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	

DECLARATION OF SETH JAMES NIELSON

I declare that all statements made herein on my own knowledge are true and that all statements made on information and belief are believed to be true, and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable under Section 1001 of Title 18 of the United States Code.

Date: 2025-03-26

By: _____
Seth James Nielson, Ph.D.

Table of Contents

I. ASSIGNMENT 4

II. QUALIFICATIONS AND BACKGROUND INFORMATION 4

III. OVERVIEW OF CONCLUSIONS FORMED 13

IV. LEVEL OF ORDINARY SKILL IN THE ART 14

V. LEGAL STANDARDS 15
- A. Terminology 15
- B. Legal Standards 15
- C. Anticipation 16
- D. Obviousness 16
- E. Technology Overview 20

VI. MATERIALS CONSIDERED 25

VII. THE ’689 PATENT 25
- A. Overview of the ’689 Patent 26
- B. Prosecution History of the ’689 Patent 26
- C. Claim Construction 26

VIII. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES 27
- A. U.S. Patent App. Pub. No. 2003/0140235 (“Immega”) 28
- B. U.S. Patent App. Pub. No. 2007/0061567 to Day et al. (“Day”) 36
- C. Immega-Day Combination 39
- D. U.S. Patent No. 6,002,770 (“Tomko”) 47
- E. Immega-Day-Tomko Combination 49
  - i. Device Components 50
  - ii. Data Encryption 52
- F. U.S. Patent No. 8,108,318 (“Mardikar ’318”) 58
- G. U.S. Patent No. 8,234,697 (“Chhabra”) 67
- H. Mardikar-Chhabra Combination 73
- I. U.S. Patent App. Pub. No. 2004/0111625 (“Duffy”) 84
- J. Mardikar-Chhabra-Duffy Combination 95

IX. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE ’689 CLAIMS UNPATENTABLE 100
- A. Ground 1A: Combination of Immega and Day Renders Obvious Claims 1-4 and 6-8 100
- B. Ground 1B – Combination of Immega, Day, and Tomko Renders Obvious Claims 5 and 9-21 125

C. Ground 2A: Combination of Mardikar ’318 and Chhabra Renders Obvious Claims 1-4 and 6-7 134
D. Ground 2B: Combination of Mardikar ’318, Chhabra, and Duffy Renders obvious Claims 1-21 177
X. CONCLUSION 195

I. ASSIGNMENT

1. I have been retained on behalf of USAA Federal Savings Bank ("USAA") to offer technical opinions related to 10,044,689 ("the '689 patent") (USAA-1001). I understand that USAA is requesting that the Patent Trial and Appeal Board ("PTAB" or "Board") to institute an *inter partes* review ("IPR") proceeding of the '689 patent.

2. I have been asked to provide my independent analysis of the '689 patent based on the prior art publications cited in this declaration.

3. I am not and never have been, an employee of USAA. I received no compensation for this declaration beyond my normal hourly compensation based on my time actually spent analyzing the '689 patent, the prior art publications cited below, and issues related thereto, and I will not receive any added compensation based on the outcome of any IPR or other proceeding involving the '689 patent.

II. QUALIFICATIONS AND BACKGROUND INFORMATION

4. I am over the age of 18 and am competent to write this declaration. I have personal knowledge, or have developed knowledge of these technologies based upon education, training, or experience, of the matters set forth herein. My qualifications are summarized here and explained in more detail in my curriculum vitae, which is attached as Appendix A to this report. Appendix A also includes a

list of my publications and the cases in which I have testified at deposition, hearing, or trial within the past four years.

5. I am the Founder and Chief Scientist of Crimson Vista, a computer security research and engineering company. Furthermore, I hold appointments at the University of Texas at Austin as an Adjunct Associate Professor in the department of Computer Science and as a Cybersecurity Fellow in the Robert Strauss Center for International Security and Law. The following paragraphs summarize my professional experience.

6. I hold a Ph.D. in Computer Science from Rice University, awarded in 2009. I also received B.S. and M.S. degrees in Computer Science from Brigham Young University in 2000 and 2004 respectively. In addition to my academic degrees, I hold a CISSP certification.

7. In terms of industry practice, I worked professionally in various engineering positions from 2000 to 2011. Employers and clients include Microsoft, Google, Metrowerks, and various smaller entities. The engineering projects included testing systems, software development kits, engineering applications, networking components, security systems, file systems, cryptography components, web components, package management, and virtual-machine-based infrastructure. I also worked with software development infrastructure such as testing systems, source code repositories, code reviews, network security

components, remote access systems, virtual private networks, routing, firewalls, webmail components, web servers, embedded devices, embedded deployment, and cross-architecture toolchains. Throughout my engineering years I wrote hundreds of thousands of lines of computer code in C++, C, Python, Perl, Java, Go, Ruby, and other languages.

8. I have provided professional services in a wide range of computer science areas from 2009 to the present. These services include forensic source code review, forensic data collection and analysis, evaluation of security and privacy, risk assessment, threat analysis, and audit and compliance. My clients have included companies of all sizes including Fortune 50 entities, Tier-1 banks, security companies, medical companies, heavy industry, insurance companies, software companies, and start-ups. I was also invited to provide some analysis for United States Department of Justice in an antitrust investigation. The technologies related to these engagements include secure email, cloud-based multimedia delivery, document signing, anti-virus and anti-intrusion, high-performance routing, networking protocol stacks in mobile devices, PBX telecommunications software, VoIP, high-frequency trading, e-commerce, antivirus, cloud systems, digital radios, mobile devices, video games, industrial controls, deep learning systems, medical software, cryptocurrency, and peer-to-peer communications.

9. In my various projects, I have investigated various cybersecurity incidents, intrusions, and compromises. My assignments include a forensic reconstruction of the intrusion, analysis of the impact, remediation, and attribution. I have identified intrusion vectors that include email, software vulnerability, poorly controls credentials, insider attacks, and so forth. These investigations made use of various professional tools and data sources from logging systems, SIEMs, and IDS/IPS components. In one instance, I identified a novel technique related to electronic document (email) modification. In addition to my work with clients, I provide training and education to professionals. These trainings, which I presented at various venues, include topics related to data security, data privacy, protecting intellectual property, Blockchain basics, and improving a company's security posture. I am also on the program committee for the International Cryptographic Module Conference (ICMC).

10. I also contribute to industry research. I was the primary investigator on a DOD-funded research project for protecting systems from Ransomware. I also am a named contributor on another research grant to Curuvar, LLC. In this partnership, I assisted in developing insider-proof systems and secure enclaves for government networks.

11. As part of contributing to the technical community, I co-founded and co-led the Crypto Done Right project. This project was originally hosted by Johns

Hopkins University and funded by a grant from Cisco. However, I transitioned the project into a completely independent non-profit entity as one of the founding directors. Crypto Done Right was designed to bridge the gap between cryptography SME's and the IT professionals that use it. This project completed its operations in 2025.

12. I also maintain ties to Academia. During the 2014-2019 time period I taught the Network Security and Advanced Network Security courses at the Johns Hopkins University. I developed my own curriculum focused on mobile code, cryptography, autonomous agents, intrusion analysis, and education psychology. I published a paper related to my curriculum in the Journal of Computer Science Education entitled, "PLAYGROUND: Preparing Students for the Cyber Battleground." From 2016-2019, I was the Director of Advanced Research Projects at the Johns Hopkins University Information Security Institute (JHUISI). During this time, I published "Potential Forensic Analysis of IoT Data: An Overview of the State-of-the-Art and Future Possibilities" in the 2017 IEEE International Conference on Internet of Things (iThings). I also published "Cracking a Continuous Flow Reactor: A Vulnerability Assessment for Chemical Additive Manufacturing Devices" in 2018 IEEE International Symposium on Technologies for Homeland Security (HST). From 2020 to the present, I have held the position of adjunct professor at the University of Texas at Austin. I have taught

the undergraduate Network Security and Privacy class in the Computer Science department. I also teach the Introduction to Cybersecurity Technology class in the Law School. I have also mentored independent study courses for Computer Science students on topics of computer security and artificial intelligence.

13. In addition to published research, I mentored capstone projects related to IDS/IPS, intrusion detection, cryptography, drone security, iOS security, BitCoin, SSL vulnerabilities, and Twitter "botnets." Many of these projects involved industry collaboration. For example, we coordinated with the company OnBoard Security to develop better security for anti-collision protocols for air traffic. I also gave a talk on "Detecting Malicious Sandboxes" at the Workshop on Defensive Deception and Trust in Autonomy, in association with the 2018 Naval Applications of Machine Learning Workshop.

