

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Francisco Martinez de Velasco Cortina, et al.
U.S. Patent No.: 10,762,187
Issue Date: September 1, 2020
Appl. Serial No.: 14/659,502
Filing Date: March 16, 2015
Title: SYSTEM AND METHOD FOR PROVIDING SECURE
TRANSACTIONAL SOLUTIONS

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. 10,762,187
PURSUANT TO 35 U.S.C. §§ 311-319, 37 C.F.R. § 42

TABLE OF CONTENTS

I.	REQUIREMENTS FOR IPR—37 C.F.R. §42.104.....	1
A.	Grounds for Standing—37 C.F.R. §42.104(a).....	1
B.	Challenge and Relief Requested—37 C.F.R. §42.104(b)	1
II.	THE '187 PATENT	2
A.	Summary	2
B.	Prosecution History.....	3
III.	LEVEL OF ORDINARY SKILL	4
IV.	CLAIM CONSTRUCTION—37 C.F.R. §42.104(b)(3)	4
V.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	5
A.	Ground 1A: Maes-Niwa Renders Obvious Claims 1-6, 8-13 and 15-21 ..	6
1.	Maes (EX1004)	6
2.	Niwa (EX1005)	7
3.	The Maes-Niwa Combination (MNC)	8
4.	Claim Analysis	13
B.	Ground 1B: Maes-Niwa-Shults Renders Obvious Claims 7 and 14	51
1.	Shults (EX1008).....	51
2.	The Maes-Niwa-Shults Combination (MNSC).....	51
3.	Claim Element Analysis.....	53
C.	Ground 2A: Maes-Bjorn Renders Obvious Claims 1-6, 8-13, and 15-21 ..	54
1.	Bjorn (EX1006).....	54
2.	The Maes-Bjorn Combination.....	56
3.	Claim Element Analysis.....	62
D.	Ground 2B: Maes-Bjorn-Shults Renders Obvious Claims 7 and 14.....	78
1.	The Maes-Bjorn-Shults Combination (MBSC)	78
2.	Claim Element Analysis.....	79
E.	Ground 3A: Maes-Walker Renders Obvious Claims 1-6 and 15-21.....	79
1.	Walker (EX1007)	79
2.	The Maes-Walker Combination	79
3.	Claim Element Analysis.....	80
F.	Ground 3B: Maes-Walker-Shults Renders Obvious Claim 7.....	86
1.	The Maes-Walker-Shults Combination (MWSC).....	86
2.	Claim Element Analysis.....	86
VI.	PAYMENT OF FEES—37 C.F.R. §42.103.....	87

VII.	MANDATORY NOTICES—37 C.F.R. § 42.8(a)(1)	87
A.	Real Party-In-Interest—37 C.F.R. § 42.8(b)(1)	87
B.	Related Matters—37 C.F.R. § 42.8(b)(2)	87
C.	Lead And Back-Up Counsel—37 C.F.R. § 42.8(b)(3)	87
D.	Service Information	88

LIST OF EXHIBITS

EX1001	U.S. Patent No. 10,762,187 to de Velasco Cortina, et al. (the “’187 Patent”)
EX1002	The Prosecution History of the ’187 Patent (the “Prosecution History”)
EX1003	Expert Declaration of Seth Nielson, Ph.D.
EX1004	U.S. Patent No. 6,016,476 to Maes et al. (“Maes”)
EX1005	U.S. Patent No. 6,453,301 to Niwa (“Niwa”)
EX1006	U.S. Patent No. 6,035,398 to Bjorn (“Bjorn”)
EX1007	U.S. Patent No. 6,163,771 to Walker et al. (“Walker”)
EX1008	U.S. Patent App. Pub. No. 2002/0011519 to Shults (“Shults”)
EX1009	RESERVED
EX1010	U.S. Patent No. 6,434,159 to Woodward, et al. (“Woodward”)
EX1011-1020	RESERVED
EX1021	U.S. Patent No. RE36,788E (“Mansvelt”)
EX1022	U.S. Patent No. 6,098,053 (“Slater”)
EX1023	U.S. Patent No. 10,706,412 (“the ’412 Patent”)
EX1024-1029	RESERVED
EX1030	Complaint for Patent Infringement, <i>Mobility IP Holdings, Inc. v. Apple Inc.</i> , No. 7:26-cv-00075 (W.D. Tex. Mar. 4, 2026)

- EX1031 Complaint for Patent Infringement, *Mobility IP Holdings, Inc. v. Samsung Electronics Co, Ltd. and Samsung Electronics America, Inc.*, No. 2:26-cv-157 (E.D. Tex. Feb. 27, 2026)
- EX1032 Stipulation by Apple
- EX1033 Stipulation by Samsung
- EX1034 Combined Civil and Criminal Federal Court Management Statistics (Jun. 30, 2026) | United States Courts, available at: https://www.uscourts.gov/sites/default/files/document/fcms_na_distprofile0630.2026.pdf
- EX1035 U.S. Patent No. 5,698,836 to Fujioka (“Fujioka”)
- EX1036 U.S. Provisional Application No. 60/304,216 to Williamson, et al. (“Berardi Prov.”)
- EX1037 U.S. Patent Application Publication No. 2004/0049451 to Berardi, et al. (“Berardi App.”)
- EX1038 U.S. Patent No. 6,213,391 to Lewis (“Lewis”)
- EX1039 U.S. Patent No. 5,832,090 to Raspotnik (“Raspotnik”)

LISTING OF CLAIMS

Element	Claim Language
[1.pre]	A mobile device, comprising:
[1.1]	short range radio frequency (RF) circuitry;
[1.2]	memory configured to store biometric authentication information and payment information;
[1.3]	a biometric module configured to read biometric information;
[1.4]	an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and
[1.5.1]	a secure module configured to:
[1.5.2]	generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;
[1.5.3]	encrypt the key
[1.5.4]	[encrypt] ... the payment information stored in memory; and
[1.5.5]	provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction.
[2]	The mobile device of claim 1, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.
[3]	The mobile device of claim 1, wherein the payment information is associated with a primary account number.
[4]	The mobile device of claim 1, wherein the secure module is configured to provide the encrypted key and payment information to a point of sale (POS) device.

[5]	The mobile device of claim 1, wherein the biometric authentication information is stored separately from the payment information.
[6]	The mobile device of claim 1, wherein the payment information is stored in a memory accessible only by the secure module.
[7]	The mobile device of claim 1, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.
[8.pre]	A system, comprising:
[8.1]	a mobile device, comprising:
[8.2]	short range radio frequency (RF) circuitry;
[8.3]	memory configured to store biometric authentication information and payment information;
[8.4]	a biometric module configured to read biometric information;
[8.5]	an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and
[8.6.1]	a secure module configured to:
[8.6.2]	generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;
[8.6.3]	encrypt the key
[8.6.4]	[encrypt] ... the payment information stored in memory; and
[8.6.5]	provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction; and
[8.7.1]	a point of sale (POS) device configured to:

[8.7.2]	receive, from the secure module, the encrypted key and payment information; and
[8.7.3]	transmit, to a central database, the encrypted key and payment information; and
[8.8]	a central database configured to validate the key and the payment information.
[9]	The system of claim 8, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.
[10]	The system of claim 8, wherein the payment information is associated with a primary account number.
[11]	The system of claim 8, wherein the POS device includes an RF reader.
[12]	The system of claim 8, wherein the biometric authentication information is stored separately from the payment information.
[13]	The system of claim 8, wherein the payment information is stored in a memory accessible only by the secure module.
[14]	The system of claim 8, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.
[15.pre]	A method for secure transactions using a mobile device, comprising:
[15.1]	storing biometric authentication information and payment information in memory;
[15.2]	reading biometric information using a biometric reader;
[15.3]	determining whether the biometric information read by the biometric reader corresponds to the biometric authentication information stored in memory;

[15.4]	generating a key when the biometric information read by the biometric reader is determined to correspond to the biometric authentication information stored in memory;
[15.5]	encrypting the key
[15.6]	[encrypting] ... the payment information stored in memory; and
[15.7]	providing the encrypted key and payment information for use in a transaction.
[16]	The method of claim 15, further comprising reading biometric information provided by a user to complete the transaction.
[17]	The method of claim 15, wherein the payment information is associated with a primary account number.
[18]	The method of claim 15, further comprising providing the encrypted key and payment information to a point of sale (POS) device.
[19]	The method of claim 15, wherein the biometric authentication information is stored separately from the payment information.
[20]	The method of claim 15, wherein the payment information is stored in a memory accessible only by a secure module.
[21]	The method of claim 15, wherein the payment information is provided using a short range RF circuitry.

Apple Inc. (“Apple”) and Samsung Electronics Co., Ltd. (“Samsung”) (collectively, “Petitioners”) petition for IPR of claims 1-21 (“Challenged Claims”) of U.S. Patent No. 10,762,187 (“the ’187 Patent”) assigned to Mobility IP Holdings, Inc. (“Patent Owner” or “Mobility”).

I. REQUIREMENTS FOR IPR—37 C.F.R. §42.104

A. Grounds for Standing—37 C.F.R. §42.104(a)

Petitioners certify that the ’187 Patent is available for IPR, and that Petitioners are not barred or estopped from requesting IPR of the Challenged Claims on the below-identified grounds.

B. Challenge and Relief Requested—37 C.F.R. §42.104(b)

Petitioners request an IPR of the Challenged Claims on the grounds set forth in the table below, and request that each of the Challenged Claims be found unpatentable for the reasons described within the Petition and the supporting evidence cited herein, including the Declaration of Seth Nielson, Ph.D. (EX1003, ¶¶1-49, 375-376, *generally*).

Ground	Claims	Prior Art Basis
1A	1-6, 8-13, 15-21	§103 - Maes (EX1004) in view of Niwa (EX1005)
1B	7, 14	§103 - Maes in view of Niwa and Shults (EX1008)

2A	1-6, 8-13, 15-21	§103 - Maes in view of Bjorn (EX1006)
2B	7, 14	§103 - Maes in view of Bjorn and Shults (EX1008)
3A	1-6, 15-21	§103 - Maes in view of Walker (EX1007)
3B	7	§103 - Maes in view of Walker and Shults

The '187 Patent was filed on March 16, 2015 and claims priority to several earlier-filed applications, the earliest of which was filed on July 9, 2002. As shown below, each of the references applied in Grounds 1A-3B qualifies as prior art even if the July 9, 2002 date is taken as the date of the alleged invention of the Challenged Claims. Without conceding that the Challenged Claims are entitled to its priority claims, this Petition nonetheless treats July 9, 2002 as the “Critical Date” of the claimed subject matter for purposes of the analysis herein.

Reference	Filed	Published	Pre-AIA Prior Art Basis
Maes (EX1004)	01/16/1998	01/18/2000	§102(a), (b), (e)
Niwa (EX1005)	01/23/2000	09/17/2002	§102(e)
Bjorn (EX1006)	11/14/1997	03/07/2000	§102(a), (b), (e)
Shults (EX1008)	05/03/2001	01/31/2002	§102(a), (e)
Walker (EX1007)	08/28/1997	12/19/2000	§102(a), (b), (e)

II. THE '187 PATENT

A. Summary

The '187 Patent generally describes an “RF cellular telephone [that] can be used as a substitute for credit cards, transforming the cellular telephone into the

media of commercial transactions and transform telephony into the identification media for commercial establishments or authorities” EX1001, 13:43-49; *see also id.*, 1:7-12, 2:3-9, 13:17-26; EX1003, ¶¶50-57.

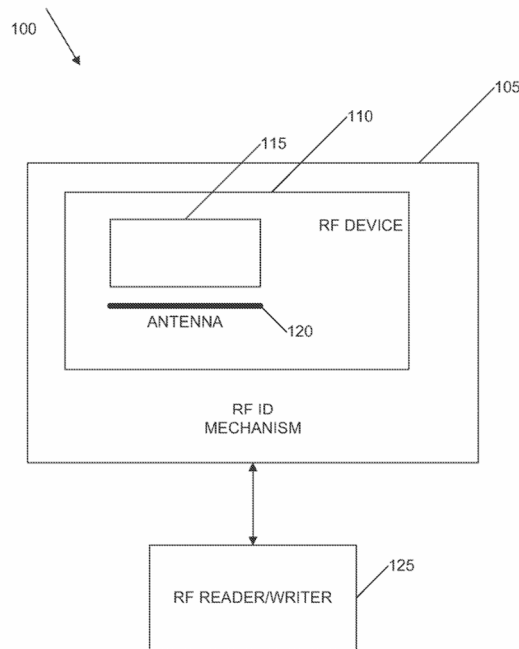


FIG. 1

EX1001, Fig. 1.

B. Prosecution History

During prosecution of the application for the '187 Patent, the Examiner allowed the claims over Walker (EX1007) after the Board found on appeal that Walker did not disclose generating a key when biometric information is authenticated. EX1002, 2, 28-30, 37, 51.

As this Petition demonstrates, however, the Examiner's decision to allow the '187 Patent was in error. There is no indication that the Examiner had reviewed Maes (EX1004) (cited during prosecution of applications in the '187 Patent family), Niwa (EX1005), or Bjorn (EX1006) before allowing the '187 Patent. The prior-art combinations based on these references (and Walker) presented herein demonstrate earlier disclosure of the exact feature that the Board found missing from Walker alone. EX1003, ¶¶58-61.

III. LEVEL OF ORDINARY SKILL

A person of ordinary skill in the art ("POSITA") relating to the '187 Patent's subject matter as of July 9, 2002 would have had (1) at least a bachelor's degree in computer science, computer engineering, or a related field, and (2) at least two years of industry experience including researching or developing software related to secure communication systems/networks. EX1003, ¶35. Additional education could substitute for professional experience, and professional experience for education. *Id.*

IV. CLAIM CONSTRUCTION—37 C.F.R. §42.104(b)(3)

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
"payment information" (Claims 1, 3-6, 8, 10, 12-13, 15, 17-21)	"information used to process a transaction that includes at least credit card information"

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, ¶¶62-64. Petitioners reserve the right to respond to any construction offered by Patent Owner or adopted by the Board.

V. THE CHALLENGED CLAIMS ARE UNPATENTABLE

Grounds 1A-3B below demonstrate that the Challenged Claims of the '187 Patent would have been obvious to a POSITA before the Critical Date based on prior-art combinations involving Maes, Niwa, Shults, Bjorn, and Walker. Each of these references is analogous art in the same field as the '187 Patent (*e.g.*, secure transactions and communications) and/or reasonably pertinent to problem(s)

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.

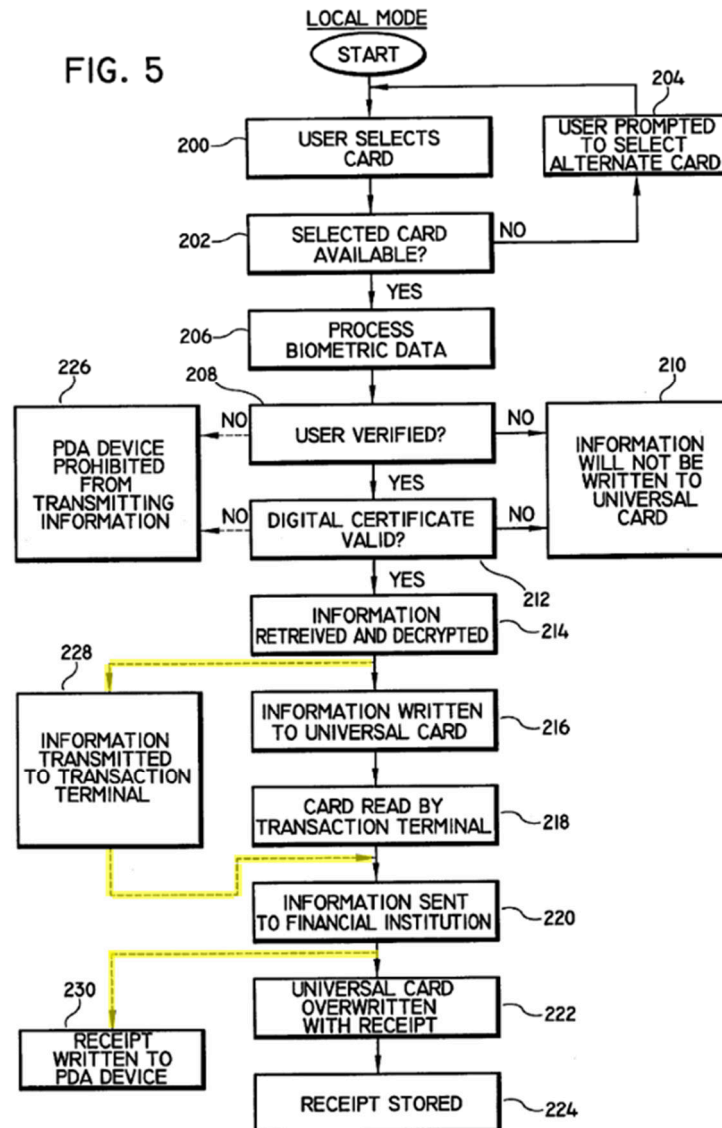
purportedly addressed by the '187 Patent (*e.g.*, verifying or authenticating users in secure transactions). *See* EX1001, 13:17-26, 13:43-49, 14:4-10; EX1004, 1:10-17; EX1005, 5:51-6:58, Abst.; EX1006, 1:5-51, Abst.; EX1008, [0003], [0009], [0030], Abst.; EX1007, 1:6-10, 3:59-4:4, Abst.; EX1003, ¶75.

