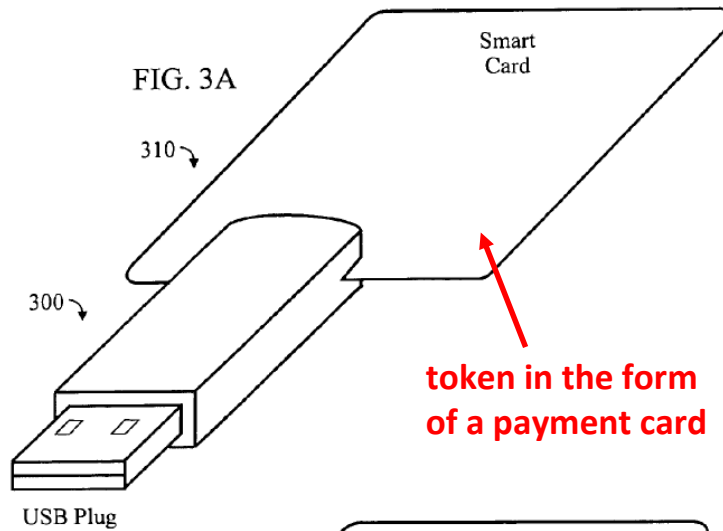
Ryan's token comprises the *secure element*, the *secure element interrogator*, and the *communications controller*, and its connection module connects the token to a "host device such as PC, PDA, smart cellular phone or similar device" (*host device comprises a cellular network device*). *Supra*, §IV.C.4, Elements [79.pre], [60.2]-[60.4]; EX1006, 15:29-33. Ryan further explains that the token "may remain in the apparatus capable of interacting with the personal token (e.g., cell phone, PDA)" such that the cell phone or PDA houses all three components and the host device is *a mobile phone or a PDA* (Claim 69). EX1006, 13:39-44; EX1003, ¶196.

Claims 70/71

Ryan explains that the token device (100)'s major components are "mounted on a circuit board (PCB...)" (*mounting structure comprises a substrate*) and "within a housing" (*mounting structure comprises a packaging case*). EX1006, 4:34-47, 17:35-57, 15:29-33, FIG. 1A; EX1003, ¶¶197-198.

Claim 72

Ryan discloses that the token includes a smart card 310. EX1006, 20:11-18; EX1003, ¶199.



EX1006, FIG. 3A

Claim 73

Ryan discloses that the “compact personal token apparatus is suitably in the general form of a fob.” EX1006, 12:63-65, 13:32-34, 13:67-14:1, 15:52-54, 16:16-18, 17:6-10, 19:45-47, 19:61-63; EX1003, ¶200.

Claim 74

Ryan discloses that the token can take a variety of suitable forms, including separable fobs and cards (e.g., PCMCIA card), thereby rendering obvious [74]. EX1006, 19:61-67, 13:34-37, 20:2-3, EX1001, 3:29-37; EX1003, ¶201.

Claim 75

Ryan discloses that the “device (smart fob, USB key fob) can function as a

dongle for software license authentication.” EX1006, 29:15-16; EX1003, ¶202.

Claim 76

Ryan discloses that the token “can be embodied in a format (form factor) such as that of an SD (secure digital) card.” EX1006, 16:4-10, 13:34-37; EX1003, ¶203.

D. GROUND 2B – Ryan-Abbott-Peart Renders Obvious Claims 3, 5, 9-13, 16-19, 21, 24, 26, 30, 33, 35, 39-43, 46-49, 51, 54, 59, 62, 78, and 87

1. Peart

Peart discloses a system and method for securing transaction information using a seeded cryptographic algorithm in which variable data is hashed to derive a seed and an “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, ¶204.

The “unpredictable number” is integrated into the encrypted transaction information, sent in an authorization message and later validated by a verifying entity (e.g., “an ‘acquirer’ or account issuer”), thereby establishing transaction authenticity. EX1008, Abstract, 2:21-30, 5:4-54, 6:7-7:30, 8:21-35, 9:19-10:2, FIG. 1, 3, 4; EX1003, ¶205.

2. Ryan-Abbott-Peart Combination

a) Peart is Analogous Art to the '924 Patent

Peart is analogous art to the '924 Patent, both because it is within the same field of endeavor (EX1001, 1:24-28; *supra*, IV.D.1; EX1008, 5:35-54, cl. 1), and because Peart is reasonably pertinent to the problems the '924 Patent purports to solve. *See, e.g.*, EX1001, 1:44-50; EX1008 5:1-34; EX1003, ¶206.