14. I am also the author of two books. The first is entitled "Cryptography in Python: Learning Correct Cryptography by Example" and covers the practical implementation of a wide range of cryptography algorithms. The second book, entitled, "Discovering Cybersecurity: A Technical Introduction for the Absolute Beginner" provides a technical overview of cybersecurity basics for readers with no background in engineering or computer science.

15. Finally, I have testified in numerous expert engagements and have been qualified as an expert in court. Many of these engagements are related to my

forensic analysis, but I have also testified on matters related to patent infringement and validity, copyright, DMCA, and cybersecurity norms and industry standards.

16. My curriculum vitae, included as an appendix to this declaration, includes a list of publications on which I am a named author. It contains further details regarding my experience, education, publications, and other qualifications to render an expert opinion in connection with this proceeding.

17. In writing this Declaration, I have considered the following: my own knowledge and experience, including my work experience in the fields of cryptography and related security techniques; my experience in teaching those subjects; and my experience in working with others involved in those fields. In addition, I have analyzed the following publications and materials, in addition to other materials I cite in my declaration:

18. I have reviewed the ’689 patent (USAA-1001), and relevant excerpts of the prosecution history (USAA-1002) of the ’689 patent. Among various textbooks, documents, and publications, I have also reviewed the following prior art references:

- 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-1008 U.S. Patent No. 5,748,744 to Levy et al. ("Levy")
- 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-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-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")

19. Counsel (Fish & Richardson) has informed me that I should consider these materials through the lens of one of ordinary skill in the art related to the '689 patent at the time of the earliest possible priority date of the '689 patent, and I have done so during my review of these materials. I have been informed by Counsel to use March 25, 2009, the filing date of earliest provisional application to which priority is claimed.

20. I have no financial interest in the outcome of this proceeding. I am being compensated for my work as an expert on an hourly basis. My

compensation is not dependent on the outcome of these proceedings or the content of my opinions.

21. My opinions, as explained below, are based on my education, experience, and expertise in the fields relating to the ’689 Patent. Unless otherwise stated, my testimony below refers to the knowledge of one of ordinary skill in the art as of the earliest possible priority date. Any figures that appear within this document have been prepared with the assistance of Counsel and reflect my understanding of the ’689 Patent and the prior art discussed below.

III. OVERVIEW OF CONCLUSIONS FORMED

22. This declaration explains the conclusions that I have formed based on my analysis of all of the considered materials and my personal experience. To summarize those conclusions, based upon my knowledge and experience and my review of the prior art references listed above, I believe that:

- Ground 1A renders claims 1-4 and 6-8 obvious.
- Ground 1B renders claims 5 and 9-21 obvious.
- Ground 2A renders claims 1-4 and 6-7 obvious.
- Ground 2B renders claims 1-21 obvious.

23. In support of these conclusions, I provide an overview of the references in Section VIII and more detailed comments regarding the obviousness of claims 1-21 ("**the Challenged Claims**") of the '689 patent in Section IX.

IV. LEVEL OF ORDINARY SKILL IN THE ART

24. In my opinion, 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. 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.*

25. Based on my experiences, I have a good understanding of the capabilities of a POSITA. Indeed, I have taught, participated in organizations, and worked closely with many such persons over the course of my career. Based on my knowledge, skill, and experience, I have an understanding of the capabilities of a POSITA. For example, from my industry experience, I am familiar with what a POSITA would have known and found predictable in the art. From teaching and supervising my post-graduate students, I also have an understanding of the

knowledge that a person with this academic experience possesses. Furthermore, I possess those capabilities myself.

V. LEGAL STANDARDS

A. Terminology

26. I have been informed by Counsel and understand that the best indicator of claim meaning is its usage in the context of the patent specification as understood by one of ordinary skill. I further understand that the words of the claims should be given their plain meaning unless that meaning is inconsistent with the patent specification or the patent's history of examination before the Patent Office. Counsel has also informed me, and I understand that, the words of the claims should be interpreted as they would have been interpreted by one of ordinary skill at the time of the invention was made (not today). The '689 patent was filed Dec.12, 2017, and claims priority to provisional application 61/163,406, filed Mar. 25, 2009, which I refer to as the "Critical Date" in this proceeding. Because I do not know at what date the invention as claimed was made, if ever, I have used the Critical Date of the '689 patent as the point in time for claim interpretation purposes.

B. Legal Standards

27. I have been informed by Counsel and understand that documents and materials that qualify as prior art can render a patent claim unpatentable as being anticipated or obvious.

28. I am informed by Counsel and understand that all prior art references are to be looked at from the viewpoint of a person of ordinary skill in the art at the time of the invention, and that this viewpoint prevents one from using his or her own insight or hindsight in deciding whether a claim is anticipated or rendered obvious.

C. Anticipation

29. I understand that patents or printed publications that qualify as prior art can be used to invalidate a patent claim as anticipated or as obvious.

30. I understand that, once the claims of a patent have been properly construed, the second step in determining anticipation of a patent claim requires a comparison of the properly construed claim language to the prior art on a limitation-by-limitation basis.

31. I understand that a prior art reference "anticipates" an asserted claim, and thus renders the claim invalid, if all limitations of the claim are disclosed in that prior art reference, either explicitly or inherently (i.e., necessarily present).

D. Obviousness

32. I understand that even if a patent is not anticipated, it is still invalid if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a POSITA. I have been informed by Counsel and understand that a

claim is unpatentable for obviousness and that obviousness may be based upon a combination of references. I am informed by Counsel and understand that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. However, I am informed by Counsel and understand that a patent claim composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. I am informed by Counsel and understand that when a patented invention is a combination of known elements, a court determines whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue by considering the teachings of prior art references, the effects of demands known to people working in the field or present in the marketplace, and the background knowledge possessed by a person having ordinary skill in the art.

33. I am informed by Counsel and understand that a patent claim composed of several limitations is not proved obvious merely by demonstrating that each of its limitations was independently known in the prior art. I am informed by Counsel and understand that identifying a reason those elements would be combined can be important because inventions in many instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known. I am

informed by Counsel and understand that it is improper to use hindsight in an obviousness analysis, and that a patent's claims should not be used as a "roadmap."

34. I am informed by Counsel and understand that an obviousness inquiry requires consideration of the following factors: (1) the scope and content of the prior art, (2) the differences between the prior art and the claims, (3) the level of ordinary skill in the art, and (4) any so called "secondary considerations" of non-obviousness, which include: (i) "long felt need" for the claimed invention, (ii) commercial success attributable to the claimed invention, (iii) unexpected results of the claimed invention, and (iv) "copying" of the claimed invention by others. I have been informed by Counsel and understand that an obviousness evaluation can be based on a single reference or a combination of multiple prior art references. I understand that the prior art references themselves may provide a suggestion, motivation, or reason to combine, but that the nexus linking two or more prior art references is sometimes simple common sense. I have been informed by Counsel and understand that obviousness analysis recognizes that market demand, rather than scientific literature, often drives innovation, and that a motivation to combine references may be supplied by the direction of the marketplace.

35. I have been informed by Counsel and understand that if a technique has been used to improve one device, and a person of ordinary skill at the time of invention would have recognized that it would improve similar devices in the same

way, using the technique is obvious unless its actual application is beyond his or her skill. I have been informed by Counsel and understand that practical and common sense considerations should guide a proper obviousness analysis, because familiar items may have obvious uses beyond their primary purposes. I have been informed by Counsel and understand that a person of ordinary skill looking to overcome a problem will often be able to fit together the teachings of multiple prior art references. I have been informed by Counsel and understand that obviousness analysis therefore takes into account the inferences and creative steps that a person of ordinary skill would have employed at the time of invention.

36. I have been informed by Counsel and understand that a proper obviousness analysis focuses on what was known or obvious to a person of ordinary skill at the time of invention, not just the patentee. Accordingly, I understand that any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.

37. I have been informed by Counsel and understand that a claim can be obvious in light of a single reference, without the need to combine references, if the elements of the claim that are not found explicitly or inherently in the reference can be supplied by the common sense of one of skill in the art. I have been informed by Counsel and understand that there must be a relationship between any

such secondary considerations and the invention, and that contemporaneous and independent invention by others is a secondary consideration supporting an obviousness determination.

38. In sum, my understanding is that prior art teachings are properly combined where one of ordinary skill having the understanding and knowledge reflected in the prior art and motivated by the general problem facing the inventor, would have been led to make the combination of elements recited in the claims. Under this analysis, the prior art references themselves, or any need or problem known in the field of endeavor at the time of the invention, can provide a reason for combining the elements of multiple prior art references in the claimed manner.

