

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Guy Fielder
U.S. Patent No.: 10,044,689 Attorney Docket No.: 38093-0012IP1
Issue Date: August 7, 2018
Appl. Serial No.: 15/839,144
Filing Date: December 12, 2017
Title: SYSTEM AND METHOD FOR AUTHENTICATING USERS

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. 10,044,689 PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42**

TABLE OF CONTENTS

I.	REQUIREMENTS	1
	A. Grounds for Standing.....	1
	B. Challenge and Relief Requested.....	1
	C. Claim Construction	3
II.	THE '689 PATENT	3
	A. Specification	3
	B. Prosecution History.....	4
	C. POSITA.....	4
III.	THE CHALLENGED CLAIMS ARE UNPATENTABLE	4
	A. GROUND 1A – Immega-Day Renders Claims 1-4 and 6-8 Obvious	5
	1. Prior Art and Proposed Combination.....	5
	(a) Immega.....	5
	(b) Day	10
	(c) Immega-Day.....	12
	2. Claim 1	17
	3. Claim 2	26
	4. Claim 3	27
	5. Claim 4	27
	6. Claim 6	28
	7. Claim 7	29
	8. Claim 8	29
	B. GROUND 1B – Immega-Day-Tomko Renders Claims 5 and 9-21 Obvious.....	31
	1. Prior Art and Proposed Combination.....	31
	(a) Tomko.....	31
	(b) Immega-Day-Tomko.....	33
	i. Device Components.....	33
	ii. Data Encryption.....	36
	2. Claim 5	40
	3. Claim 9	40
	4. Claim 10	43
	5. Claim 11	43
	6. Claim 12	43
	7. Claim 13	43

8.	Claim 14	43
9.	Claim 15	43
10.	Claim 16	43
11.	Claim 17	45
12.	Claim 18	45
13.	Claim 19	45
14.	Claim 20	45
15.	Claim 21	46
C.	GROUND 2A – Mardikar-318 and Chhabra Render Claims 1-4 and 6-7	
	Obvious	46
1.	Prior Art and Proposed Combination.....	46
	(a) Mardikar-318.....	46
	(b) Chhabra.....	48
	(c) Mardikar-Chhabra	52
2.	Claim 1	55
3.	Claim 2	71
4.	Claim 3	72
5.	Claim 4	73
6.	Claim 6	74
7.	Claim 7	74
D.	GROUND 2B – Mardikar-318, Chhabra, and Duffy Render Claims 1-21	
	Obvious	75
1.	Prior Art and Proposed Combination.....	75
	(a) Duffy	75
	(b) Mardikar-Chhabra-Duffy	76
2.	Claim 1	77
3.	Claim 2	78
4.	Claim 3	79
5.	Claim 5	80
6.	Claim 8	80
7.	Claim 9	82
8.	Claim 10	85
9.	Claim 11	85
10.	Claim 12	85
11.	Claim 13	85
12.	Claim 14	86
13.	Claim 15	86
14.	Claim 16	86

15.	Claim 17	88
16.	Claim 18	88
17.	Claim 19	88
18.	Claim 20	88
19.	Claim 21	88
IV.	314(a)	88
V.	CONCLUSION AND PAYMENT OF FEES	92
VI.	MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1)	92
A.	Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)	92
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2)	93
C.	Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)	93
D.	Service Information	94

EXHIBITS

USAA-1001	U.S. Patent No. 10,044,689 to Fielder (“the ’689 Patent”)
USAA-1002	Excerpts from the Prosecution History of the ’689 Patent (“the Prosecution History”)
USAA-1003	Declaration and Curriculum Vitae of Dr. Seth James Nielson
USAA-1004	U.S. Patent App. Pub. No. 2003/0140235 to Immega et al. (“Immega”)
USAA-1005	U.S. Patent No. 6,002,770 to Tomko et al. (“Tomko”)
USAA-1006	U.S. Patent App. Pub. No. 2007/0061567 to Day et al. (“Day”)
USAA-1007	[RESERVED]
USAA-1008	U.S. Patent No. 5,748,744 to Levy et al. (“Levy”)
USAA-1009	[RESERVED]
USAA-1010	U.S. Patent No. 8,108,318 to Mardikar (“Mardikar-318”)
USAA-1011	U.S. Patent App. Pub. No. 2009/0307140 to Mardikar (“Mardikar-140”)
USAA-1012	U.S. Patent App. Pub. No. 2009/0305673 to Mardikar (“Mardikar-673”)
USAA-1013	U.S. Patent No. 8,234,697 to Chhabra (“Chhabra”)
USAA-1014	U.S. Patent App. Pub. No. 2004/0111625 to Duffy et. al. (“Duffy”)
USAA-1015	U.S. Patent App. Pub. No. 2008/0098225 to Baysinger (“Baysinger”)

- USAA-1016 John Viega, Matt Messier, and Pravir Chandra, *Network Security with OpenSSL: Cryptography for Secure Communications* (1st ed. 2002)(“Viega”).
- USAA-1017 Niels Ferguson and Bruce Schneier, *Practical Cryptography* (1st ed. 2003) (“Ferguson”)
- USAA-1018 RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2 (August 2008), available at: [RFC 5246 - The Transport Layer Security \(TLS\) Protocol Version 1.2](#)
- USAA-1019 ITU-T Recommendation X.509 (August 2005)
- USAA-1020 Complaint, *PACid Technologies, LLC v. USAA Federal Savings Bank*, Case No. 1:24-cv-321 (W.D. Tex. Mar. 27, 2024)
- USAA-1021 [RESERVED]
- USAA-1022 Combined Civil and Criminal Federal Court Management Statistics (Dec. 31, 2024) | United States Courts (uscourts.gov), available at: https://www.uscourts.gov/sites/default/files/2025-02/fcms_na_distprofile1231.2024.pdf
- USAA-1023 (Excerpts) Gordon Padwick, “Special Edition Using Microsoft Outlook 2000,” Que, First printing May 1999, Library of Congress Catalog Card Number 98-87795 (“Padwick”).
- USAA-1024 [RESERVED]
- USAA-1025 [RESERVED]
- USAA-1026 [RESERVED]
- USAA-1027 Declaration of June Ann Munford (Viega, Ferguson, Padwick)
- USAA-1028 U.S. Patent App. Pub. No. 2003/0005336 to Poo, et al. (“Poo”)

- USAA-1029 U.S. Patent App. Pub. No. 2007/0136604 to Kuhlman, et al
("Kuhlman")
- USAA-1030 U.S. Patent App. Pub. No. 2005/0081040 to Johnson, et al.
("Johnson")
- USAA-1031 (Excerpts) Vir V. Phoha, "Internet Security Dictionary,"
Springer, 2002, ISBN 0-387-95261-6 ("Phoha").
- USAA-1032 U.S. Patent App. Pub. No. 2008/122796 to Jobs, et al. ("Jobs")
- USAA-1033 U.S. Patent App. Pub. No. 2002/0099952 to Lambert, et al.
("Lambert")
- USAA-1034 U.S. Patent App. Pub. No. 2006/0258368 to Granito, et al.
("Granito")
- USAA-1035 U.S. Patent App. Pub. No. 2005/0246469 to Chu ("Chu")
- USAA-1036 Knaggs, P. and Welsh, S., 2004. ARM: Assembly Language
Programming. Bournemouth University, School of Design,
Engineering, and Computing ("Knaggs")
- USAA-1037 U.S. Patent App. Pub. No. 2002/0010819 to Dye ("Dye")

LISTING OF CLAIMS

Claim 1	
[1.pre]	A method, comprising:
[1.a.i]	by an application running on a mobile device, and via a user interface associated with said application, communicating with a user to receive a unique user input, generating, by said application, a secret based upon said unique user input, and
[1.a.ii]	storing said secret at said mobile device, said secret being stored with an identifier
[1.a.iii]	so as to be retrievable when the unique user input is again received at the mobile device;
[1.b]	receiving at the mobile device from a remote computing device a first communication, and providing the user, via the mobile device, an opportunity to respond to the first communication;
[1.c.i]	in response to the providing, authenticating the user at the mobile device by receiving a candidate user input; and
[1.c.ii]	said mobile device verifying said user to the remote computing device in a second communication encoded using said secret.
Claim 2	
[2]	The method of claim 1, wherein the secret comprises an encryption key.
Claim 3	
[3]	The method of claim 1, wherein the secret comprises a static portion and a dynamic portion.
Claim 4	
[4]	The method of claim 1, wherein the first communication comprises a request for user credentials of the user of the mobile device.

Claim 5	
[5]	The method of claim 1, wherein the secret is stored in an encrypted format.
Claim 6	
[6]	The method of claim 1, wherein the unique user input comprises user credentials.
Claim 7	
[7]	The method of claim 1, wherein the first and second communications comprise two related communications of a communication session.
Claim 8	
[8]	The method of claim 1, further comprising generating a candidate identifier using the received candidate user input, and recovering the secret from said mobile device if the candidate identifier matches the identifier.
Claim 9	
[9.pre]	A mobile device, comprising
[9.a]	a processor, a storage device, and a memory, said memory storing processor-executable instructions, which instructions, when executed by said processor, cause said processor to perform steps comprising:
[9.b]	configuring an application running on said mobile device for communication with at least one remote computer-based station, said configuring including communicating with a user via a user interface to receive a unique user input,
[9.c.i]	upon receipt of said unique user input, generating a secret,
[9.c.ii]	storing said secret in said storage device, said secret being stored with an identifier
[9.c.iii]	so as to be retrievable when the unique user input is again received;

[9.d]	upon receipt at the mobile device of a first communication from said remote computer-based station, providing the user, via the mobile device, an opportunity to respond to the first communication;
[9.e.i]	authenticating the user by receiving, in response to the providing, a proffered user input, generating a candidate identifier using the proffered user input received, and
[9.e.ii]	recovering the secret from said storage device if the candidate identifier matches the identifier; and
[9.f]	verifying said user to the remote computing device in a second communication encoded using said secret.
Claim 10	
[10]	The mobile device of claim 9, wherein the secret comprises an encryption key.
Claim 11	
[11]	The mobile device of claim 9, wherein the secret comprises a static portion and a dynamic portion.
Claim 12	
[12]	The mobile device of claim 9, wherein the first communication comprises a request for user credentials of the user of the mobile device.
Claim 13	
[13]	The mobile device of claim 9, wherein the secret is stored in an encrypted format.
Claim 14	
[14]	The mobile device of claim 9, wherein the proffered user input comprises user credentials.
Claim 15	

[15]	The mobile device of claim 9, wherein the first and second communications comprise two related communications of a communication session.
Claim 16	
[16.pre]	A non-transitory computer-readable medium having stored thereon processor-executable instructions, which instructions, when executed by a processor, cause said processor to perform steps comprising:
[16.a]	configuring an application running on a processor-based platform on which said instructions are executed for communication with at least one remote computer-based station, said configuring including receiving a unique user input,
[16.b.i]	upon receipt of said unique user input, generating a secret,
[16.b.ii]	storing said secret in a memory of said processor-based platform, said secret being stored with an identifier
[16.b.iii]	so as to be retrievable when the unique user input is again received;
[16.c]	upon receipt at the processor-based platform of a first communication from said remote computer-based station, providing the user, via the mobile device, an opportunity to respond to the first communication;
[16.d.i]	authenticating the user by receiving, in response to the providing, a proffered user input, generating a candidate identifier using the proffered user input, and
[16.d.ii]	recovering the secret from said memory if the candidate identifier matches the identifier; and
[16.e]	verifying said user to the remote computing device in a second communication encoded using said secret.
Claim 17	
[17]	The non-transitory computer-readable medium of claim 16, wherein the secret comprises an encryption key.
Claim 18	

[18]	The non-transitory computer-readable medium of claim 16, wherein the secret comprises a static portion and a dynamic portion.
Claim 19	
[19]	The non-transitory computer-readable medium of claim 16, wherein the first communication comprises a request for user credentials of a user of the processor-based platform.
Claim 20	
[20]	The non-transitory computer-readable medium of claim 16, wherein the secret is stored in an encrypted format.
Claim 21	
[21]	The non-transitory computer-readable medium of claim 16, wherein the proffered user input comprises user credentials.

USAA Federal Savings Bank (“Petitioner” or “USAA”) petitions for Inter Partes Review (“IPR”) under 35 U.S.C. §§ 311–319 and 37 C.F.R. § 42 of claims 1-21 (“the Challenged Claims”) of U.S. Patent No. 10,044,689 (“the ’689 Patent”). As explained herein, at least a reasonable likelihood exists that USAA will prevail with respect to at least one of the Challenged Claims, which are unpatentable based on prior art teachings described herein. Accordingly, USAA respectfully submits that the Board should institute IPR and the Challenged Claims should be canceled as unpatentable.

I. REQUIREMENTS

A. Grounds for Standing

USAA certifies that the ’689 Patent is available for IPR. USAA files this petition within one year of service of a 3/27/24 complaint against USAA in *PACid Technologies, LLC v. USAA Federal Savings Bank*, Case No. 1:24-cv-321 (WDTX). USAA-1020. USAA is not barred or estopped from requesting an IPR challenging the Challenged Claims on the below-identified grounds.

B. Challenge and Relief Requested

USAA requests IPR and cancellation of the Challenged Claims on the grounds below. The declaration of Dr. Nielson (USAA-1003) is furnished herewith.

Ground	Claims	Basis
1A	1-4, 6-8	Immega-Day
1B	5, 9-21	Immega-Day-Tomko
2A	1-4, 6-7	Mardikar-Chhabra
2B	1-21	Mardikar-Chhabra-Duffy

The '689 Patent was filed 12/12/2017 and claims priority, via several applications, to a provisional application filed 3/25/2009 (“Critical Date”). USAA does not concede that the Challenged Claims are entitled to the claimed priority, but applies prior art before that date. Applied references are prior art as below:

Reference	Date(s)	Basis
Immega (USAA-1004)	12/2/2002 (filed), 6/24/2003 (published)	Pre-AIA §102(a),(b),(e)
Day (USAA-1006)	9/10/2006 (filed), 3/15/2007 (published)	Pre-AIA §102(a),(b),(e)
Tomko (USAA-1005)	9/15/1997 (filed), 12/14/1999 (published)	Pre-AIA §102(a),(b),(e)
Mardikar-318 (USAA-1010)	12/19/2008 (filed)	Pre-AIA §102(e)
Mardikar-140 (USAA-1011)	10/10/2008 (filed)	Pre-AIA §102(e)
Mardikar-673 (USAA-1012)	12/22/2008 (filed)	Pre-AIA §102(e)
Chhabra (USAA-1013)	3/31/2008 (filed)	Pre-AIA §102(e)

Reference	Date(s)	Basis
Duffy (USAA-1014)	6/10/2004 (published)	Pre-AIA §102(b)

C. Claim Construction

All claim terms should be construed according to the Phillips standard.

Phillips v. AWH Corp., 415 F. 3d 1303 (Fed. Cir. 2005); 37 C.F.R. §42.100.

USAA submits that no claim terms need be construed to resolve issues of controversy in the present Petition, but reserves the right to respond to construction issues PACid raises. *See Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011).

For example, USAA notes that the recited term “secret” is used in the ’689 Patent consistent with its plain and ordinary meaning. USAA-1003, ¶51; USAA-1001, 9:53-55, 10:21-23, 27:35-63; USAA-1004, [0034], USAA-1017, 136, 347-362; USAA-1010, 7:28-42; USAA-1031, 3.

II. THE ’689 PATENT

A. Specification

The ’689 Patent is directed to “authenticating users” through verification of unique user inputs (e.g., user credentials). USAA-1001, Abstract. A security application on a computing device allows “generation of a secret,” “prompts, e.g., via a user interface of the device, entry of the unique user input” in response to “receiving an identifier associated with the secret,” “verifies the unique user

inputs,” and “provides the secret for use in encoding a communication with a remote computer-based station.” *Id.*, Abstract.

However, the claimed subject matter was conventional by the Critical Date. USAA-1003, ¶49.

B. Prosecution History

During prosecution, the examiner allowed the claims without a prior art rejection and did not consider any of the art applied in this Petition. USAA-1003, ¶50.

C. POSITA

A person of ordinary skill in the art relating to the subject matter of the '689 Patent (“POSITA”) would have had a working knowledge of cryptography and related security techniques. The person would have had a bachelor’s degree in an academic discipline emphasizing the design of computer or software technologies, in combination with training or at least one to two years of related work experience with securing and processing of data or information, including but not limited to cryptography. USAA-1003, ¶24. Alternatively, the person could have had a Master of Science degree in a relevant academic discipline with less than a year of related work experience in the same discipline. *Id.*

III. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. GROUND 1A – Immega-Day Renders Claims 1-4 and 6-8 Obvious

1. Prior Art and Proposed Combination

(a) *Immega*

Immega is directed to a “method for permitting the secure transmission of electronic messages by using biometric certification,” where the messages include email. USAA-1004, Abstract, [0006]; USAA-1003, ¶52. For the method, Immega describes at least two users, the “sender” and the “receiver” (though both the sender and the receiver both send and receive messages) and their respective “computers,” which may be a cellular telephone or personal digital assistant. *Id.*, [0041]-[0044], [0050]-[0067].

Sender and receiver “cross-enroll biometric feature sets” using devices with “fingerprint sensor[s],” allowing “confirmation of identity of both parties at both ends of a message exchange” and “user-specific encryption of messages.” USAA-1004, [0008]. The method further employs a “difference key,” generated by subtracting a live-scan fingerprint feature set (“LFFS”) of a user from that user’s modified enrolled fingerprint feature set (modified “EFFS” or “MEFFS”), to encrypt electronic messages and other fingerprint data. *Id.*, Abstract, [0009]-[0011]; USAA-1003, ¶53.

Immega describes an algorithm for generating MEFFSs for a user, with reference to FIG. 3A (below). USAA-1004, [0044]. First, “the centroid of the

fingerprint is determined,” then a “random number is used to generate a displacement vector,” which is used “to slightly shift or displace all features of the [EFFS] by a random displacement vector.” *Id.* This MEFFS “is then assigned to a specific person with whom messages will be exchanged.” *Id.*; USAA-1003, ¶54.