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

Ryan already describes secure transaction environments employing cryptographic protection of transaction data including “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, 32:23-31; EX1003, ¶207. 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.D.1; EX1008, Abstract, 2:21-3:15, 7:22-30; EX1003, ¶208.

A POSITA would have found it obvious to utilize Peart’s suggestions in the Ryan-Abbott system, for enhanced secure transaction data transmission, consistent with the express desires of both Ryan and Abbott. 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; EX1003, ¶209.

In Ryan-Abbott-Peart, the transaction information is encrypted at the secure element (per Peart), such that the output is encrypted data. *Supra*, §§IV.C.1, IV.D.1. Multiple considerations would have led a POSITA to implement this combination. EX1003, ¶210.

First, a POSITA would have been motivated to incorporate Peart's cryptographic algorithm into Ryan-Abbott, to promote a self-contained cryptographic mechanism for protecting transaction data before it leaves a secure processing environment. *Supra*, §IV.D.1; EX1006, 1:45, 2:3-9, 2:66-67, 10:35-12:39, 22:24-41, 24:60-61. Even if transaction initiation or form population occurs through less trusted host-side mechanisms, the transaction data itself is cryptographically protected at the secure element. EX1003, ¶211.

Second, a POSITA would have been motivated to incorporate Peart into Ryan-Abbott for transaction uniqueness and protection against replay attacks. Application of Peart's suggestions would predictably support replay-attack protection independent of the external communication channel. EX1008, Abstract, 2:66-67, 5:35-41, 6:29-40, FIG. 3; EX1003, ¶212.

Third, a POSITA would have been motivated to incorporate Peart's algorithm into Ryan-Abbott, because the use of a seed derived from variable data and a repeatable cryptographic process (per Peart) promotes 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, ¶213.

c) A POSITA would have Reasonably Expected Success

Ryan describes cryptographic computation and secure storage, and Peart specifies a known method for generating transaction-specific cryptographic values derived from variable data such as counters and other transaction parameters. 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; EX1003, ¶214.

3. Analysis

Claims 10, 40

[10.pre]/[40.pre]

Supra, §IV.C.4, Element [1.pre]. EX1003, ¶215.

[10.1]/[40.1]

Supra, §IV.C.4, Element [1.1]. EX1003, ¶216.

[10.2]/[40.2]

Supra, §IV.C.4, Element [1.2], Claim [8]. EX1003, ¶216.

[10.3]/[40.3]

Supra, §IV.C.4, Element [1.3]. EX1003, ¶217.

[10.4]/[40.4]

Ryan-Abbott-Peart further provides transmitting the transaction information as track data. Peart discloses that information from a transaction device (*token*) to an external reader (*computer terminal*) “is transmitted in magnetic stripe or multi-track magnetic stripe format” (*track data*). EX1008, 8:54-9:18. A POSITA would have been motivated to implement Peart’s suggestion in Ryan-Abbott to further promote information transferred from the communications controller to the computer terminal “in a format recognizable by a merchant system or account issuer.” EX1008, 8:54-62; EX1003, ¶219.

Claims 3, 12, 24, 33, 42, 54, 62

In the combined system, the encryption algorithm and the transaction counter are stored at least temporarily in the secure element, such that the token encrypts the information including the transaction counter using the secret key. EX1003, ¶220; *supra*, §IV.D.2 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; EX1008, 5:35-54.

Claims 5, 26, 35

Supra, §IV.C.4, Claim [8] (regarding *payment card application*); *supra*, §IV.D.3, Element [10.4] (regarding *track data*). EX1003, ¶221.

Claims 9, 18, 21, 30, 39, 48, 51, 59, 78, 87

[9.1]/[30.1]/[39.1]/[59.1]/[78.1]/[87.1]/[18.1]/[48.1]

Supra, §IV.C.4, Claim [8]. EX1003, ¶222.

[9.2]/[30.2]/[39.2]/[59.2]/[78.2]/[87.2]/[18.2]/[48.2]

Supra, §IV.C.4, Element [1.3], Claim [8]. EX1003, ¶223.

[9.3]/[21]/[30.3]/[39.3]/[51]/[59.3]/[78.3]/[87.3]

Supra, §IV.D.3, Element [10.4] (track data provides *card-present data*);
EX1001, 5:12-36. EX1003, ¶224.

Claims 11 and 41

Supra, §IV.C.4, Claim 2. EX1003, ¶225.