A. Ground 1A: Maes-Niwa Renders Obvious Claims 1-6, 8-13 and 15-21

1. Maes (EX1004)

Maes describes a “portable information and transaction processing device,” such as a “portable client PDA” that “provide[s] direct communication capability with peripheral devices (such as POS [point-of-sale] ... terminals) ... through wireless communications such as radio frequency (RF) ... communication.” EX1004, Abstract, 4:16-28, 4:65-6:27, Fig. 1; EX1003, ¶¶65-74.

In some embodiments, “[t]he PDA includes a Universal Card, which is [a] common generic smartcard with a unique imprint provided by a service provider, on which selected financial or personal information stored in the PDA can be downloaded to perform certain consumer transactions.” EX1004, Abstract; *see also id.*, 4:29-30, 5:24-35. Maes emphasizes, however, “that the invention may interact with electronic fund transfer systems or transaction terminals having wireless or direct communication capabilities without even having to use the Universal Card 26.” EX1004, 12:5-8.



EX1004, Fig. 5 (highlighting added).

2. Niwa (EX1005)

Like Maes, Niwa describes “[a] method of authorizing a commercial transaction ... by activating a fingerprint identification device, and the provider of goods or services receives at least an authentication code of the customer over the

network from the fingerprint identification device.” EX1005, Abstract; EX1003, ¶¶76-80.

Niwa explains that “[t]he card issues an authorization code only when the fingerprint of the customer 52 matches the stored fingerprint.” EX1005, 4:32-34.

In Niwa, “[d]ata transfer is ... conducted between the fingerprint identification device 50 . . . and the provider of goods and/or services 60, 62 or 64 (action 112).” EX1005, 5:63-67. “The data transfer preferably includes at least one of the authentication code, payor bank identification number, customer account number, and delivery address.” EX1005, 5:67-6:3. Niwa states that “[m]ost preferably, the data of this transfer are in encrypted form.” EX1005, 6:3-4; *see also id.*, 6:13-25, 6:54-58.

3. The Maes-Niwa Combination (MNC)

Maes’s PDA transmits selected card information for a transaction over an RF link to a point-of-sale (POS) terminal. EX1004, 12:5-29; *supra*, §V.A.1. Maes teaches that the user can provide an authorization number for the transaction to the merchant, which the merchant in turn provides to a central server to verify the user in a process for authorizing the transaction. EX1004, 12:39-54, 12:65-13:5. In particular, Maes focuses on an example scenario where the user “verbally” conveys the authorization number to the merchant, such as where the merchant lacks an electronic POS terminal. EX1004, 12:39-54, Fig. 6.

To the extent Maes does not expressly disclose that the authorization number is transmitted from the PDA to the POS terminal over an RF link, Niwa complements Maes in teaching that not only payment information but also an authentication code (similar to Maes's authorization number) can be electronically transmitted to a merchant. *Supra*, §V.A.2. In particular, Niwa describes a “[d]ata transfer ... conducted between [a] fingerprint identification device 50 . . . and [a] provider of goods and/or services 60, 62 or 64” where “[t]he data transfer preferably includes at least one of the authentication code, payor bank identification number, customer account number, and delivery address.” EX1005, 5:63-6:4,² Fig. 3 (step 112). For a POS transaction, “the data (*e.g.*, at least one of the authentication code, payor bank identification number, customer account number, delivery address, etc.) would be provided to, for example, the merchant 70 ... at the point of sale.” EX1005, 6:54-58.

A POSITA would have found it obvious to implement Maes's system in accordance with Niwa's suggestion for transmitting payment information and an authorization number from a user device to a merchant for use in a transaction over a common electronic channel. EX1003, ¶¶81-90. In the resulting Maes-Niwa Combination (MNC), Maes's PDA transmits not only the selected card information

² All emphasis in this Petition is added unless otherwise noted.

but also the authorization number/code to the merchant's POS terminal over an electronic channel in the form of Maes's RF link. EX1003, ¶¶81-90. The merchant then provides both the selected card information and the authorization number to a financial institution to authorize the transaction in accordance with Maes's teachings. EX1004, 12:55-13:5.

Multiple reasons would have prompted a POSITA to pursue MNC. EX1003, ¶¶81-90

First, a POSITA would have been motivated to pursue the combination to make beneficial use of the authorization number/authentication code not only in transactions where the merchant lacks an electronic card reader, but also in transactions involving electronic POS terminals. EX1003, ¶¶81-90. Maes explains that "[s]ince the authorization number is a function of the unexpired digital certificate that was obtained from the central server 60 ..., the central server 60 inform[s] the merchant the user was properly verified." EX1004, 13:1-5. The authorization number/code can be similarly used to aid in verifying the user regardless of whether the authorization number is conveyed to the merchant verbally or over an electronic channel such as Maes's RF link. EX1003, ¶¶81-90.

Second, a POSITA would have been motivated to pursue MNC to increase the security of the transaction. EX1003, ¶¶81-90. Verbal communication of the authorization number/code at the POS risks exposing the number to unauthorized

bystanders who may be listening for or who may otherwise overhear the number when spoken to the merchant. EX1003, ¶¶81-90. Transmitting the authorization number/code electronically as taught in Niwa obviates the need to verbally communicate the authorization number/code, thereby preventing any bystanders or aural listening devices from obtaining an audibly conveyed number. *Id.*

Moreover, per Niwa, all information electronically transmitted in a transaction including card information and the authorization number/code can be encrypted, further improving security. EX1005, 4:43-47, 6:3-4; EX1004, 5:1-4, 5:14-17, 6:9-14, 13:33-38 (discussing information transmitted in encrypted form); EX1003, ¶¶81-90; *infra*, [1.5.1]. Niwa's teaching to apply encryption to an authentication number/code when transmitted electronically (over RF in MNC) provides an independent basis for combining Maes and Niwa, even beyond Niwa's antecedent of transmitting these items electronically. Encrypting the transmission would have been obvious and beneficial to prevent unauthorized entities from intercepting and reading the transmitted information for the transaction in the clear. EX1003, ¶¶81-90.

Third, a POSITA would have been motivated to pursue MNC to improve the efficiency of the transaction at the point of sale. By electronically transmitting the authorization number/code over the same communication channel (*i.e.*, Maes's RF link) that carries the selected card information, the user need only utilize a single

communication modality to convey all necessary information for the transaction to the merchant (either at once or in phases). EX1003, ¶¶81-90. Electronic transmission of the authorization number/code eliminates the time and effort involved in the user manually reading the authorization number/code to the merchant. This would predictably yield a more frictionless experience for users at the POS, which a POSITA would expect to beneficially increase usage of Maes's payment technology. EX1003, ¶¶81-90. It would also improve accuracy as electronic transmission by avoiding the risk of human error in communicating or transcribing the authorization number/code. *Id.*

Fourth, a POSITA would have pursued MNC because it involves nothing more than the predictable application of a known technique (*e.g.*, Niwa's electronic data transfer) to a known device ready for improvement (*e.g.*, Maes's PDA device in its direct-RF-transmission embodiments) to yield predictable results (*e.g.*, RF transmission containing both the card information and authorization number, forwarded to the service provider or financial institution for validation). *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007).

A POSITA also would have reasonably expected success implementing the combination. EX1003, ¶¶81-90. Long before the '187 Patent's Critical Date (July 9, 2002), it was known how to transmit a wide range of information over short-range RF links and Maes already describes how to transmit card information and other

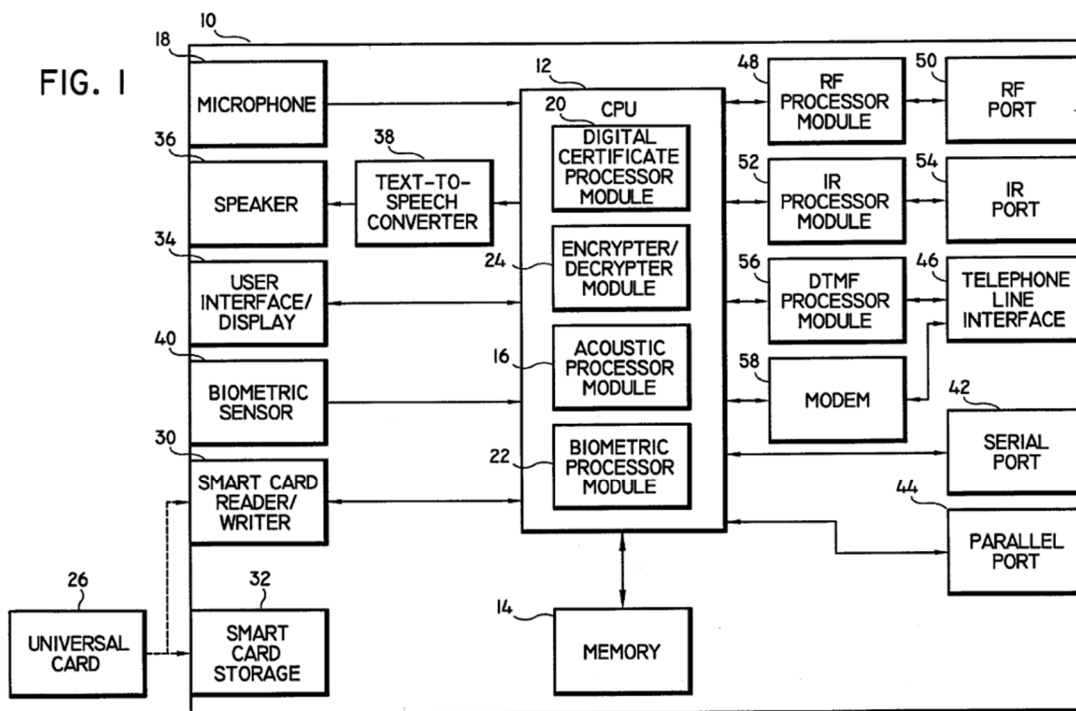
encrypted information over an RF link. EX1004, 6:9-15, 13:34-38; EX1003, ¶¶81-90.

4. Claim Analysis

(a) [1.pre]

MNC renders [1.pre] obvious. EX1003, ¶¶130-132.

Maes discloses a “portable client PDA” (*mobile device*), e.g., PDA device 10 depicted in Fig. 1 below. EX1004, Abstract, 4:65-6:27; EX1003, ¶131.



EX1004, Fig. 1; EX1003, ¶131.

Maes’s PDA “provide[s] direct communication capability with peripheral devices (such as POS ... terminals) and is capable of transmitting or receiving

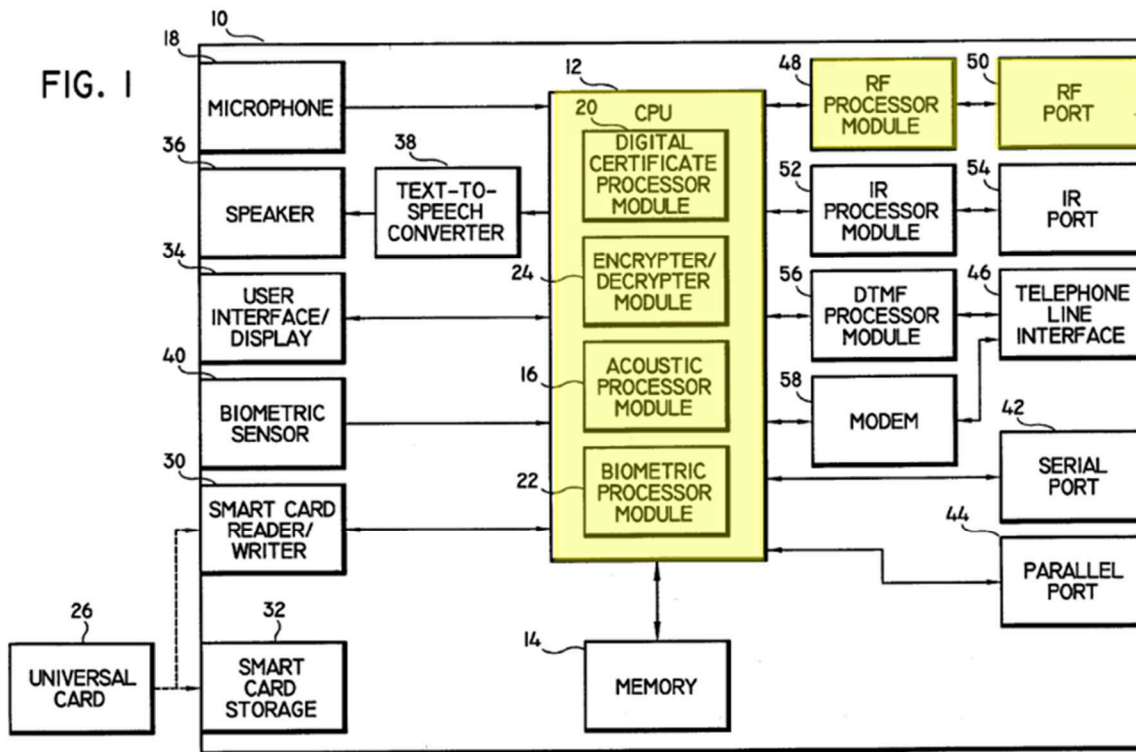
information through wireless communications such as radio frequency (RF) ... communication.” EX1004, Abstract; *see also id.*, 6:8-19, 12:5-29, Fig. 3.

(b) [1.1]

MNC renders [1.1] obvious. EX1003, ¶¶133-136.

Maes’s PDA (*mobile device*) “is capable of transmitting or receiving information through wireless communications such as radio frequency (RF) ... communication.” EX1004, Abstract.

With reference to Fig. 1 (reproduced below), Maes explains that “the portable information and transaction processing (PDA) device 10” is “equipped with an RF processor module 48, operatively connected between the CPU 12 and an RF port 50, for processing incoming RF information received by the RF port 50, and for generating transmission signals which are outputted from the RF port 50 using conventional constructions and techniques.” EX1004, 6:1-27, 4:65-5:26. From these and related descriptions, a POSITA would have understood that PDA 10 includes *short range radio frequency (RF) circuitry* such as RF port 50, RF processor module 48, and/or CPU 12. EX1003, ¶135.



EX1004, Fig. 1 (highlighted).