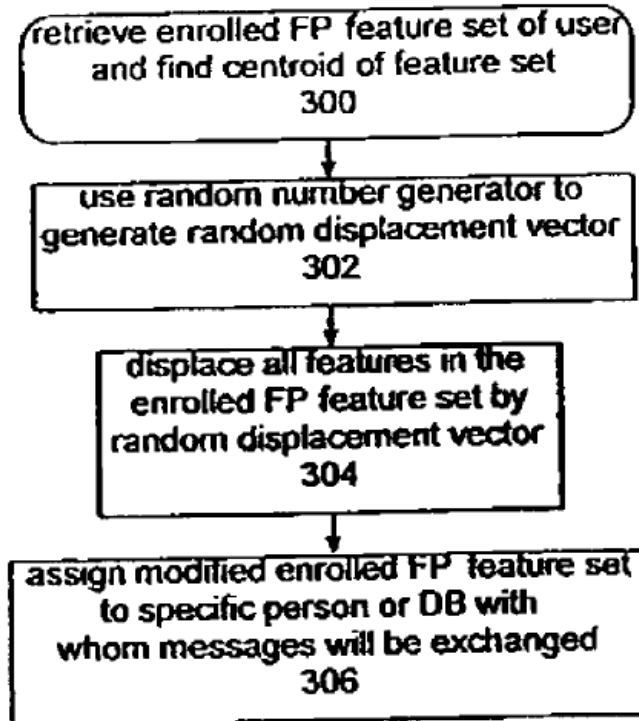
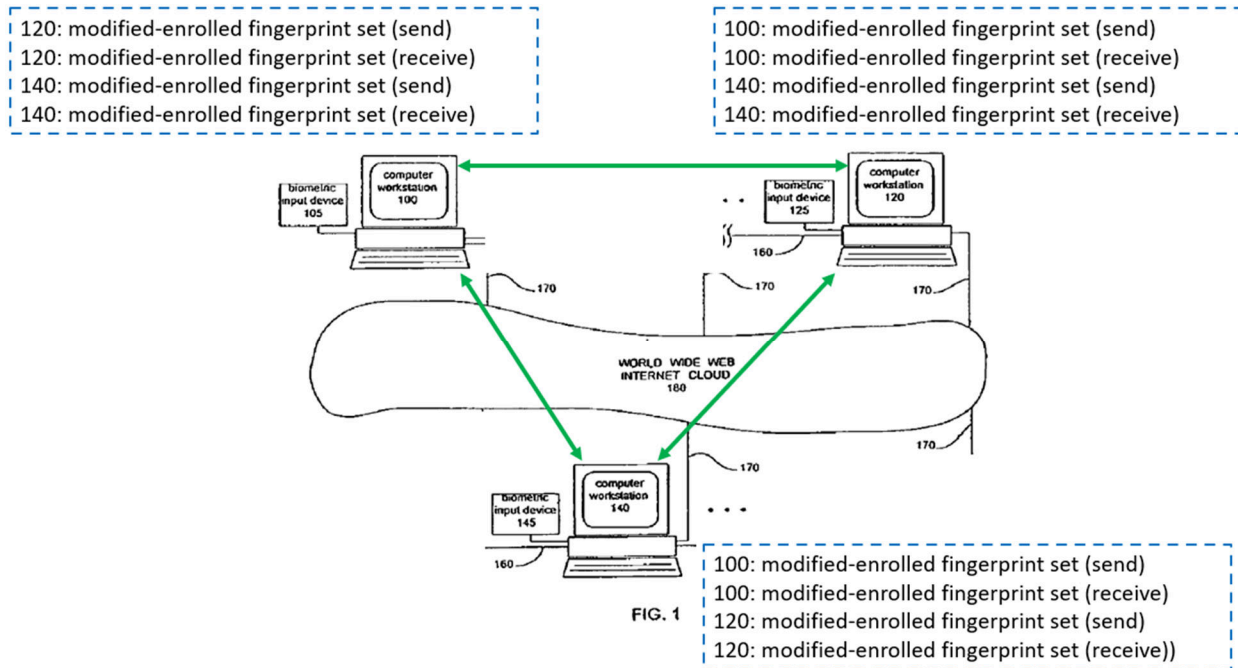


FIG. 3A

USAA-1004, FIG. 3A

“Many uniquely modified [EFFSs], one (or more) for each person with whom messages will be exchanged, may be created and securely stored.” USAA-1004, [0044]. “[B]oth the sender and the receiver [are required] to cross-enroll biometric feature sets” on “each other’s computer.” USAA-1004, [0008]. Therefore, through cross-enrollment, a device stores, for each communication

partner, the MEFFS for sending encrypted communications to a particular partner, and the MEFFS created by the particular partner and used by the device to decrypt communications received from the partner, illustrated below. USAA-1003, ¶¶55-56.



USAA-1004, FIG. 1(excerpt, annotated). USAA-1003, ¶56.

After users' MEFFSs are cross-enrolled, users can share "biometrically certified message[s]," discussed with respect to FIG. 6 (below). USAA-1004, [0063]. FIG. 6's algorithm describes how the sender and receiver confirm their identities by twice sending their respective encrypted LFFS, which the recipient uses to compare against the stored MEFFS that was exchanged during cross-enrollment. USAA-1004, [0063]-[0065]. During this process, the receiver generates the receiver's "difference key" "by subtracting the receiver's first

[LFFS] from the receiver's [MEFFS]" (612) and the sender similarly generates the receiver's "difference key" "by subtracting the first [LFFS] of the receiver from the stored [MEFFS] of the receiver" (620); the sender does the same. USAA-1004, [0064]-[0065]; USAA-1003, ¶57.

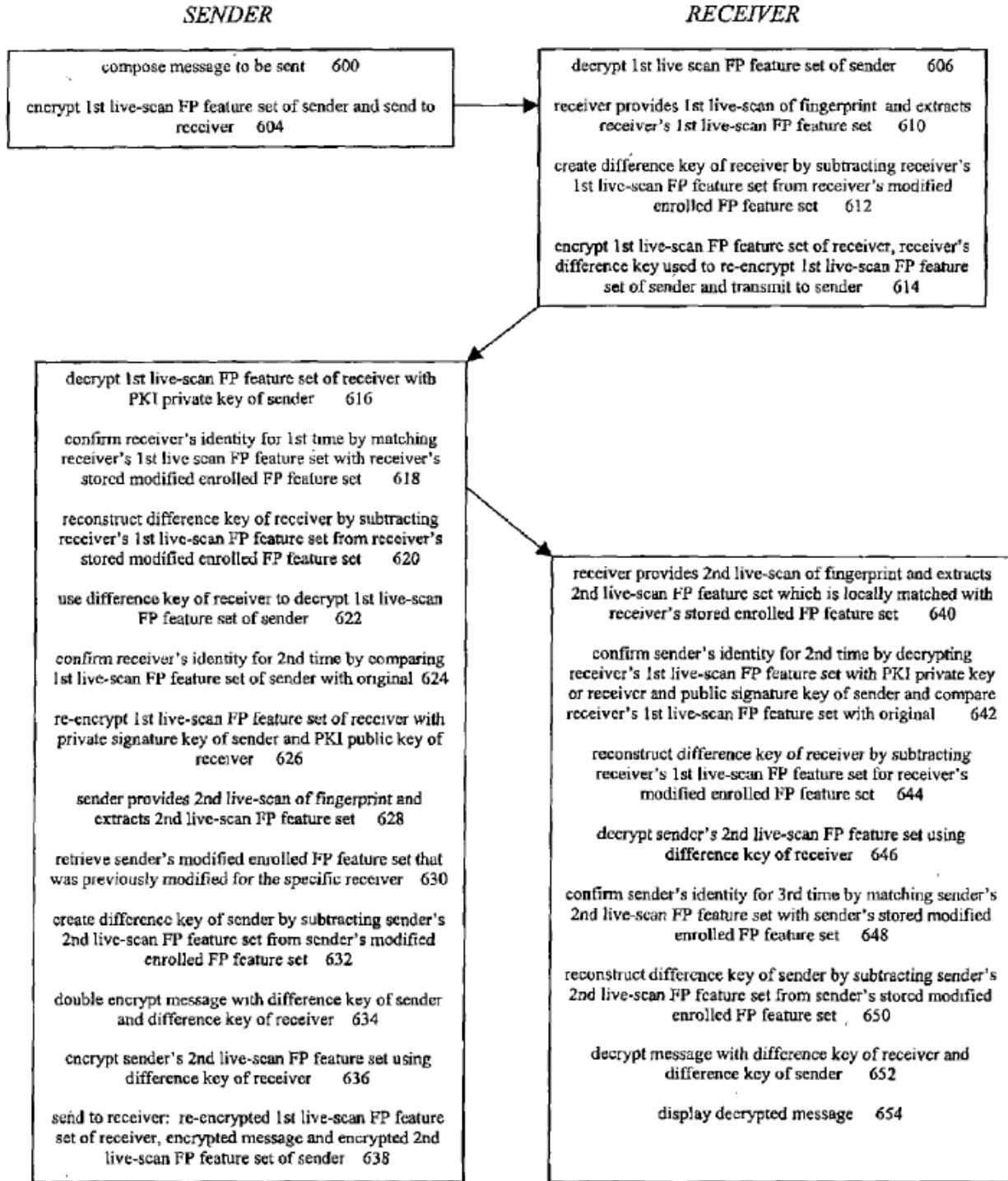


FIG. 6

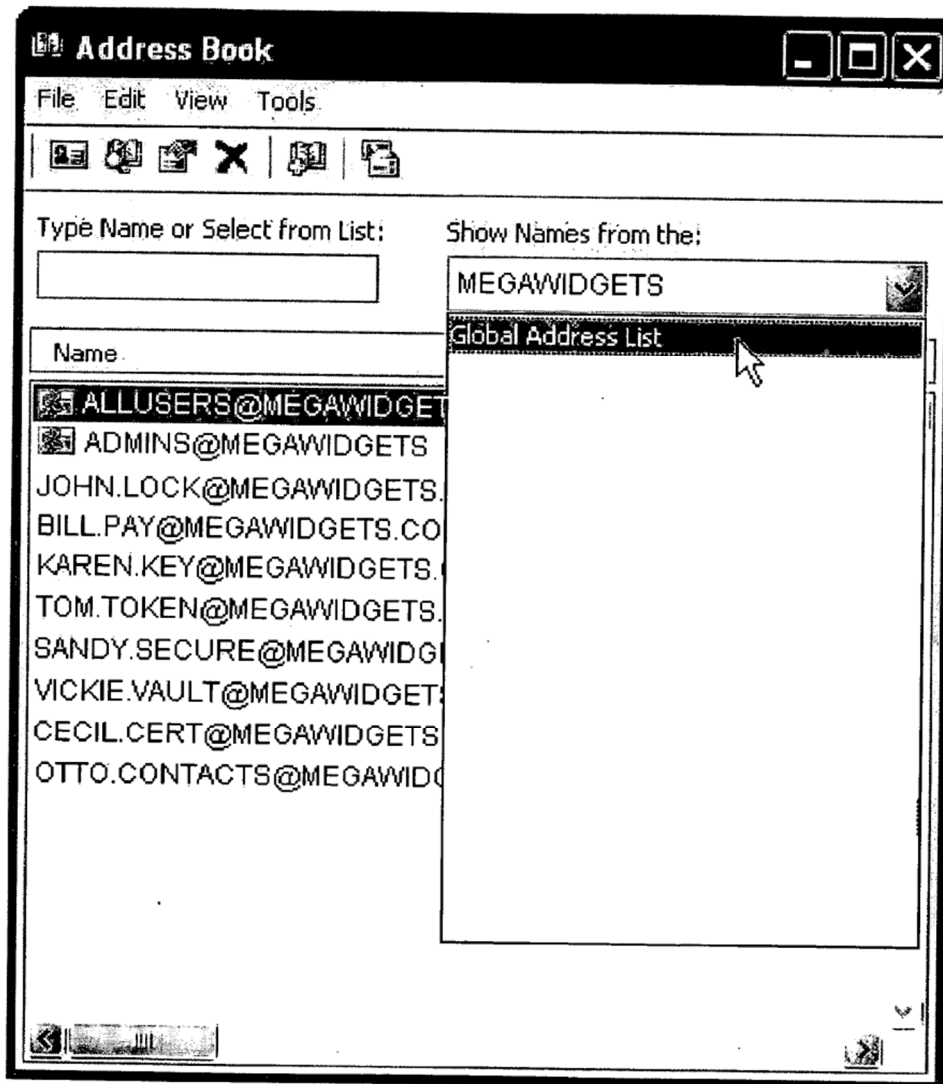
USAA-1004, FIG. 6

“When the receiver receives [the] transmission, the receiver provides a second live-scan fingerprint (step 638) and extracts a second [LFFS], which is then matched against the stored fingerprint feature set of the receiver (the receiver must prove his/her identity for decryption to continue) (step 640),” and the receiver generates the sender’s “difference key” “by subtracting the sender’s second [LFFS] from the sender’s stored [MEFFS] (step 650).” USAA-1004, [0066]. Immega additionally describes “an optional algorithmic subroutine that gives the sender direct confirmation that the correct person has received the message,” whereby the “receiver’s second [LFFS] (generated at step 640) is encrypted ... and transmitted to the sender (after step 654)” for the sender to compare with the MEFFS of the receiver. USAA-1004, [0067]; USAA-1003, ¶58.

(b) *Day*

Day is directed to a “system by which documents and other network resources may be kept secure and private” using “public key encryption” to “provide security, encryption, and privacy for files, e-mail and other messages.” *Id.* It “seeks to maintain the integrity of and/or security information in” files and emails by using “personal digital IDs for signatures[,] ensuring that the emails or files coming from a specific individual only.” USAA-1006, [0096]. USAA-1003, ¶¶59-62.

In Day, “the secure email utility is an extension to MS Outlook and provides a very simple interface for users to secure their e-mail.” USAA-1006, [0119]. “To further simplify the use of email encryption for any incoming digitally signed emails, the secure email utility automatically updates and stores the public credentials (key) within the user’s Contacts database.” USAA-1006, [0170]; *see id.*, [0120], [0181]-[0182], [0186]. An example Contacts data is shown below:



USAA-1006, FIG. 26

(c) *Immega-Day*

Immega explains that, after MEFFSs are generated, they are “securely stored” and “assigned to a specific person with whom messages will be exchanged.” USAA-1004, [0009]-[0010], [0012], [0044], [0059]. To the extent that Immega is not explicit about implementation details regarding the storage of MEFFSs in a computing device, a POSITA would have naturally looked to references, such as Day, that offer these details. USAA-1003, ¶¶63-74.

Like Immega, Day describes “provid[ing] security, encryption, and privacy for files, e-mail and other messages.” USAA-1006, Abstract. Day describes a “secure email utility” that “automatically configures and associates the personal digital ID with an email program.” USAA-1006, [0014], [0020]. Similar to Immega, Day’s system uses “personal digital IDs for signatures” to “encrypt [an] email or file so that only authorized individuals can” view the content. USAA-1006, [0096].

In combination, the system (“Immega-Day”) includes computing devices, per Immega, each including a secure email utility integrated with an email program such as Outlook, per Day, and secures email transmission using MEFFSs to encrypt communications, per Immega. USAA-1004, [0041]-[0042], [0062]-[0068], FIGS. 1-6; USAA-1006, [0014], [0097], [0119]-[0120], [0170]; USAA-

1003, ¶66. Further, MEFFSs are stored, per Immega, in each device's email contacts database, per Day. §III.A.1(b)-(c); USAA-1003, ¶66.

Per Immega, in the combination, MEFFSs are "securely stored" and "assigned to a specific person with whom messages will be exchanged." USAA-1004, [0009]-[0010], [0012], [0044], [0059]. Per Day, in Immega-Day, the utility stores MEFFSs in email utility's contact database, which is, e.g., "an extension to MS Outlook and provides a very simple interface for users to secure their e-mail." USAA-1006, [0119]; USAA-1003, ¶67. Additionally, in Immega-Day, per Day, "[w]hen a signed message is received by Outlook and the sender of the e-mail is not within the Outlook's contact list; the secure email utility automatically creates a contact and saves the sender's certificate." USAA-1006, [0120]; USAA-1003, ¶67. Similarly, per Day, to "further simplify the use of email encryption for any incoming digitally signed emails, the secure email utility automatically updates and stores the public credentials (key) within the user's Contacts database," which "not only provides easy storage of contact information, but also a transparent tool for managing individual public certificates to send and receive secure email." USAA-1006, [0170].

In further detail, in Immega-Day, the Contacts database, per Day, stores all MEFFS necessary for secure email communication, per Immega, among communicating computing devices. USAA-1003, ¶68. Specifically, both the

receiver's MEFFS (modified for the sender) and the sender's MEFFS (modified for the receiver), per Immega, are securely stored in the receiver's Contacts address book, in the contact entry associated with the sender, per Day. USAA-1003, ¶68; USAA-1004, [0044], USAA-1006, [0119]-[0120]. That is, the secure information that the receiver uses to securely communicate with the sender is stored together in an entry associated with the sender in the receiver's Contacts database. *Id.*

Similarly, the sender's Contacts address book includes an entry for the receiver, where that entry includes both the sender's MEFFS (modified for the receiver) and the receiver's MEFFS (modified for the sender) and an identification of the sender (e.g., sender's email address). *Id.* Immega-Day further provides the MEFFS for each person with whom a user communicates. USAA-1003, ¶68 (describing an example with Alice, Bob, and Carol). Therefore, the combination's address book includes the "[m]any uniquely [MEFFSs], one (or more) for each person with whom messages will be exchanged," per both Immega and Day. USAA-1003, ¶68; USAA-1004, [0044], USAA-1006, [0119]-[0120], [0170].

Since Day's systems run on conventional operating systems (e.g., Windows), a POSITA would have understood and found obvious that the Contacts list storing the identifier and secret would be stored in a hierarchical directory, e.g., a Windows hierarchical directory. USAA-1003, ¶69 (citing USAA-1023, 298, 337); USAA-1006, [0098].

Further, Immega-Day's secure email utility is an application running on the device. USAA-1003, ¶70. Day describes a "secure email utility" that "associates the personal digital ID with an email program." USAA-1006, [0014], [0020]. A POSITA would have understood and found obvious that a utility is an application running on a computing device. USAA-1003, ¶70, (citing USAA-1023, 14). Further, Immega describes "an algorithmic flow chart for securely exchanging [EFFSs] between two users, for later use in biometrically certified messages" and "algorithmic flow chart subroutines for modifying the [EFFS] of the user." USAA-1004, [0043]-[0044], FIGS. 2-3A. To the extent that Immega is silent with respect to which computer component executes the algorithms, a POSITA would have found obvious to perform these algorithms using an application executing on the communicating computing devices, per Day. USAA-1003, ¶70 (citing USAA-1023, 14). Thus, per Immega and Day, a POSITA would have understood and found obvious that the Immega-Day combination's secure email utility runs as an application on a computing device and is used for enrolling fingerprint feature sets and secure communication. USAA-1003, ¶70.

A POSITA would have found obvious that enhancing the encryption/decryption techniques based on MEFFSs, per Immega, with Day's teachings regarding storage and organization of email encryption keys in a Contacts database introduces multiple advantages. USAA-1003, ¶71. For

example, Day explains that storing communication partners' credentials "simplify[ies] the use of email encryption for any incoming digitally signed emails." USAA-1006, [0170]; USAA-1003, ¶71. Thus, upon receiving an encrypted communication, a device need not retrieve remotely-stored decryption credentials since the credentials are stored locally. USAA-1003, ¶71. A POSITA would have further recognized the benefits of storing the MEFFSs, as in Immega, in a Contacts address book, per Day, would have simplified email communication by co-locating all information required for communicating with another individual (email address, biometric information, keys) in a single record, creating a "transparent tool for managing individual" the communication keys needed "to send and receive secure email." USAA-1003, ¶71; USAA-1006, [0134], [0170]. Further, the combination leverages an existing email component, Contacts, simplifying the system design and administration. USAA-1003, ¶71; USAA-1006, [0170]. Thus, a POSITA would have been motivated to incorporate Day's teaching of storing encryption data in the email system's existing Contacts database. USAA-1003, ¶71.

A POSITA would have found relevant solutions within Day and expected success in incorporating Day's teachings. USAA-1003, ¶72. Day describes "[u]sing public key encryption technology" to "provide security, encryption, and privacy for ... e-mail," and Immega similarly teaches using biometrics to "add

convenient security to email, by augmenting public key or other encryption.”

USAA-1004, [0008]; USAA-1006, Abstract.

Moreover, configuring the devices, as in Immega, to leverage Day’s teachings would have required only routine programming knowledge well within the skill of a POSITA prior to the Critical Date. USAA-1003, ¶73. Indeed, the change would have amounted to nothing more than the use of a known technique to improve similar devices – in each instance a device equipped with a fingerprint sensor – in a similar way, and combining prior art elements according to known methods to yield the predictable results described above. *KSR v. Teleflex*, 550 U.S. 398, 417 (2007); USAA-1003, ¶73.

Furthermore, the elements of the resulting combination would each perform functions they had been known to perform prior to the combination—receiver’s device would perform the same functions generate and store MEFFSs used to send and receive secure email and, per Day, would store the MEFFSs in a Contacts address book located in a directory and that includes the “[m]any uniquely [MEFFSs], one (or more) for each person with whom messages will be exchanged,” per Day. USAA-1003, ¶74. Accordingly, a POSITA would have naturally expected success when incorporating Day’s teachings into Immega. *Id.*

2. Claim 1

[1.pre]

To the extent the preamble is limiting, Immega-Day renders obvious [1.pre].

USAA-1004, Abstract, [0006], [0008] (“This allows confirmation of identity of both parties at both ends of a message exchange.”), [0013] (“Once the sender’s identity is confirmed”), [0017] (“checks the identity of the sender”), [0018] (“receiver’s identity is then checked”), [0019] (“receiver then confirms the sender’s identity”); USAA-1003, ¶155. At a high level, Immega describes a “method for permitting the secure transmission of electronic messages by using biometric certification is provided,” where “[e]nrolled fingerprint feature sets, which have been uniquely modified for a particular person with whom messages will be exchanged, are cross-enrolled between the sender and receiver such that the biometric identity of both the sender and receiver can be checked during message sending and receiving.” USAA-1004, Abstract. Immega further describes “an algorithmic method to provide biometric security to electronic messages, such as electronic mail (also known as email), certifying the physical identity of both the sender and receiver.” USAA-1004, [0006]. Immega also describes several instances of checking or confirming the identity of a receiver or sender. USAA-1004, [0008], [0013], [0017], [0018], [0019]. Thus, a POSITA would have understood that Immega provides a method for authenticating (e.g., checking biometric identity of a user) a user. USAA-1003, ¶155.