39. I have been informed by Counsel and understand that, according to 35 U.S.C. §316(e), in an *inter partes* review, "the petitioner shall have the burden of proving a proposition of unpatentability," including a proposition of obviousness, "by a preponderance of the evidence."

E. Technology Overview

40. The '689 Patent describes a "security application for a computing device, e.g., a mobile phone." USAA-1001, Abstract. The '689 Patent further states that "a computing device is any physical or virtual device that may be used to perform embodiments of the invention," and "the physical device may be implemented on a general purpose computing device (i.e., a device with a

processor(s) and an operating system) such as, but not limited to, a desktop computer, a laptop computer, a gaming console, a mobile device (e.g., smart phone, a personal digital assistant, gaming device)." USAA-1001, 3:57-67. However, the '689 Patent, does not describe any particular operation of such devices, so I provide a brief overview of how a POSITA would have understood processors and operating systems to operate in conventional systems. USAA-1001, *generally*. While there are some limited exceptions (e.g., quantum computers), I further note that computing devices continue to operate as I describe below.

41. Typical processors (often referred to as Central Processing Units, or CPUs) are designed to execute instructions that are stored in memory, e.g., RAM. For example, Jobs explains that "[t]he one or more ***programs are stored in the memory*** and configured to be executed by the one or more processors," and that the processor executes a large variety of programs, e.g. "an operating system 126, a communication module (or set of instructions) 128, a contact/motion module (or set of instructions) 130, a graphics module (or set of instructions) 132, a text input module (or set of instructions) 134, a Global Positioning System (GPS) module (or set of instructions) 135, and applications (or set of instructions) 136." USAA-1032, [0012], [0115]. Similarly, Chu states that "the CPU 1710 executes instructions and manipulates data stored in the system memory." USAA-1035,

[0148]. Knaggs similarly describes how applications and data are stored in memory, explaining, "[a] program is a series of instructions that causes a computer to perform a particular task," and "[a]ctually, a computer program includes more than instructions, it also contains the data and the memory addresses that the microprocessor needs to accomplish the tasks defined by the instructions." USAA-1036, 1.

42. Many instructions executed by processors operate on data stored in memory, as Chu indicates: "the CPU 1710 executes instructions and ***manipulates data stored in the system memory***." USAA-1035, [0148] (emphasis added). For a simple operation such as "X = Y + Z," a processor would typically execute instructions that load the value (e.g., 1) at the memory location indicated by the variable Y into a first register[1]; load the value (e.g., 2) at the memory location indicated by the variable Z into a second register; add the values in the two registers; and finally store the result (e.g., 3) at the memory location indicated by the variable Z. Such instructions are computer codes in binary language (1's and 0's) that directly operate in the processor. However, the instructions are often described in assembly "language" that make the binary operations somewhat more readable for humans. For example, Knaggs describes the ARM (a type of

---

[1] A register is a high-speed memory cell.

processor) instruction set (that is, the set of operations that can be performed by the ARM processor), which include instructions such as "[t]he LDR (Load Register) instruction [which] can load a 32-bit word from memory into a register," and "the STR (Store Register) instructions [which] will store a 32-bit word from a register to memory." USAA-1036, 4, 40, 57.[2]

43. However, such memory has (and continues to have) two drawbacks: (1) it is erased when the device is powered off, so data stored in memory is lost on reboot, and (2) it is more costly per unit storage than hard disk drives. For that reason, devices typically also include storage, such as a hard disk drive, which are less expensive per unit storage and store data persistently (i.e., data are not lost during a reboot unless the disk fails). For example, Lambert states that the "hard disk drive 141 is illustrated as storing operating system 144, application programs 145, other program modules 146 and program data 14." USAA-1033, [0033]. Granito describes a "storage device 1030 [that] is capable of providing mass

---

[2] While a detailed description of assembly language (e.g., as described in Knaggs) is beyond the scope of this declaration, it is apparent that a POSITA would have understood that both programs and program data were (and are) stored in memory so they are available to the processor.

storage for the computing device 1000," and "[i]n one implementation, the storage device 1030 is a computer-readable medium." USAA-1034, [0081].

44. Since storage is substantially slower than memory, before a processor operates on data, most systems move the data from storage to memory, operate on the data, then eventually copy the results back to storage. For example, Dye describes prior art example:

> Prior art computer system architectures generally operate as follows. First, programs and data are generally stored on the hard disk 120. If a software compression application is being used, data may be stored on the hard disk 120 in compressed format. At the direction of the CPU 102, the programs and data are transferred from the hard disk 120 through the I/O subsystem controller 116 to system memory 110 via the memory controller 108.

USAA-1037, [0044].

> When the computer system desires to store or cache data on the hard disk 120 in a compressed format, the data is read by the CPU 102 and compressed by the software compression application. The compressed data is then stored on the hard disk 120. If compressed data is stored in system memory 110 which must be decompressed, the CPU 102 is required to read the compressed data, decompress the data and write the decompressed data back to system memory 110.

USAA-1037, [0046].

VI. MATERIALS CONSIDERED

45. My analysis and conclusions set forth in this declaration are based on my educational background and experiences in the field (*see* Section II). Based on my knowledge and experience, I believe that I am considered to be an expert in the field. Also, based on my knowledge and experience, I understand and know of the capabilities of persons of ordinary skill in the field around 2009, and I taught, participated in organizations, and worked closely with many such persons in the field during that time frame.

46. As part of my independent analysis for this declaration, I have considered the following: the background knowledge/technologies that were commonly known to persons of ordinary skill in this art during the time before the earliest claimed priority date for the ’689 patent; my own knowledge and experiences gained from my work experience in the field of the ’689 patent and related disciplines; and my experience in working with others involved in this field and related disciplines. In addition, I have analyzed the publications and materials listed above.

47. My analysis and conclusions set forth in this declaration are based on the perspective of a POSITA.

VII. THE ’689 PATENT

A. Overview of the ’689 Patent

48. The ’689 Patent is directed to “authenticating users” through verification of a unique user input (e.g., user credentials). USAA-1001, Title, Abstract. A security application on a computing device, such as a mobile phone, allows “generation of a secret,” “prompts, e.g., via a user interface of the mobile phone, 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.

49. As demonstrated below with respect to the applied prior art, the ’689’s claimed subject matter was conventional by the Critical Date.

B. Prosecution History of the ’689 Patent

50. During prosecution, the examiner issued a notice of allowance without a single prior art rejection against the claims, and did not consider any of the prior art or prior art combinations applied in my declaration, which as explained in more detail below render the Challenged Claims obvious.

C. Claim Construction

51. Counsel has informed me that 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. I do note that the recited term “secret” use in the ’689 Patent is consistent with its plain and ordinary

meaning. For example, Phoha defines a secret as a "quantity known only to the principals that can be used for AUTHENTICATION and encryption of information flow between them." USAA-1031, 3 (emphasis in the original). The '689 patent explains that secrets can for example be used for encryption, stating that "***secrets used for encryption in a chat session*** may be different than ***secrets used for encryption in an email communication***." USAA-1001, 10:29-31. However, consistent with the plain and ordinary meaning, the '689 indicates that while the term "secret" is broad enough to encompass an encryption key, it could alternatively or additionally encompass other forms of data. USAA-1001, 27:43-60 (independent claim 1 reciting a "secret"), 27:65-67 (claim 4, depending from claim 1, reciting that "the secret comprises an encryption key"); *see also* USAA-1017, 136 ("we have two types of secrets: the keys and the data"). Further, in the '689 patent, secrets are also known only to the principals, e.g., "[s]ecrets in the secrets file (112) are shared secrets," and "[s]hared secrets (118) correspond to ***data known only to the members of the group***." USAA-1001, 9:61-63. Further, as I explain below, the use of secret in references such as Immega and Mardikar-318 are also consistent with the plain and ordinary meaning, e.g., as stated in Phoha's definition. USAA-1004, [0034]; USAA-1010, 7:28-42; USAA-1017, 136, 347-362.

VIII. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES

A. U.S. Patent App. Pub. No. 2003/0140235 ("Immega")

52. 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]. For the method, Immega describes at least two users, referred to as the "sender" and the "receiver" (though both the sender and the receive both send and receive messages) and their respective "computers," which may be a cellular telephone or personal digital assistant. *Id.*, [0041]-[0044], [0050]-[0067].