A POSITA would have understood Maes's RF circuitry to be *short-range* circuitry. EX1003, ¶136. Maes describes the RF link L2 as a direct wireless channel between the PDA held by the user and the POS transaction terminal 80. EX1004, 12:5-29. Maes expressly treats its RF port 50 and IR port 54 as interchangeable options for the direct link, and IR communication is a short range line-of-sight technology. EX1004, 3:34-36, 12:16-17, 13:35-36. Maes also distinguishes its direct device-to-terminal RF link from the long-range wireless communications used to connect the PDA to remote central server 60 in client/server mode. EX1004, 7:65-

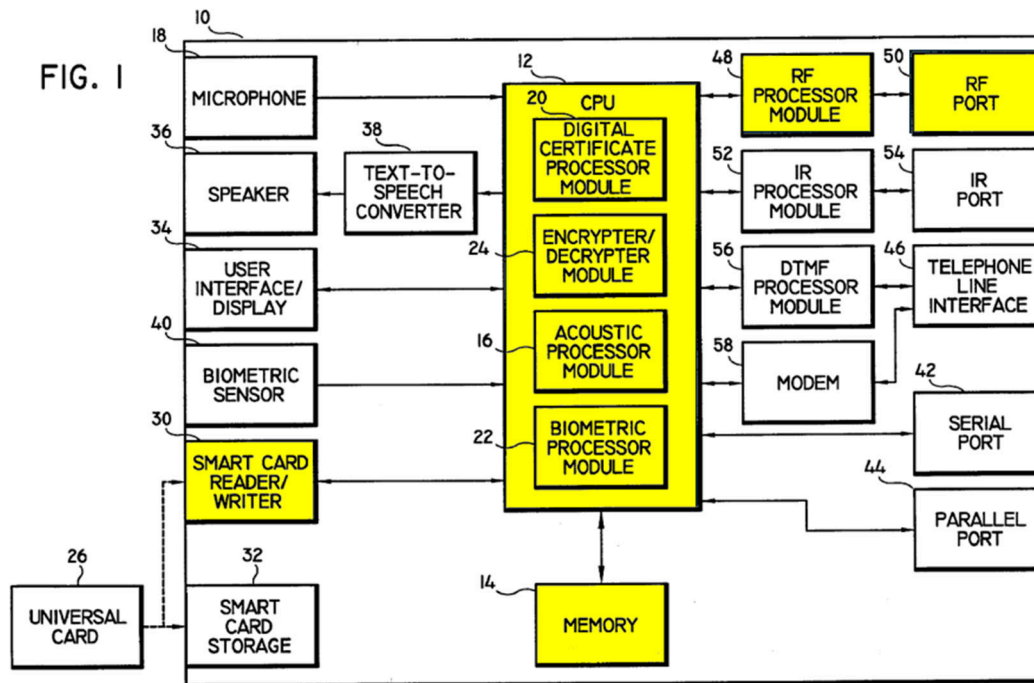
8:14. Accordingly, Maes's RF circuitry that is used for a direct link between the PDA and a nearby transaction terminal is *short range*. EX1003, ¶136.

(c) [1.2]

MNC renders [1.2] obvious. EX1003, ¶¶137-141.

Maes discloses that the PDA (*mobile device*) “includes a memory for storing financial and personal information of the user.” EX1004, Abstract; *see also id.*, (“selecting one of the pre-enrolled credit cards that are stored in the PDA”).

In more detail, and with reference to Fig. 1 (reproduced below), Maes explains that “[t]he heart of the device is a central processing unit (CPU) 12, which controls the operations of the PDA device 10 via programs stored in a memory 14 and executed by the CPU 12.” EX1004, 5:1-4. “The CPU 12 also includes a digital certificate processor module 20, for processing a digital certificate obtained in the client/server mode of operation ... a biometric processor module 22 for processing biometric data ... to provide user verification,” and “an encrypter/ decrypter module 24 for encrypting the personal and financial information before being stored in memory 14 and for decrypting such information when accessed by the user.” EX1004, 5:8-17; *see also id.*, 5:18-24 (describing special-purpose processors and associated memory).



EX1004, Fig. 1 (highlighted).

The “financial information” stored in Maes’s memory 14 includes information for at least one credit card (*payment information*). EX1003, ¶140. For example, Maes explains that “the user may ... download [credit ... card] information into the PDA device 10 by establishing a communication link (L1) with [a] central server 60.” EX1004, 7:1-4. “Alternatively, the credit cards ... may be loaded into the PDA device 10 by directly reading information contained on such cards through a smartcard reader/writer 30 of the PDA device 10.” *Id.*, 7:4-7. In “[t]he local mode of operation,” “the user select[s] a pre-enrolled credit card that is stored in memory 14” of the PDA device 10. *Id.*, 10:29-33, Figs. 1, 5. Then, a “consumer transaction may be performed by transmitting the selected card information directly from the

PDA device to the ... POS transaction terminal through an established communication link” *Id.*, 12:10-13; *see also id.*, 13:33-38. Maes’s “selected card information” thus provides **payment information** stored in a **memory** (*e.g.*, memory 14) of the PDA device 10 (**mobile device**) as claimed. *Supra*, §IV; EX1003, ¶140.

The “personal information” stored in memory 14 further includes **biometric authentication information**, such as a voice or fingerprint model belonging to an authorized user of the PDA. EX1003, ¶141. For example, Maes explains that “biometric voice data is [] sent to [an] acoustic processor module 16 wherein such data is processed (step 206) by comparing the current biometric voice data with the user’s voice models stored in memory 14.” EX1004, 10:57-61. Maes further discloses that “[a] biometric sensor 40 of any conventional type may also be provided for collecting biometric data ... such as a finger, thumb or palm print, a handwriting sample, a retinal vascular pattern, or a combination thereof, to provide biometric verification” EX1004, 5:54-60; *see also id.*, 5:13-17 (“encrypting the personal and financial information before being stored in memory 14”), 10:66-11:8, Figs. 1, 5. From these and related descriptions, a POSITA would have understood that Maes’s PDA 10 memory (*e.g.*, memory 14) stores **biometric authentication information** used by the biometric processor module 22 to authenticate the user attempting a transaction. EX1003, ¶141. Additionally or alternatively, it would have been obvious to store **biometric authentication information** in the memory of the

PDA for each of the biometric modalities contemplated in Maes, as doing so would beneficially allow the biometric processor module 22 to authenticate a user in local mode by comparing the input from biometric sensor 40 to reference biometric models for those modalities stored in the memory (just as Maes expressly discloses comparison of a spoken input into microphone 16 to the user's stored voice model). *Id.*

(d) [1.3]

MNC renders [1.3] obvious. EX1003, ¶¶142-145.

Maes's microphone 18 and biometric sensor 40, alternately or together, provide a “*biometric module configured to read biometric information*,” as claimed. EX1003, ¶143. Microphone 18 reads voice-based biometric information, while biometric sensor 40 reads other forms of biometric information.³ EX1004, 5:53-62, 10:53-61, 11:1-14.

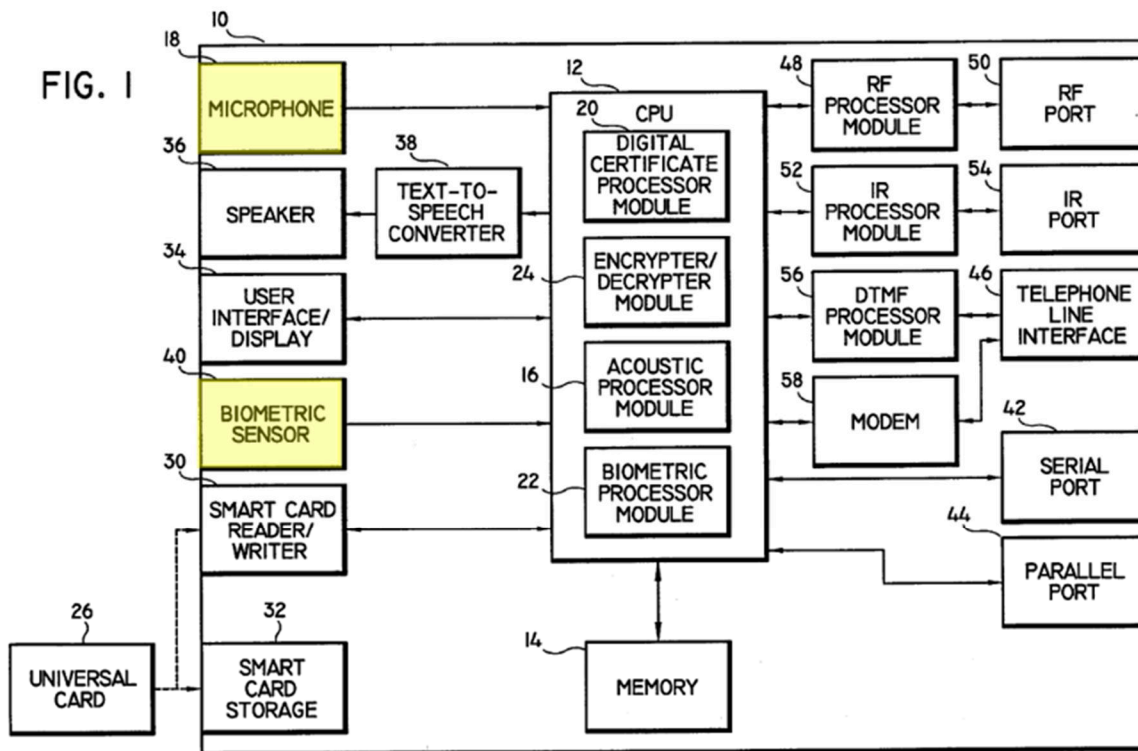
³ To the extent the claimed “biometric module” has a computational processing component, Maes further discloses that acoustic processor module 16 processes voice data read from microphone 18 and biometric processor module 22 processes other forms of biometric data read from biometric sensor 40. EX1004, 5:5-7, 5:58-62, 10:57-61. In this case, the microphone 18 together with acoustic processor

For example, Maes explains that the PDA includes “a microphone and local central processing unit (CPU) for processing voice commands and for processing biometric data to provide user verification.” EX1004, Abstract. “[U]sing voice activated commands to select the desired card, the microphone 18 functions as a biometric sensor for receiving biometric voice data.” EX1004, 10:53-57, Fig. 1.

Likewise, with respect to Fig. 1 (reproduced below), Maes describes a “biometric sensor 40 of any conventional type ... for collecting biometric data (other than voice data which is received by the microphone 18) such as a finger, thumb or palm print, a handwriting sample, a retinal vascular pattern, or a combination thereof, to provide biometric verification as an alternative to, or in addition to, voice biometric verification.” EX1004, 5:54-60. “This data is then processed by the biometric processor module 22 to provide user verification (*i.e.*, biometric security)

module 16 and/or biometric sensor 40 together with biometric processor module 22 provide alternate mappings to the claimed “*biometric module*,” and indeed, it also would have been obvious to implement these components as a single unit since they already cooperate with each other to perform the functions disclosed in Maes. EX1003, ¶143. Notably, Maes confirms that its functional components can be configured and arranged in different manners within the CPU 12 or special-purpose processors may be provided for different functions. EX1004, 4:45-64, 5:17-24.

prior to accessing the financial and personal information stored in memory 14.” *Id.*, 5:60-63; *see also id.*, Abstract, 5:54-63, 10:49-11:8, Figs. 1, 5.



EX1004, Fig. 1 (highlighted).

(e) [1.4]

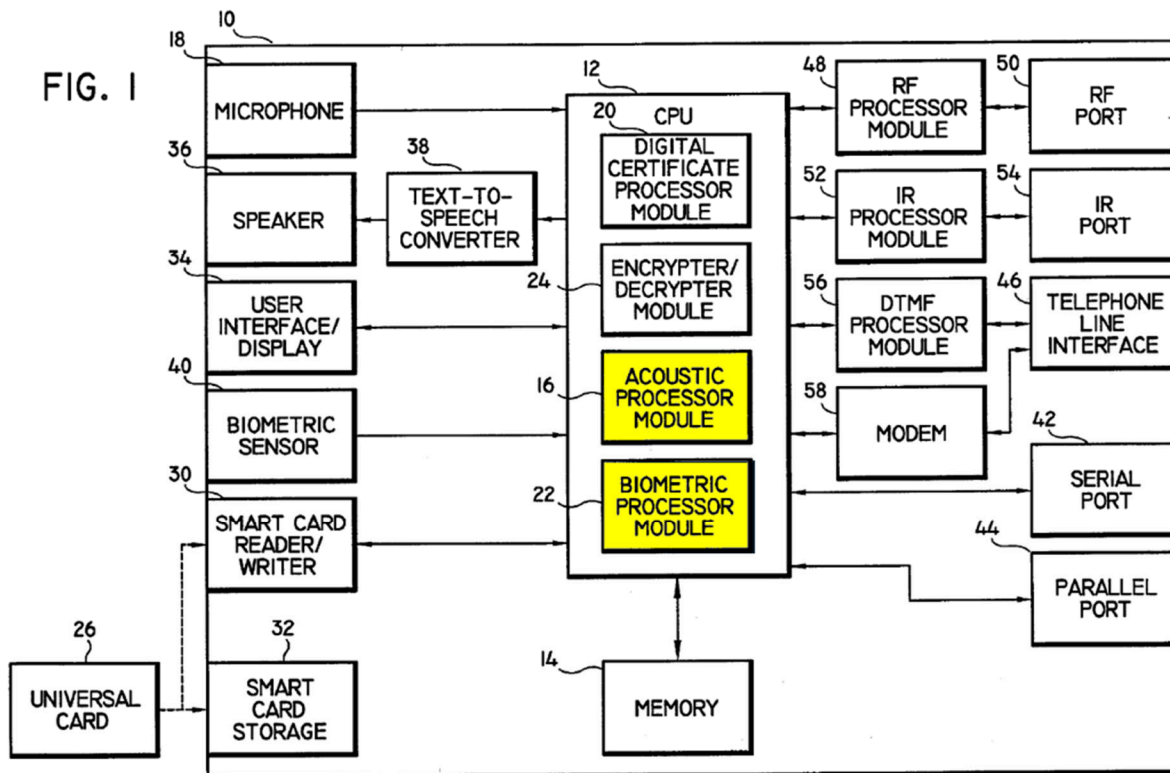
MNC renders [1.4] obvious. EX1003, ¶¶146-149.

Maes’s “acoustic processor module 16,” alternately or together with “biometric processor module 22,” provides an “*authentication module*” of the

mobile device.⁴ EX1003, ¶147. Maes discloses that “[t]he acoustic processor module 16 is [] used for performing local speaker verification.” EX1004, 5:7-8. Maes separately discloses that “the CPU 12 [] includes ... a biometric processor module 22 for processing biometric data in addition to, or alternative to voice data, to provide user verification.” EX1004, 5:9-14. Maes ties these two modules together as alternately or together providing the same verification determination, stating that “[a]fter the biometric data is processed by the acoustic processing module 16 (when voice verification is utilized) or the biometric processor module 22 (when other biometric verification methods are used), or both, a determination is made as to whether the user is an authorized user (step 208).” EX1004, 11:9-13; *see also id.*, 5:53-63, 10:48-11:14, Fig. 5. A POSITA would have understood from these and related disclosures that either module alone, or the two operating together, can provide the authentication determination recited by [1.5] depending on whether voice-based biometrics, alternate biometric modalities, or both are employed. EX1003, ¶147.

⁴ To the extent the “authentication module” is a single unit, Maes’s modules 16 and 22 are both implemented together on CPU 12. It also would have been obvious to implement both modules 16 and 22 as a combined unit in CPU 12 since both perform similar authentication functions as described above. EX1003, ¶147.

Maes explains that voice data read from microphone 18 is “sent to the acoustic processor module 16” for comparison “with the user’s voice models stored in memory 14.” EX1004, 10:57-61; *generally id.*, 10:48-11:8, Fig. 5. Similarly, “a biometric sensor 40 of any known type may be used in lieu of, or in conjunction with the microphone, to collect biometric data to be processed by the biometric processor module 22 using known techniques, *e.g.*, finger, thumb or palm print data” EX1004, 10:66-11:8. “After the biometric data is processed by the acoustic processing module 16 (when voice verification is utilized) or the biometric processor module 22 (when other biometric verification methods are used), or both, a determination is made as to whether the user is an authorized user (step 208).” EX1004, 11:9-13; *see also id.*, 5:60-63.



EX1004, Fig. 1 (highlighted).