Claims 13 and 43

Supra, §IV.C.4, Claim 4. EX1003, ¶226.

Claims 16, 46

Supra, §IV.C.4, Claim 6. EX1003, ¶227.

Claims 17, 47

Supra, §IV.C.4, Claim 7. EX1003, ¶228.

Claims 19, 49

Supra, §IV.C.4, Claim 8. EX1003, ¶229.

E. GROUND 2C – Ryan-Abbott-Smets Renders Obvious Claims 65, and 83

1. Ryan-Abbott-Smets Combination

As discussed above, Ryan already provides a hardware and software framework capable of performing cryptographic operations and interacting with both contact and contactless payment environments, e.g., “ISO 7816, ISO 14443

and ISO 15693.” *Supra*, §IV.C.1; *see e.g.*, EX1006, 3:18-23, 5:13-30 (“Each electronic certificate includes transaction data and identification data...”), 13:54-57 (“The translation module moves signals between a USB interface and a smart card interface. The smart card interface may be selected from the group consisting of ISO 7816, ISO 14443 and ISO 15693.”), 15:11-25, 19:24-40 (“The flash memory device may be any suitable device including, but not limited to, Secure Digital (SD) card format, and including SIM card. (A crypto controller is a processor chip capable of encrypting and decrypting data to be stored in internal or external memory.)”), 28:30-37; EX1003, ¶230.

Ryan describes crypto capability, e.g., “security features such as Advanced Crypto Engine (ACE)... triple DES encryption and RSA.” EX1006, 2:53-60. This indicates that the hardware platform is suitable for implementing dynamic authentication calculations like CVC3. EX1003, ¶231.

A POSITA would have been motivated to integrate Smets’s backward-compatible formatting of transaction data (e.g., CVC3) into Ryan’s smart fob architecture. *Supra*, §IV.A.2; EX1005, [0026] (“payment card 1 computes a CVC3 number based on a portion of the UN and transmits the computed CVC3 number to terminal... Payment card 1 may use a secret encryption key stored on the card for computing the CVC3 number”); EX1006, 3:18-23, 5:13-30, 13:54-57, 14:6-7 (“The fob is capable of interfacing with the Internet and

emulating a smart card.”), 15:11-25, 19:24-40, 28:30-37; EX1003, ¶232. In the combined system, the microprocessor of Ryan’s secure element would be responsible for generating the dynamic CVC3, using stored keys and transaction inputs (e.g., unpredictable number, transaction counter), in accordance with Smets. *Id.* Multiple reasons would have prompted a POSITA to combine the teachings of Ryan, Abbott, and Smets. *Id.*

First, a POSITA would have been motivated to implement such combination for enhanced backward compatibility. EX1005, [0014]. Doing so in Ryan would facilitate interoperability of the smart fob with legacy payment infrastructure while still leveraging contactless and dynamic authentication capabilities. EX1003, ¶233. This aligns with Ryan’s goal of bridging environments. EX1006, 16:56-17:2. The combination therefore would enhance Ryan’s existing “virtual-to-real-world” transaction model with robust, standardized payment security. EX1003, ¶233.

Second, a POSITA would have been motivated to implement this combination because it would strengthen security and flexibility. EX1003, ¶234. Smets emphasizes that dynamic values are transaction-specific, as “[t]he dynamic authentication value changes with each transaction” and “unauthorized person cannot use that CVC3 number as the authentication value for the next or any other transactions.” EX1005, [0010]. Meanwhile, Ryan already supports secure storage

and processing, as the token “can generate secret cryptographic keys (Public & Private Key Infrastructure) and store private data.” *See e.g.*, EX1006, 12:5-15. By embedding Smets’s dynamic authentication and bitmap-based placement, Ryan’s token device would gain fraud-resistant, interoperable payment capability, while preserving its modular, multi-interface design. EX1003, ¶234. Moreover, Smets highlights flexibility via bitmaps, which complements Ryan’s modular and multi-standard architecture, allowing the same hardware to support multiple issuer-specific configurations without redesign. *See e.g.*, EX1005, Abstract, [0014]-[0015], [0023], [0028], [0033], [0040].