[1.a.i]

Immega-Day renders obvious [1.a.i]. USAA-1004, [0008], [0041]-[0044], FIG. 3A; §III.A.1(c); USAA-1003, ¶¶40-44 (§V.E), 156-159. First, Immega teaches that the receiver's device can comprise a "computer or any device equipped to execute the steps" described in Immega, including "cellular telephones, personal digital assistants and the like" ("mobile device"). USAA-1004, [0041]; *see also id.*, [0021]-[0029], FIGS. 7-9. Moreover, the receiver's device ("mobile device") includes a "fingerprint sensor" that "provides a biometric input, unique to each individual, which can be used to certify identity of both the sender and the receiver for electronic messaging or 'email.'" USAA-1004, [0042].

During a cross-enrollment process, a user enrolls one or more fingerprints at the receiver's device ("receive a unique user input") to obtain an enrolled fingerprint feature set. USAA-1004, [0042] ("The fingerprint sensor provides a biometric input, unique to each individual, which can be used to certify identity"), [0043], FIG. 2. Then, upon receipt of the fingerprints, the receiver's device ("mobile device") processes the enrolled fingerprint feature set of the user and generates the receiver's MEFFS ("secret") based on the receiver's live-scan fingerprint ("a unique user input"). USAA-1004, [0008], [0041], [0042] ("fingerprint sensor provides a biometric input, unique to each individual"), [0044], FIG. 3A; USAA-1003, ¶158 (citing USAA-1028, USAA-1029, USAA-1030). Immega explains that its invention requires "both the sender and the

receiver to cross-enroll biometric feature sets.” USAA-1004, [0008]. For example, a user uses a “fingerprint sensor” on his/her device to generate a “biometric identifier file, which is a user’s ‘enrolled fingerprint feature set’ (typically a minutiae file) that has been uniquely modified, or processed, for each recipient so that only the designated individual can employ it for messaging.” USAA-1004, [0008]. Thus, the MEFFS is generated based on, or responsive to, the processing of the received fingerprint data. *Id.*; USAA-1003, ¶158. A POSITA would have understood that a MEFFS is a “secret.” USAA-1003, ¶158 (citing USAA-1031); USAA-1004, [0009], [0012]-[0014], [0018]-[0019], [0064]-[0067]; §I.C. FIG. 3A illustrates generating a MEFFS. USAA-1004, [0044].

Moreover, as discussed above in §III.A.1(c), the Immega-Day device’s secure email utility (“an application running on a mobile device”) performs the enrollment process, including generating the secret. USAA-1003, ¶156; USAA-1006, [0014], [0020].

[1.a.ii]

Immega-Day renders obvious [1.a.ii]. USAA-1004, [0008], [0010], [0012], [0013], [0044], [0047], [0059], [0066]; USAA-1003, ¶¶160-166. The receiver’s MEFFS (“secret”) is stored at the receiver’s computing device (“mobile phone”) with an identification of the “person with whom messages will be exchanged” (e.g., email address) (“identifier”). USAA-1004, [0008], [0044], [0047]; USAA-

1003, ¶160. Immega first explains that, after being generated, MEFFS—including a user’s own MEFFS—are “securely stored” and “assigned to a specific person with whom messages will be exchanged.” USAA-1004, [0009]-[0010], [0012], [0044], [0059], FIG. 2. Thus, Immega discloses or suggests securely storing, at the receiver’s device, a MEFFS of the receiver “assigned to [the] specific person with whom messages will be exchanged.” *Id.*; USAA-1003, ¶160.

As discussed in §III.A.1(c), in Immega-Day, the receiver’s MEFFS is securely stored in a Contacts address book that includes the “[m]any uniquely [MEFFS], one (or more) for each person with whom messages will be exchanged.” USAA-1003, ¶161; USAA-1004, [0044], USAA-1006, [0119]-[0120]. Day explains, “To further simplify the use of email encryption for any incoming digitally signed emails, the secure email utility automatically updates and stores the public credentials (key) within the user’s Contacts database,” which “not only provides easy storage of contact information, but also a transparent tool for managing individual public certificates to send and receive secure email.” USAA-1006, [0170]. Thus, the receiver’s MEFFS (“secret”) is stored with an identification of the person with whom the Contacts entry is associated (e.g., email address) (“identifier”). USAA-1003, ¶¶161-166.

[1.a.iii]

Immega-Day renders obvious [1.a.iii]. USAA-1004, [0009], [0050], [0065]; USAA-1003, ¶167. The receiver's MEFFS ("secret") is retrievable when the receiver ("user") applies his/her fingerprint ("unique user input"). *Id.* When a user applies "a live-scan of the [user's] fingerprint," the "stored [MEFFS] of the [user] ... is then retrieved."¹ *Id.*

[1.b]

Immega-Day renders obvious [1.b]. USAA-1004, [0009], [0041], [0042], [0062], [0065], FIG. 6; USAA-1003, ¶168. FIG. 6 of Immega shows "an algorithm flow chart for sending and receiving a biometrically certified message with higher security protection," which "requires cross-enrollment of modified enrolled feature sets" of both users. USAA-1004, [0062].

Per FIG. 6, the receiver device ("mobile device") receives from a sender's device ("remote computing device") a communication ("first communication"). USAA-1004, [0041]-[0042], [0065], FIG. 1. The communication includes "the re-encrypted first live-scan fingerprint feature set of the receiver (previously re-encrypted with the receiver's public key at step 626) (step 638), the encrypted message (previously encrypted with the 'difference key' of the sender at step 634),

¹ Immega's sender/receiver are interchangeable because messages are sent back-and-forth. USAA-1003, ¶167, n.9; USAA-1004, [0009], [0041].

and the encrypted second live-scan fingerprint feature set of the sender (previously encrypted with the ‘difference key’ of the sender at step 636).” USAA-1004, [0065].

Regarding providing the user, via the mobile device, an opportunity to respond to the first communication, Immega teaches that, “[w]hen the receiver receives transmission, the receiver provides a second live-scan fingerprint feature set” and the receiver encrypts the receiver’s second live-scan fingerprint feature set and transmits it back to the sender. USAA-1004, [0066]-[0067]. Thus, a POSITA would have understood that Immega teaches or at least renders it obvious. USAA-1003, ¶¶170-171. Specifically, through its teaching of the “algorithmic subroutine that gives the sender direct confirmation that the correct person has received the message,” Immega teaches or renders obvious “providing the user via the mobile device, an opportunity to respond to the first communication” upon receiving the first communication. USAA-1004, [0066]-[0067]; USAA-1003, ¶¶170-171 (citing USAA-1023); *see* USAA-1004, [0020]. In particular, after receiving the sender’s message (“first communication”), the receiver (“user”) using his/her device (“via the mobile device”) sends the receiver’s second live-scan fingerprint feature set, thus affording the user an opportunity to respond to the sender’s message. *Id.*

Finally, because the sender and receiver are exchanging email, a POSITA would have understood and found obvious that the sender’s device is remote

relative to the receiver's device. USAA-1003, ¶172; USAA-1004, [0042], FIG. 1 (showing "computer workstations 100-150, which are networked directly 160 or connected 170 to the World Wide Web Internet "cloud" 180" but otherwise remote from one another).

[1.c.i]

Immega-Day renders obvious [1.c.i]. USAA-1004, [0008], [0019], [0042], [0066], FIG. 6; USAA-1003, ¶¶173-174. Responsive to receiving the first communication and providing the user an opportunity to respond, the receiver device ("mobile device") prompts the receiver ("user") to "provide[] a second live-scan fingerprint" ("receiving a candidate user input"). USAA-1004, [0019] ("Upon receiving the encrypted message and feature sets, the receiver provides a second live-scan fingerprint"), [0066]. Immega explains that "when the receiver receives [the] transmission [from step 638], the receiver provides a second live-scan fingerprint," shown in FIG. 6 in step 640. USAA-1004, [0066], FIG. 6. To input a fingerprint, the sender and receiver devices are "equipped with a fingerprint sensor" ("user interface"). USAA-1004, [0008], FIG. 1 (biometric input device); *see also id.*, [0022]-[0023], [0042].

The receiver's live-scan fingerprint ("candidate user input") is then used to "extract a second live-scan fingerprint finger set, which is then matched against the stored fingerprint feature set of the receiver" (i.e., the receiver must prove his/her

identity for the decryption process to continue), thus “authenticating the user at the mobile device by receiving a candidate user input.” USAA-1004, [0066]; USAA-1003, ¶174.

[1.c.ii]

Immega-Day renders obvious [1.c.ii]. USAA-1004, [0064]-[0065], [0067], FIG. 6; USAA-1003, ¶¶175-177. Immega describes a “subroutine that gives the sender direct confirmation that the correct person has received the message” after verifying the user. USAA-1004, [0067]. Specifically, the receiver device transmits to the sender (“remote computing device”) a direct confirmation message (“second communication”) that comprises the “receiver’s second live-scan fingerprint feature set ... encrypted, preferably with the ‘difference key’ of the sender (reconstructed in step 650).” USAA-1004, [0067]; USAA-1003, ¶175. Immega explains that the confirmation message (“second communication”) “enables a notification to be displayed to the sender that the message has been received and decrypted by the proper person” (“verifying said user to the remote computing device”). USAA-1004, [0067].

Immega states that the message is “preferably” encrypted with the sender’s difference key, but Immega is not so limited. USAA-1003, ¶176. It would have been an obvious design choice to encrypt it with the receiver’s difference key because the sender is already in possession of it (per 620), which the sender would

use for decrypting the message. *Id.*; USAA-1004, [0065]. The receiver would similarly already be in possession of it (per 612). USAA-1004, [0064]. Thus, use of the receiver's difference key would require no additional transmissions or exchanges by either party and is equally secure. USAA-1003, ¶176; USAA-1004, [0011], [0064]-[0065].

Moreover, because the “difference key” that is used to encode the second communication is “reconstructed by subtracting the first [LFFS] of the receiver from the stored [MEFFS] of the receiver,” a POSITA would have understood and found obvious that the second communication is encoded using the receiver's stored MEFFS (“secret”). USAA-1003, ¶177; USAA-1004, [0065].

3. Claim 2

[2]

Immega-Day renders obvious [2]. USAA-1004, [0009]; USAA-1003, ¶178; *supra*, [3] (Ground-1A); §III.A.1(c). The process used for encrypting the communication uses information derived from MEFFS. USAA-1003, ¶178.

Therefore, a POSITA would have understood and found obvious that the MEFFS is an encryption key. *Id.* Specifically, Immega teaches that messages are encrypted using a “difference key,” which is derived from a user's LFFS and the user's MEFFS (“secret”). USAA-1004, [0009]. Because the receiver's MEFFS (“secret”) is used directly to derive the “difference key” (which is used for

encryption), a POSITA would have found obvious that the MEFFS itself also is an encryption key. USAA-1003, ¶178 (citing USAA-1026, defining “encryption key”). *Id.*

4. Claim 3

[3]

Immega-Day renders obvious [3]. USAA-1004, [0044], FIG. 3A; USAA-1003, ¶179. Immega describes how the MEFFS (“secret”) is generated by “modifying the enrolled fingerprint feature set of the user.” USAA-1004, [0044], FIG. 3A. Then, “[a] random number is used to generate a displacement vector (step 302) to slightly shift or displace all features of the enrolled fingerprint feature set by a random displacement vector (step 304),” resulting in the [MEFFS].” *Id.* Thus, a POSITA would have understood that the MEFFS (“secret”) comprises an enrolled fingerprint feature set (“static portion”) and a displacement vector generated from a random number (“dynamic portion”). USAA-1003, ¶179. Indeed, as Immega teaches, the same enrolled fingerprint feature set is used to generate each MEFFS (and thus is static), while a different displacement vector is used for each communication partner (and thus is dynamic). *Id.*

5. Claim 4

[4]

Immega-Day renders obvious [4]. USAA-1003, ¶¶180-181. Immega describes “giv[ing] the sender direct confirmation that the correct person has

received the message,” whereby, responsive to the sender’s message, the receiver sends the sender the “receiver’s second [LFFS].” USAA-1004, [0066]-[0067]. Thus, to the extent that Immega does not explicitly describe that the sender’s message comprises a request for the receiver’s user credentials, a POSITA would have found this obvious. USAA-1003, ¶180.

The ’689 Patent lists “a username and password” as examples of “user credentials,” indicating “[o]ther forms of user credentials may be used.” USAA-1001, 13:9-16. Thus, a POSITA would have understood that the receiver’s live-scan fingerprint (included in a LFFS) comprises user credentials. USAA-1004, Abstract, [0042]; USAA-1003, ¶181; *infra*, [6] (Ground-1A). A POSITA would have understood that Immega teaches or at least renders obvious that the sender’s first communication, which elicits the receiver’s second live-scan fingerprint feature set (“user credentials”), comprises a request for the receiver’s user credentials. USAA-1003, ¶181.

6. Claim 6

[6]

Immega-Day renders obvious [6]. USAA-1003, ¶182. The receiver’s live-scan fingerprint (“unique user input”) comprises user credentials. USAA-1004, Abstract, [0008], [0042]; USAA-1003, ¶182. From this and related description, a POSITA would have understood and found obvious that the user’s live-scan

fingerprint is/includes user credentials. USAA-1003, ¶182 (citing USAA-1028, USAA-1029, USAA-1030); USAA-1004, [0042] (“fingerprint sensor provides a biometric input, unique to each individual, which can be used to certify identity”).

7. Claim 7

[7]

Immega-Day renders obvious [7]. USAA-1004, [0067]; USAA-1003, ¶183. Immega teaches that the direct confirmation message (“second communication”) “gives the sender direct confirmation that the correct person has received the message” (“first communication”). USAA-1004, [0067]. Thus, the first and second communications comprise two related communications of a communication session (e.g., a message and a responsive message confirming receipt). USAA-1003, ¶183.

8. Claim 8

[8]

Immega-Day renders obvious [8]. USAA-1003, ¶¶184-188. First, Immega teaches generating a LFFS (“candidate identifier”) using the sender’s live-scan fingerprint (“received candidate user input”). USAA-1003, ¶184. For example, Immega explains that, “[u]pon receiving the encrypted message and feature sets, the receiver provides a second live-scan fingerprint and extracts a second live-scan fingerprint feature set” (generates a candidate identifier) “to initiate the decryption process.” USAA-1004, [0019].

Next, Immega teaches determining if the LFFS (“candidate identifier”) matches the identifier. USAA-1003, ¶185. For example, Immega describes determining “[i]f the receiver’s second [LFFS] is valid” by “extract[ing] a second [LFFS], which is then matched against the stored fingerprint feature set of the receiver (the receiver must prove his/her identity for the decryption process to continue).” USAA-1004, [0019], [0066]. As discussed in §III.A.1(c), in Immega-Day, the receiver’s MEFFS is securely stored in a Contacts address book that includes the “[m]any uniquely [MEFFS], one (or more) for each person with whom messages will be exchanged.” USAA-1003, ¶185; USAA-1004, [0044], USAA-1006, [0119]-[0120]. Thus, a POSITA would have understood and found obvious that the MEFFS (“secret”) is stored with both an identification of “person with whom messages will be exchanged” (e.g., person’s email address), as discussed for [1.a.ii] (Ground 1A), and further with an identification of the receiver. *Id.*; [1.a.ii] (Ground 1A). Specifically, a POSITA would have understood and found the latter obvious at least because the MEFFS is stored in a Contacts address book of the receiver, so all contact information stored therein would have been understood to be stored with an identification of the owner of the address book (i.e., the receiver). USAA-1003, ¶¶185-186 (citing USAA-1023, 152-155). Thus, a POSITA would have understood or found obvious that the MEFFS is stored with an identifier that collectively includes an identifier of the sender (e.g., email address) and an

identifier of the receiver. USAA-1003, ¶185. In this way, a POSITA would have understood and found obvious that, in matching the receiver's second LFFS against the stored fingerprint feature set of the receiver (thus matching the receiver's LFFS with the receiver), the receiver's second LFFS ("candidate identifier") is matched with the receiver (which the "identifier" comprises). USAA-1003, ¶187.

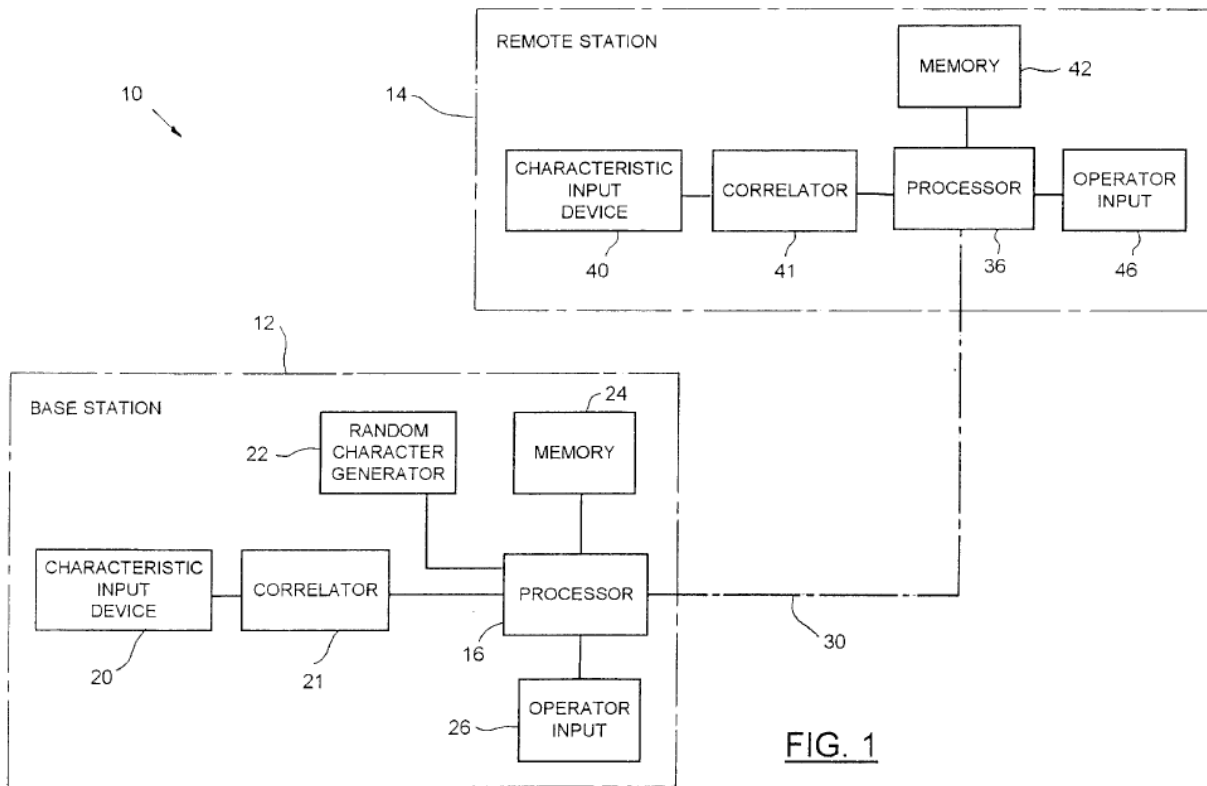
If the receiver's LFFS matches the identifier, Immega teaches retrieving the MEFFS so that the receiver can "reconstruct" the difference key for decryption. USAA-1003, ¶188; USAA-1004, [0066]. Specifically, Immega explains that "the 'difference key' of the [receiver] is then reconstructed by subtracting the [receiver's second [LFFS]] from the receiver's stored [MEFFS]." USAA-1004, [0019], [0066]. That is, since the MEFFS ("secret") is needed to determine the difference key, and the difference key is used to decode the message, a POSITA would have understood and found obvious that Immega teaches retrieving the MEFFS ("secret") when decoding the message. USAA-1004, [0019]; USAA-1003, ¶188.