53. Immega explains that "both the sender and the receiver [are required] to cross-enroll biometric feature sets" on "each other's computer," and their devices "must be equipped with a finger print sensor." USAA-1004, [0008]. "This allows confirmation of identity of both parties at both ends of a message exchange" and "allows user-specific encryption of messages." *Id.* The method further employs a "difference key," generated by subtracting a live-scan fingerprint feature set of a user from that user's modified enrolled fingerprint feature set, to encrypt electronic messages and other fingerprint data. *Id.*, Abstract, [0009]-[0011]. A POSITA would have understood that a "live-scan fingerprint feature set" is the result of a user scanning a finger on a finger print reader at a particular point in time.

54. In more detail, Immega describes an algorithm for generating modified enrolled fingerprint feature sets for a user, with reference to FIG. 3A (below). USAA-1004, [0044]. First, at step 300, "the centroid of the fingerprint is determined," and at step 303, a "random number is used to generate a displacement vector," which is used in step 304 "to slightly shift or displace all features of the enrolled fingerprint feature set by a random displacement vector." *Id*. This "modified enrolled fingerprint feature set is then assigned to a specific person with whom messages will be exchanged (step 308)." *Id.*

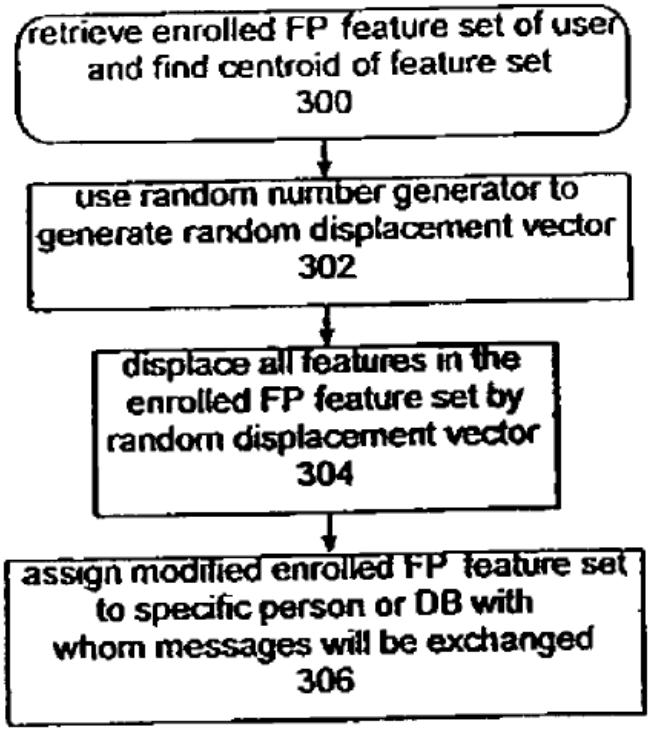


FIG. 3A

USAA-1004, FIG. 3A

55. Immega further explains that "[m]any uniquely modified enrolled feature sets, one (or more) for each person with whom messages will be exchanged, may be created and securely stored." USAA-1004, [0044]. Immega explains that "both the sender and the receiver [are required] to cross-enroll biometric feature sets" on "each other's computer." USAA-1004, [0008]. From Immega's FIG. 2 and related description, a POSITA would have understood that "cross-enrolled" indicates that information derived from the enrollment process is stored at both the sender and the receiver. USAA-1004, [0043], FIG. 2.

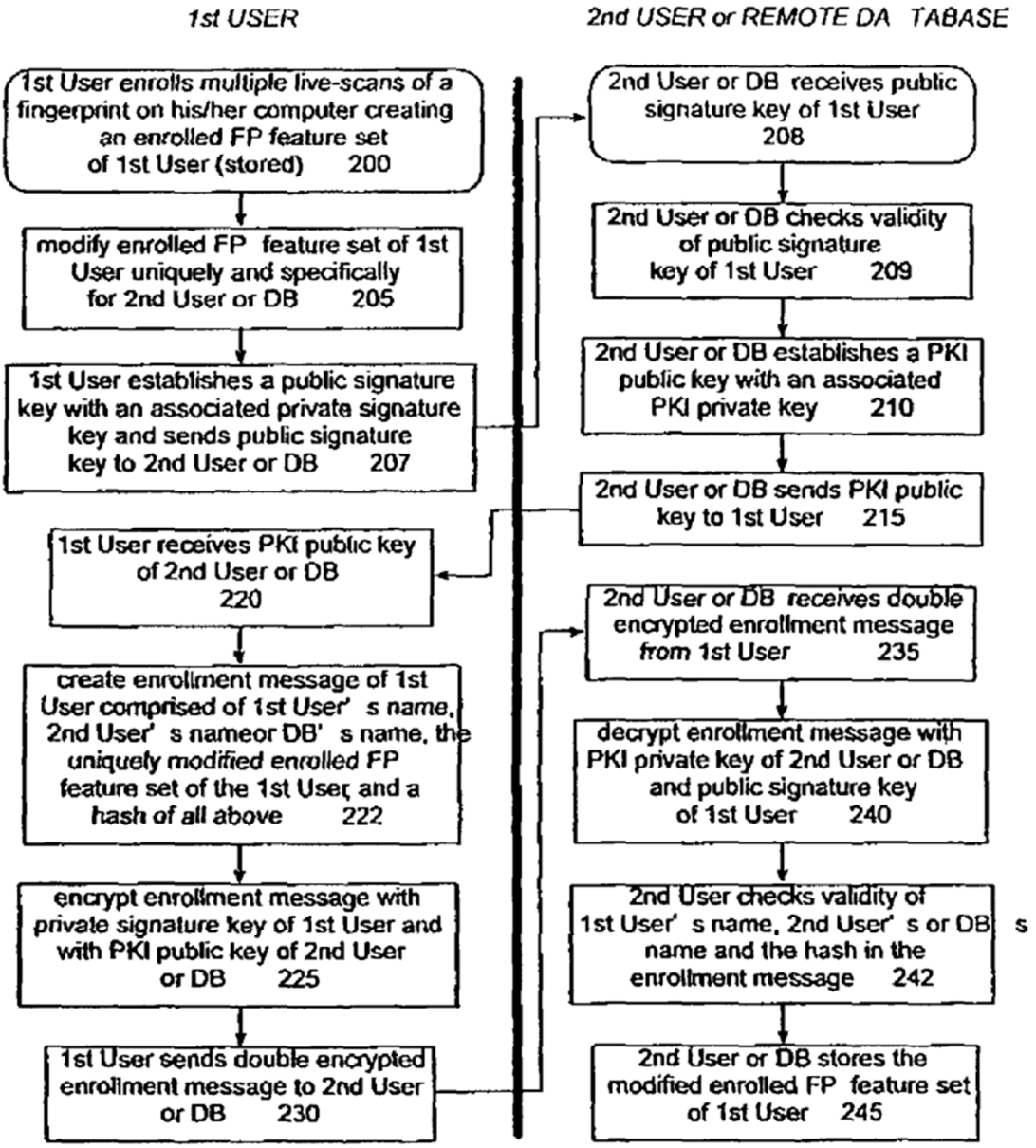
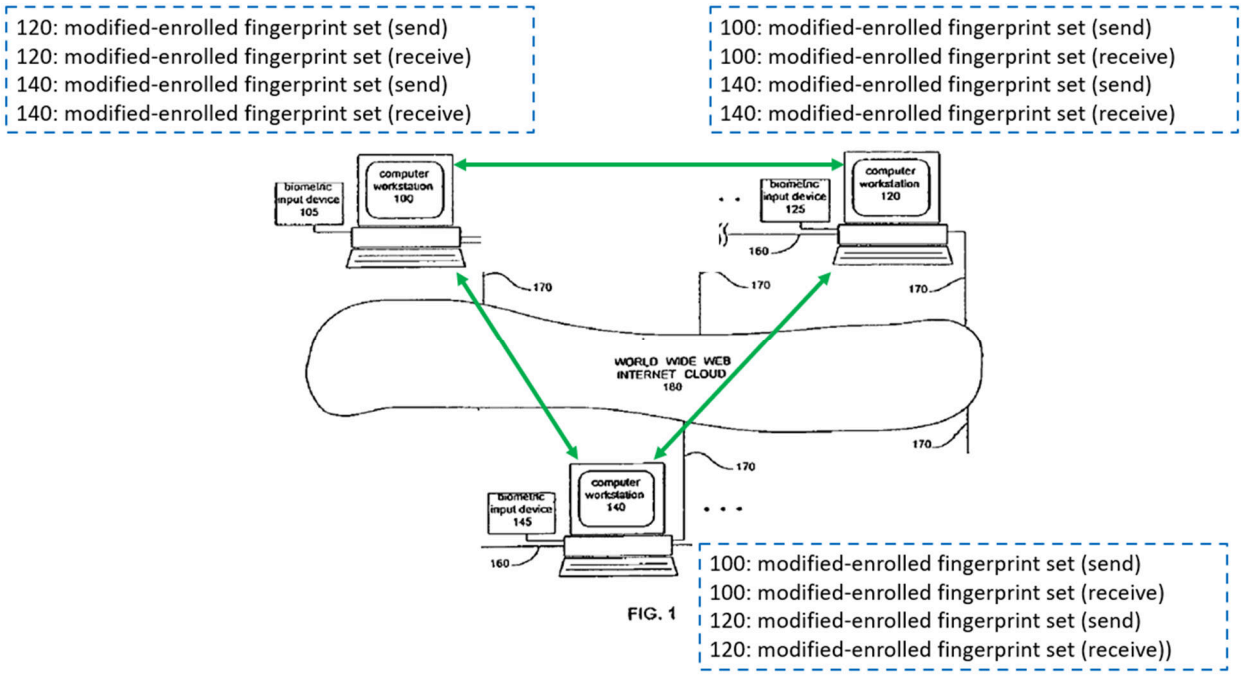