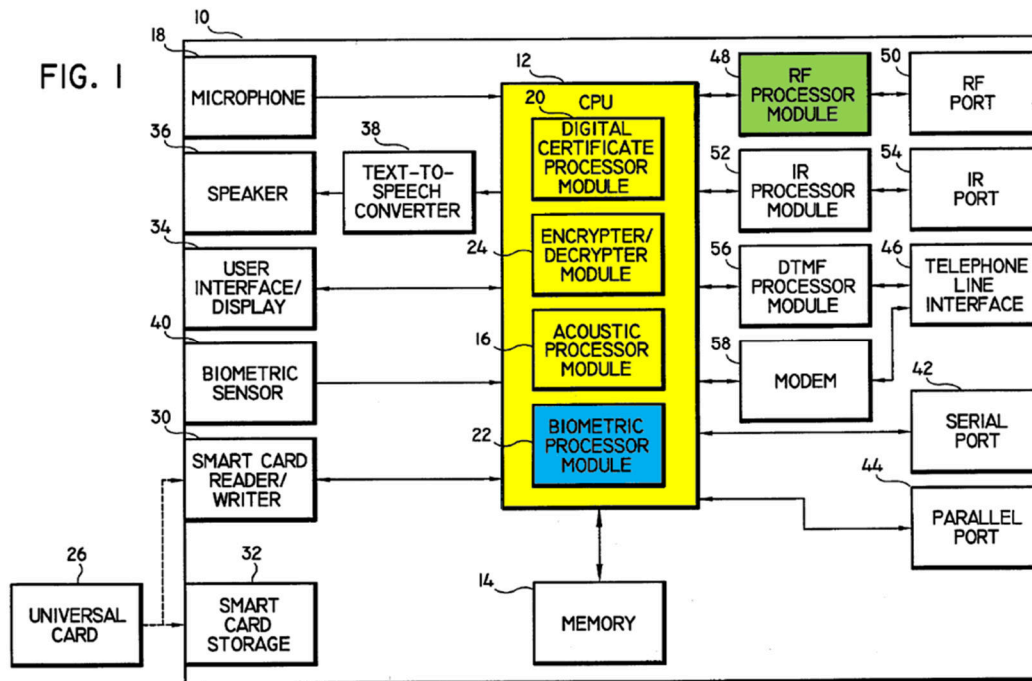
From these and related disclosures, a POSITA would have understood that Maes's PDA determines whether the biometric information read from the microphone 18 and/or the biometric sensor 40 corresponds to biometric authentication information stored in memory. EX1004, 6:56-7:35, 10:49-51, 14:42-46, Figs. 1, 3, 5; EX1003, ¶149.

(f) [1.5.1]

MNC renders [1.5.1] obvious. EX1003, ¶¶150-154.

Maes's CPU 12, including encrypter/decrypter module 24, and in cooperation with RF processor module 48, provides a "*secure module*" as claimed.⁵ EX1003, ¶151.

⁵ To the extent the "secure module" is a single unit, it would have been obvious to combine CPU 12 (including encrypter/decrypter module 24) with RF processor module 48. EX1003, ¶151. Both CPU 12 and RF processor module 48 are processing devices, and it was well known how to centralize processing functions on a single processing device before the Critical Date. *Id.* Maes acknowledges that different processing functions may be separated or combined. its functional components can be configured and arranged in different manners within the CPU 12 or special-purpose processors may be provided for different functions. EX1004, 4:45-64, 5:17-24. Combining these processing components in a single processor would have been beneficial for many implementations of MNC to reduce the hardware complexity and expense associated with separate processors. EX1003, ¶151.



EX1004, Fig. 1 (highlighted).

Maes discloses that “[t]he heart of the device is a central processing unit (CPU) 12, which controls the operations of the PDA device 10 via programs stored in a memory 14 and executed by the CPU 12.” EX1004, 5:1-4, Fig. 1.

Maes’s CPU 12 is secure. EX1003, ¶153. For example, the CPU 12 requires successful biometric verification and a valid digital certificate before allowing access to and transmission of the user’s financial and personal information. EX1004, 5:60-63, 12:19-23; EX1003, ¶153. Maes explains that CPU 12 enforces that condition on transmission, stating that “the CPU 12 of the PDA device 10 will prohibit the selected card information from being retrieved and transmitted to the transaction terminal 80 if the user is not biometrically verified and/or if the digital

certificate is not valid (step 226).” EX1004, 12:19-23. Maes further explains that “[t]he CPU 12 also includes ... a biometric processor module 22 for processing biometric data ... to provide user verification.” EX1004, 5:8-14. This verification precedes access to the information held on the PDA, as biometric data “is then processed by the biometric processor module 22 to provide user verification (*i.e.*, biometric security) prior to accessing the financial and personal information stored in memory 14.” EX1004, 5:60-63.

Maes’s CPU 12 including encrypter/decrypter module 24, in coordination with RF processor module 48, performs the operations recited in [1.5.2] through [1.5.5] for reasons addressed further below. *Infra*; [1.5.2]-[1.5.5]; EX1004, 5:1-4, 5:14-17, 6:9-14, 12:63-65; EX1003, ¶154. Maes thus provides a “**secure module**” at least to the same extent as disclosed in the ’187 Patent itself. *Cf.* EX1001, 14:32-34, 14:55-60.

(g) [1.5.2]

MNC renders [1.5.2] obvious. EX1003, ¶¶155-159.

Maes’s PDA generates an “authorization number” when the user is biometrically authenticated. EX1004, 5:60-63; 12:43-49, 12:63-65; EX1003, ¶156. According to Maes, “[t]he merchant can verify that local verification of the user has been properly obtained” by transmitting the “authorization number to [a] central server 60.” EX1004, 12:55-13:1. “Since the authorization number is a function of

the unexpired digital certificate that was obtained from the central server 60 in the client/server mode, the central server 60 [may then] inform the merchant that the user was properly verified” EX1004, 12:55-13:5; *see also id.*, 6:56-7:35, Fig. 3.

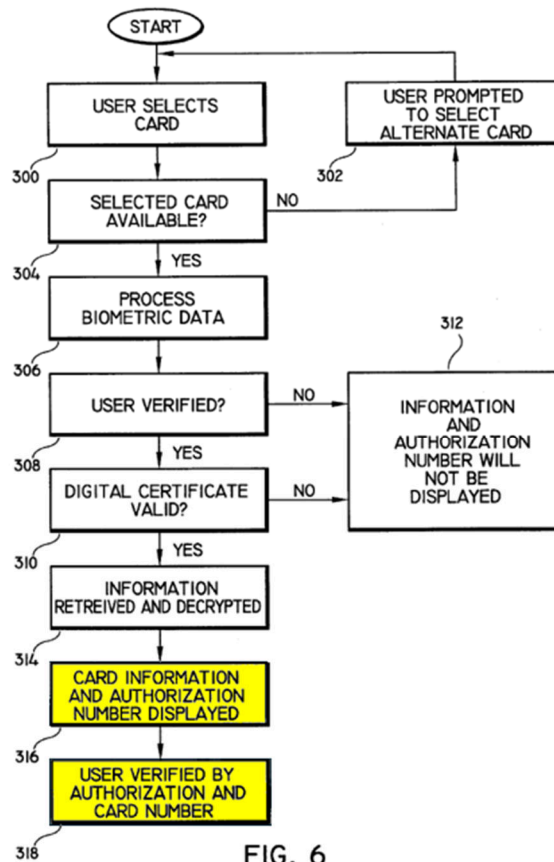
Maes’s “authorization number” (or similarly, Niwa’s authentication code) provides a “**key**” as claimed.⁶ EX1003, ¶157. Indeed, Maes discloses that the “authorization number” (**key**) is derived from a digital certificate and generated by the PDA when the **biometric information** (e.g. voice, fingerprint, or other biometric input) read by the **biometric reading device** (e.g., microphone 18 or biometric sensor 40) is determined by the **authentication module** (e.g., acoustic processor module 16

⁶ The ’187 Patent specification never expressly identifies any “key” that meets all the claimed functions, including being (i) generated when the read biometric information is determined to correspond to stored biometric authentication information (Element [1.5.2]), (ii) encrypted (Element [1.5.3]), (iii) provided for use in a transaction (Element [1.5.5]), and (iv) validated by a central database along with payment information (Element [8.8]). *See* EX1001, 2:32-39, 10:65-11:4, 12:5-18, 13:3-7, 14:55-61, 22:21-26 (describing cryptographic keys in contexts different from what is claimed); EX1003, ¶157. Maes’s authorization number in MNC nonetheless fulfills each of these claim requirements and functions as a key for authorizing a transaction. EX1004, 6:47-55, 12:30-13:5; EX1003, ¶157.

or biometric processor module 22) to correspond to the ***biometric authentication information*** (e.g., reference voice models or other reference biometric data) stored in ***memory*** (e.g., memory 14). EX1004, 12:63-13:5 (“the merchant will be requested to provide the authorization number (which is generated upon user verification), ... [s]ince the authorization number is a function of the unexpired digital certificate that was obtained ... in the client/server mode, the central server 60 informs the merchant that the user was properly verified ...”), 6:42-55 (“an authorization number, which is unique to the current digital certificate, will be displayed on the PDA device 10 upon user verification”), 12:30-39 (“an authorization number which is based on the current valid digital certificate and generated upon user verification”), 14:47-67 (“authorization number produced by the PDA device of User A upon local verification”); EX1003, ¶157.

For instance, Maes discloses that “if the user is biometrically verified (step 308) and the PDA device 10 contains an unexpired digital certificate (step 310), the selected card information is retrieved from memory 14 and decrypted (step 314).” EX1004, 12:40-47; *see also id.*, Figs. 5-6. “The desired credit card information, as well as an authorization number, is then displayed on the user interface/display 34 (step 316)” and is “communicated to the merchant in order to process the transaction.” EX1004, 12:47-54. “If the selected card information corresponds to a credit card that was previously enrolled (*i.e.*, registered) with the service provider”

the merchant will “upon transmitting the selected card information ... be requested to provide the authorization number (which is generated upon user verification), in addition to the expiration date of the credit card.” EX1004, 12:61-66. And, “[s]ince the authorization number is a function of the unexpired digital certificate that was obtained from the central server 60 in the client/server mode, the central server 60 inform the merchant that the user was properly verified (step 318).” EX1004, 13:1-5.



EX1004, Fig. 6 (highlighted).

In MNC, Maes’s CPU 12—an aspect of the “*secure module*” (*supra*, [1.5.1])—generates the authorization number (*key*). EX1004, 5:1-4, 12:63-65; EX1003, ¶159. This would have been understood or at least obvious to a POSITA since “[t]he heart of the device is [the] central processing unit (CPU) 12, which controls the operations of the PDA device 10 via programs stored in a memory 14 and executed by the CPU 12.” EX1004, 5:1-4; EX1003, ¶159.

(h) [1.5.3]

MNC renders [1.5.3] obvious. EX1003, ¶¶160-164.

Maes's authorization number (or similarly, Niwa's authentication code) provides a "**key**" generated by the PDA upon biometric verification of the user. EX1004, 12:43-49, 12:63-13:5; *supra*, [1.5.2], *supra* §V.A.3; EX1003, ¶161.

Further, Niwa describes a "[d]ata transfer ... conducted between [a] fingerprint identification device 50 (or other fingerprint identification circuitry if employed) and [a] provider of goods and/or services 60, 62 or 64 (action 112)." EX1005, 5:63-67; *see also* [1.5.5], *infra*. "The data transfer preferably includes at least one of the authentication code, payor bank identification number, customer account number, and delivery address." EX1005, 5:67-6:4. "Most preferably, the data of this transfer are in encrypted form." EX1005, 5:63-6:4; *see also id.*, 2:38-47, 4:42-47, 4:59-63, 7:47-52, 8:44-49, 10:12-14.

As described above in the combination overview, MNC implement's Maes's system in accordance with Niwa's suggestion for transmitting payment information and an authorization number/code for a secured transaction from a user device over a common electronic channel, such that Maes's PDA would transmit the selected card information and authorization number to a POS terminal over the RF link. *Supra*, §V.A.3; EX1003, ¶163. Further, per Niwa, to improve security and prevent unauthorized access to underlying information used in the transaction, it would have been obvious for the data transferred from the PDA including the selected card information and the authorization number (**key**) "are in encrypted form." EX1005,

5:63-6:4; *see also id.*, 2:38-47, 4:42-47, 4:59-63, 7:47-52, 8:44-49, 10:12-14; EX1003, ¶163. A POSITA would have known how to encrypt information for transmission over the RF link, and would have recognized the security benefits of doing so, as Maes relatedly teaches that information transmitted over an RF link including information “containing unique identifying information pertaining to the consumer” can be encrypted in an RF transmission. EX1004, 13:24-38.

In MNC, a POSITA would have understood that Maes’s encrypter/decrypter module 24 (a component of Maes’s CPU 12 and the “*secure module*” (*supra*, [1.5.1])) would encrypt information for the transaction that is to be transmitted from the PDA. EX1004, 5:14-17; EX1005, 6:3-4; EX1003, ¶164. At the very least, it would have been obvious for encrypter/decrypter module 24 to perform this function since Maes identifies encrypter/decrypter module 24 as providing encryption services to the PDA. EX1004, 5:14-17; EX1003, ¶164.

(i) [1.5.4]

MNC renders [1.5.4] obvious. EX1003, ¶¶165-167.

Maes explains that “[t]he CPU 12 further includes an encrypter/decrypter module 24” (an aspect of the “*secure module*” (*supra*, [1.5.1])) “for encrypting the personal and financial information before being stored in memory 14 and for decrypting such information when accessed by the user.” EX1004, 5:14-17, Fig. 1. In addition, per Niwa, MNC encrypts the stored credit card information (*payment*

information) by encrypting it for transmission over Maes's RF link. EX1005, 4:43-47, 6:3-4 ("Most preferably, the data of this transfer are in encrypted form.").

Thus, MNC renders obvious encrypting the payment card information (*payment information*) stored in memory. EX1004, 5:14-17; EX1003, ¶167.

(j) [1.5.5]

MNC renders [1.5.5] obvious. EX1003, ¶¶168-178.

Maes discloses that "the consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal through an established communication link L2 (step 228, Fig. 3) (*i.e.*, via ... the RF port 50).⁷" EX1004, 12:10-15; *see also id.*, 13:34-38 (transmit "via ... RF")⁷, 3:33-36; 6:6-14; 8:6-8; 8:8-14; 12:5-29; 12:14-17;; 14:59-65, 12:5-29, Figs. 1, 5, 6.

⁷ At col. 13:34-38, Maes states that the selected card information and encrypted information file "would be transmitted to the POS terminal (via the Universal Card, RF or IR)." In Maes, the PDA is the device that has RF transmission capabilities. *See e.g.*, EX1004, 6:6-14, 12:5-29, Fig. 1. A POSITA would have understood Maes's use of "RF" here to refer to an RF transmission from the PDA, consistent with Maes's recitation of "RF" as an alternative to the Universal Card and IR.

Maes also discloses conveying the “authorization number” to the merchant “in order to process the transaction.” EX1004, 12:43-54 (“[I]f the user is biometrically verified (step 308) and the PDA device 10 contains an unexpired digital certificate (step 310), the selected card information is retrieved from memory 14 and decrypted (step 314). The desired credit card information, as well as an authorization number, is then displayed on the user interface/display 34 (step 316). This information can then be verbally communicated to the merchant in order to process the transaction.”), 12:66-13:5 (“The merchant will then transmit ... the displayed authorization number to the central server 60.”), Fig. 6.

Like Maes, Niwa discloses a “[d]ata transfer ... conducted between [a] fingerprint identification device 50 (or other fingerprint identification circuitry if employed) and [a] provider of goods and/or services 60, 62 or 64 (action 112).” EX1005, 5:63-67; *see also* [1.5.5], *infra*. “The data transfer preferably includes at least one of the authentication code, payor bank identification number, customer account number, and delivery address.” EX1005, 5:67-6:4; *see also id.*, 2:38-47, 4:42-47, 4:59-63, 7:47-52, 8:44-49, 10:12-14.

Niwa’s authentication code is highly similar to Maes’s authorization number. EX1003, ¶172. Indeed, both are generated only if the user successfully passes biometric authentication, and both are used by the payor bank or similar financial institution to assess the legitimacy of a transaction request and to determine whether

to authorize the requested transaction. EX1005, 6:23-26; EX1004, 12:30-13:5. Niwa further teaches that the authentication code can be electronically transferred and provided to the merchant together with other payment information for a transaction. EX1005, 6:48-58.

As described above, MNC implement's Maes's system in accordance with Niwa's suggestion for transmitting payment information and an authorization number/code for a secured transaction from a user device over a common electronic channel, such that Maes's PDA would transmit (in encrypted form) the selected card information (*payment information*) and authorization number/code (*key*) to a POS terminal over the RF link (*via the short range RF circuitry*). *Supra*, §V.A.3; EX1004, 12:5-29, 13:33-38; EX1003, ¶¶173-173B (citing corroborating exhibits EX1008, EX1036-EX1039).