B. GROUND 1B – Immega-Day-Tomko Renders Claims 5 and 9-21 Obvious

1. Prior Art and Proposed Combination

(a) *Tomko*

Tomko describes “permitting the secure handling of data between two remote stations,” which “involves the generation of an encrypted decryption key which is based,” e.g., “on a fingerprint information signal from a user of a first station.” USAA-1005, Abstract. The encrypted key is “stored at both stations” so “a message encrypted with the key may be decrypted at either station by retrieving the encrypted key,” inputting a fingerprint signal to recover the decryption key, and “applying the decryption key to the encrypted message.” *Id.*; USAA-1003, ¶¶75-77.



USAA-1005, FIG. 1

A system includes two remote stations, including base station 12 and remote station 14 “connected for two-way communication,” with each station having a processor 16/36, characteristic input device 20/40, and memory 24/42. USAA-1005, 2:18-41, FIG. 1.

Tomko describes “[d]eveloping an encrypted decryption key” where the key is generated and stored in memory in an encrypted form. USAA-1005, 2:48-5:11, 6:56-65.

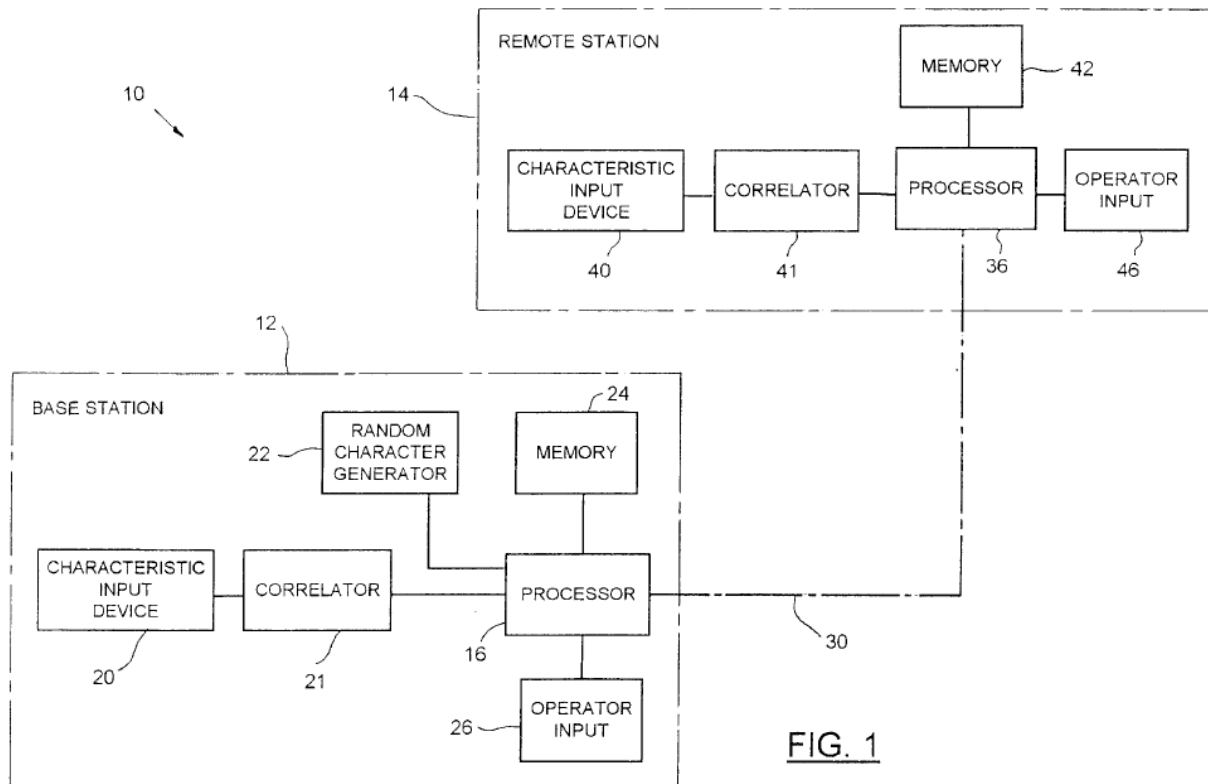
(b) *Immega-Day-Tomko*

A POSITA would have found obvious integration of Tomko’s teachings relating to hardware components and data encryption into Immega-Day, further enhancing security and offering implementation details. USAA-1003, ¶¶78-90.

i. Device Components

Immega describes “secure transmission of electronic messages” using “biometric certification.” USAA-1004, Abstract, [0006]. The receiver’s device can comprise a “computer or any device equipped to execute the steps” described in Immega. USAA-1004, [0041]. To the extent that Immega does not describe hardware components, a POSITA would have included these components for processing and storing in Immega’s method, as was well-known, per Tomko, and executing the secure email utility (application) of Immega-Day. USAA-1003, ¶¶79, 40-44 (§V.E), 63-77 (§§VIII.C-D); *supra* §§III.A.1(c), III.B.1(a).

Like Immega and Day, Tomko is directed to “secure handling of data between two remote stations” using fingerprints. USAA-1005, Abstract. In Tomko’s FIG. 1 (below), each device includes a processor 16/36, characteristic input device 20/40, and memory 24/42. USAA-1005, 2:18-41, FIG. 1. Processor 16 is used to process received user input (e.g., a fingerprint via the characteristic input device 20) to derive and encrypt a decryption key stored in memory 24. USAA-1005, 2:49-4:65. The processor also assists in sending messages, including obtaining the encrypted decryption key when a user “applies his fingerprint to the characteristic input device.” USAA-1005, 5:13-26; USAA-1003, ¶80.



USAA-1005, FIG. 1

Given the similarities among Immega, Day, and Tomko, a POSITA would have naturally looked to Tomko for implementation details regarding the Immega-Day devices, including what components would be included. USAA-1003, ¶81. Combining the teachings of Immega-Day and Tomko would have merely involved combining prior art elements according to known methods to yield predictable results. *Id.* Indeed, both systems involve communications between devices that are secured with fingerprints. USAA-1004, Abstract; USAA-1005, Abstract; USAA-1003, ¶81. A POSITA would have been motivated to combine the teachings of Immega-Day and Tomko to realize the implementation details, *e.g.*, processor, memory, and other components, to execute the functionality of the device. *Id.*; USAA-1004, [0041] (“any device equipped to execute the steps described”). The combination (“Immega-Day-Tomko”) would have been predictable and foreseeable and a POSITA would have had a reasonable expectation of success because 1) Immega, Day, and Tomko disclose secure communications between remote devices secured using fingerprint information (USAA-1004, Abstract; USAA-1005, Abstract; USAA-1006, Abstract) and 2) the combination merely involves incorporating known features explicitly disclosed by Tomko and understood by a POSITA as likely present, but not explicitly disclosed by Immega. USAA-1003, ¶81. The combination is predictable, at least in part, because elements of the combined system would each perform similar functions

they had been known to perform prior to the combination. *Id.* For example, the devices in Tomko would still perform the same or similar functions, including generating and sharing MEFFSs and transmitting secure communications with the use of that data, as it did prior to the combination with Tomko. *Id.*

ii. Data Encryption

As discussed above, Immega teaches storing the receiver's MEFFS ("secret"). *Supra*, [1.a.ii] (Ground-1A). Immega further teaches that, during cross-enrollment, the receiver encrypts the receiver's MEFFS ("secret"). USAA-1004, [0047], claim 4. Specifically, Immega describes creating an "enrollment message (step 222) comprised of the first user's name, the second user's name[, and] the uniquely [MEFFS]" that is double encrypted and sent to the second user. USAA-1004, [0047]. To the extent that Immega is not explicit about the timing of storing the receiver's MEFFS ("secret"), it would have been obvious to a POSITA to encrypt it prior to storing it. USAA-1003, ¶82.

Tomko teaches generating "an encrypted version of a message decryption key" which is based on a fingerprint information signal from a user of a first station" and used to "encrypt messages." USAA-1005, Abstract, 2:42-5:11. Notably, Tomko teaches that the finger-print based key is "stored in memory 24" as an "encrypted version." USAA-1004, 4:60-65. In Immega-Day-Tomko, during cross-enrollment, the receiver device stores the double encrypted enrollment

message prior to transmitting the enrollment message to the sender device, as illustrated in modified FIG. 2 below. USAA-1003, ¶83.

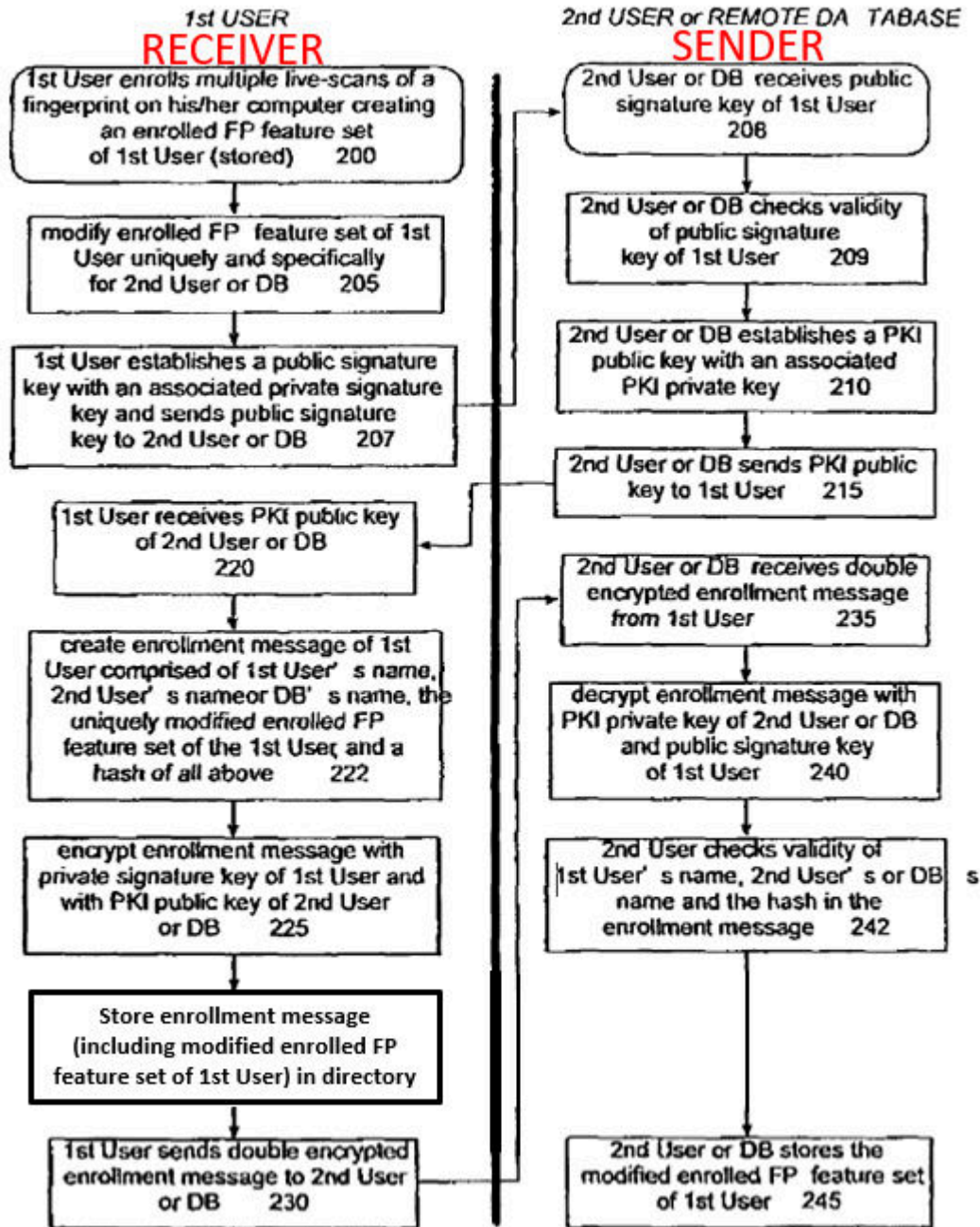


FIG. 2

USAA-1004, FIG. 2 (modified, annotated)

Indeed, as discussed in [1.a.ii], Immega teaches securely storing MEFFS “assigned to a specific person with whom messages will be exchanged.” USAA-1004, [0044], [0009]-[0010], [0012], [0059], FIG. 12. Moreover, as discussed in [1.a.ii], for the receiver’s device to distinguish the receiver’s MEFFSs from one another, it would have been obvious that each MEFFS would be stored with an identifier identifying the user for which the MEFFS facilitates communication. USAA-1003, ¶84. This information is already included in Immega’s enrollment message (e.g., first and second user’s names, MEFFS). USAA-1004, [0047]. Thus, it would be obvious to a POSITA that, in Immega-Day-Tomko, during enrollment, the receiver’s device stores the encrypted enrollment message for each user with whom messages are exchanged. USAA-1003, ¶84. When the receiver’s device later required use of the receiver’s MEFFS, the receiver would apply his/her fingerprint to retrieve the enrollment message/MEFFS, per Immega, and decrypt it. *Id.*; USAA-1004, [0009], [0050], [0045]-[0047].

A POSITA would have found obvious that enhancing Immega’s method based on Tomko’s teachings of storing an encrypted decryption key would introduce multiple advantages and been motivated to do so at least because of the added security benefits of locally storing encrypted versions of sensitive information. USAA-1003, ¶85. Tomko explains that storing an encrypted version of the decryption key allows the decryption key to “be passed to the remote

station” and “remain secure even if intercepted.” USAA-1004, 4:60-65.

Moreover, the recipient “remote station stores the received decryption key in its memory 42,” further benefiting from a secure encrypted decryption key. *Id.*; USAA-1003, ¶85. A POSITA would have further recognized the benefits of storing the decryption key in an encrypted format locally, especially in instances where the base station is not sufficiently secure. USAA-1003, ¶¶85-87 (citing USAA-1008); USAA-1005, 6:10-12; USAA-1008, Abstract, 3:26-37, 1:14-39.

A POSITA would have found relevant solutions within Tomko and expected success in incorporating Tomko’s solutions within Immega given that Tomko describes various methods for “[d]eveloping an encrypted decryption key,” and Immega similarly teaches encrypting its MEFFSs. USAA-1004, [0047]; USAA-1005, 2:48-5:11; USAA-1003, ¶88.

Moreover, configuring Immega’s devices to leverage Tomko’s teachings would have required only routine programming knowledge well within the skill of a POSITA prior to the Critical Date. USAA-1003, ¶89. Indeed, the change would have amounted to nothing more than the use of a known technique to improve similar devices – in each instance a device equipped with a fingerprint sensor – in a similar way, and combining prior art elements according to known methods to yield the predictable results described above. *KSR*, 550 U.S. at 417; USAA-1003, ¶89.

Furthermore, the elements of the resulting combination would each perform functions they had been known to perform prior to the combination—receiver’s device would perform the same functions generate and store MEFFSs used to send and receive secure email but, per Tomko, would store the MEFFSs in an encrypted form for improved security. USAA-1003, ¶90. Accordingly, a POSITA would have naturally expected success when incorporating Tomko’s teachings. *Id.*

2. Claim 5

[5]

Immega-Day-Tomko renders obvious [5]. USAA-1004, [0047]; USAA-1005, Abstract, 2:42-5:11; USAA-1003, ¶189. As discussed in §III.B.1(b), in Immega-Day-Tomko, during enrollment, the receiver’s device stores the encrypted enrollment message for each user with whom messages will be exchanged before transmitting the enrollment message, thus encrypting the “secret” prior to storing it. USAA-1003, ¶189; §III.B.1(b). Notably, Tomko teaches that the finger-print based key is “stored in memory 24” as an “encrypted version.” USAA-1004, 4:60-65.

3. Claim 9

[9.pre]

Immega-Day-Tomko renders obvious [9.pre]. USAA-1004, [0041]; USAA-1003, ¶¶190, 40-44 (§V.E). Immega explains that the receiver’s device can comprise a “computer or any device equipped to execute the steps,” including

“cellular telephones, personal digital assistants and the like” (“mobile device”).

USAA-1004, [0041]; *see also id.*, [0021]-[0029], FIGS. 7-9; *supra*, Claim [1]

(Ground-1A).

[9.a]

Immega-Day-Tomko renders obvious [9.a]. As discussed above, the Immega-Day-Tomko combination includes a processor, a storage, device, and a memory storing executable instructions that are executed by the processor, as was well known by the Critical Date. USAA-1003, ¶¶191, 40-44 (§V.E), 78-81 (§VIII.E.i). Additionally, Immega establishes that the receiver device is “equipped to execute the steps described” in Immega for authenticating communications, so a POSITA would have understood and found obvious that the processor would be used to execute the method using the stored application. *Id.*; USAA-1004, [0041].

[9.b]

Immega-Day-Tomko renders obvious [9.b]. USAA-1004, [0041]; USAA-1003, ¶192. As discussed above in §III.A.1(c), §III.B.1(b), the Immega-Day-Tomko device’s secure email utility (“an application running on a mobile device”) performs the enrollment process, including generating the secret. USAA-1003, ¶192; USAA-1006, [0014], [0020]; *supra* [1.a.i] (Ground-1A). The secure email utility communicates with a user via a user interface to receive a unique user input. *Supra* [1.a.i] (Ground-1A); USAA-1003, ¶192. Moreover, a POSITA would have

understood and found obvious that the application running on the device would be configured to execute the methods described in Immega. USAA-1003, ¶192; USAA-1004, [0041] (“any device equipped to execute the steps described”).

[9.c.i]

Supra, [1.a.i] (Ground-1A).

[9.c.ii]

Supra, [1.a.ii] (Ground-1A). Since the secret is stored in the user’s Contacts database, e.g., Outlook Contacts, a POSITA would have understood that the secret is stored in the storage device. USAA-1003, ¶¶194-196 (citing USAA-1001, 27:1-8; USAA-1023, 298, 337; USAA-1035, [0158], [0161]), 40-44 (§V.E); §III.A.1(c)).

[9c.iii]

Supra, [1.a.iii] (Ground-1A).

[9.d]

Supra, [1.b] (Ground-1A).

[9.e.i]

Supra, [1.c.i] (Ground-1A).

[9.e.ii]

Supra, [8] (Ground-1A) and [9.c.ii] (Ground-1B).

[9.f]

Supra, [1.c.ii] (Ground-1A).

4. Claim 10

[10]

Supra, [2] (Ground-1A).

5. Claim 11

[11]

Supra, [3] (Ground-1A).

6. Claim 12

[12]

Supra, [4] (Ground-1A).

7. Claim 13

[13]

Supra, [5] (Ground-1B).

8. Claim 14

[14]

Supra, [6] (Ground-1A).

9. Claim 15

[15]

Supra, [7] (Ground-1A).

10. Claim 16

[16.pre]

Supra, [9.a] (Ground-1B).

To the extent the preamble is limiting, Immega-Day-Tomko renders obvious [16.pre]. *Supra*, [9.a] (Ground-1B); USAA-1003, ¶¶208, 40-44 (§V.E), 78-81

(§VIII.E.i).

[16.a]

Immega-Day-Tomko renders obvious [16.a]. USAA-1004, [0041]; USAA-1003, ¶¶209-212, 40-44 (§V.E). As discussed above in §III.A.1(c), §III.B.1(b), the Immega-Day-Tomko device's secure email utility is an application running on a processor-based platform. USAA-1003, ¶210. For example, Immega explains sender and receiver are "any device equipped to execute the steps described, depending on the context," including "cellular telephones, personal digital assistants and the like." USAA-1004, [0041]. A POSITA would have understood that such devices are processor-based platforms. USAA-1003, ¶210 (citing USAA-1032, [0008], [0098]; USAA-1034, [0075]-[0076]).

The processor-based platform executes instructions for communication with at least one remote computer-based station, e.g., the sender. *Supra* [1.b] (Ground-1A); USAA-1003, ¶211 (citing USAA-1032, [0098]; USAA-1034, [0075]-[0076]).

The secure email utility is configured to receive a unique user input. *Supra*, [9.b] (Ground-1B).

[16.b.i]

Supra, [1.a.i] (Ground-1A).

[16.b.ii]

Supra, [1.a.ii] (Ground-1A). Since the secret is used by the processor (e.g., to encrypt and decrypt), a POSITA would have understood that the secret is stored

in memory. USAA-1003, ¶¶215-218 (citing USAA-1001, 27:3; USAA-1035, [0148], [0158]), 40-44 (§V.E).