FIG. 2

USAA-1004, FIG. 2

56. Therefore, through the cross-enrollment process, a device stores, for each communication partner, the modified enrolled feature set created by the device for sending encrypted communications to a particular partner, and the

modified enrolled feature set created by the particular partner and used by the device to decrypt communications received from the partner, as I illustrate in the dotted boxes below.



USAA-1004, FIG. 1 (excerpt, annotated)

57. After users' modified enrolled feature sets are cross-enrolled, users can securely send and receive "biometrically certified message[s]," as discussed with respect to FIG. 6 (below). USAA-1004, [0063]. The algorithm of FIG. 6 includes a series of steps by which the sender and receiver both confirm their identities with one another by twice sending their respective encrypted live-scan fingerprint feature sets, which the recipient uses to compare against the stored modified enrolled feature set 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 live-scan fingerprint feature set from the receiver's modified enrolled fingerprint feature set (step 612)" and the sender similarly generates the receiver's "difference key" "by subtracting the first live-scan fingerprint feature set of the receiver from the stored modified enrolled fingerprint feature set of the receiver (step 620)." USAA-1004, [0064]-[0065]. Additionally, the sender generates the sender's "difference key" "by subtracting the second live-scan fingerprint feature set of the sender from the modified enrolled fingerprint feature set of the sender that was previously modified for the specific receiver (step 632)." USAA-1004, [0065]. The sender uses the sender's "difference key" "to encrypt the message (originally composed at step 600 by the sender) (step 634)" and "to encrypt the second live-scan fingerprint feature set of the sender (step 636)." USAA-1004, [0065]. "Finally, the sender transmits to the receiver 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), 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].

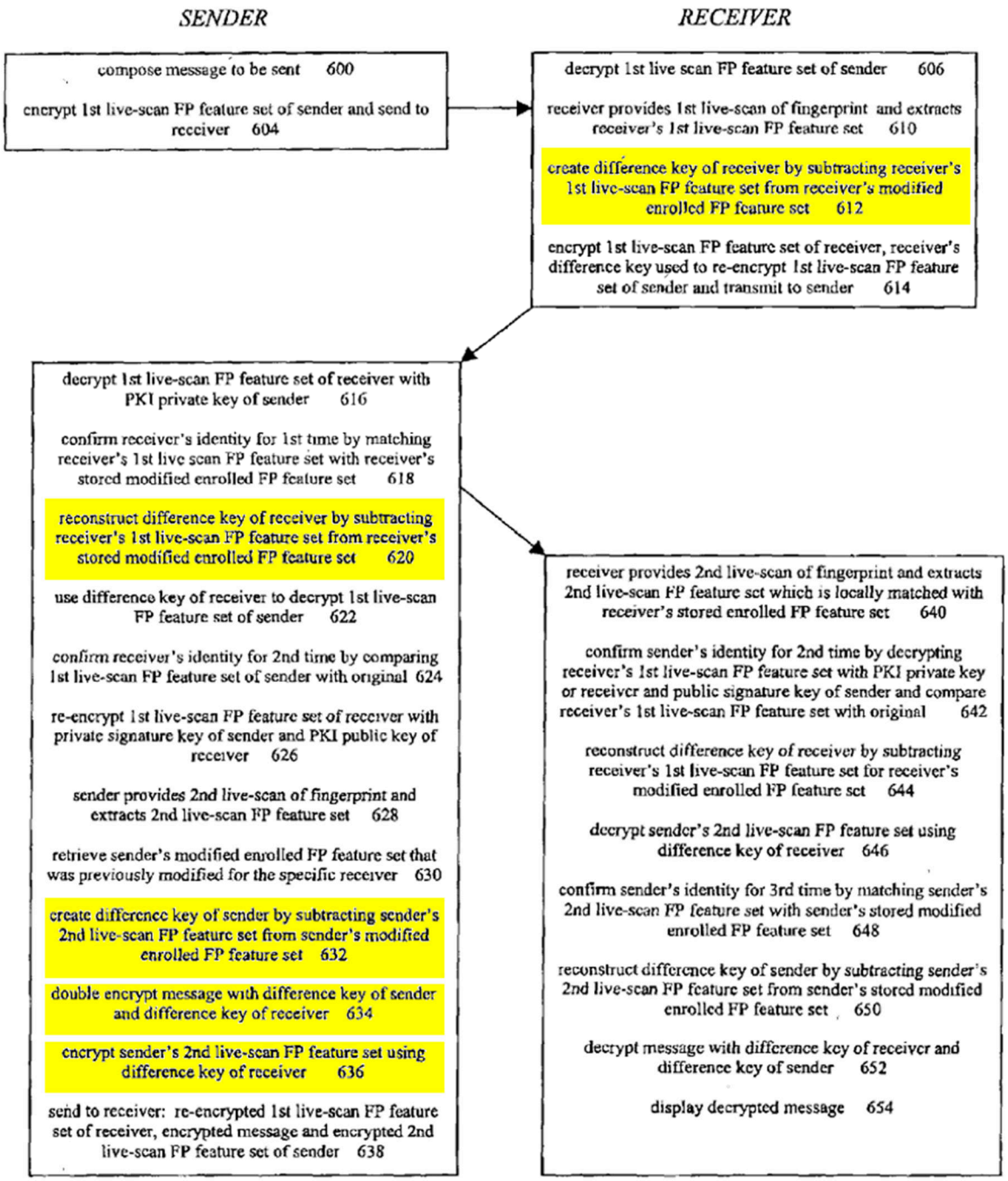


FIG. 6

USAA-1004, FIG. 6 (annotated)

58. "When the receiver receives [the] transmission, the receiver provides a second live-scan fingerprint (step 638) and extracts a second live-scan fingerprint feature set, 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) (step 640)," and the receiver generates the sender's "difference key" "by subtracting the sender's second live-scan fingerprint feature set from the sender's stored modified enrolled fingerprint feature set (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 live-scan fingerprint feature set (generated at step 640) is encrypted … and transmitted to the sender (after step 654)" for the sender to compare with the modified enrolled fingerprint feature set of the receiver. USAA-1004, [0067]. This process "enables a notification to be displayed to the sender that the message has been received and decrypted by the proper person." USAA-1004, [0067].