In MNC, CPU 12 in coordination with RF processor module 48 (aspects of the “*secure module*” (*supra*, [1.5.1])) are configured to perform operations for providing the selected card information and authorization number to the POS terminal over the RF link. EX1003, ¶178. For example, Maes explains that CPU 12 is coupled to the RF port 50 through RF processor module 48. EX1004, 6:9-14 (“[T]he device may preferably be equipped with an RF processor module 48, operatively connected between the CPU 12 and an RF port 50, ... for generating

transmission signals which are outputted from the RF port 50.”). EX1004, 6:9-14, Fig. 1; *see also id.*, 5:1-4, 6:9-14, 12:19-23; EX1003, ¶178.

(k) [2]

MNC renders [2] obvious. EX1003, ¶¶179-183.

As explained at [1.3], Maes’s **biometric module** (microphone 18 and/or biometric sensor 40) is configured to read biometric information. *Supra*, [1.3].

Per Maes, in MNC, the biometric information is read in a local mode of operation that Maes describes as “performed to initiate a consumer transaction,” and that “is commenced by the user selecting a pre-enrolled credit card that is stored in memory 14.” EX1004, 3:53-54, 10:30-32, Figs. 1, 5.

Maes further explains that biometric verification governs whether the selected card information reaches the transaction terminal, stating that “the CPU 12 of the PDA device 10 will prohibit the selected card information from being retrieved and transmitted to the transaction terminal 80 if the user is not biometrically verified and/or if the digital certificate is not valid (step 226).” EX1004, 12:19-23. Maes’s authorization number is also only generated and made available for a transaction if the user has been biometrically verified, and the authorization number is used by the central server in the process of completing a transaction. EX1004, 12:34-39, 12:55-13:5, Fig. 6.

From these and related descriptions, a POSITA would thus have understood that Maes's *biometric module* reads biometric information provided by a user to complete the transaction. EX1004, 10:30-32, 12:19-23; EX1003, ¶183.

(l) [3]

MNC renders [3] obvious. EX1003, ¶¶184-187.

As explained at [1.2], Maes's selected card information is *payment information* as claimed. *Supra*, [1.2]. The selected card information can include information regarding a pre-enrolled credit card that the user selects for the transaction. EX1004, Abstract ("selecting one of the pre-enrolled credit cards that are stored in the PDA"); 2:23-30 ("a user can store his or her credit card ... (*i.e.*, financial) information"), 4:1-11, 6:61-67, 11:51-57; EX1003, ¶185.

Maes describes enrolling such a card by "providing the service provider with the user's credit card ... information." EX1004, 6:64-65. And Maes recognizes that a payment card carries an account number, referring to "the account number provided on a credit card ..." EX1004, 6:40-41.

A POSITA would have understood the account number carried on the user's selected card — the number identifying the cardholder's account — to be associated with that card's "primary account number" (PAN), the standard term in the payment-card art for the account number carried on a payment card. EX1003, ¶187

(corroborated by EX1021, 1:17-21 (“typically a primary account number (PAN).”); EX1022, 1:66-2:2).

(m) [4]

MNC renders [4] obvious. EX1003, ¶¶188-191.

As explained at [1.5.5], in MNC, CPU 12 in coordination with RF processor module 48 (aspects of the “*secure module*” (*supra*, [1.5.1])) provide the encrypted authorization number (*encrypted key*) and the selected card information (*payment information*) via the short-range RF circuitry (*e.g.* including RF port 50). *Supra*, [1.5.1], [1.5.5].

Maes further explains that the recipient of the PDA’s RF transmission is a POS terminal, stating that “the consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal through an established communication link L2 (step 228, Fig. 3) (*i.e.*, via the serial port 42, the parallel port 44 modem 42, the IR port 54 or the RF port 50)” EX1004, 12:10-16. Niwa also discloses transmitting data “at the point of sale.” EX1005, 6:48-58.

From these and related descriptions, a POSITA would have understood that MNC’s CPU 12 in coordination with RF processor module 48 (aspects of the “*secure module*” (*supra*, [1.5.1])) are configured to provide the encrypted

authorization number (*encrypted key*) and the selected card information (*payment information*) via the short range RF circuitry to a *POS device*. EX1003, ¶191.

(n) [5]

MNC renders [5] obvious. EX1003, ¶¶192-197.

As an initial matter, the “stored separately” limitation in claim 5 cannot mean that the biometric authentication information and the payment information are stored in separate memories because claim 5 depends from claim 1, and [1.2] requires that both pieces of information be stored in the same “memory.”⁸ *Supra*, [1.2]. It is sufficient, therefore, that the biometric authentication information and the payment information be stored separately in the same memory, such as in logically distinct regions of, or under distinct access controls, within that memory. EX1003, ¶193. This is consistent with the specification of the ’187 Patent, which discloses a security-management unit and cryptographic block that gate access to memory using

⁸ Related U.S. Patent No. 10,706,412 similarly recites in claim 1 “a memory ... configured to store biometric authentication information and payment information,” and recites in dependent claim 3 “wherein the biometric authentication information is stored separately from the secured payment information.” EX1023, cls. 1, 3. This further evidences that “stored separately” in the ’187 Patent family does not require storage in separate memory devices.

cryptographic keys (*see* EX1001, 2:32-37, 10:65-11:4, 14:55-60, 22:22-26), and describes that information contained on the RF device is “protected by sundry cryptographic methods” (*id.* at 8:38-39), indicating that different categories of sensitive data can be logically segregated within a single memory such as through distinct access-control or cryptographic regimes. EX1003, ¶193. The specification nowhere discloses physically distinct memory chips for the biometric and payment information. EX1003, ¶193.

In MNC, per Maes, biometric authentication information includes the user’s voice models or other biometric data, which Maes stores in memory 14. EX1004, 10:59-61 (“comparing the current biometric voice data with the user’s voice models stored in memory 14”), 5:53-62 (describing alternative forms of biometric data). The payment information, *e.g.*, the user’s encrypted card information, is likewise stored in memory 14. EX1004, Abstract (“a memory for storing financial and personal information of the user”), 2:60-66, 3:20-24, 5:1-4, 5:14-17, 7:1-7; 11:24-29, 12:44-47; *supra*, [1.2].

A POSITA would have understood that Maes’s voice models or alternate biometric data (*biometric authentication information*) and its encrypted card information (*payment information*) are stored in different locations of memory and are therefore “*stored separately*” from one another as recited in claim 5. EX1003, ¶195. Indeed, the encrypted financial/card information and the biometric data would

be stored separately in distinct locations of the memory to enable them to be accessed separately for their distinct purposes as described in Maes. *Id.*

Maes also discloses cryptographic separation of the payment information from the biometric authentication information within memory 14. In particular, Maes discloses that “CPU 12 further includes an encrypter/decrypter module 24 for encrypting the personal and financial information before being stored in memory 14 and for decrypting such information when accessed by the user.” EX1004, 5:14-17. The card information is thus stored in memory 14 in encrypted form, protected by “an encryption key unique to the PDA device 10.” EX1004, 11:27-32. The biometric authentication data, such as the user’s voice models and any fingerprint, palm print, handwriting, or retinal templates, is not described as being encrypted under that same key or protected under the same regime. Maes discloses that the biometric authentication data is instead accessed through a distinct processing path via the acoustic processor module 16 or the biometric processor module 22 for the purpose of user verification. EX1004, 5:1-17, 5:53-62, 11:9-14. The payment information and the biometric authentication information are therefore stored under distinct access-control regimes within memory 14. EX1003, ¶196.

Additionally, Maes discloses that access to the payment information is gated by an additional layer of protection in the form of the digital certificate that does not gate access to the biometric authentication information. Under Maes’s architecture,

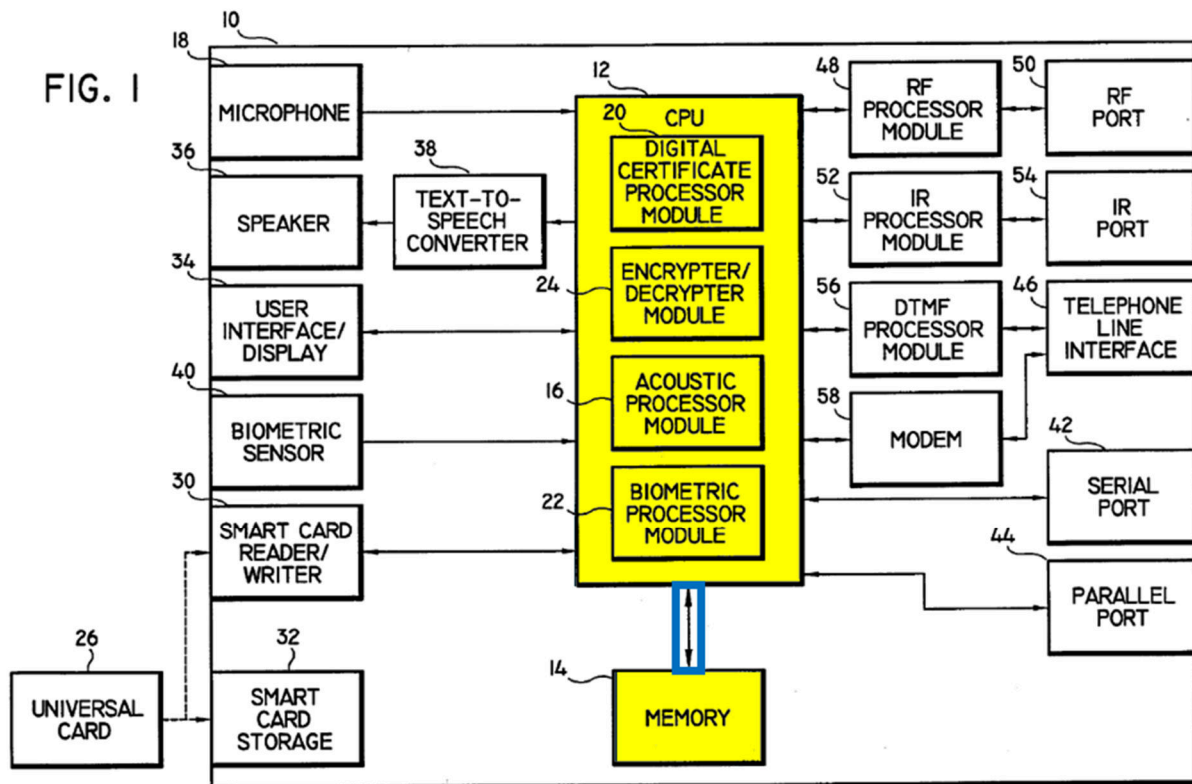
biometric verification alone is not sufficient to access the stored card information. The PDA device 10 also requires a valid, unexpired digital certificate stored in memory 14, which is separately decrypted by the encrypter/decrypter module 24 and validated by the digital certificate processor module 20 before the encrypter/decrypter module 24 will retrieve and decrypt the card information. EX1004, 7:42-54, 11:16-32. Biometric verification, by contrast, is performed directly against the stored voice data or biometric data without need for a valid digital certificate. EX1004, 11:9-14; Fig. 5 (steps 206-212). This access-control architecture further demonstrates how the payment and biometric information are “*stored separately*” within Maes’s memory 14. EX1003, ¶197.

(o) [6]

MNC renders [6] obvious. EX1003, ¶¶198-203.

In MNC, the payment information is stored in memory 14. *See* [1.2], *supra*. That memory is accessible by the CPU 12 (aspect of the “*secure module*” (*supra*, [1.5.1])). EX1003, ¶200. For example, Maes explains that “[t]he CPU 12 then searches the memory 14 for the desired information (step 202)” and that “the requested card information is then retrieved from memory 14 and stored in the encrypter/decrypter module 24.” EX1004, 10:44-45, 11:27-29.

Maes's Fig. 1, reproduced below, illustrates memory 14 connected to CPU 12 and to no other device 10 component. EX1004, Fig. 1; EX1003, ¶201.



EX1004, Fig. 1 (highlighted).

Maes further describes various restrictions on access to financial or card information stored in memory 14. For example, the financial information is encrypted by the encrypter/decrypter module 24 using an encryption key unique to the PDA device 10, and is decrypted through that module before use. EX1004, 5:14-17, 11:26-29. Additionally, biometric verification is required “prior to accessing the financial and personal information stored in memory 14.” EX1004, 5:58-62. Moreover, a valid, unexpired digital certificate is independently required, and even a successfully verified user cannot access the financial information without one. EX1004, 3:63-4:2, 11:23-25. Maes then expressly prohibits the CPU 12 from

retrieving and transmitting the financial information unless both the biometric verification and digital certificate checks succeed, stating that “the CPU 12 of the PDA device 10 will prohibit the selected card information from being retrieved and transmitted to the transaction terminal 80 if the user is not biometrically verified and/or if the digital certificate is not valid.” EX1004, 12:20-25.

From these and related descriptions, a POSITA would have understood that MNC’s card information (*payment information*) is stored in a memory 14 (*memory*) accessible only by CPU 12 (aspect of the “*secure module*”). EX1003, ¶203.

(p) [8.pre]

MNC, per Maes, discloses a “*system*” comprising a PDA (*mobile device*), point-of-sale (POS) transaction terminal (*POS device*), and central server 60 with servers of a financial institution 70 (*central database*). *Supra*, [1.pre]; *infra*, [8.1], [8.7.1], [8.8]; EX1003, ¶204.

(q) [8.1]

Supra, [1.pre]; EX1003, ¶205.

(r) [8.2]

Supra, [1.1]; EX1003, ¶206.

(s) [8.3]

Supra, [1.2]; EX1003, ¶207.

(t) [8.4]

Supra, [1.3]; EX1003, ¶208.

(u) [8.5]

Supra, [1.4]; EX1003, ¶209.

(v) [8.6.1]

Supra, [1.5.1]; EX1003, ¶210.

(w) [8.6.2]

Supra, [1.5.2]; EX1003, ¶211.

(x) [8.6.3]

Supra, [1.5.3]; EX1003, ¶212.

(y) [8.6.4]

Supra, [1.5.4]; EX1003, ¶213.

(z) [8.6.5]

Supra, [1.5.5]; EX1003, ¶214.

(aa) [8.7.1]

MNC renders [8.7.1] obvious. EX1003, ¶¶215-216.

For example, per Maes, the merchant's POS terminal (*POS device*) is configured to receive, process, and transmit information electronically for a transaction. *See e.g.*, EX1004, 12:5-8, 12:10-18, 13:34-38, Fig. 3; EX1003, ¶216.

(bb) [8.7.2]

MNC renders [8.7.2] obvious. EX1003, ¶¶217-220. In MNC, the POS terminal (*POS device*) receives from the PDA's *secure module* (e.g., CPU 12 and RF module 48) the encrypted authorization number (*key*) and the selected card information (*payment information*). EX1004, 12:5-29, 13:34-38, Figs. 1, 5, 6; EX1005, 6:3-4; EX1003, ¶¶217-220.

(cc) [8.7.3]

MNC renders [8.7.3] obvious. EX1003, ¶¶221-223. In MNC, the POS terminal (*POS device*) transmits to central server 60 and financial institution 70 (*central database*), the encrypted authorization number (*key*) and the card information used in the transaction (*payment information*). EX1004, 11:38-40, 12:55-63, 12:65-13:5, Fig. 3; EX1003, ¶¶221-223. To the extent the “*central database*” is a single entity, consolidating the functions of Maes's central server 60 and financial institution 70 into a single back-end would have been obvious to achieve well known and predictable benefits of centralization, including lower overhead costs, reduced coordination costs, and reduced latency in communicating between otherwise distant systems. *Id.*; *KSR*, 550 U.S. at 416 (“the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results”); *In re Larson*, 340 F.2d 965, 968 (CCPA

1965) (consolidation of separate components is “merely a matter of obvious engineering choice”); EX1003, ¶¶221-223.

(dd) [8.8]

MNC renders [8.8] obvious. EX1003, ¶¶224-226. In MNC, the central server 60 and financial institution 70 (*central database*) validate the authorization number (*key*) and the card information used in the transaction (*payment information*). EX1004, 6:34-39, 6:63-7:3, 7:19-35, 12:55-13:5, 13:47-56, Fig. 3; EX1003, ¶¶224-226.

(ee) [9]

Supra, [2]; EX1003, ¶227.

(ff) [10]

Supra, [3]; EX1003, ¶228.

(gg) [11]

MNC renders [11] obvious. EX1003, ¶¶229-230.

Maes discloses that the PDA and POS device communicate over an RF link, and that the PDA transmits information for a transaction received by the PDA via RF. EX1004, 12:5-8, 12:10-15, 13:34-38, Abst. From these disclosures, a POSITA would have understood the merchant’s terminal (*POS device*) to include an RF reader. EX1003, ¶230. Indeed, an RF reader would be inherent or obvious for the POS device to receive the information that Maes expressly discloses is transmitted

to the POS device from the PDA via RF. EX1004, 12:5-8, 12:10-15, 13:34-38, Abstract; EX1003, ¶230.