[16.b.iii]

Supra, [1.a.iii] (Ground-1A).

[16.c]

Supra, [1.b] (Ground-1A).

[16.d.i]

Supra, [1.c.i] (Ground-1A).

[16.d.ii]

Supra, [8] (Ground-1A).

[16.e]

Supra, [1.c.ii] (Ground-1A).

11. Claim 17

[17]

Supra, [2] (Ground-1A).

12. Claim 18

[18]

Supra, [3] (Ground-1A).

13. Claim 19

[19]

Supra, [4] (Ground-1A).

14. Claim 20

[20]

Supra, [5] (Ground-1B).

15. Claim 21

[21]

Supra, [6] (Ground-1A).

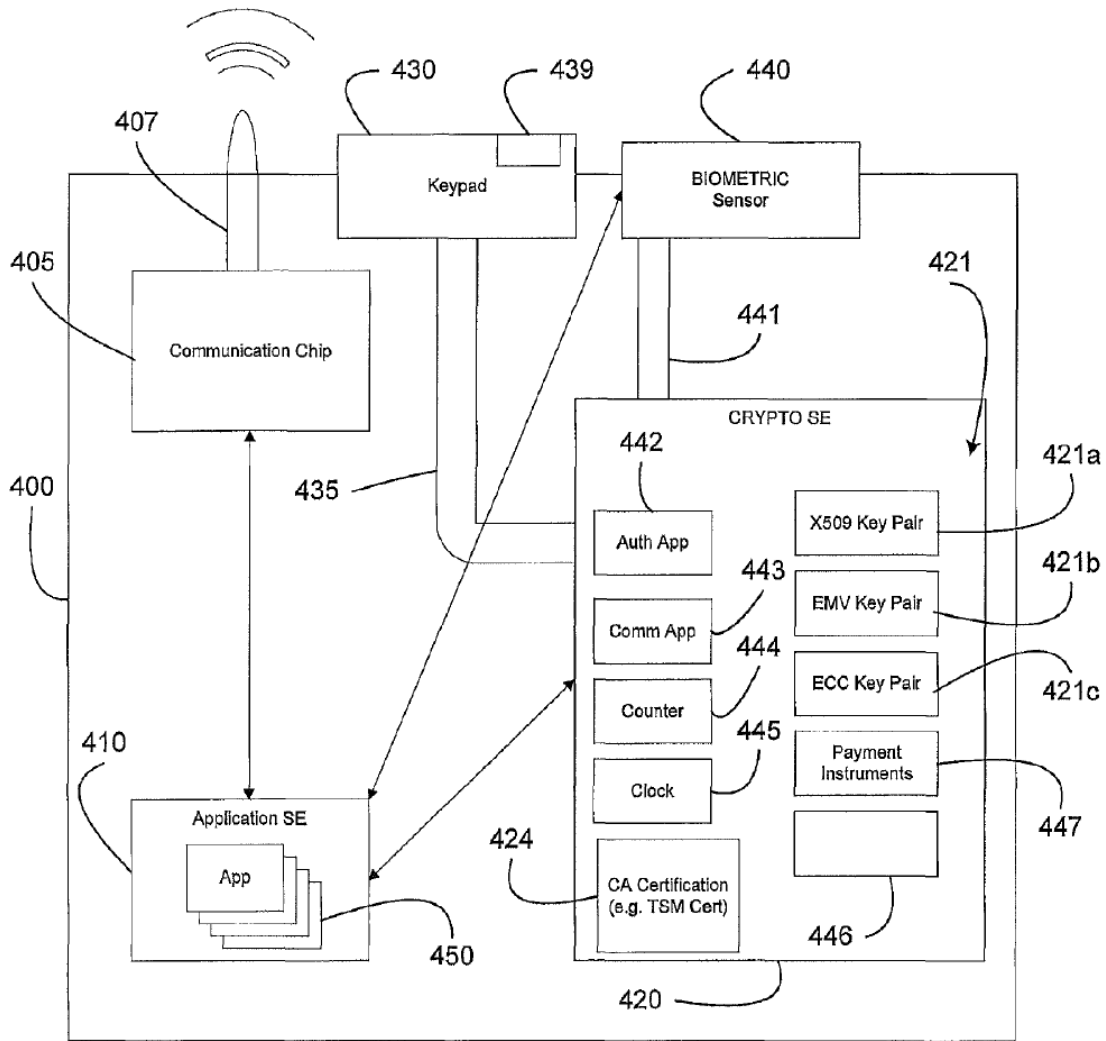
C. GROUND 2A – Mardikar-318 and Chhabra Render Claims 1-4 and 6-7 Obvious

1. Prior Art and Proposed Combination

(a) *Mardikar-318*

Mardikar-318 discloses methods for securing “financial transactions initiated from an electronic device,” including authenticating a user based on “biometric information” input to the device through an included biometric sensor. USAA-1010, Abstract, 1:15-17, 3:11-33, FIGS. 4, 5a, 5b, 6a. USAA-1003, ¶¶91-107.

Mardikar-318’s FIG. 4 (below) “shows an example...client device 400...such as a mobile phone” that “may include a communication chip 405...secure elements 410, 420...and a biometric sensor 440.” USAA-1010, 6:43-49.



USAA-1010, FIG. 4

Mardikar-318 explains that a secure element (SE) may be “a smart card” with a CPU and storage that “makes it possible for the card to keep some secrets....” *Id.*, 7:45-57. For example, FIG. 4’s “Application SE” and “Crypto SE” “may be pre-loaded with applications...for facilitating financial transactions” with a service provider (SP) such as “PayPal,” and Crypto SE 420 may store

“authentication data,” “payment instruments,” “certificates,” “crypto keys,” and “unique biometric authentication information related to a specific user.” *Id.*, 7:58-63, 8:62-9:59.

In that regard, Crypto SE’s biometric authentication application evaluates user biometric data received from biometric sensor 440, both for purposes of registering/storing the user’s derived biometric profile(s), and for purposes of authorizing requested transactions on the basis of comparisons against one or more previously registered profiles. *Id.*, 9:60-65, 10:42-13:36; FIGS. 4, 5a, 5b, 6a, 6b, 6c.

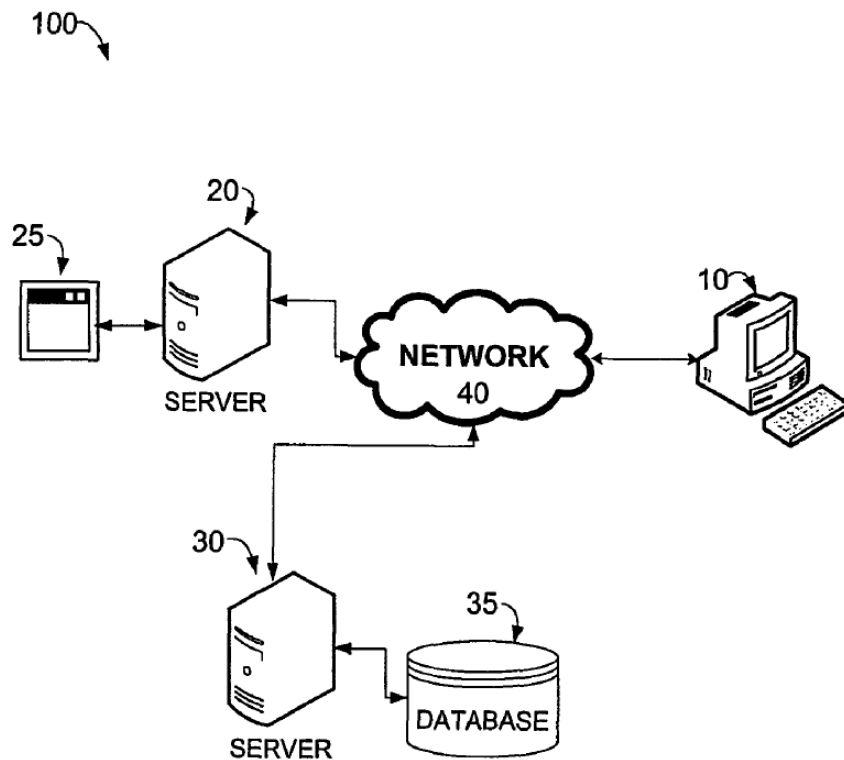
For example, Mardikar-318 explains that “PayPal...may provide payment processing for online transactions on behalf of the customer so that the customer does not expose payment information directly to the merchant.” *Id.*, 6:13-29. In that regard, “the customer may pre-register his account with the payment provider system...and then use the payment provider system to make purchases” using device 400 “when redirected to the payment provider system from the merchant’s site.” *Id.* “After the financial transaction is authorized, the...payment provider system completes the transaction.” *Id.*, 12:22-30,3:11-33, 4:27-36, 13:37-14:19.

(b) *Chhabra*

Like Mardikar-318, Chhabra describes secure mobile Internet transactions that are facilitated through “an on-line payment service (e.g. PayPal®).” USAA-1013, Abstract, 10:47-65, 5:41-11:29, FIGS. 1, 3, 4, 5. USAA-1003, ¶¶108-113.

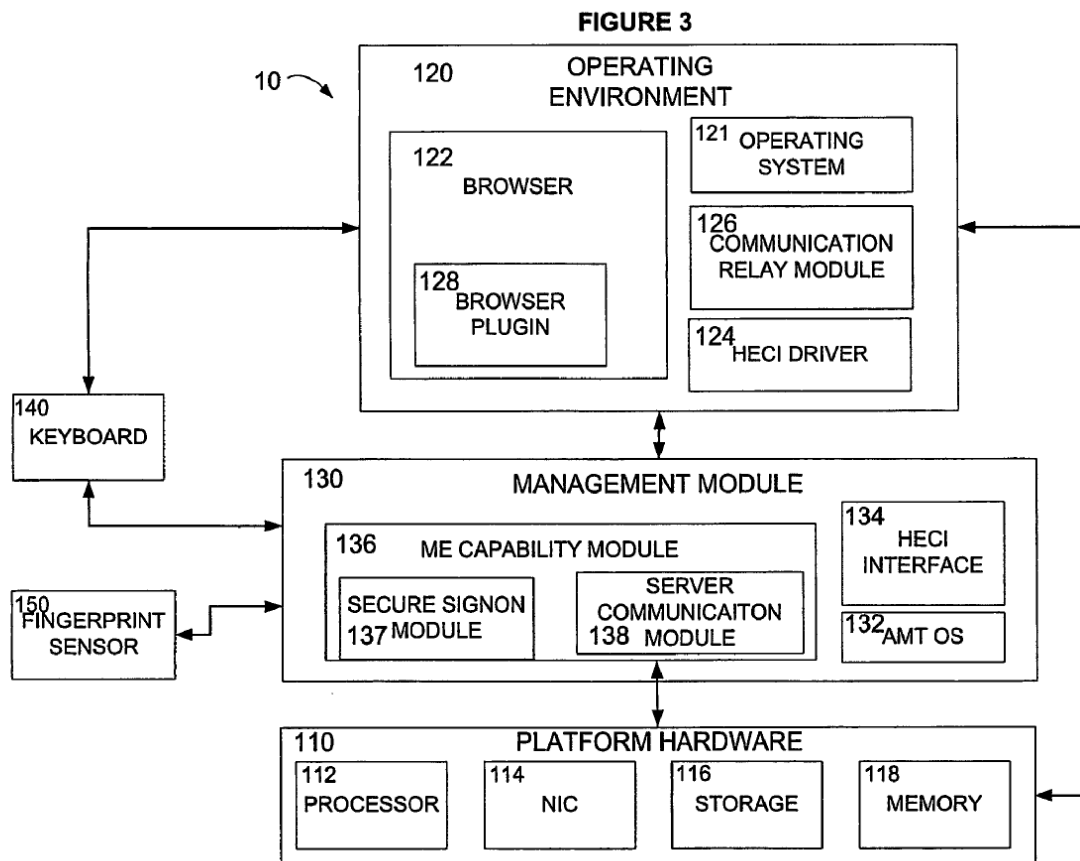
Chhabra’s FIG. 1 (below) illustrates “a system for sending credentials securely to a remote server” 20 from a user computing platform 10 featuring a “web browser as an application for retrieving and viewing web content.” *Id.*, 1:6-13, 1:24-25, 3:44-56, 2:64-7:64.

FIGURE 1



USAA-1013, FIG. 1

As shown in Chhabra's FIG. 3 (below), platform 10 features a "management module" 130 that "may request a user's input for authorization" in the context of a web-based financial transaction facilitated by remote servers 20 and/or 30, which the user provides through "a sensor such as...fingerprint sensor 150..." *Id.*, 9:32-44.

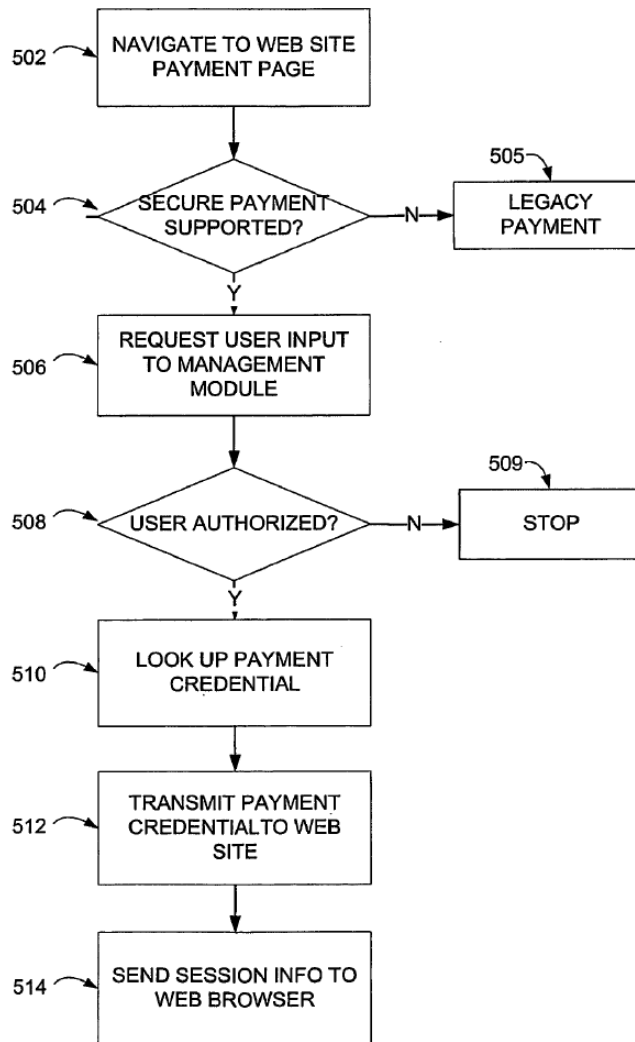


USAA-1013, FIG. 3

Chhabra's FIG. 5 (below) illustrates "a method for a secure payment transaction" in which "a user desiring to complete a financial transaction on a web site...may be automatically redirected to a payment page" that requests user

payment and authorization credentials. *Id.*, 10:40-55. “If the user is authorized” through a process involving a table/database lookup and fingerprint matching, the management module may look up in a table/database “the appropriate identifier or credential needed,” and “encrypt and transmit the requisite...payment credential” to the server. *Id.*, 3:3-25, 7:44-56, 11:10-29, 9:45-11:9, FIG. 2.

FIGURE 5



USAA-1013, FIG. 5

(c) *Mardikar-Chhabra*

A POSITA would have been motivated and found it obvious to apply Chhabra's authentication techniques to Mardikar-318's system, thereby enabling a user to conveniently and securely log in to a payment provider's site when redirected to that site during a browser session, and/or to securely and conveniently complete an associated financial transaction during that browser session. USAA-1010, 6:13-29, FIGS. 4, 5a, 5b; USAA-1013, 10:40-55, FIGS. 1, 3, 4, 5; USAA-1003, ¶¶114-116.

For instance, in view of the strong similarities between their respective systems and goals, a POSITA would have found it obvious to supplement Mardikar-318 with Chhabra's teachings on biometric authentication for browser-based web transactions facilitated by a payment provider's remote server. USAA-1003, ¶¶117-123; USAA-1010, 4:58-62, 6:19-29, 7:58-9:3, 9:60-65, 10:42-12:43, FIG. 4; USAA-1013, 6:45-48, 9:32-44, 10:40-11:9, 13:58-14:24, FIGS. 3, 5.

For example, Crypto SE's authentication application would, consistent with Chhabra, "request user input for authorization" in response to a message communicated to device 400 from the remote server, upon or after the user's redirection to the payment provider's site. USAA-1013, 9:32-44, 6:45-48, 10:65-11:9, 13:58-14:24, FIGS. 1, 3, 4, 5; USAA-1010, 6:24-29, FIG. 4; USAA-1003, ¶124.

Upon receiving the user's biometric input, the Crypto SE application would "verify or confirm that the user is authorized" through a table/database lookup and "fingerprint matching," with a "positive match" yielding authentication. USAA-1013, 7:44-56, 9:45-64, 10:65-11:9; USAA-1010, 9:60-65, 11:44-51; USAA-1003, ¶125.

And, upon authentication, the Crypto SE application would complete the transaction by "look[ing] up the appropriate payment credential," and would "encrypt and transmit the...payment credential" to the remote server. USAA-1013, 3:3-25, 9:55-10:16, 11:10-29, FIG. 2; USAA-1010, 11:62-12:21, 12:22-43; USAA-1003, ¶126.

A POSITA would have been motivated to enhance Mardikar-318's system based on Chhabra in this and other ways because doing so would provide the user with a more convenient and secure process for completing web-based financial transactions, among additional advantages, including:

1. Securely and conveniently sending user credentials for SP login. USAA-1013, 1:31-33, 7:65-10:55, FIGS. 4, 5; USAA-1010, 4:9-11, 6:13-29, FIGS. 4, 5a, 5b; USAA-1003, ¶¶127-128.
2. Securely and conveniently sending payment information. USAA-1010, 4:9-11, 6:19-23; USAA-1013, 1:31-33, FIG. 4; USAA-1003, ¶129.

3. Enabling “a payment provider system (PP), such as PayPal” to provide secure “payment processing for online transactions,” thereby enhancing user convenience, transaction security, and overall PP utility. USAA-1010, 5:34-47, 6:19-23, FIG. 3; USAA-1013, 1:34-45, 7:65-11:29, FIGS. 4, 5; USAA-1003, ¶130.
4. Providing strong second factor authentication for web-based transactions. USAA-1010, 4:7-17, 5:34-61, FIG.3; USAA-1013, 3:26-43; USAA-1012, [0005]-[0014], [0020], [0030]-[0031]; USAA-1003, ¶¶131-132.

Moreover, configuring Mardikar-318’s systems to leverage Chhabra’s teachings would have required only routine programming knowledge that was well within the skill of a POSITA. USAA-1003, ¶133. Indeed, the change would have amounted to nothing more than the use of a known technique to improve similar devices in a similar way, and combining prior art elements according to known methods to yield the predictable results described above. *KSR*, 550 U.S. at 417; USAA-1003, ¶133; USAA-1010, 9:60-65, 10:42-12:43, FIG. 4; USAA-1013, 6:45-48, 9:32-44, 10:40-11:9, 13:58-14:24, FIGS. 3, 5. In addition, the elements of the resulting combination would each perform functions they had been known to perform prior to the combination. USAA-1003, ¶133. Accordingly, a POSITA

would have had more than a reasonable expectation of success when incorporating Chhabra's teachings into Mardikar-318. *Id.*

2. Claim 1

[1.pre]

To the extent the preamble is limiting, Mardikar-Chhabra renders obvious [1.pre]. USAA-1003, ¶229.

Mardikar-318 discloses a variety of methods for securing “financial transactions initiated from an electronic device,” including methods for authenticating a user based on “biometric information” input to the device through an included biometric sensor. USAA-1010, Abstract, 1:15-17, 3:11-33, 7:28-42, FIGS. 4, 5a, 5b, 6a; USAA-1003, ¶230.

[1.a.i]

Mardikar-318 explains that “client device 400 may be implemented as a wireless telephone.” USAA-1010, 4:7-49. For example, as shown in Mardikar-318's FIGS. 4 and 5b (below), client device 400 features a communication chip 405 that enables communication with other devices over a network. USAA-1010, 1:60-64, 4:7-49, FIGS. 3, 4, 5a, 5b; USAA-1003, ¶¶231-232.