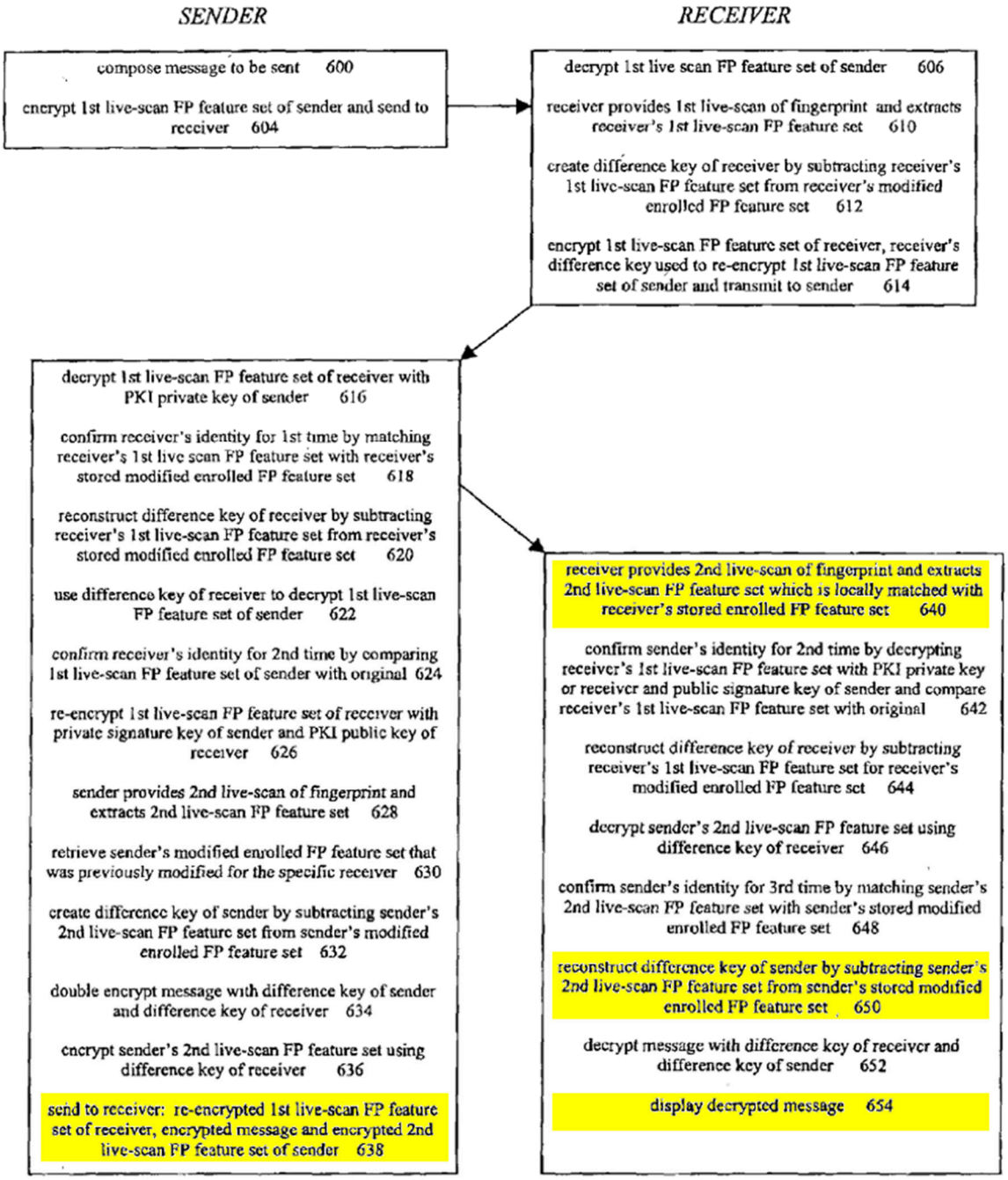


FIG. 6

USAA-1004, FIG. 6 (annotated)

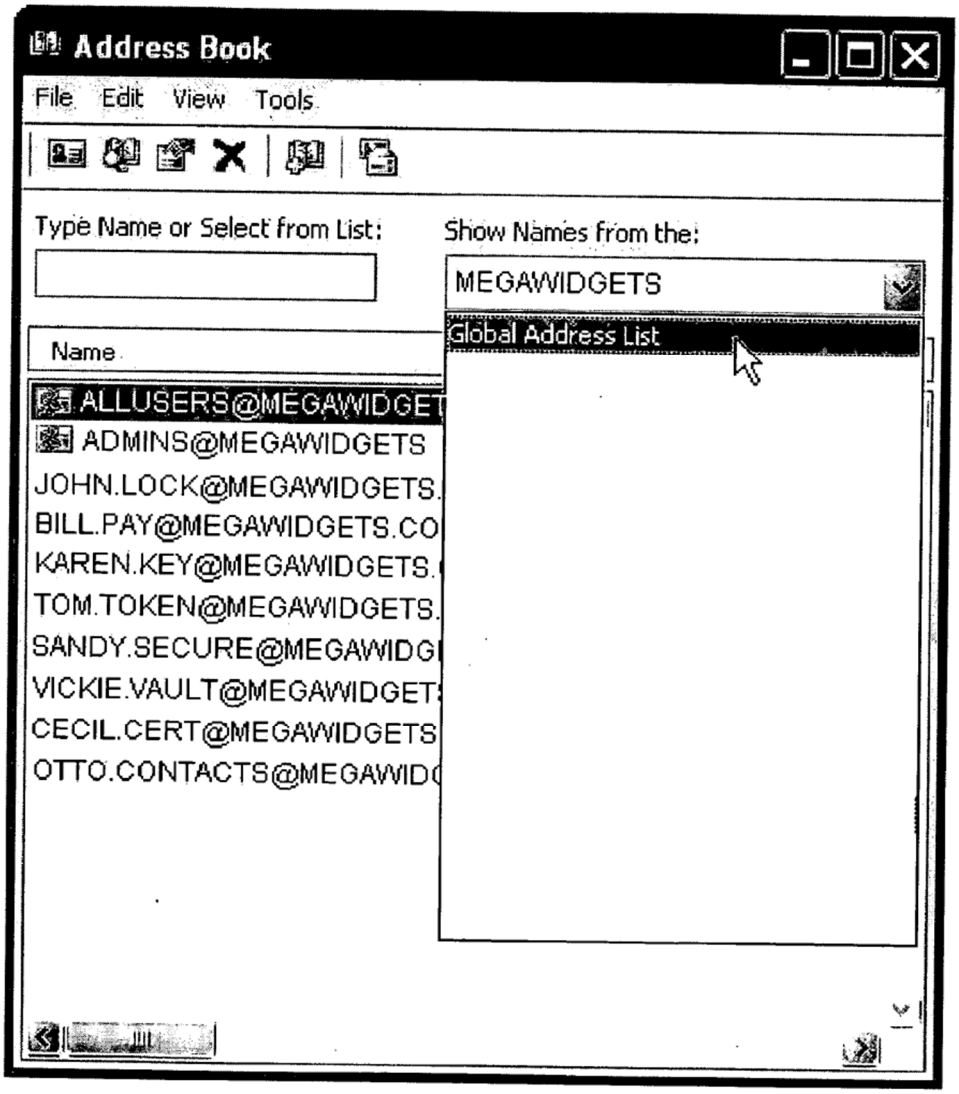
B. U.S. Patent App. Pub. No. 2007/0061567 to Day et al. ("Day")

59. Day is directed to a "system by which documents and other network resources may be kept secure and private." USAA-1006, Abstract. In particular, Day uses "public key encryption technology" to "provide security, encryption, and privacy for files, e-mail and other messages." USAA-1006, Abstract.

60. Day's system "seeks to maintain the integrity of and/or security information in the forms of files, emails, and the like," by using "personal digital IDs for signatures[,] ensuring that the emails or files coming from a specific individual only." USAA-1006, [0096]. Additionally, "such digital IDs may be used to encrypt the email or file so that only authorized individuals can acquaint themselves with the content of such encrypted emails and files." *Id.*

61. 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 "greatly simplify[] the sending of encrypted e-mail," "[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]. "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]. An example Contacts data is shown below:



USAA-1006, FIG. 26

62. In an example, two users, John and Mary, each have their own personal digital ID and the other user's public key stored on his/her own computer. USAA-1006, [0181]. "As users like John and Mary receive and open signed incoming email messages, the secure email utility automatically updates and

associates the sender's digital certificate (personal digital ID) in their address books in their profile." USAA-1006, [0181]. Then, "when Mary receives a signed email from John, John's personal digital ID (his public key) is automatically added to the 'John' contact in Mary's address book. If there is not a contact named 'John' in Mary's address book, the secure email utility would automatically create a 'John' contact profile appropriately labeled and associated with John's public key." USAA-1006, [0182]. In Day, "[u]sers can only encrypt messages for those contacts for which such users have public personal digital IDs stored in their Contacts." USAA-1006, [0186].

C. Immega-Day Combination

63. Immega explains that, after modified enrolled feature sets are generated, they are "securely stored" and "assigned to a specific person with whom messages will be exchanged." USAA-1004, [0044]. Additionally, Immega explains that "[m]any uniquely modified enrolled feature sets, one (or more) for each person with whom messages will be exchanged, may be created and securely stored." *Id.* Immega further explains that a user stores his/her own modified enrolled fingerprint feature sets. USAA-1004, [0009], [0010], [0012], [0044], [0059]. To the extent that Immega is not explicit about implementation details regarding the storage of modified enrolled feature sets in a computing device, a

POSITA would have naturally looked to related prior art, such as Day, that offers these additional details.