(hh) [12]

Supra, [5]; EX1003, ¶231.

(ii) [13]

Supra, [6]; EX1003, ¶232.

(jj) [15.pre]

Supra, [1.pre]; EX1004, 1:11-17 (“portable information and transaction processing system and method”), 14:18-21 (“perform the methods and functions of the present invention”); EX1003, ¶¶233-234.

More specifically, in MNC, the PDA device 10 (***mobile device***) performs the operations of [1.pre]-[6]. *Supra*, [1.pre]-[6]; EX1003, ¶234.

(kk) [15.1]

Supra, [1.2]; EX1003, ¶235.

(ll) [15.2]

Supra, [1.3]; EX1003, ¶¶236-237.

Maes's microphone 18 and biometric sensor 40 provide the ***biometric reader***, for the reasons discussed at [1.3] (describing the ***biometric module***). *Supra*, [1.3]; EX1003, ¶237.

(mm) [15.3]

Supra, [1.4]; EX1003, ¶238.

(nn) [15.4]

Supra, [1.5.2]; EX1003, ¶239.

(oo) [15.5]

Supra, [1.5.3]; EX1003, ¶240.

(pp) [15.6]

Supra, [1.5.4]; EX1003, ¶241.

(qq) [15.7]

Supra, [1.5.5]; EX1003, ¶242.

(rr) [16]

Supra, [2]; EX1003, ¶243.

(ss) [17]

Supra, [3]; EX1003, ¶244.

(tt) [18]

Supra, [4]; EX1003, ¶245.

(uu) [19]

Supra, [5]; EX1003, ¶246.

(vv) [20]

Supra, [6]; EX1003, ¶247.

(ww) [21]

Supra, [1.5.5]; EX1003, ¶¶248-249.

As explained at [1.5.5], in MNC, the PDA transmits the selected card information (*payment information*) to the POS terminal over the RF link (*short range RF circuitry*). *Supra*, [1.5.5], [1.1]; EX1003, ¶249.

B. Ground 1B: Maes-Niwa-Shults Renders Obvious Claims 7 and 14

1. Shults (EX1008)

Shults describes “a portable cellular telephone or a personal digital assistant.” EX1008, [0009]. Shults explains that “[t]he hand-held or portable aspect of apparatus 100 is particularly advantageous when it is used for purchasing or other types of financial transactions.” EX1008, [0024]; *see also id.*, [0030], [0043]. Shults discloses that the electronic identity of a customer using the portable apparatus “is provided by a radio-frequency identification (RFID) circuit 104.” *Id.*, [0030]; EX1003, ¶¶114-115.

2. The Maes-Niwa-Shults Combination (MNSC)

A POSITA would have found it obvious to implement the RF circuitry in Maes’s PDA using RFID in accordance with Shults’s teachings. EX1004, 6:9-15, 12:10-15; EX1008, [0024], [0030], [0031]; EX1003, ¶¶116-125. Multiple reasons would have motivated the combination. EX1003, ¶¶116-125.

First, a POSITA would have been motivated to use RFID in Maes's PDA because Shults confirms that an RFID-based electronic identity is "particularly advantageous when it is used for purchasing or other types of financial transactions" and Maes's PDA is used for exactly this purpose. EX1004, 6:9-15, 12:10-15; EX1008, [0024]; EX1003, ¶¶116-125.

Second, a POSITA would have been motivated to implement RFID in Maes's PDA to enable transactions with existing point-of-sale systems without requiring modification to those systems. EX1003, ¶¶116-125; EX1008, [0037] ("intended to be used with existing point-of-sale systems").

Third, a POSITA would have been motivated to use RFID in Maes's PDA to achieve a cost-effective implementation using off-the-shelf, commercially available components. EX1003, ¶¶116-125. Shults expressly teaches that RFID circuit 104 can be implemented with a conventional, commercially available system such as "a Texas Instruments TIRIS system," "a ROADCHECK system from Mark IV Inc.," or "an ASSET ID system from HID Corp." EX1008, [0031]; EX1003, ¶¶116-125. Thus, RFID would have been beneficial to increase interoperability and avoid the expense of developing a custom short-range RF solution. *Id.*

Fourth, a POSITA would have been motivated to implement RFID in Maes's PDA because doing so merely involved the application of a known RF technique (e.g., RFID) that was both consistent with Maes's RF-based embodiments and well

within the POSITA's technical grasp. *KSR*, 550 U.S. 398, 417, 421 (2007). A POSITA seeking to implement RF-based identification in Maes's PDA would have looked to Shults's RFID circuit 104 as a familiar, readily available element performing its established function, requiring nothing more than ordinary skill to apply it in the PDA's RF circuitry. EX1004, 6:9-15, 12:10-15; EX1008, [0030], [0031]; EX1003, ¶¶116-125.

A POSITA would have reasonably expected success applying RFID to Maes's PDA, especially as Maes already contemplates the use of RF circuitry "using conventional constructions and techniques," and Shults's RFID circuit 104 represents such a conventional construction. EX1004, 6:9-15; EX1008, [0031]; EX1003, ¶¶116-125.

3. Claim Element Analysis

(a) [7]

MNSC renders [7] obvious. EX1003, ¶¶250-252.

In MNSC, the PDA device 10 (*mobile device*) includes short range RF circuitry (*see supra*, Ground 1A at [1.1]), and that circuitry further includes an RFID circuit consistent with Shults's teachings. *Supra*, §§V.B.1-2, Ground 1A at [1.1]; EX1008, [0030]; EX1003, ¶251.

Therefore, a POSITA would have understood that in MNSC, the mobile device's *short-range RF circuitry comprises an RFID device*. *Supra*, §V.B.2; EX1008, [0030]; EX1003, ¶252.

(b) [14]

Supra, Ground 1B at [7]. EX1003, ¶253.

C. Ground 2A: Maes-Bjorn Renders Obvious Claims 1-6, 8-13, and 15-21

1. Bjorn (EX1006)

Bjorn describes “cryptographic key generation using biometric data.” EX1006, 1:1-7. In Bjorn, a message is created from a received fingerprint and “[a] message digest function is applied to the message to create a cryptographic key.” EX1006, 1:42-46, 1:50-51. Bjorn states that “[f]or one embodiment, a one-way hash function or message digest function is used to create the hash.” EX1006, 3:45-52; EX1003, ¶¶91-94.

With reference to Fig. 3 (reproduced below), Bjorn explains that “[a]t block 320, a template is created for the user.” EX1006, 4:21-23. “For one embodiment, the fingerprint template is a digital image of the fingerprint.” EX1006, 8:32-33. “At block 325, the template is hashed.” EX1006, 4:25. Bjorn adds that “[f]or one embodiment, this hash is the cryptographic key.” EX1006, 4:25-26. Bjorn further states that “[t]his cryptographic key is identified with the specific fingerprint, and

thus with a specific user.” EX1006, 4:28-30. “At block 335, the template is stored,” although “[t]he cryptographic key itself is not stored anywhere on the system.” EX1006, 4:47-48. Bjorn notes that “the template is stored in a database, or other more centralized location.” EX1006, 4:47, 4:51-53.

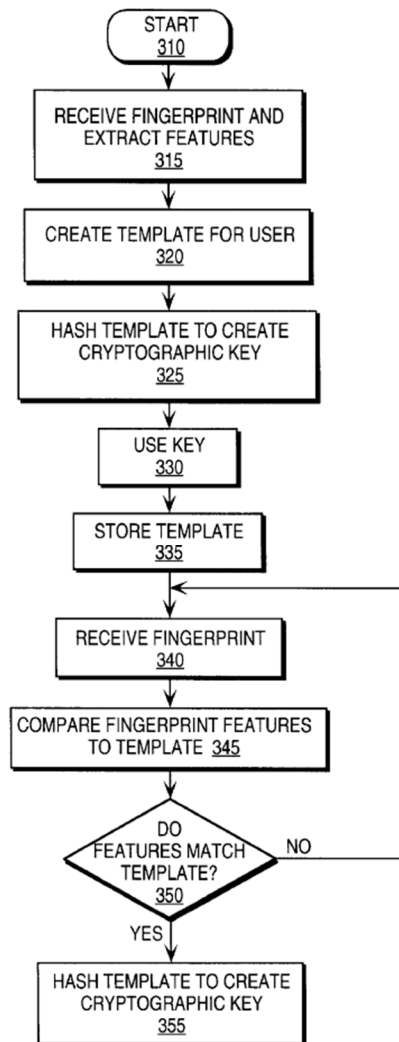


FIG. 3

According to Bjorn, “if [a] new fingerprint matches the template” then the system “appl[ies] the message digest function to the stored template to generate the cryptographic key.” EX1006, claim 3. Thus, “[a]t block 355, the template is again

hashed to create a cryptographic key.” EX1006, 5:10-11. Bjorn explains that “[s]ince the template was used to generate the first cryptographic key, the same key is generated.” EX1006, 5:11-12. Bjorn’s cryptographic key can then be used in a cryptographic function to encrypt or decrypt desired data item(s). EX1006, 4:38-45; *see also id.*, 5:15-6:23 & Fig. 4, Figs. 5-8.

2. The Maes-Bjorn Combination

The Maes-Bjorn Combination (“MBC”) integrates, in Maes, Bjorn’s technique for generating a cryptographic key from biometric data such as a user’s fingerprint. *Supra*, §V.C.1; EX1003, ¶¶95-108. In MBC, Maes’s encrypted information file (*see* EX1004, 13:19-39), which Maes’s PDA device 10 transmits to the merchant’s POS terminal along with payment information for a POS transaction, is modified to include a cryptographic key generated in accordance with Bjorn’s techniques (*e.g.*, as described with respect to Figs. 3 or 4 of Bjorn) in response to biometric authentication of the user (*e.g.*, in response to determining that the user’s fingerprint obtained at the POS matches a stored template (*e.g.*, “a digital image of the fingerprint”), per Bjorn steps 350 or 460) . EX1004, 8:32-34, 13:19-39; EX1003, ¶¶95-108. In the combined Maes-Bjorn device, Bjorn’s block-355/470 key regeneration is triggered by the local biometric verification Maes already performs on the PDA. EX1006, 5:3-12, Figs. 3-4; EX1004, 5:54-57, 11:9-13; EX1003, ¶¶95-108.

Multiple reasons would have motivated a POSITA to implement the combination, with a reasonable expectation of success, as the combination is a natural extension of what Maes and Bjorn each already teach. EX1003, ¶¶95-108. Maes expressly describes the encrypted information file as containing “unique identifying information pertaining to the consumer including, but not limited to, ... the consumer’s name and account number.” EX1004, 13:26-32. Maes thus contemplates that additional unique identifying information, beyond name and account number, may be included to enable “the financial institution (e.g., credit card company) [to] verify the identity of the consumer during a purchase transaction.” EX1004, 13:20-24; EX1003, ¶¶95-108.

Bjorn’s cryptographic key is precisely such information. EX1003, ¶¶95-108. Bjorn teaches “generat[ing] a unique cryptographic key using biometric data” from a user’s fingerprint and applying a message digest function to produce the key. EX1006, 1:5-8, 4:26-33, Abstract; *supra*, §V.C.1. Bjorn further teaches that “[t]his cryptographic key is identified with the specific fingerprint, and thus with a specific user.” EX1006, 4:29-31. A POSITA would thus have recognized that Bjorn’s key is exactly the type of “unique identifying information” that Maes contemplates could be included in the encrypted information file that would allow the financial information to verify the identity of the consumer in a secure transaction. EX1004, 13:26-30; EX1003, ¶¶95-108. Bjorn’s key would supplement the user’s name and

account number in the file or would provide an obvious substitution for the name and/or account number, since each serves to identify the user. EX1003, ¶¶95-108.

A POSITA would have sought to include Bjorn's key in Maes's information file to strengthen the financial institution's ability to verify the user. EX1004, 13:22-24; EX1003, ¶¶95-108. The "name and account number" example file contents given in Maes may be uniquely associated with a user, but they are less secure because they are not typically closely held secrets. An unauthorized holder of a lost or stolen card could readily obtain the cardholder's name and account number from public sources (e.g., mail theft, data breaches, or skimming devices), so name and account number alone would not always reliably confirm that the presenter is the authorized user. EX1004, 13:22-24, 13:30-32; EX1003, ¶¶95-108. Bjorn's key, by contrast, is derived from the user's fingerprint rather than the card. This key uniquely identifies the authorized user in a way not obtainable by an unauthorized holder, as it supplies an identifier not otherwise available from the card, better ensuring MBC will not authorize a transaction unless the presenter is the authorized user. EX1004, 13:22-24; EX1006, 4:28-30; EX1003, ¶¶95-108.

The combination also would have been obvious considering that Maes and Bjorn also each independently teach fingerprint-based authentication. EX1003, ¶¶95-108. Maes's sensor may collect data from "a finger, thumb or palm print," among other biometrics. EX1004, 5:53-58; see also id., 11:1-5. Bjorn likewise

generates its key from fingerprint data. EX1006, Abstract, 1:5-8. Incorporating Bjorn's key thus requires no conceptual departure, it merely uses fingerprint data Maes already collects for an additional, complementary purpose. EX1003, ¶¶95-108.

A POSITA also would have turned to Bjorn because its approach improves security by maintaining no persistent copy of the key on the device EX1006, 4:47-48 ("The cryptographic key itself is not stored anywhere on the system."). The key must instead be produced each time it is required. EX1006, 5:8-12. Regenerating the key only upon successful fingerprint verification advances Maes's aim of biometric security that "protects against the unauthorized access to the user's financial and personal information" and reduces the risk of the key leaking. EX1004, 4:9-10; EX1003, ¶¶95-108.

Maes's enrollment process already stores biometric data including fingerprint data at the central server. EX1004, 7:24-31, 5:53-59. A POSITA would have understood that enrolling a fingerprint template as Bjorn teaches requires no change to Maes's architecture. EX1004, 5:56-59, 7:28-31; EX1006, 3:14-15; EX1003, ¶¶95-108. In MBC, Maes's POS terminal transmits the encrypted file to the institution, where comparison and verification take place, with the template stored there, as Bjorn teaches may be "a database, or other more centralized location." EX1004, 13:34-38, 13:22-24; EX1006, 4:47, 4:51-53; EX1003, ¶¶95-108.

Bjorn teaches that hashing the stored template reproduces the same key. EX1006, 5:10-12 (“[T]he template is again hashed to create a cryptographic key,” and “[s]ince the template was used to generate the first cryptographic key, the same key is generated.”); EX1003, ¶¶95-108. In MBC, consistent with Bjorn’s teachings, the PDA regenerates the key from the template for inclusion in the encrypted information file, so that the financial institution may compare the regenerated key from the file to the reference key to verify that the user engaged in the transaction is the authorized user associated with the account. EX1004, 13:34-38; EX1006, 5:10-12, 4:28-30; EX1003, ¶¶95-108. A POSITA thus would have been motivated to generate a key for inclusion in Maes’s information file according to Bjorn’s techniques because Bjorn’s techniques allow the key to be accurately regenerated at the PDA despite potential variations in the fingerprint read by the device at the point of sale, such that the financial institution can perform a straightforward comparison between the new key and the reference key to reliably verify the user’s identity. EX1004, 2:1-13, 12:61-63; EX1003, ¶¶95-108.

This server-side verification also mitigates an attack vector left open by local verification alone. EX1003, ¶¶95-108. In Maes, an attacker with PDA access could conceivably alter the locally stored reference template to pass local verification. EX1004, 10:59-11:5; EX1003, ¶¶95-108. Institution-side verification using Bjorn’s

key would frustrate this attack, since the enrolled template held by the institution is independent of the PDA. See EX1006, 1:35-37; EX1003, ¶¶95-108.