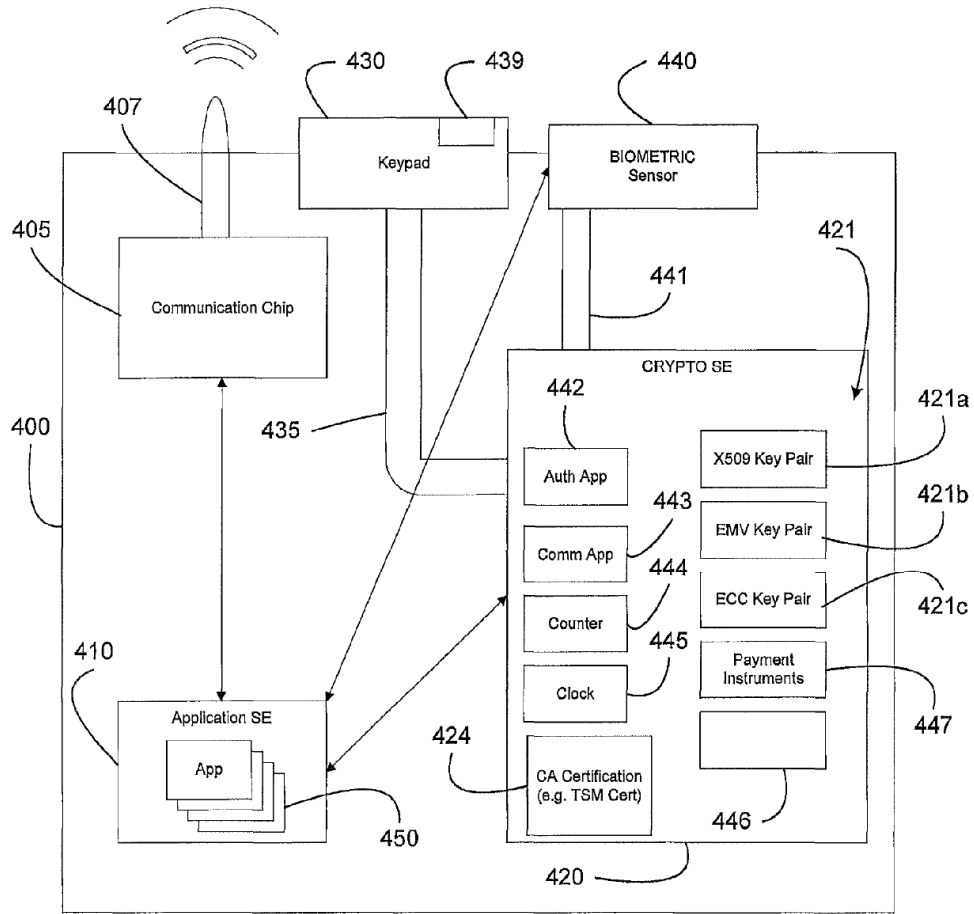


FIG. 4

USAA-1010, FIG.4

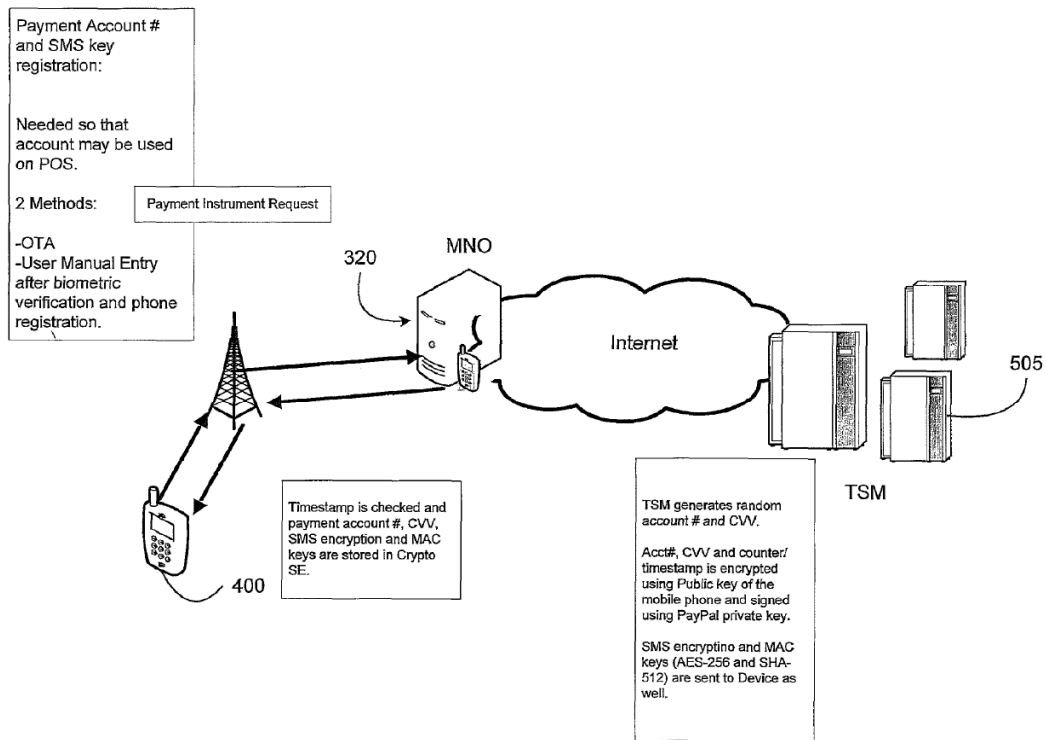


FIG. 5b

USAA-1010, FIG. 5b

A POSITA would have further understood and found obvious that device 400 includes another mobile device: Crypto SE 421, a smart card that includes a CPU, non-volatile storage, and means to “establish a direct, secure transmission” with other devices using SSL. USAA-1010, 7:28-42, 7:27-9:23, 9:66-10:4, 12:4-21, FIG. 4; USAA-1013, 5:59-7:64, FIG. 3; *see also* USAA-1017, 347-362; USAA-1003, ¶233.

A POSITA would have understood and found obvious that a biometric authentication application “on the Crypto SE 420” (“application running on a mobile device”) evaluates biometric data (“unique user input”) received from

biometric sensor 440 (“user interface associated with said application”) and, “as part of a registration or certification procedure,” generates a “biometric profile” or “biometric signature” (“secret”) from the biometric data. USAA-1010, 7:28-42, 9:60-65, 10:42-11:7; 15:54-16:45, FIGS. 4, 5a, 5b; USAA-1003, ¶234.

Mardikar-318 explains that “[r]egistration may include” unlocking “a payment credential...by registering the user’s unique biometric profile using the biometric sensor 440 (FIG. 4)...by registering a thumb-print twice....” USAA-1010, 10:47-60, 7:28-42, 15:54-16:45; USAA-1013, 7:44-51, 7:57-64, 8:33-35, 9:31-39, 9:45-50, 11:2-7, FIG.4; USAA-1003, ¶235.

For example, device 400’s user, via the biometric sensor 440 (“user interface”), communicates with the user of the client device to receive one or more unique user inputs, that the sensor captures and sends those inputs to Crypto SE 420, and that the application generates and stores the user’s unique biometric profile/signature based upon the received inputs. USAA-1003, ¶236; USAA-1010, 2:58-59, 7:28-42, 9:60-65, 10:42-11:7, 15:54-16:45, FIGS. 4, 5a, 5b; USAA-1013, Abstract, 7:44-64, 8:33-40, 9:31-39, 9:45-50, 11:2-7, FIG. 4; *see also* USAA-1011, [0040]-[0046], FIGS. 4, 5.

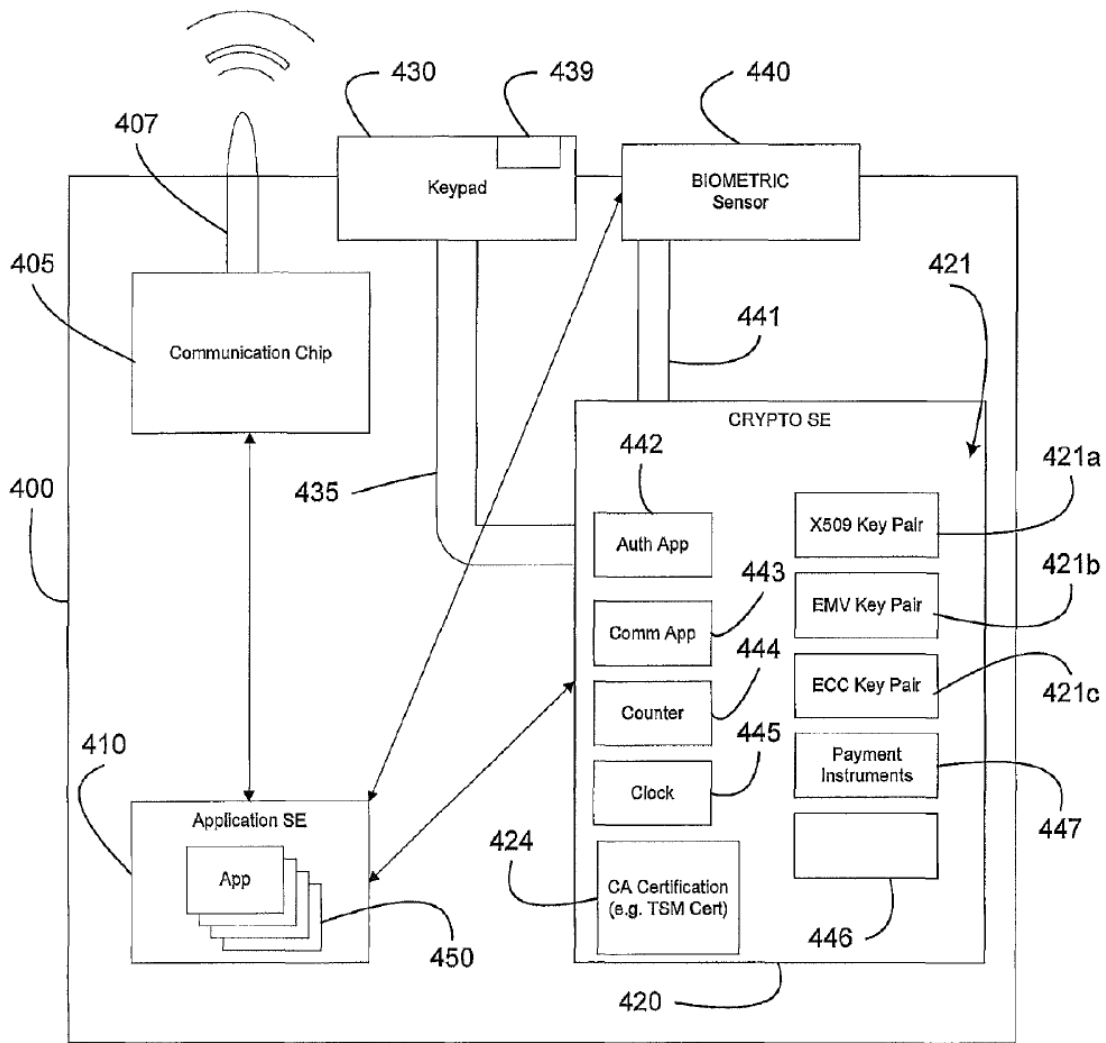
A POSITA would have understood and found obvious that Mardikar-Chhabra’s “biometric profile” is a “secret,” both because Mardikar-318 and Chhabra emphasize the importance of maintaining the security/secretcy of the

user's biometric data, and because sensitive data was commonly understood to be a type of "secret." USAA-1010, 7:28-9:23, FIG. 4; USAA-1013, 5:59-7:64, FIG. 3; *see also* USAA-1017, 136 ("we have two types of secrets: the keys and the data"), 347-362; USAA-1003, ¶237.

[1.a.ii]

A POSITA would have understood and found obvious that Mardikar-Chhabra stores the user's "biometric profile" ("secret") at Crypto SE 420 with an identifier so as to be retrievable when the user's biometric data ("unique user input") is again applied to the mobile device. USAA-1010, Abstract, 2:37-39, 7:41-43, 7:44-57, 9:36-47, 9:60-65, 10:42-11:7, FIGS. 4, 5a, 5b, 15:54-16:45; USAA-1003, ¶238.

As shown in Mardikar-318's FIG.4 (below), Crypto SE 420 is "arranged for loading and storing...unique biometric authentication information related to a specific user," for comparison to further biometric inputs. USAA-1003, ¶¶239-240; USAA-1010, 9:36-65, 10:42-11:7, 11:44-51, FIGS. 4, 5a, 5b; USAA-1013, 9:45-11:9, 7:44-56; *see also* USAA-1011, [0041]-[0046], FIG. 4.



USAA-1010, FIG. 4

Mardikar and Chhabra describe a multitude of identifiers with which the user's "biometric profile"/"reference digital templates" are stored, including user account identifiers and encryption key identifiers that the Mardikar-Chhabra system uses to retrieve the user's biometric profile for comparison during a transaction. USAA-1003, ¶241; USAA-1010, 4:58-5:2, 6:23-27 ("map the account

to an email address”); 10:26-40 (“binds public keys with respective user identities,” “public key certificates issued by the CA”), 10:41-11:7, FIGS. 5a (“TSM issues cert based on account # or for IMEI #”), 5b (“account #, CVV, SMS encryption and MAC keys are stored in Crypto SE”); USAA-1013, 2:22-34.

For example, Mardikar-318 describes the “biometric profile” “related to” the user as being generated through the registration system illustrated in Mardikar-318’s FIGS. 5a and 5b (below), which yields registration of the client device 400 (e.g., with a trusted service manager), unlocking of “a payment credential or CA certificate 424” that is “pre-loaded on the device 400,” and association of the certificate 424 with the “user account.” USAA-1010, 10:5-11:7, FIGS. 5a, 5b; USAA-1003, ¶242.

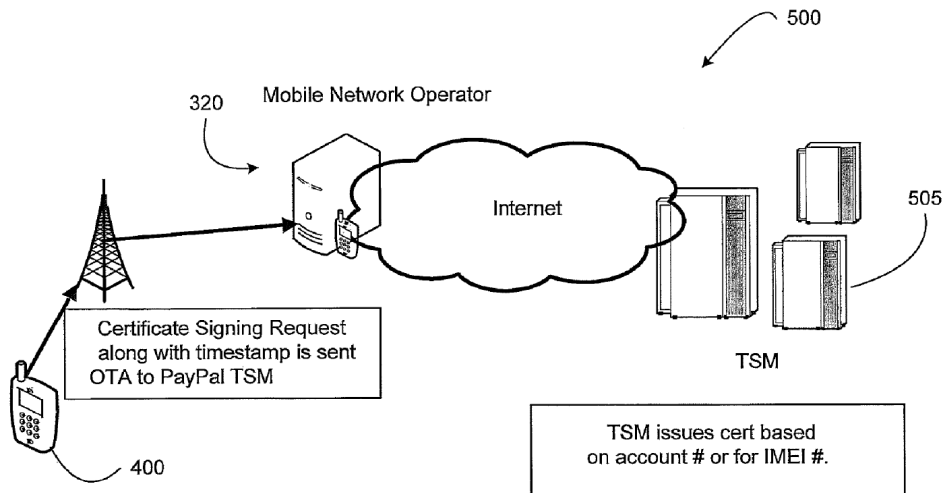


FIG. 5a

USAA-1010, FIG. 5a

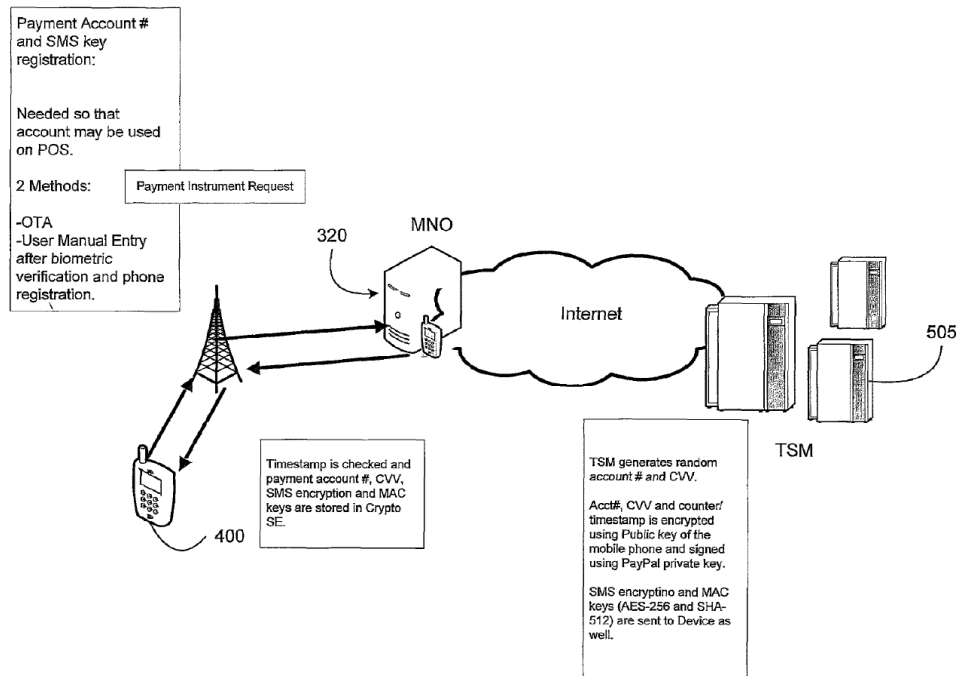


FIG. 5b

USAA-1010, FIG. 5b

For example, “a payment credential or CA certificate 424” may “be unlocked by registering the user’s unique biometric profile”; the “certificate 424 is entered and associated with...user account,” and a certificate “based on” the associated account or IMEI number is issued to device 400, which stores the “account #, CVV...encryption and MAC keys...in Crypto SE.” USAA-1010, 10:42-11:7, FIGS. 5a, 5b; USAA-1003, ¶243.

[1.a.iii]

As explained *supra* [1.a.ii], *infra* [1.b], [1.c.i], a POSITA would have understood and found obvious that the account or IMEI numbers, server name,

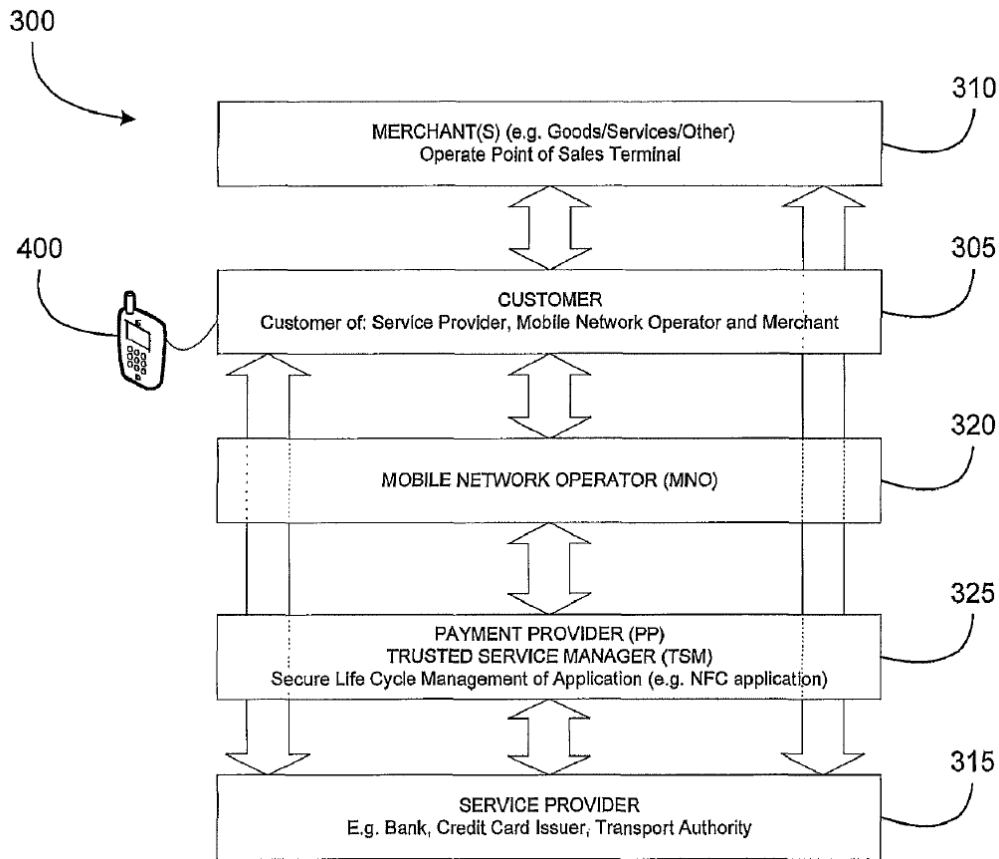
server domain, encryption keys, and MAC keys, etc., that Mardikar-Chhabra associates through registration with the “biometric profile”/“biometric signature” are identifiers that allow the profile/signature to be retrievable when the user’s biometric data (“unique user input”) is again received at client device 400 (“the mobile device”) through biometric sensor 440. USAA-1003, ¶244; USAA-1010, Abstract, 2:37-39, 7:41-43, 7:44-57, 9:36-47, 9:60-65, 10:42-11:7, 12:4-21, 15:54-16:45, FIGS. 4, 5a, 5b; USAA-1013, 2:22-34 (“fingerprint, biometric identifier”), 4:18-21, 8:22-43, 10:8-14; USAA-1016, 10, 11-17.