64. Like Immega, Day is directed to a system for "provid[ing] security, encryption, and privacy for files, e-mail and other messages" through encryption. 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]. Day's "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]. Similar to Immega, in Day's system, "personal digital IDs for signatures" are used to "encrypt [an] email or file so that only authorized individuals can acquaint themselves with the content of such encrypted emails and files." USAA-1006, [0096]. Further, in Day, "the secure email utility automatically updates and stores the senders' public key from incoming email in Outlook clients Contacts Address Book," 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, [0134], [0223].

65. Day further explains that, to "greatly simplify[] the sending of encrypted e-mail," "[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]. "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].

66. In combination, the Immega-Day system ("Immega-Day") includes computing devices, per Immega, each of which includes a secure email utility integrated with an email program such as Outlook, per Day, and secures email transmission using modified enrolled fingerprint sets to encrypt and decrypt communications, per Immega. USAA-1004, [0041], [0042], [0062]-[0068], FIGS. 1-6; USAA-1006, [0014], [0097], [0119]-[0120], [0170]. Further, modified enrolled fingerprint sets are stored, per Immega, in each device's email contacts database, per Day. §VIII.B.

67. Per Immega, in the combination, generated modified enrolled feature sets 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 the combination, those modified enrolled feature sets are stored by the utility 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]. Additionally, in the combination, 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]. 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].

68. In further detail, in Immega-Day, the Contacts database, per Day, stores all modified enrolled fingerprint feature set necessary for secure email communication, per Immega, among communicating computing devices. Specifically, both the receiver's modified enrolled fingerprint feature set (modified for the sender) and the sender's modified enrolled fingerprint feature set (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-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 modified enrolled fingerprint feature set (modified for the receiver) and the receiver's modified enrolled fingerprint feature set (modified for the sender) and an identification of the sender (e.g., sender's email address). *Id.* Additionally, if user Alice communicates with Bob and Carol and has cross-enrolled with them, then Alice's Contact's address book would contain (1) a "Bob" entry that includes Alice's modified enrolled fingerprint feature set (modified for Bob), Bob's modified enrolled fingerprint feature set (modified for Alice), and Bob's email address; and (2) an "Alice" entry that includes Alice's modified enrolled fingerprint feature set (modified for Carol), Carol's modified enrolled fingerprint feature set (modified for Alice), and Carol's email address. *Id.* Therefore, the combination's address book includes the "[m]any uniquely modified enrolled feature sets, one (or more) for each person with whom messages will be exchanged," per both Immega and Day. USAA-1004, [0044], USAA-1006, [0119]-[0120], [0170].

69. Since Day's systems run on a conventional operating system such as Windows, a POSITA would have understood and found obvious that the Contacts list that stores the identifier and secret would be stored in a directory at least because operating systems such as Windows store data in file systems organized as hierarchical directories. USAA-1006, [0098]; USAA-1023, 298, 337. For

example, Padwick states that "C/W Outlook can access information about items stored in your *Personal Address Book* (PAB)" (emphasis in the original) which is stored in a Windows directory such as "local settings." USAA-1023, 298, 337.

70. Further, Immega-Day's secure email utility is an application running on the device. Specifically, Day describes a "secure email utility" that "automatically configures and associates the personal digital ID with an email program." USAA-1006, [0014], [0020]. As I describe below with reference to Outlook 2000 (which is "one of the ***applications*** included in versions of Microsoft Office 2000,"), a POSITA would have understood and found obvious that a utility is an application running on a computing device. USAA-1023, 14. Further, Immega describes "an algorithmic flow chart for securely exchanging enrolled fingerprint feature sets between two users, for later use in biometrically certified messages" and "algorithmic flow chart subroutines for modifying the enrolled fingerprint feature set 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, as taught in related prior art such as Day. For example, Day states that a "secure email utility is an extension to MS Outlook" that "associates the digital ID with Microsoft's Outlook/Outlook Express clients." USAA-1006, [0014], [0097].

Since Padwick explains that Outlook 2000 is "one of the ***applications*** included in versions of Microsoft Office 2000," and Day describes the secure email utility is an extension of Outlook, a POSITA would have understood and found obvious that Immega-Day combination's secure email utility runs as an application. USAA-1023, 14 (emphasis added). Thus, from the teachings of both 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.

71. A POSITA would have found obvious that enhancing the encryption/decryption techniques based on modified enrolled fingerprint feature sets, per Immega, with Day's teachings regarding storage and organization of email encryption keys in a Contacts database introduces multiple advantages. For example, Day explains that storing communication partners' credentials "simplif[ies] the use of email encryption for any incoming digitally signed emails." USAA-1006, [0170]. Thus, upon receiving an encrypted communication, a device need not retrieve remotely-stored decryption credentials since the credentials are stored locally. A POSITA would have further recognized the benefits of storing the feature sets, 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 (name, email address, biometric

information, encryption keys, etc.) in a single record, creating a "transparent tool for managing individual" the communication keys needed "to send and receive secure email." USAA-1006, [0134], [0170]. Further, the combination leverages an existing email component, Contacts, rather than introducing a separate component that must be securely stored and managed, simplifying the system design and administration. USAA-1006, [0170]. As such, a POSITA would have been motivated to incorporate Day's teaching of storing encryption data in the email system's existing Contacts database at least for these reasons.

72. A POSITA would have found relevant solutions within Day and would have expected success in incorporating Day's teachings. For instance, 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.

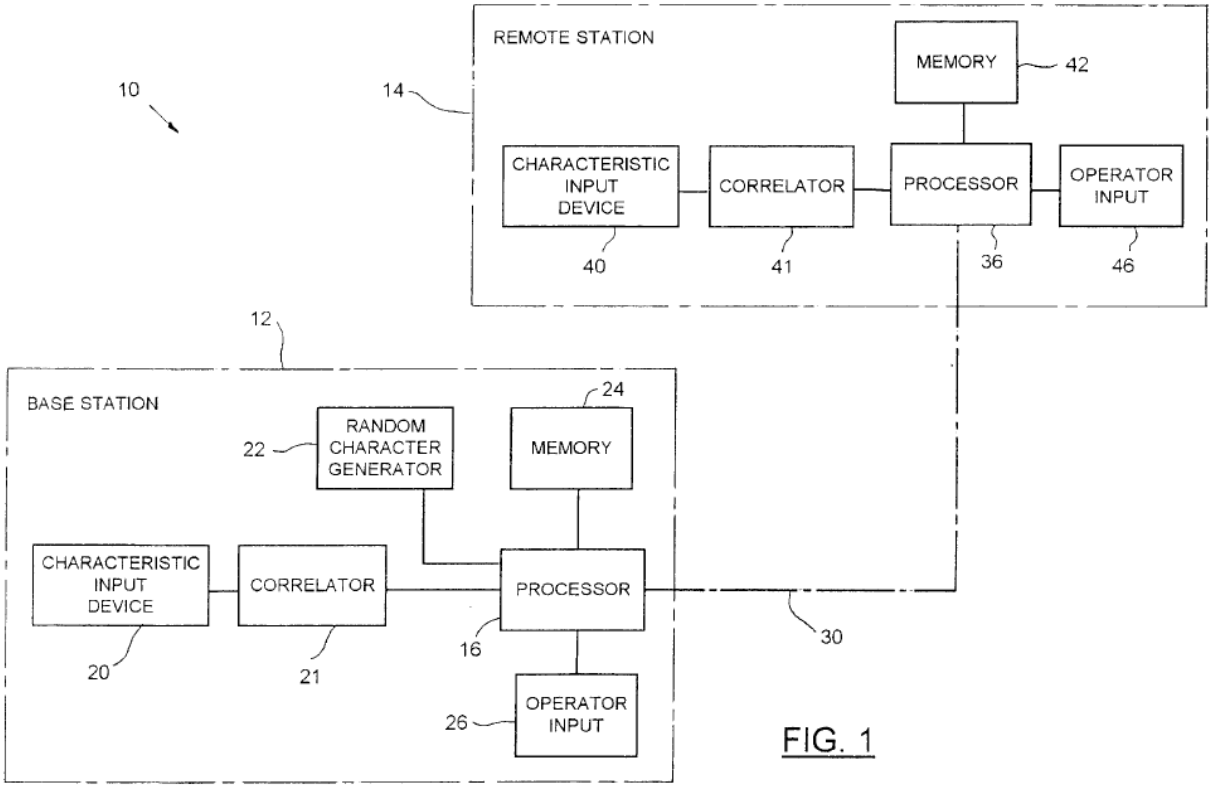
73. Moreover, configuring the devices, as in Immega, to leverage Day's teachings would have required only routine programming knowledge well within the skill of a POSITA prior to the earliest effective filing date. Indeed, the change would have amounted to nothing more than the use of a known technique to improve similar devices – in each instance a computing 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.