A POSITA would have been further motivated to integrate Bjorn's techniques because its key is fully functional in standard cryptographic operations, including encryption and decryption already contemplated by Maes. EX1003, ¶¶95-108. Bjorn confirms that its fingerprint-derived key can serve as a private key in a public-key cryptosystem to sign or encrypt documents, generated using well-known functions such as MD5. EX1006, 3:56-58, 4:31-33, 4:36-45. This is significant because Maes's system relies on encryption to safeguard a variety of information, including the encrypting the digital certificate and the card information stored on the PDA using "any known encryption technique or algorithm." EX1004, 9:52-56, 11:29-34, 10:11-14; *see also id.*, 5:15-19. A POSITA would have selected Bjorn's key for these operations, since the key can only be regenerated upon successful fingerprint verification, ensuring decryption of the digital certificate occurs only upon a matching fingerprint. EX1006, 5:1-13; EX1004, 3:31-40, 9:52-56; EX1003, ¶¶95-108.

A POSITA would have reasonably expected success, as Maes and Bjorn are directed to the same field of secure electronic transactions employing biometric authentication and cryptographic techniques, and each uses conventional, well-understood components (*e.g.*, fingerprint sensors, hash functions such as MD5, and

standard encryption/decryption modules). *See* EX1006, 3:24-35, 3:44-58, 4:19-20; EX1004, 5:15-19, 10:11-14.

3. Claim Element Analysis

(a) [1.pre]

The Maes-Bjorn Combination (“MBC”) described above (*supra*, §V.C.2) renders [1.pre] obvious in view of Maes’s disclosures for at least the reasons addressed above in Ground 1A. *Supra*, Ground 1A at [1.pre]; EX1003, ¶254.

(b) [1.1]

Supra, Ground 1A at [1.1]; EX1003, ¶255.

(c) [1.2]

MBC renders [1.2] obvious. EX1003, ¶¶256-258.

As discussed, per Maes, the memory of the PDA (***mobile device***) is configured to store credit card information (***payment information***) for use in transactions. EX1004, 5:8-24, 7:1-7; *supra*, Ground 1A at [1.2]; EX1003, ¶257.

Further, in MBC, per Bjorn, the information stored in memory further includes a “fingerprint template” representing an authorized user’s fingerprint scan. EX1006, 4:21-24 (“At block 320, a template is created for the user.”), 4:47-53 (“At block 335, the template is stored.”), Fig. 3; *see also* 5:31-39, 5:49-54, Fig. 4. Bjorn describes various information that can be included in the fingerprint template, each of which renders obvious the claimed “***biometric authentication information***,”

including “a digital image of the fingerprint.” EX1006, 8:32-34; *see also id.*, 14:3-4 (“comparing the fingerprint image to the fingerprint template”).⁹

(d) [1.3]

Supra, Ground 1A at [1.3]; EX1003, ¶259.

(e) [1.4]

Supra, Ground 1A at [1.4]; EX1003, ¶¶260-261.

In MBC, Bjorn reinforces the obviousness of [1.4]. For example, Bjorn describes a processor that authenticates a user by comparing data from a current scan of the user’s fingerprint to a stored template, and determining whether they match. EX1006, 4:64-5:9 & Fig. 3 (steps 345, 350), 5:65-6:10 & Fig. 4 (steps 455, 460).

(f) [1.5.1]

Supra, Ground 1A at [1.5.1]; EX1003, ¶262.

⁹ For embodiments where the fingerprint template is a “digital image of the fingerprint,” a POSITA would have understood that Bjorn’s processes described with respect to Figs. 3-4 could omit extracting features from the fingerprint. It would have been obvious to a POSITA in this case to perform a comparison between the received fingerprint (blocks 340/450) and the fingerprint image in the stored template (blocks 345/455). EX1006, 8:32-34, 14:3-4.

(g) [1.5.2]

MBC renders [1.5.2] obvious. EX1003, ¶¶263-268.

Bjorn describes generating a cryptographic key (*key*) in response to authentication. For example, as shown in Fig. 3, Bjorn discloses key generation at step 355 in response to determining a match between the user's current fingerprint and fingerprint data of an authorized user in a stored template:

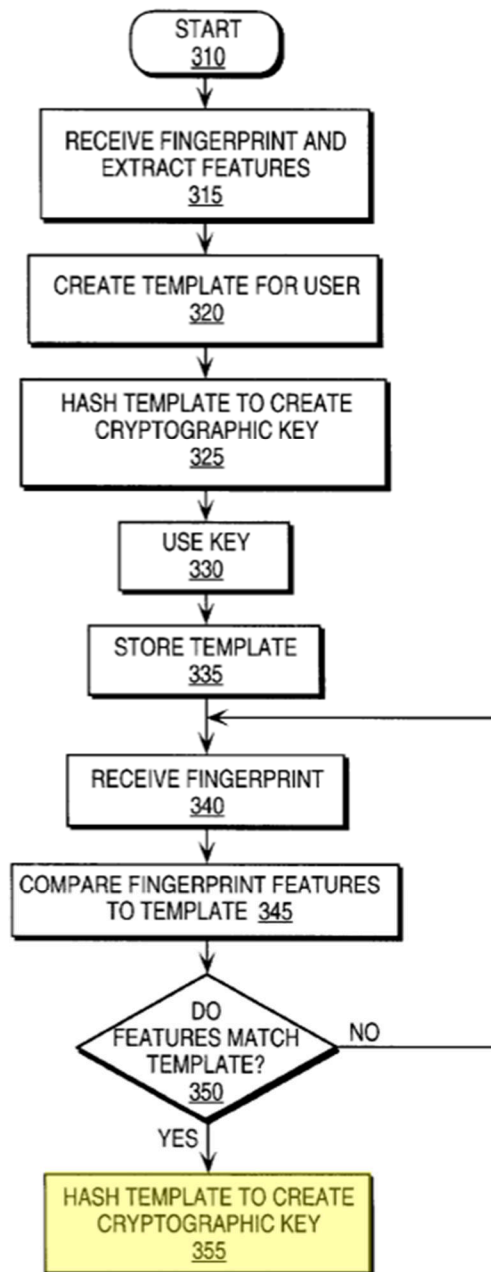


FIG. 3

EX1006, Fig. 3 (annotated)

See also EX1006, 4:60-5:13, 5:61-6:23 & Fig. 4; *supra*, §V.C.1.

Bjorn does not store or otherwise retain the cryptographic key: “[t]he cryptographic key itself is not stored anywhere on the system.” EX1006, 4:47-48.

Instead, the key is produced when needed, and only in response to successful authentication based on the fingerprint match. EX1006, 5:8-12; EX1003, ¶266.

As addressed in detail above (*supra*, §V.C.2), it would have been obvious to implement Maes in accordance with Bjorn’s teachings regarding generation of a cryptographic key based on biometric information. EX1003, ¶267. In MBC, Bjorn’s key generation is triggered by local biometric verification consistent with Maes’s biometric verification on the PDA, and as similarly described with respect to Figs. 3 and 4 of Bjorn (*e.g.*, blocks 340-355 and 450-470). EX1006, 5:3-12, Figs. 3-4; EX1004, 5:54-57, 11:9-13; *supra*, §V.C.2; EX1003, ¶267. In MBC, Maes’s CPU 12—an aspect of the “*secure module*” (*supra*, Ground 1A at [1.5.1]) generates the Bjorn-like cryptographic key (*key*).

From these and related descriptions, a POSITA would have understood that MBC’s *secure module* generates a key when the fingerprint template (*biometric information*) read by the *biometric reading device* (*e.g.*, biometric sensor 40) is determined by the *authentication module* (*e.g.*, biometric processor module 22) to correspond to the *biometric authentication information* (*e.g.*, fingerprint template) stored in *memory* (*e.g.*, memory 14). EX1003, ¶268.

(h) [1.5.3]

MBC renders [1.5.3] obvious. EX1003, ¶¶269-272.

In MBC, Bjorn's cryptographic key (**key**) is carried in an information file that accompanies the selected card information for a transaction. *Supra*, §V.C.2, [1.5.2]; EX1003, ¶270. Per Maes, that file, which "contain[s] unique identifying information pertaining to the consumer." EX1004, 13:30-31.

Further, in MBC, the PDA's CPU 12 (**secure module**) encrypts the information file, including Bjorn's cryptographic key, using the encrypter/decrypter module 24. EX1004, 5:14-17; EX1003, ¶271. Per Maes, in the PDA device 10, the CPU 12's encrypter/decrypter module 24 (an aspect of MBC's "**secure module**" (*supra*, Ground 1A at [1.5.1])) performs encryption, with Maes explaining that "[t]he CPU 12 further includes an encrypter/decrypter module 24 for encrypting the personal and financial information before being stored in memory 14 and for decrypting such information when accessed by the user." EX1004, 5:14-17, Fig. 1. Given the availability of the encrypter/decrypter module 24 to perform encryption, it would have been obvious to utilize module 24 in MBC's PDA to encrypt the information file including the cryptographic key consistent with Maes's teaching that the information file is encrypted. EX1004, 5:14-17, 13:30-31; *see* Ground 1A at [1.5.1], [1.5.3], *supra* §V.C.2; EX1003, ¶271.

Thus, a POSITA would have understood that, because Bjorn's cryptographic key (**key**) is included in the encrypted information file, MBC's secure module **encrypts the key**. EX1004, 5:14-17, 13:30-31; *supra*, §V.C.2; EX1003, ¶272.

(i) [1.5.4]

Supra, Ground 1A at [1.5.4]; EX1003, ¶273.

(j) [1.5.5]

MBC renders [1.5.5] obvious. EX1003, ¶¶274-277.

Maes discloses the PDA transmitting the selected card information (***payment information***) to a POS terminal via short-range RF circuitry for use in a secure transaction. For example, Maes explains that “[t]he selected card information[] ... would be transmitted to the POS terminal (via ... RF ...) and then transmitted in encrypted form directly to the processing financial institution together with the purchase details.” EX1004, 13:34-38; *see also id.*, 12:5-29, Figs. 3, 5.

Maes further discloses that the information transmitted via RF from the PDA to the POS terminal can include an “encrypted information file” that “contain[s] unique identifying information pertaining to the consumer” for use in validating consumer in the transaction. EX1004, 13:24-38.

For the reasons addressed in detail above (*supra*, §V.C.2), it would have obvious to incorporate a cryptographic key (***key***), generated in accordance with Bjorn’s techniques when the user is biometrically authenticated, in the “encrypted information” that Maes’s PDA transmits to the POS terminal via RF. *Supra*, §V.C.2, IV.A; EX1003, ¶277. In MBC, the PDA thus transmits to the POS terminal via short-range RF both the encrypted information file including Bjorn’s (encrypted)

cryptographic key (*encrypted key*) and the selected card information (*payment information*) for use in the transaction. *Id.*

(k) [2]

Supra, Ground 1A at [2]; EX1003, ¶278.

(l) [3]

Supra, Ground 1A at [3]; EX1003, ¶279.

(m) [4]

Supra, Ground 1A at [4]; EX1003, ¶280.

(n) [5]

Supra, Ground 1A at [5]; EX1003, ¶281.

(o) [6]

Supra, Ground 1A at [6]; EX1003, ¶282.

(p) [8.pre]

MBC, per Maes, discloses a “*system*” comprising a PDA (*mobile device*), point-of-sale (POS) transaction terminal (*POS device*), servers of a financial institution 70 (*central database*), optionally further including central server 60. *Supra*, [1.pre]; *infra*, [8.1], [8.7.1], [8.8]; EX1003, ¶283.

(q) [8.1]

Supra, Ground 2A at [1.pre]; EX1003, ¶284.

(r) [8.2]

Supra, Ground 2A at [1.1]; EX1003, ¶285.

(s) [8.3]

Supra, Ground 2A at [1.2]; EX1003, ¶286.

(t) [8.4]

Supra, Ground 2A at [1.3]; EX1003, ¶287.

(u) [8.5]

Supra, Ground 2A at [1.4]; EX1003, ¶288.

(v) [8.6.1]

Supra, Ground 2A at [1.5.1]; EX1003, ¶289.

(w) [8.6.2]

Supra, Ground 2A at [1.5.2]; EX1003, ¶290.

(x) [8.6.3]

Supra, Ground 2A at [1.5.3]; EX1003, ¶291.

(y) [8.6.4]

Supra, Ground 2A at [1.5.4]; EX1003, ¶292.

(z) [8.6.5]

Supra, Ground 2A at [1.5.5]; EX1003, ¶293.

(aa) [8.7.1]

Supra, Ground 1A at [8.7.1]; EX1003, ¶294.

(bb) [8.7.2]

MBC renders [8.7.2] obvious. EX1003, ¶¶295-296.

Per Maes, “[t]he selected card information, as well as the encrypted information file, would be transmitted to the POS terminal.” EX1004, 13:34-38. Accordingly, in MBC, per Maes, the PDA transmits the encrypted information file including the encrypted version of Bjorn’s cryptographic key (*encrypted key*) and the selected card information (*payment information*) using CPU 12 and RF module 48 (aspects of the “*secure module*” (*supra*, Ground 1A [1.5.1])) to the POS device over RF link L2. EX1004, 12:10-16, 13:19-37; EX1005, 6:3-4; *supra*, Ground 1A and 2A at [1.5.1], [1.5.5], [4]; EX1003, ¶296. The POS device thus *receives, from the secure module*, the encrypted version of Bjorn’s cryptographic key (*encrypted key*) and the selected card information (*payment information*). EX1003, ¶296.

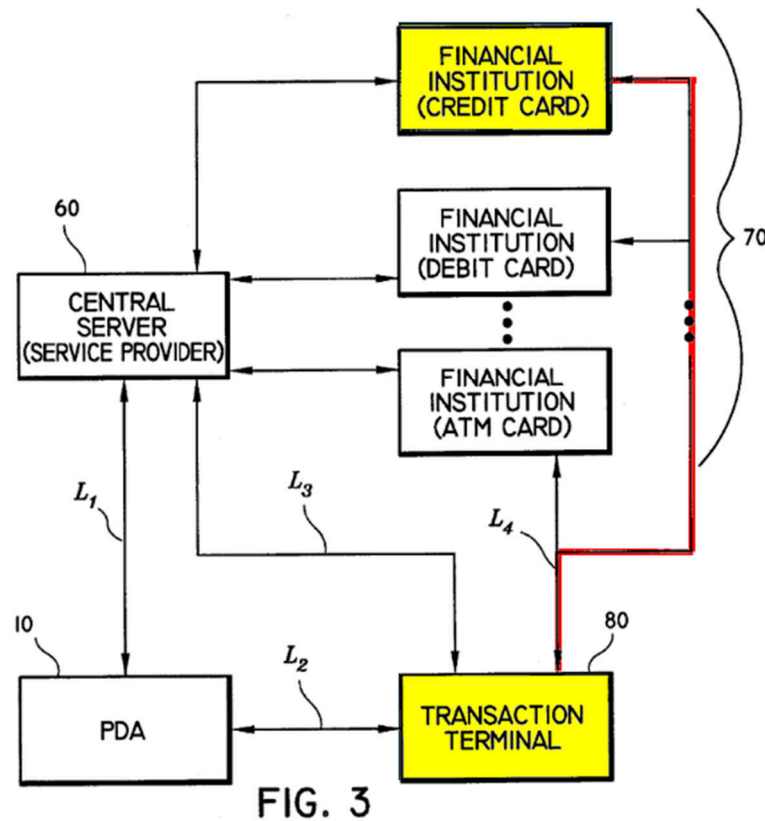
(cc) [8.7.3]

MBC renders [8.7.3] obvious. EX1003, ¶¶297-302.

Per Maes, “[t]he selected card information, as well as the encrypted information file, would be transmitted to the POS terminal (via the Universal Card, RF or IR) and then transmitted in encrypted form directly to the processing financial

institution together with the purchase details.” EX1004, 13:34-38; *see also id.*, 11:37-40, Fig.3.

Maes’s Fig. 3 (reproduced below) depicts communication link L4 between the transaction terminal 80 and the financial institutions 70. The POS terminal forwards information received from the PDA to the financial institution. EX1004, 11:37-40, 13:34-38, Fig. 3; EX1003, ¶299.



EX1004, Fig. 3 (highlighted).

In MBC, Bjorn's cryptographic key (*key*) is carried in Maes's encrypted information file. *Supra*, §V.C.2, Ground 2A at [1.5.3]; EX1003, ¶300.

As explained below, MBC's processing financial institution, optionally together with central server 60, provides the *central database*. *Infra*, [8.8]; EX1003, ¶301.

A POSITA would thus have understood that in MBC, the POS device transmits, to a central database, the encrypted key and payment information. EX1004, 11:37-40, 13:34-38, Fig. 3; *supra*, §V.C.2; *infra*, [8.8]; EX1003, ¶302.