In that regard, Mardikar-Chhabra’s Crypto SE application verifies “that the user is authorized” to complete a given transaction through a process including “a table or database lookup, [and] fingerprint matching...” USAA-1013, 8:22-35, 9:45-64, 10:40-55, 10:65-11:9, FIGS. 4, 5; USAA-1010, 9:45-64, 11:44-51, 13:16-21; USAA-1003, ¶245.

A POSITA would have understood and found obvious that the user’s registered “biometric profile”/“biometric signature” is stored in the Crypto SE with an identifier associating the “biometric profile” with a corresponding account, including identifiers in the associated certificate 424. USAA-1003, ¶246; USAA-1010, 4:20-26, 10:42-11:7, FIGS. 5a, 5b.

Mardikar-318 further explains that a user may maintain separate accounts with each of several SPs, and register each based on unique user biometric data. USAA-1010, 2:2-3, 2:11-14, 9:53-65, 10:25-11:7, FIGS. 3, 5b; USAA-1003, ¶247.

In that regard, Mardikar-318's FIG. 3 (below) illustrates various SPs, and a POSITA would have understood and found obvious that Crypto SE would, in each registration procedure for each service provider, generate a unique "biometric profile"/"biometric signature" that would thereafter be stored in the Crypto SE with associated identifiers, so as to be retrievable when the user's biometric data is again applied in the course of a transaction. USAA-1003, ¶248; USAA-1010, 10:55-58, 2:11-14, 3:19-22, 7:27-43, 9:37-43, FIGS. 4, 5a, 5b; USAA-1013, 7:44-51.



USAA-1010, FIG. 3.

[1.b]

A POSITA would have understood and found obvious that Mardikar-Chhabra receives at device 400 (“the mobile device”) from a payment provider’s remote server (“remote computing device”) a first communication, and provides the user, via device 400, an opportunity to respond to this first communication.

USAA-1003, ¶249; USAA-1010, 6:19-29, 9:60-65, 10:42-11:7, 12:4-21, FIGS. 4, 5a, 5b; USAA-1013, 4:18-21, 8:22-43, 10:8-14, 10:40-55; USAA-1016, 10-17; USAA-1018, 33-63.

As explained above, “a user desiring to complete a financial transaction on a web site...may be automatically redirected to a payment page....” USAA-1013, 10:40-55; USAA-1003, ¶¶250-251.

Chhabra explains that the communication “between computing platform 10 and remote server 20 may utilize a secure connection such as” SSL and/or TLS, and that the client device may “encrypt and transmit” a string including the user’s credential(s) “using for example a TLS or an SSL cryptographic protocol.” USAA-1003, ¶252; USAA-1013, 4:18-21, 8:22-43, 10:8-14.

As a first step toward completing the secure SSL/TLS transaction, a POSITA would have understood and found obvious that the Mardikar-Chhabra client and remote server would engage in an SSL “handshake,” during which the client would receive a message (“first communication”) from the server including the server’s certificate. USAA-1003, ¶253; USAA-1010, 12:4-21, 10:65-67; USAA-1013, 4:18-21, 8:22-43, 10:8-14; USAA-1016, 10-12, 17.

Furthermore, a POSITA would have understood and found obvious that the user, via the mobile device, is provided an opportunity to respond to the message from the server containing the server’s certificate, by verifying the received certificate against the CA certificate already stored in device 400, and upon verification, giving payment information to complete a transaction. USAA-1003,

¶254; USAA-1010, 12:4-21; USAA-1013, 4:18-21, 8:22-43, 10:8-14; USAA-1016, 10, 11-17.

[1.c.i]

A POSITA would have understood and found obvious that, in response to receiving the message from the remote server, device 400 would prompt the user to again provide their unique biometric input (“a candidate user input”) through biometric sensor 440, to authenticate the user by comparing that input against the user’s registered biometric profile, as part of the process of completing the desired financial transaction. USAA-1003, ¶¶255-261; USAA-1010, Abstract, 1:15-17, 3:11-33, 4:27-36, 6:13-29, 7:28-42, 9:60-65, 10:42-12:30, 13:37-14:19, 15:54-16:45, FIGS. 4, 5a, 5b, 6a; USAA-1013, 3:3-25, 7:44-56, 9:55-10:16, 11:10-29.

And, as explained above, Mardikar-Chhabra further enables authenticated web transactions. USAA-1003, ¶¶262-266.

[1.c.ii]

A POSITA would have understood and found obvious that device 400 verifies the user to the remote server in a second communication (containing payment information to complete a transaction) encoded using the biometric profile (“secret”), and the remote server that sends the first communication including the server’s certificate would be the same remote server that receives the second communication. USAA-1003, ¶267; USAA-1010, 4:20-21, 5:48-51, 5:65-

6:1, 6:19-29, 9:60-65, 10:42-11:7, 12:4-21, FIGS. 3, 4, 5a, 5b; USAA-1013, 4:18-21, 8:22-43, 10:8-14, 10:40-55; USAA-1016, 10-17.

For example, Mardikar-318 explains that a trusted service manager may additionally “act as a payment provider system (PP), such as PayPal...” USAA-1010, 6:13-29, 4:20-21, 5:48-51, 5:65-6:1, FIG. 3; USAA-1003, ¶¶268-269.

A POSITA would have accordingly understood and found obvious that a single remote server operated by, e.g., PayPal, would advantageously/efficiently perform the processes described by Chhabra with respect to both the “remote server 20” and the “database server 30.” USAA-1010, 4:20-21, 5:48-51, 5:65-6:1, 6:19-29, 9:60-65, 10:42-11:7, FIGS. 3, 4; USAA-1013, 7:65-11:29, FIGS. 1, 4, 5; USAA-1003, ¶270.

More, a POSITA would have understood and found obvious that, to complete the desired transaction through a secure SSL connection, the client would earlier have to establish that connection to the server through the SSL handshake. USAA-1003, ¶271; USAA-1010, 4:20-21, 5:48-6:29, 9:60-65, 10:42-11:7, 12:4-21, FIGS. 3, 4, 5a, 5b; USAA-1013, 4:18-21, 8:22-43, 10:8-55; USAA-1016, 10-17; USAA-1018, 33-63.

Regarding the second communication being encoded using the secret, a POSITA would have understood and found obvious that the Crypto SE application would “encrypt and transmit the requisite http request string and payment

credential over the public network” upon, and as an immediate consequence of, verifying/authenticating the user based on the registered biometric profile to which the payment credential relates. USAA-1003, ¶272; USAA-1013, 8:33-49, 9:65-10:16, 11:10-29, FIGS. 4, 5; USAA-1010, 11:62-12:43, 16:33-40.

In that regard, the POSITA would have understood and found obvious that the second communication is encoded as an immediate consequence of the client device’s successful authentication check using the biometric profile, and therefore at least implicitly conveys to the remote server that the user has been authorized to proceed with the requested transaction based on the biometric profile. USAA-1003, ¶273; USAA-1010, 11:62-12:43, 16:33-40; USAA-1013, 8:33-49, 9:65-10:16, 11:10-29, FIGS. 4, 5.

Mardikar-318 further describes enabling a remote server to additionally “identify the client device and its user” through “signature” information that the client device correlates with payment information and encodes into the transmitted communication. USAA-1003, ¶274; USAA-1010, 12:22-43; USAA-1013, 7:44-56.

From this and related description, a POSITA would have understood and found obvious that the “signature information” in the transmitted second communication that is used to identify the user would be information of the user’s registered biometric profile, which could then be used by the TSM for fraud

detection as described by Mardikar-318. USAA-1003, ¶275; USAA-1010, 11:62-14:19; USAA-1012, Abstract, FIG. 2, [0029]-[0033]; USAA-1014, [0033], [0036], [0082]-[0085].

Indeed, Mardikar-318 interchangeably refers to the registered user authentication data as a “biometric profile”/“biometric signature,” and a POSITA would have found obvious that storage of “biometric profile”/“biometric signature” information at the remote server would enable the server to compare the “biometric signature” information transmitted by the client device to the “biometric signature” information stored by the server, for purposes of further authentication/security (“verifying said user to the remote computing device”). USAA-1003, ¶276; USAA-1010, 7:28-43, 10:5-11:7, 12:31-43, 15:54-16:50, FIGS. 5a, 5b; USAA-1012, Abstract, FIG. 2, [0029]-[0033]; USAA-1013, 7:44-56; USAA-1014, [0033], [0036], [0082]-[0085].

In that regard, a POSITA would have understood and found obvious that the second communication is encoded using the biometric profile, at least because²

² To the extent that a POSITA would have understood the recited ’689 patent’s “a second communication encoded using said secret” language to encompass a second communication that is encoded as an immediate consequence of a process using

information about (i.e., an encoding of) the biometric profile (i.e., the secret) is included in the second communication. USAA-1003, ¶¶277-286.

3. Claim 2

[2]

Mardikar-318 describes binding “public keys with respective user identities by means of a certificate authority (CA)” through a “registration and issuance process” by which “the user identity, the public key, their binding, validity conditions and other attributes are made unforgeable in public key certificates issued by the CA.” USAA-1010, 10:26-40; USAA-1003, ¶¶287-288.

A POSITA would have understood and found obvious to bind the user’s public key (“encryption key”) with their unique user identity based on the user’s unique biometric profile, which is already generated by the client device and

the secret, and/or that is encoded to implicitly convey information based on the secret, Mardikar-Chhabra additionally renders that language obvious in view of Mardikar-Chhabra’s encoding of a message as an immediate consequence of the successful authentication check, and in view of that message at least implicitly conveying that the user has been authorized using the biometric profile. USAA-1003, ¶277; USAA-1010, 11:62-12:43, 16:33-40; USAA-1013, 8:33-49, 9:65-10:16, 11:10-29, FIGS. 4, 5.

registered with the CA as part of the same registration process. USAA-1003, ¶289; USAA-1010, 9:60-65, 10:26-11:7, FIGS. 5a, 5b.

More, a POSITA would have found it obvious to generate the user's key-pair based on the user's unique biometric profile during the registration process for a given SP, and to store the same together in the Crypto SE, as doing so would provide an efficient, secure, and convenient means of implementing related teachings. USAA-1003, ¶¶290-292; USAA-1010, 7:28-42, 9:37-46, 13:56-59, 10:26-14:19, FIGS. 5a, 5b; USAA-1014, [0008], [0033]-[0036], [0043], [0081]-[0085], [0117], FIGS. 2, 6, 10, USAA-1015, [0007]-[0009], [0016]-[0017], [0024], FIGS. 1, 1A, 3; USAA-1019, §7.1.

The resulting stored secret would include both the biometric profile and the generated key-pairs. USAA-1003, ¶293; USAA-1010, 7:28-9:23, FIG. 4; USAA-1013, 5:59-7:64, FIG. 3; USAA-1017, 136.

4. Claim 3

[3]

As discussed *supra* [2], Mardikar-Chhabra's secret comprises an encryption key. A POSITA would have understood and found obvious that this secret comprises a static portion and a dynamic portion, at least insofar as Mardikar-318 explains that "[a] random counter," and/or "[t]imestamps may be used to prevent

replays” and “[k]eys may be rotated periodically using the SMS key establishment scheme.” USAA-1003, ¶294; USAA-1010, 10:2-4, 10:65-11:16, 14:17-19.

As explained *supra* [1.c.ii], the second communication (message to remote server containing payment information) is encoded using the secret, a POSITA would have understood and found obvious that a counter, a timestamp, and keys periodically rotated, are used in encoding the second communication, and thus are considered a dynamic portion of the secret, where the biometric profile comprises a static portion. USAA-1003, ¶295; USAA-1012, Abstract, [0011]-[0013], [0029], [0031]-[0033], [0039]-[0041], FIG. 2.

5. Claim 4

[4]

As discussed at [1.b]-[1.c], Mardikar-Chhabra’s client device receives a first communication from the remote server including the server’s certificate as part of the SSL handshake and, after establishing a secure SSL channel, the client sends a second communication to the server including payment information, among other credentials. USAA-1003, ¶296.

A POSITA would have understood and found obvious that the first communication includes a request for user credentials of the user of the client device for at least two reasons: (1) because the following steps in the SSL handshake involve the client device sending its certificate to the server; and (2)

because the first communication is part of a process of establishing a secure SSL channel for the transmission, by the client device to the server, of “payment information” including additional user credentials. USAA-1003, ¶297; USAA-1010, 12:4-26; USAA-1016, 10-17; USAA-1018, 33-63. Indeed, Chhabra expressly describes that the remote server sends a request for the user to provide user credentials “as required to complete the financial transaction...” USAA-1013, 10:40-55, Abstract, 2:22-34, 3:3-14, 3:26-31, 11:11-16, FIGS. 4, 5.

6. Claim 6

[6]

A POSITA would have understood and found obvious that the user’s unique biometric input is/includes user credentials. USAA-1003, ¶¶298-299; USAA-1010, FIG. 6b, 11:44-55; USAA-1013, 2:22-28, 5:60-64, 6:38-45, 7:44-48, 7:57-64, 9:31-39, 11:2-9, FIG. 3.

7. Claim 7

[7]

As explained *supra* [1], the first communication is received by the client device from the remote server as part of the SSL handshake that establishes the secure channel through which the client device sends the second communication, with both communications occurring in the context of the same web-based transaction (“two related communications of a communication session”). USAA-

1003, ¶¶300; USAA-1010, 6:19-29, 9:60-65, 10:42-11:7, 12:4-21, FIGS. 4, 5a, 5b;
USAA-1013, 4:18-21, 8:22-43, 10:8-55; USAA-1016, 10-17; USAA-1018, 33-63.

**D. GROUND 2B – Mardikar-318, Chhabra, and Duffy Render
Claims 1-21 Obvious**

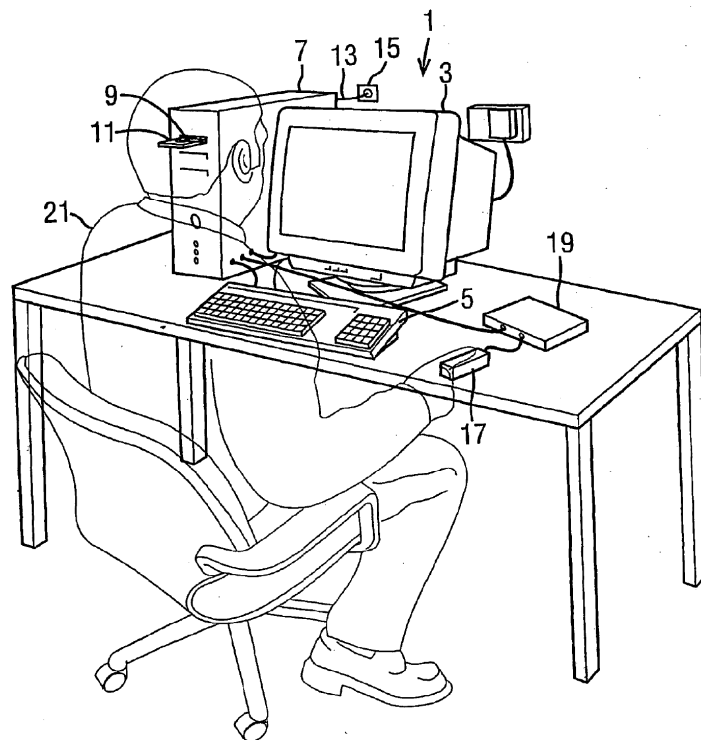
1. Prior Art and Proposed Combination

(a) *Duffy*

Duffy describes “a computer system including a fingerprint sensor and a
cryptography unit” that generates “a cryptographic key” “using biometric data....”

USAA-1014, Abstract, [0001], [0015], [0029], [0088], FIG. 1. USAA-1003,
¶¶134-146.

Fig. 1



USAA-1014, FIG. 1

Duffy teaches mitigating system vulnerabilities associated with storage of cryptographic keys by storing a combination of (1) an intermediate key (“biometric value K_{bio} ”) (reflecting a post-enrollment biometric capture) with (2) a “mapping key K_{map} ” (generated during biometric enrollment), without keeping a permanent record of the private key, which can be regenerated whenever needed by combining the biometric value and the mapping key. USAA-1014, Abstract, [0003], [0008], [0031]-[0044], [0081], [0113], [0117], FIGS. 2, 5, 6.

(b) *Mardikar-Chhabra-Duffy*

A POSITA would have been motivated to integrate Duffy’s technology into Mardikar-Chhabra’s system, including the use of K_{map} , to further enhance Mardikar-Chhabra’s security associated with a user’s private keys by regenerating an entire key whenever needed, while permanently storing the K_{map} portion generated during the enrollment/registration process, thereby reducing the ability of malicious actors to compromise the user’s cryptographic engine. USAA-1003, ¶147; USAA-1014, [0088].

For example, Mardikar-Chhabra-Duffy would generate a “mapping key” from a combination of a biometric value (e.g., Mardikar-Chhabra’s biometric signature/profile) with a private key, storing the mapping key locally (e.g., in Crypto SE), and only forming the entire private key whenever needed, based on the mapping key (K_{map}) and the biometric value. USAA-1003, ¶¶148-152; USAA-

1010, 7:26-51, 10:54-62; USAA-1013, 2:22-28, 5:60-64, 7:44-64; USAA-1014, Abstract, [0008], [0031]-[0036], [0043]-[0044], [0113], [0117], FIGS. 2, 6, 7A, 7B, 8.

Configuring Mardikar-Chhabra's system to leverage Duffy's teachings would have required only routine programming knowledge that was well within the skill of a POSITA. USAA-1003, ¶153. Indeed, the change would have amounted to nothing more than the use of a known technique to improve similar devices in a similar way to yield the predictable results described above. *KSR*, 550 U.S. at 417; USAA-1003, ¶153-154; USAA-1010, 4:37-5:1 (client device 400), 7:27-8:47, 10:25-11:7, 11:11-14:28; USAA-1013, 5:59-7:21, 7:44-64, 7:65-10:24, 10:25-11:29; USAA-1014, [0029], [0030]-[0044], [0088].

Accordingly, a POSITA would have had a reasonable expectation of success when incorporating Duffy's teachings into Mardikar-Chhabra. *Id.*

2. Claim 1

Mardikar-Chhabra-Duffy renders claims 1-4, and 6-7 obvious for at least the same reasons discussed above in the analyses of these claims under the Mardikar-Chhabra ground. *Supra*, Ground-2A; USAA-1003, ¶¶301-303. If the Board were to require the recited "secret" appearing in [1.a.i] and [1.c.ii] to represent or include a cryptographic key, Mardikar-Chhabra-Duffy further renders obvious those limitations. As described above, Mardikar-Chhabra-Duffy generates a

modified biometric signature/profile (“secret”), that is, a mapping key, through a combination of a biometric value and a private key, in accordance with Duffy.

USAA-1003, ¶303.

Mardikar-Chhabra-Duffy also further renders obvious [1.c.ii]’s “encoded using said secret.” Specifically, Duffy describes “generat[ing] a digital signature, using the private key K_{pri} ...to authenticate the source and integrity of a message” to the remote computing device, which allows the server to execute any underlying transaction. USAA-1003, ¶304; USAA-1014, [0036], [0033], [0083]-[0085], FIG. 10.