Furthermore, a POSITA would have expected a high likelihood of success in implementing the combination, because Ryan already provides processing, cryptographic capability, and interface translation layers, while Smets provides a standardized method for encoding dynamic authentication data in legacy-compatible formats. EX1003, ¶235. Ryan’s architecture is compatible with Smets’s teaching of generating and placing the dynamic data into existing magnetic-stripe data structures in a backward-compatible manner, because Ryan explicitly includes translation and formatting functionality between interfaces and contemplates direct interaction with contact and contactless standards such as ISO 7816 and ISO 14443. *Id.* Thus, a POSITA would have found it obvious that a microprocessor would handle the CVC3, UN, and ATC data in a manner compliant

with Smets. *Id.*

2. Analysis

Claims 65, 83

As discussed above, the Ryan-Abbott-Smets combination structures its transaction data stored in the secure element, including a dynamic authentication code (e.g., CVC3) (*dynamic card verification code*) computed from the unpredictable number (UN), in accordance with Smets, for compatibility with existing magnetic stripe infrastructure and enhanced security through dynamic authentication. *Supra*, §§IV.A.2-4, IV.C.1-4, IV.E.1; EX1005, [0010], [0014], [0024]-[0026], [0037]-[0039], FIG. 5; EX1003, ¶236.

As discussed in [60.2], Ryan teaches that the flash memory 150 includes and is managed by a micro-controller (*secure element*), disclosing and rendering obvious a microprocessor. EX1006, 3:9-13; 19:31-40, 29:35-36; EX1003, ¶237. In the combined system, the *microprocessor* of the secure element uses application-level (e.g., “a ‘PayPass-MagStripe’ application”) dynamic authentication to calculate the dynamic CVC3 (*dynamic card verification code*), from the UN and optionally “the card’s application transaction counter (ATC),” using a secret encryption key stored on the secure element, in accordance with Smets. *Supra*, §§IV.A.2-3, IV.E.1; EX1005, [0010], [0014], [0024]-[0025], [0026], [0037]-[0039].

**F. GROUND 2D – Ryan-Abbott-Peart-Smets Renders Obvious
Claims 15, 20, 45, 50**

A POSITA would have been motivated to combine Ryan with Abbott, Peart, and Smets for the reasons described above. EX1003, ¶238; *supra*, §§IV.C.3, IV.D.2, IV.E.1.

1. Analysis

Claims 15, 20, 45, 50

Supra, §IV.G.2, Ground 2C, Claim [65]; *see also id.* (the combination’s “‘PayPass-MagStripe’ application” providing *an application level protocol* for dynamic authentication of the secure element). EX1003, ¶239.

**G. GROUND 2E/2F – Ryan-Abbott-Smets-Kisliakov Renders
Obvious Claims 2, 23, 32, 53, 61, 80 / Ryan-Abbott-Peart-Smets-
Kisliakov Renders Obvious Claims 11, 41**

1. Combination

Even if Ryan, Abbott, Smets, and/or Peart, did not disclose transaction data communications comprising communications formatted according to ISO 7816-4, the combinations render obvious based on Kisliakov’s express teachings. EX1003, ¶¶240-241. Kisliakov provides express implementation details of the ISO 7816-4 file-system form Ryan’s memory 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]. A POSITA would have formatted

the commands and responses on that link — the processor module and the flash memory it addresses—as ISO 7816-4 APDUs, in accordance with Kisliakov, promoting a defined addressing scheme for the secure element’s storage such that distinct categories of cardholder data occupy separate files the reader can select individually. EX1010, [0268], [0323], [0326], [0351], [0414]; EX1003, ¶241. To be clear, a POSITA would have combined each set of references for reasons described above. *Supra*, Grounds 2A-2D.

2. Analysis

Claims 2, 11, 23, 32, 41, 53, 61, 80

Even if Ryan-Abbott-Smets (or Ryan-Abbott-Peart-Smets) did not disclose or make obvious *ISO 7816-4* type of commands and responses (APDUs) (*plurality of transaction data communications*) between the secure element and the secure element interrogator (the processor module and the memory it addresses), the combination provides such features through Kisliakov’s express disclosure. *Supra*, §§IV.B.1-2, IV.G.1, IV.G.1; EX1003, ¶242.

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 '924 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). Petitioner is not aware of any disclaimers, reexamination certificates, or IPR petitions addressing the '924 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: IPR50095-0311IP@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 IPR50095-00311IP@fr.com

D. Service Information

Please address all correspondence and service to the address listed above.
Petitioners consent to electronic service by email at IPR50095-0311IP@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. IPR2026-00502)

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 13,810 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:

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET, SUITE 2200
SAN DIEGO, CA
UNITED STATES
(619) 238-1900

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