(dd) [8.8]

MBC renders [8.8] obvious. EX1003, ¶¶303-307.

In MBC, the processing financial institution provides a *central database*. EX1004, 13:34-38, Fig. 3; *supra*, §V.C.2; EX1003, ¶304. Maes explains that the institution retains information provided at enrollment and applies it to information transmitted in a transaction, stating that the institution “would posses[s] the requisite key (provided by the service provider upon enrollment) to decode (*i.e.*, decrypt) the transmitted information to verify the identity of the user.” EX1004, 13:51-55. Because the processing financial institution retains records obtained at enrollment and retrieves them to check information presented during a transaction, a POSITA would have understood that MBC’s financial institution comprises a database. EX1004, 13:51-55; EX1003, ¶304.

In MBC, the financial institution compares Bjorn’s cryptographic key (*key*) transmitted in Maes’s encrypted information file against the reference key regenerated from the user’s enrolled template. EX1004, 13:34-38, 13:51-55; *supra*, §V.C.2; EX1003, ¶305. Bjorn explains that the cryptographic key is associated with a specific user, stating that “[t]his cryptographic key is identified with the specific

fingerprint, and thus with a specific user.” EX1006, 4:28-30. Because the comparison determines whether the transmitted key matches the reference key regenerated for that user and associated with the authorized user’s payment account, a POSITA would have understood that the comparison validates the key. EX1003, ¶305.

Maes explains that the processing financial institution “would provide an authorization number for the transaction to the merchant if the consumer was verified or, on the other hand, deny the transaction and inform the merchant if the consumer is not authorized to use the selected card.” EX1004, 13:56-60. Because the processing financial institution determines whether the consumer is authorized to use the selected card, a POSITA would have understood that the institution validates the selected card information (*payment information*). EX1004, 13:56-60; EX1003, ¶306.

A POSITA would thus have understood that in MBC, the central database validates the key and the payment information. EX1004, 13:51-55, 13:56-60; *supra*, §V.C.2; EX1003, ¶307.

(ee) [9]

Supra, Ground 2A at [2]; EX1003, ¶308.

(ff) [10]

Supra, Ground 2A at [3]; EX1003, ¶309.

(gg) [11]

Supra, Ground 1A at [11]; EX1003, ¶310.

(hh) [12]

Supra, Ground 2A at [5]; EX1003, ¶311.

(ii) [13]

Supra, Ground 2A at [6]; EX1003, ¶312.

(jj) [15.pre]

Supra, Ground 2A at [1.pre]; EX1003, ¶¶313-314.

In MBC, the PDA performs the operations of [1.pre]-[6] (and corresponding operations of [15.pre]-[21]). *Supra*, Ground 2A at [1.pre]-[6]; EX1003, ¶314.

(kk) [15.1]

Supra, Ground 2A at [1.2]; EX1003, ¶315.

(ll) [15.2]

Supra, Ground 2A at [1.3]; EX1003, ¶¶316-317.

Maes's biometric sensor 40 provides a **biometric reader**, for the reasons discussed at [1.3] (describing the **biometric module**). *Supra*, Ground 2A at [1.3]; EX1003, ¶317.

(mm) [15.3]

Supra, Ground 2A at [1.4]; EX1003, ¶318.

(nn) [15.4]

Supra, Ground 2A at [1.5.2]; EX1003, ¶319.

(oo) [15.5]

Supra, Ground 2A at [1.5.3]; EX1003, ¶320.

(pp) [15.6]

Supra, Ground 2A at [1.5.4]; EX1003, ¶321.

(qq) [15.7]

Supra, Ground 2A at [1.5.5]; EX1003, ¶322.

(rr) [16]

Supra, Ground 2A at [2]; EX1003, ¶323.

(ss) [17]

Supra, Ground 2A at [3]; EX1003, ¶324.

(tt) [18]

Supra, Ground 2A at [4]; EX1003, ¶325.

(uu) [19]

Supra, Ground 2A at [5]; EX1003, ¶326.

(vv) [20]

Supra, Ground 2A at [6]; EX1003, ¶327.

(ww) [21]

Supra, Ground 2A at [1.5.5]; EX1003, ¶¶328-329.

As explained at [1.5.5], in MBC, the PDA transmits the selected card information (*payment information*) to the POS terminal over the RF link (*short range RF circuitry*). *Supra*, Ground 2A at [1.5.5], [1.1]; EX1003, ¶329.

D. Ground 2B: Maes-Bjorn-Shults Renders Obvious Claims 7 and 14

1. The Maes-Bjorn-Shults Combination (MBSC)

The Maes-Bjorn-Shults Combination (MBSC) is MBC (Ground 2A), further modified in view of Shults's teachings such that Maes's PDA's RF circuitry is implemented using an RFID device. *Supra*, §V.C.2; EX1008, [0030]; EX1003, ¶¶126-127. For the reasons described in §V.B.2, which relate only to Maes and Shults, a POSITA would have been motivated to add Shults's RFID circuit to Maes's PDA and would have reasonably expected success. *Supra*, §V.B.2; EX1003, ¶¶126-127.

MBSC's PDA device 10 otherwise operates as in MBC, including transmitting the encrypted key and payment information to the POS device via the short range RF circuitry. *Supra*, §V.C.2, Ground 2A at [1.5.5]; EX1003, ¶¶126-127.

2. Claim Element Analysis

(a) [7]

Ground 1B's analysis of [7] relies only on Maes and Shults, both of which are in MBSC. *Supra*, Ground 1B at [7]; §V.D.1. EX1003, ¶¶330-331.

Accordingly, MBSC renders [7] obvious for analogous reasons. *Supra*, Ground 1B at [7]; EX1003, ¶331.

(b) [14]

Supra, Ground 2B at [7]. EX1003, ¶332.

E. Ground 3A: Maes-Walker Renders Obvious Claims 1-6 and 15-21

1. Walker (EX1007)

Walker discloses a portable smart card device for generating transaction-specific, single-use credit card numbers to enhance security in credit card transactions. EX1007, Abstract, 1:6-10, 5:49-60, 6:61-7:3, 7:37-45, 8:9-36, 10:10-21, Figs. 1, 8; EX1003, ¶109.

2. The Maes-Walker Combination

The Maes-Walker Combination ("MWC") implements Maes's biometrically verified RF-based transactions with a single-use credit card number as taught in Walker. EX1003, ¶¶110-113. A POSITA would have been motivated to incorporate generation and use of Walker's single-use credit card numbers into Maes's RF-based

system because (1) Maes expressly seeks to protect against unauthorized card use yet still transmits static card information in the clear over an RF link, leaving it vulnerable to interception and (2) Walker's single-use number directly solves this vulnerability by preventing reuse or replay of intercepted data, reflecting the predictable application of a known technique to improve a similar device in the same way, with a predictable benefit. A POSITA would have reasonably expected success given that the underlying cryptographic techniques were well known before the critical date. EX1004, 2:1-5, 6:24-29, 12:19-34; EX1007, 2:55-64, 3:59-64, 6:30-38, 6:61-7:3, 7:36-45, 10:10-21; EX1003, ¶¶110-113.

3. Claim Element Analysis

(a) [1.pre]

Supra, Ground 1A at [1.pre]; EX1003, ¶333.

(b) [1.1]

Supra, Ground 1A at [1.1]; EX1003, ¶334.

(c) [1.2]

Supra, Ground 1A at [1.2]; EX1003, ¶335. Walker further discloses **payment information** in the form of a credit card account number A stored in memory of a user device. EX1007, 1:20-21, 6:54-59, 6:66-7:1, 8:19-20, Fig. 8 (step 803); *see also id.*, 7:49-61, Fig. 1.

(d) [1.3]

Supra, Ground 1A at [1.3]; EX1003, ¶336.

(e) [1.4]

Supra, Ground 1A at [1.4]; EX1003, ¶337.

(f) [1.5.1]

Supra, Ground 1A at [1.5.1]; EX1003, ¶338.

(g) [1.5.2]

MWC renders [1.5.2] obvious. EX1003, ¶¶339-344.

In MWC, Maes's PDA generates and transmits, upon successful biometric verification, a Walker-based single-use credit card number, formed by encrypting a nonce N with a private key K and initialization variable IV, and concatenating the resulting encrypted nonce C with the IV and account number A (***payment information***), such that the encrypted nonce C (or, alternatively, the entire single-use number including C) provides a "***key***" that the financial institution uses to authorize or deny the transaction. EX1004, 9:52-10:5, 10:49-56, 11:15-19, 12:20-27, 12:40-52, 12:65-67; EX1007, 5:58-61, 6:15-27, 6:56-7:20, 8:9-19, 8:41-9:10, 11:46-52, Figs. 3B, 7, 8, 9A-9B; EX1003, ¶¶340-343; EX1002, 33, 37. Walker's single-use number directly embeds the user's credit card account number A. *Id.*

MWC's ***secure module*** generates the encrypted nonce (***key***) for a single-use credit card number (alternate mapping of ***key***) when the ***biometric information*** read

by the *biometric reading device* (e.g., biometric sensor 40) is determined by the *authentication module* (e.g., biometric processor module 22) to correspond to the *biometric authentication information* (e.g., voice or fingerprint data) stored in *memory* (e.g., memory 14). EX1003, ¶344.

(h) [1.5.3]

MWC renders [1.5.3] obvious. EX1003, ¶¶345-347.

Per Walker, and as discussed above for [1.5.2], MWC's *secure module* encrypts the nonce, thereby forming an *encrypted key*. EX1007, 8:9-19, 9:10-20, Figs. 7-8; *supra*, Ground 3A at [1.5.2].

Additionally, it was well known before the Critical Date to encrypt data transmitted in a transaction request to protect against unauthorized third-parties who have access to the transmission medium (e.g., an RF link), and a POSITA would have been motivated to further encrypt the entire single-use number (alternate mapping of *key*) in MWC (including the encrypted nonce) to prevent even the single-use number from being divulged to an unauthorized party. EX1004, 13:19-38 (Maes disclosing option for encrypting unique identifying information transmitted over RF in transaction request); EX1003, ¶347 (citing corroboration EX1005, 5:67-6:4).

(i) [1.5.4]

Supra, Ground 1A at [1.5.4]; EX1003, ¶348.

(j) [1.5.5]

MWC renders [1.5.5] obvious. EX1003, ¶¶349-350.

As discussed above in §V.E.2 and in connection with [1.5.2]-[1.5.3], MWC's *secure module* generates and transmits to a POS terminal, in response to biometric authentication of the user, a single-use card number (*key*) generated in accordance with Walker's teachings, where the single-use card number includes an encrypted nonce C (alternate mapping of *key*) and an account number A for the selected credit card (*secured payment information*). EX1004, 12:5-29 ("transmitting the selected card information directly from the PDA device to the ... POS transaction terminal" via RF), 13:34-38; EX1007, 7-3:8 ("single-use credit card number is transmitted to a merchant"), 8:31-36, 8:19-25; *supra*, Ground 3A at [1.5.2]-[1.5.3]; §V.E.2; EX1003, ¶350. Walker's nonce is encrypted in the single-use number, and further it would have been obvious to encrypt the entire transmitted single-use number as discussed above. *Supra*, [1.5.3]; EX1003, ¶350.

(k) [2]

Supra, Ground 1A at [2]; EX1003, ¶351.

(l) [3]

Supra, Ground 1A at [3]; EX1003, ¶352.

(m) [4]

Supra, Ground 1A at [4]; EX1003, ¶353.

(n) [5]

Supra, Ground 1A at [5]; EX1003, ¶354.

(o) [6]

Supra, Ground 1A at [6]; EX1003, ¶355.

(p) [15.pre]

Supra, Ground 3A at [1.pre]; EX1003, ¶¶356-357.

In MWC, the PDA performs the operations of [1.pre]-[6] (and corresponding operations of [15.pre]-[21]). *Supra*, Ground 3A at [1.pre]-[6]; EX1003, ¶357.

(q) [15.1]

Supra, Ground 3A at [1.2]; EX1003, ¶358.

(r) [15.2]

Supra, Ground 3A at [1.3]; EX1003, ¶¶359-360.

Maes's biometric sensor 40 provides a **biometric reader**, for the reasons discussed at [1.3] (describing the **biometric module**). *Supra*, Ground 3A at [1.3]; EX1003, ¶360.

(s) [15.3]

Supra, Ground 3A at [1.4]; EX1003, ¶361.

(t) [15.4]

Supra, Ground 3A at [1.5.2]; EX1003, ¶362.

(u) [15.5]

Supra, Ground 3A at [1.5.3]; EX1003, ¶363.

(v) [15.6]

Supra, Ground 3A at [1.5.4]; EX1003, ¶364.

(w) [15.7]

Supra, Ground 3A at [1.5.5]; EX1003, ¶365.

(x) [16]

Supra, Ground 3A at [2]; EX1003, ¶366.

(y) [17]

Supra, Ground 3A at [3]; EX1003, ¶367.

(z) [18]

Supra, Ground 3A at [4]; EX1003, ¶368.

(aa) [19]

Supra, Ground 3A at [5]; EX1003, ¶369.

(bb) [20]

Supra, Ground 3A at [6]; EX1003, ¶370.

(cc) [21]

Supra, Ground 3A at [1.5.5]; EX1003, ¶¶371-372.

As explained at [1.5.5], in MWC, the PDA transmits the single-use number including the encrypted nonce and payment information using *short range RF circuitry*. *Supra*, Ground 3A at [1.5.5], [1.1]; EX1003, ¶372.

F. Ground 3B: Maes-Walker-Shults Renders Obvious Claim 7

1. The Maes-Walker-Shults Combination (MWSC)

The Maes-Walker-Shults Combination (MWSC) is MWC (Ground 3A), further modified in view of Shults's teachings such that Maes's PDA's RF circuitry is implemented using an RFID device. *Supra*, §V.C.2; EX1008, [0030]; EX1003, ¶¶128-129. For the reasons described in §V.B.2, which relate only to Maes and Shults, a POSITA would have been motivated to add Shults's RFID circuit to Maes's PDA and would have reasonably expected success. *Supra*, §V.B.2; EX1003, ¶¶128-129.

MWSC's PDA device 10 otherwise operates as in MWC, including transmitting the encrypted key and payment information to the POS device via the short range RF circuitry. *Supra*, §V.E.2, Ground 3A at [1.5.5]; EX1003, ¶¶128-129.

2. Claim Element Analysis

(a) [7]

Ground 1B's analysis of [7] relies only on Maes and Shults, both of which are in MWSC. *Supra*, Ground 1B at [7]; §V.E.1. EX1003, ¶¶373-374.

Accordingly, MWSC renders [7] obvious for analogous reasons. *Supra*, Ground 1B at [7]; EX1003, ¶374.

VI. PAYMENT OF FEES—37 C.F.R. §42.103

Petitioners authorize the Patent and Trademark Office to charge any fees to Deposit Account No. 06-1050.

VII. MANDATORY NOTICES—37 C.F.R. § 42.8(a)(1)

A. Real Party-In-Interest—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—37 C.F.R. § 42.8(b)(2)

Petitioners are not aware of any disclaimers, reexamination certificates or petitions for inter partes review for the '187 Patent. The '187 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).

C. Lead And Back-Up Counsel—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: IPR50095-0313IP1@fr.com	Nicholas Stephens, Reg. No. 74,320 Andrew B. Patrick, Reg. No. 63,471 Jeremy J. Monaldo, Reg. No. 58,680 Craig A. Deutsch, Reg. No. 69,264 Usman A. Khan, Reg. No. 70,439 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 IPR50095-0313IP1@fr.com

D. Service Information

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

Petitioners consent to electronic service by email at IPR50095-0313IP1@fr.com.

Respectfully submitted,

Dated: September 18, 2026

/W. Karl Renner/

W. Karl Renner, Reg. No. 41,265
Nicholas Stephens, Reg. No. 74,320
Andrew B. Patrick, Reg. No. 63,471
Jeremy J. Monaldo, Reg. No. 58,680
Craig A. Deutsch, Reg. No. 69,264
Usman A. Khan, Reg. No. 70,439
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2026-00504)

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 13,993 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
Nicholas Stephens, Reg. No. 74,320
Andrew B. Patrick, Reg. No. 63,471
Jeremy J. Monaldo, Reg. No. 58,680
Craig A. Deutsch, Reg. No. 69,264
Usman A. Khan, Reg. No. 70,439
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, Power of Attorney, and all supporting exhibits were provided via 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 92101
(619) 238-1900

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