A POSITA would have found obvious that Mardikar-Chhabra-Duffy’s message with payment credential (“second communication”) to complete a transaction is signed (“encoded”) with a digital signature, and that the private key used to create the digital signature is regenerated using the modified biometric signature/profile of the user (“using said secret”), per Duffy. USAA-1003, ¶305.

3. Claim 2

[2]

As discussed above, the modified biometric signature/profile (“secret”) is a mapping key, which is a combination of a biometric value and a private key (“comprises an encryption key”). USAA-1003, ¶306; *supra*, §III.D.1; USAA-1014, [0008], [0043], [0117], FIGS. 2, 6.

The private key is used for encryption (“encryption key”). USAA-1014, [0002], [0082]; *supra*, Ground-2A-[2]; USAA-1003, ¶307.

4. Claim 3

[3]

Mardikar-Chhabra-Duffy’s secret is a modified biometric profile/signature, which is a “mapping key” comprising a private key. *Supra*, Ground-2B, [1]-[2]. This private key is regenerated whenever needed by combining a static portion (e.g., “an ambiguity resolution vector (ARV) 65”) stored in the “non-volatile memory” (e.g., “NVRAM 41”) and a dynamic portion generated from “new biometric data corresponding to the fingerprint of the user” received and processed each time. *Id.*; USAA-1014, [0030], [0032], [0036]-[0037], [0084], [0087], FIGS. 2, 5, 6, 9; USAA-1003, ¶308.

A POSITA would have understood and found obvious that the mapping key (“secret”) itself comprises a static portion (e.g., “an ambiguity resolution vector (ARV) 65” stored in the non-volatile memory) and a dynamic portion based on “new biometric data corresponding to the fingerprint of the user” received and processed each time, in at least two ways: (1) the mapping key comprises the private key having these two portions, and (2) the mapping key would also be regenerated (and stored in short-term memory for use to regenerate the private key) each time from the static ARV and the dynamic new fingerprint input, to further

mitigate security concerns due to permanently stored secrets. USAA-1003, ¶309; *supra*, Mardikar-Chhabra-Duffy Combination.

5. Claim 5

[5]

Mardikar-318 describes encrypting its “keys,” and “keys are stored in Crypto SE.” USAA-1010, 13:54-61, FIG. 5b; USAA-1012, [0040]; USAA-1003, ¶310.

A POSITA would have understood and found obvious that Mardikar-Chhabra-Duffy’s mapping key (the modified biometric signature/profile) (“secret”), like the other “keys,” is also encrypted prior to being stored in the Crypto SE, to achieve further enhanced security. *Supra*, [1.a.ii]; USAA-1010, 13:54-61, FIG. 5b; USAA-1005, Abstract, 2:42-5:11, 4:60-65; USAA-1003, ¶311.

6. Claim 8

[8]

As discussed *supra* [1.c.i], before sending payment information to complete a transaction, the client device authenticates the user at the client device by receiving and verifying a biometric input (“a candidate user input”). A POSITA would have understood and found obvious that the received raw biometric input (“candidate user input”) is used to generate “biometric data representative of the biometric feature” (“candidate identifier”), which is compared with “the stored

biometric signature” (“the identifier”) for authentication based on “a match.”

USAA-1003, ¶312; USAA-1010, 7:28-43, 16:25-35; USAA-1013, 7:44-49.

Also discussed above (§III.D) Mardikar-Chhabra-Duffy’s modified biometric profile/signature is a mapping key (“secret”) that is recovered each time for regenerating the private key when needed, such as in signing the message ([1.c.ii]’s “second communication”) containing payment information to complete a transaction. The private key is regenerated through combining a biometric value, generated from “images of the fingerprint” captured each time, and the stored “mapping key K_{map} .” USAA-1003, ¶313; USAA-1014, [0030]-[0036], [0074]-[0085], FIG. 9.

A POSITA would have understood and found obvious that in order to regenerate the private key for signing the message containing payment information, Mardikar-Chhabra-Duffy’s client device first generates a “biometric data representative of the biometric feature” (“candidate identifier”) using the received raw biometric input (“candidate user input”), and recovers from the Crypto SE the modified biometric signature/profile (“secret”), which is a mapping key, if there is “a match of the biometric data with the stored biometric signature” (“if the candidate identifier matches the identifier”). The recovered modified biometric signature/profile (aka mapping key) is then combined with a biometric

value also generate from the raw biometric input, to regenerate the private key, per Duffy. USAA-1003, ¶314; USAA-1010, 7:28-43, 16:25-35; USAA-1013, 7:44-49; USAA-1014, [0030]-[0044], [0074]-[0087], FIGS. 9-11.

7. Claim 9

[9.pre]

Supra, [1.a.i] (Ground-2A).

[9.a]

Mardikar-318 explains that Crypto SE, a “smart card” that “contain[s] a CPU and some non-volatile storage,” both performs “its own cryptographic operations” and, also includes means to “establish a direct, secure transmission between the Crypto SE” and other devices using SSL. USAA-1010, 7:28-9:23, 9:60-10:4, 12:4-21, FIG. 4; USAA-1013, 5:59-7:64, FIG. 3; USAA-1017, 347-362; USAA-1003, ¶316.

For example, Mardikar-318’s FIG. 4 (below) illustrates “a biometric authentication application” 442 that “reside[s] on the Crypto SE 420...” USAA-1010, 7:44-63, 9:60-65, FIG. 4; USAA-1003, ¶317.

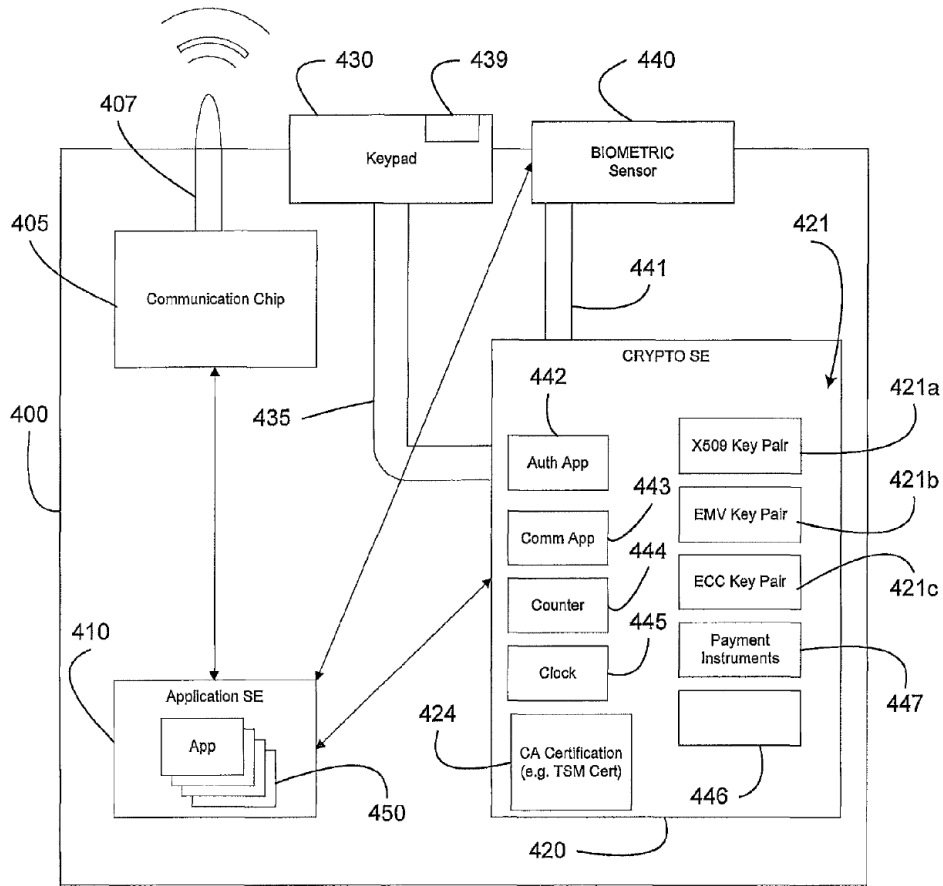


FIG. 4

USAA-1010, FIG. 4

Accordingly, a POSITA would have understood and found obvious that the mobile device includes a processor, a storage device, and a memory communicatively coupled to the processor, that the memory stores the authentication application (“processor-executable instructions”) for execution by the processor, and that the authentication application, when executed by the

processor, causes the processor to perform the authentication, cryptographic, and communication operations involved in enabling a secure web-based transaction.

USAA-1003, ¶318; USAA-1010, Abstract, 2:37-41, 14:51-15:41, FIG. 4; USAA-1012, [0037]; USAA-1013, 4:41-5:9, 12:30-37, 14:29-15:41, FIG. 3; USAA-1014, FIG. 6, [0017]-[0018], [0034].

[9.b]

Supra, [1.a.i], [1b], [1.c] (Grounds-2A-2B). A POSITA would have understood and found obvious that Mardikar-Chhabra-Duffy's authentication application on the client device communicates with a user (e.g., in collecting user's biometric input) via a biometric sensor ("user interface") and with a remote server ("at least one remote computer-based station"), e.g., at registration with the remote server and during a transaction. USAA-1003, ¶319; USAA-1010, 9:60-65.

[9.c.i]

Supra, [1.a.i] (Grounds-2A-2B).

[9.c.ii]

Supra, [1.a.ii] (Grounds-2A-2B).

[9c.iii]

Supra, [1.a.iii] (Grounds-2A-2B).

[9.d]

Supra, [1.b] (Grounds-2A-2B).

[9.e.i]³

Supra, [1.c.i], [8] (Grounds-2A-2B).

[9.e.ii]

Supra, [8] (Ground-2B).

[9.f]

Supra, [1.c.ii] (Grounds-2A-2B).

8. Claim 10

[10]

Supra, [2], [9] (Grounds-2A-2B).

9. Claim 11

[11]

Supra, [3], [9] (Grounds-2A-2B).

10. Claim 12

[12]

Supra, [4], [9] (Grounds-2A-2B).

11. Claim 13

[13]

Supra, [5], [9] (Ground-2B).

³ The “proffered user input” of [9.e.i] corresponds to the “candidate user input” of [1.c.i].

12. Claim 14

[14]

Supra, [6], [9] (Grounds-2A-2B).

13. Claim 15

[15]

Supra, [7], [9] (Grounds-2A-2B).

14. Claim 16

[16.pre]

A POSITA would have understood and found obvious that Mardikar-Chhabra-Duff's Crypto SE applications (e.g., the authentication application) are processor-executable instructions stored on a non-transitory computer-readable medium, at least insofar as Mardikar-318 describes its Crypto SE as comprising a "computer-readable medium having...instructions for generating a secure payment information message." USAA-1010, Abstract, 2:37-41, 14:51-15:41; USAA-1012, [0037]; USAA-1013, 4:41-5:9, 12:30-37, 14:29-15:41 ("processor [] executing one or more sequences of one or more instructions contained in a system memory component"), FIG. 3; USAA-1014, FIG. 6, [0017], [0018], [0034]; *sura*, [9.a]; USAA-1003, ¶¶333-334.

A POSITA would have also understood and found obvious that when executed by a processor, the instructions (e.g., in the form of the authentication

application) stored on the non-transitory computer-readable medium of the Crypto SE cause the processor to perform steps of the remaining elements of the claim.

Id.

[16.a]

Supra, [9.a]-[9.b], [16.pre]. A POSITA would have understood and found obvious that the Crypto SE, having authentication application running thereon, a “smart card” that “contain[s] a CPU” (“processor”), is a processor-based platform. USAA-1003, ¶335.

[16.b.i]

Supra, [1.a.i] (Grounds-2A-2B).

[16.b.ii]

Supra, [1.a.ii], [9.a], [16.pre]-[16.a] (Grounds-2A-2B).

[16.b.iii]

Supra, [1.a.iii] (Grounds-2A-2B).

[16.c]

Supra, [1.b] (Grounds-2A-2B).

[16.d.i]

Supra, [1.c.i] (Grounds-2A-2B).

[16.d.ii]

Supra, [8] (Ground-2B).

[16.e]

Supra, [1.c.ii] (Grounds-2A-2B).

15. Claim 17

[17]

Supra, [2], [16] (Grounds-2A-2B).

16. Claim 18

[18]

Supra, [3], [16] (Grounds-2A-2B).

17. Claim 19

[19]

Supra, [4], [16] (Grounds-2A-2B).

18. Claim 20

[20]

Supra, [5], [16] (Ground-2B).

19. Claim 21

[21]

Supra, [6], [16] (Grounds-2A-2B).

IV. 314(a)

Consistent with Congressional intent and the goals of *Fintiv*, USAA respectfully asks the Board to reach the merits of the challenges raised herein,

which are both compelling and supported by substantial evidence including Dr. Nielson's robustly corroborated testimony. *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11, 6 (PTAB Mar. 20, 2020)(precedential)("Fintiv"). USAA respectfully submits that this evidence, if unrebutted at trial, would compel a conclusion that the Challenged Claims are unpatentable, which would go far toward efficiently resolving a dispute that would otherwise continue to interfere with USAA's mission of providing services to past and present members of the U.S. Armed Forces and their families.

Moreover, as demonstrated below, the *Fintiv* factors favors institution.

Factor 1 is neutral; neither party has requested a stay in co-pending litigation. The Board has indicated that it "will not attempt to predict" how a district court might adjudicate a future motion to stay, if/when filed. *Fintiv*, 12; *Sand Revolution II, LLC v. Cont'l Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24, 7 (PTAB Jun. 16, 2020)("Sand Revolution")(informative); *Sotera Wireless Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12, 14 (PTAB Dec. 1, 2020)("Sotera")(precedential).

Factor 2 strongly favors institution. Based on PACid's 3/27/2024 filing date, an average time-to-trial of 33.9 months, and the 18-month IPR schedule, the Board is expected to issue its FWD in October 2026, three months ahead of the statistically-indicated January 2027 district court trial date. USAA-1020, 30;

USAA-1022, 37. Moreover, the District Court only just resolved a motion to dismiss with the case effectively stayed during its pendency, so any reasonable time-to-trial estimation cannot be calculated from Patent Owner's original complaint.

Factor 3 strongly favors institution; Petitioner filed this Petition immediately after the Court's 2/28/2025 denial of a motion to dismiss. By any objective standard, Petitioner filed this petition at an early stage of the litigation, which "weigh[s] against exercising the authority to deny institution under *NHK*." *Apple Inc. v. SEVEN Networks, LLC*, IPR2020-00255, Paper 13, 11-12 (PTAB Jul. 28, 2020)(quoting *Fintiv*, 11). The parties have yet to file infringement contentions, invalidity contentions, or claim construction briefs; no scheduling order has been entered and discovery has not begun.

While neither party has expended significant resources in litigation, USAA has invested substantial resources in this Petition, and those resources would be irretrievably lost if the Board declined to consider the Petition's merits. Institution and resolution of the Petition's grounds through IPR would potentially allow the parties to forego extensive expenses in co-pending litigation for which significant milestones remain. *See SEVEN Networks*, 12-15.

Factor 4 strongly favors institution; Patent Owner's complaint only alleges infringement of claims 1-2 and 4-8, while this Petition challenges claims 1-21.

USAA-1020, 17-19. Accordingly, a material number of Challenged Claims will likely be unaddressed in the litigation. *See SEVEN Networks*, 15-20.

Factor 5 should, at worst, be neutral. The parties in the parallel litigation are the same, but the *Fintiv* decision says nothing about weighing Factor 5 in favor of denial when the petitioner and the defendant are the same; *Fintiv* instead notes that “if a petitioner is unrelated” the Board has weighed that “fact against exercising discretion to deny institution.” *Fintiv*, 13-14; *see also Snap, Inc. v. SRK Technology LLC*, IPR2020-00820, Paper 15 at 16 (Oct. 21, 2020)(“*Snap*”)(precedential).

Factor 6 strongly favors institution. The strength of the merits alone outweighs any potential inefficiencies. *Fintiv*, 14-15 (noting under Factor 6 that “if the merits of a ground raised in the petition seem particularly strong ... institution of a trial may serve...overall system efficiency and integrity”).

More, USAA is one of the cutting-edge American-tech companies central to the Administration’s innovation agenda, having been granted more than 1,700 patents.⁴ USAA offers competitively-priced insurance products and brings innovative financial services to America’s service members (“America’s digital

⁴ United Services Automobile Association Patents – Key Insights and Stats, (accessed Mar. 25, 2025), available at: <https://insights.greyb.com/usaa-patents/>.

economic dominance is driven by cutting-edge American tech companies, and the American innovation and workers behind them”).⁵ In delivering these services, USAA employs around 37,000 people proudly supporting those who serve.⁶ Granting this petition increases the opportunity for USAA to continue delivering innovative services to its customers.

With Factors 2-4 and 6 disfavoring denial and Factors 1 and 5 neutral, discretion should not be exercised to deny institution. *Fintiv*, 19.

V. CONCLUSION AND PAYMENT OF FEES

The Challenged Claims are unpatentable. Please charge fees to Deposit Account 06-1050.

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

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

Petitioner, USAA Federal Savings Bank is the real party-in-interest.

⁵ Fact Sheet: President Donald J. Trump Issues Directive to Prevent the Unfair Exploitation of American Innovation (accessed Mar. 25, 2025), available at: <https://www.whitehouse.gov/fact-sheets/2025/02/fact-sheet-president-donald-j-trump-issues-directive-to-prevent-the-unfair-exploitation-of-american-innovation/>

⁶ About USAA: Serving Those Who Serve (accessed Mar. 25, 2025), available at: <https://www.usaajobs.com/about-usaa>

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

Petitioner is not aware of any disclaimers, reexamination certificates or petitions for inter partes review for the '689 Patent. The '689 Patent is the subject of a number of civil actions including: *PACid Technologies, LLC v. USAA Federal Savings Bank*, 1-24-cv-00321 (WDTX), filed March 27, 2024; *PACid Technologies, LLC v. PNC Bank, NA f/k/a BBVA USA*, 1-24-cv-00271 (WDTX), filed March 12, 2024; *PACid Technologies, LLC v. Citibank NA*, 1-24-cv-00272 (WDTX), filed March 12, 2024; *PACid Technologies, LLC v. Bank of America Corporation et al.*, 1-23-cv-00607 (WDTX), filed May 30, 2023; *PACid Technologies, LLC v. Bank of America Corporation et al.*, 1-23-cv-00251 (WDTX), filed March 7, 2023; *PACid Technologies, LLC v. Gemalto, Inc.*, 6-19-cv-00154 (WDTX); filed February 14, 2019; and *PACid Technologies, LLC v. Samsung Electronics Co., Ltd. et al.*, 2-18-cv-00133 (EDTX), filed April 6, 2018.

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

USAA provides 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: IPR38093-0012IP1@fr.com	Jennifer J. Huang, Reg. No. 64,297 Andrew B. Patrick, Reg. No. 63,471 Thomas Rozylowicz, Reg. No. 50,620 Michael T. Zoppo, Reg. No. 61,074 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070

	Fax: 877-769-7945 PTABInbound@fr.com
--	---------------------------------------------------------------------------------

D. Service Information

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

Petitioner consents to electronic service by email at IPR38093-0012IP1@fr.com

(referencing No. 38093-0012IP1).

Respectfully submitted,

Dated March 27, 2025

/Thomas A. Rozylowicz/_____
W. Karl Renner, Reg. No. 41,265
Jennifer J. Huang, Reg. No. 64,297
Andrew B. Patrick, Reg. No. 63,471
Thomas Rozylowicz, Reg. No. 50,620
Michael T. Zoppo, Reg. No. 61,074
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2025-00752)

Attorneys for Petitioner

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 13,788 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated March 27, 2025

/Thomas A. Rozylowicz/
W. Karl Renner, Reg. No. 41,265
Jennifer J. Huang, Reg. No. 64,297
Andrew B. Patrick, Reg. No. 63,471
Thomas Rozylowicz, Reg. No. 50,620
Michael T. Zoppo, Reg. No. 61,074
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on March 27, 2025 , 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:

27571 - Ascenda Law Group, PC
2150 N First Street
Suite 420
San Jose, CA, 95131
UNITED STATES

/Anastasia Renard/
Anastasia Renard
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
renard@fr.com