74. 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 modified enrolled fingerprint feature sets used to send and receive secure email and, as taught by Day, would store the modified enrolled fingerprint feature sets in a Contacts address book located in a directory and that includes the "[m]any uniquely modified enrolled feature sets, one (or more) for each person with whom messages will be exchanged," per Day. Accordingly, a POSITA would have naturally expected success when incorporating Day's teachings into Immega. *Id.*

D. U.S. Patent No. 6,002,770 ("Tomko")

75. Tomko is directed to "permitting the secure handling of data between two remote stations," which "involves the generation of an encrypted decryption key which is based," among other things, "on a fingerprint information signal from a user of a first station." USAA-1005, Abstract. Tomko explains that the encrypted key is "stored at both stations" so that "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-1005, FIG. 1

76. A system, as described in Tomko, includes two remote stations, including base station 12 and remote station 14 "connected for two-way communication" online 30. USAA-1005, 2:18-30, FIG. 1. Each of the remote stations includes a processor 16/36, characteristic input device 20/40, and memory 24/42. USAA-1005, 2:18-41, FIG. 1. For instance, a processor 16 is used to process a received user input (e.g., a fingerprint via the characteristic input device 20) to derive a decryption key and encrypt the decryption key, which is stored in memory 24. USAA-1005, 2:49-4:65. Tomko further explains that the processor

assists in sending messages, including obtaining the encrypted decryption key in response to a user "applying his fingerprint to the characteristic input device 20." USAA-1005, 5:13-26.

77. Tomko explains that "[s]ystem 10 is used, firstly, to develop an encrypted version of a message decryption key at the base station which may be transmitted to the remote station without concern for privacy and, subsequently, to encrypt messages at either of the stations for transmission to other of the stations where they may be decrypted." USAA-1005, 2:42-47. Tomko describes various methods for "[d]eveloping an encrypted decryption key" where the key is generated in an encrypted form and stored. USAA-1005, 2:48-5:11; *see id.*, 6:56-65. In particular, Tomko explains that the "encrypted version of the decryption key may be stored in memory 24," and "because the decryption key is encrypted, it may be passed to the remote station on line 30 and will remain secure even if intercepted." USAA-1005, 4:60-63. "The remote station stores the received encrypted decryption key in its memory 42." USAA-1005, 4:63-65.

E. Immega-Day-Tomko Combination

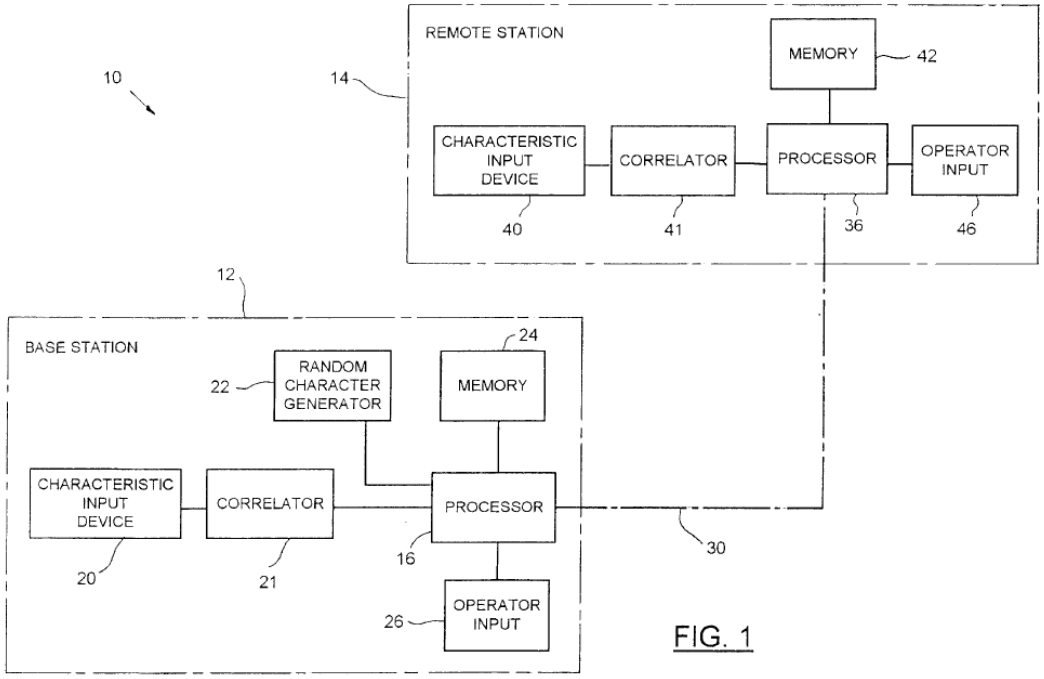
78. As explained further below, a POSITA would have found obvious integration of Tomko's teachings relating to its device hardware components and data encryption into Immega-Day's system, thereby further enhancing Immega-Day's security and offering additional implementation details.

i. Device Components

79. Immega describes a "method for permitting the secure transmission of electronic messages by using biometric certification," where the messages include email. USAA-1004, Abstract, [0006]. Immega further explains that the receiver's device can comprise a "computer or any device equipped to execute the steps" described in Immega, including "cellular telephones" and "personal digital assistants." USAA-1004, [0041]. To the extent that the device of Immega is not understood to include specific components, a POSITA would have included these components for performing the various processing and storing steps of Immega's method, as Tomko discloses, including executing the secure email utility (application) described above with respect to Immega-Day. *Supra* §§V.E (Technology Overview), VIII.C-D.

80. Like Immega and Day, Tomko is directed to "secure handling of data between two remote stations" (e.g., base station and remote station) using fingerprint information. USAA-1005, Abstract. As shown 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. The processor 16 is used to process a received user input (e.g., a fingerprint via the characteristic input device 20) to derive a decryption key and encrypt the decryption key, which is stored in memory 24. USAA-1005, 2:49-4:65. The processor also assists in sending

messages, including obtaining the encrypted decryption key in response to a user "applying his fingerprint to the characteristic input device 20." USAA-1005, 5:13-26.



USAA-1005, FIG. 1

81. In view of the similarities among Immega, Day, and Tomko's teachings, a POSITA would have naturally looked to Tomko for implementation details regarding the Immega-Day devices, including what components would be included. Combining the teachings of Immega-Day and Tomko would have merely involved combining prior art elements according to known methods to yield predictable results. Indeed, both teach systems involving communications between two devices that are secured with the use of user fingerprints. USAA-1004, Abstract; USAA-1005, Abstract. A POSITA would have been motivated to

combine the teachings of Immega-Day and Tomko to realize the implementation details, *e.g.*, inclusion of processor, memory, and other components to execute the functionality of the device. *Id.* For example, Immega describes "any device equipped to execute the steps described." USAA-1004, [0041]. The combination 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 that are explicitly disclosed by Tomko and would have been understood by a POSITA as likely present, but not explicitly disclosed by Immega. 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 modified enrolled fingerprint feature sets and transmitting secure communications with the use of that data, as it did prior to the combination with Tomko. *Id*.

ii. Data Encryption

82. Moreover, as discussed for [1.a.ii], Immega teaches storing the receiver's modified enrolled fingerprint feature set ("secret") in a directory. *See*

supra, Ground 1A, analysis of Element [1.a.ii]. Immega further teaches that, during the cross-enrollment process, the receiver encrypts the receiver's modified enrolled fingerprint feature set ("secret") during the cross-enrollment process. USAA-1004, [0047] (discussing double encrypting an enrollment message that includes a user's modified enrolled fingerprint feature set), claim 4 ("public key cryptographic techniques are used to securely exchange modified enrolled biometric feature sets"). In particular, Immega describes creating an "enrollment message (step 222) comprised of the first user's name, the second user's name[, and] the uniquely modified enrolled fingerprint feature set" 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 modified enrolled fingerprint feature set ("secret") in the directory, it would have been obvious to a POSITA to encrypt it prior to storing it.

83. In particular, 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 the Immega-Day-Tomko combination, during cross-enrollment, the receiver device would store

the double encrypted enrollment message prior to transmitting the enrollment message to the sender device, as illustrated in modified FIG. 2 of Immega below.

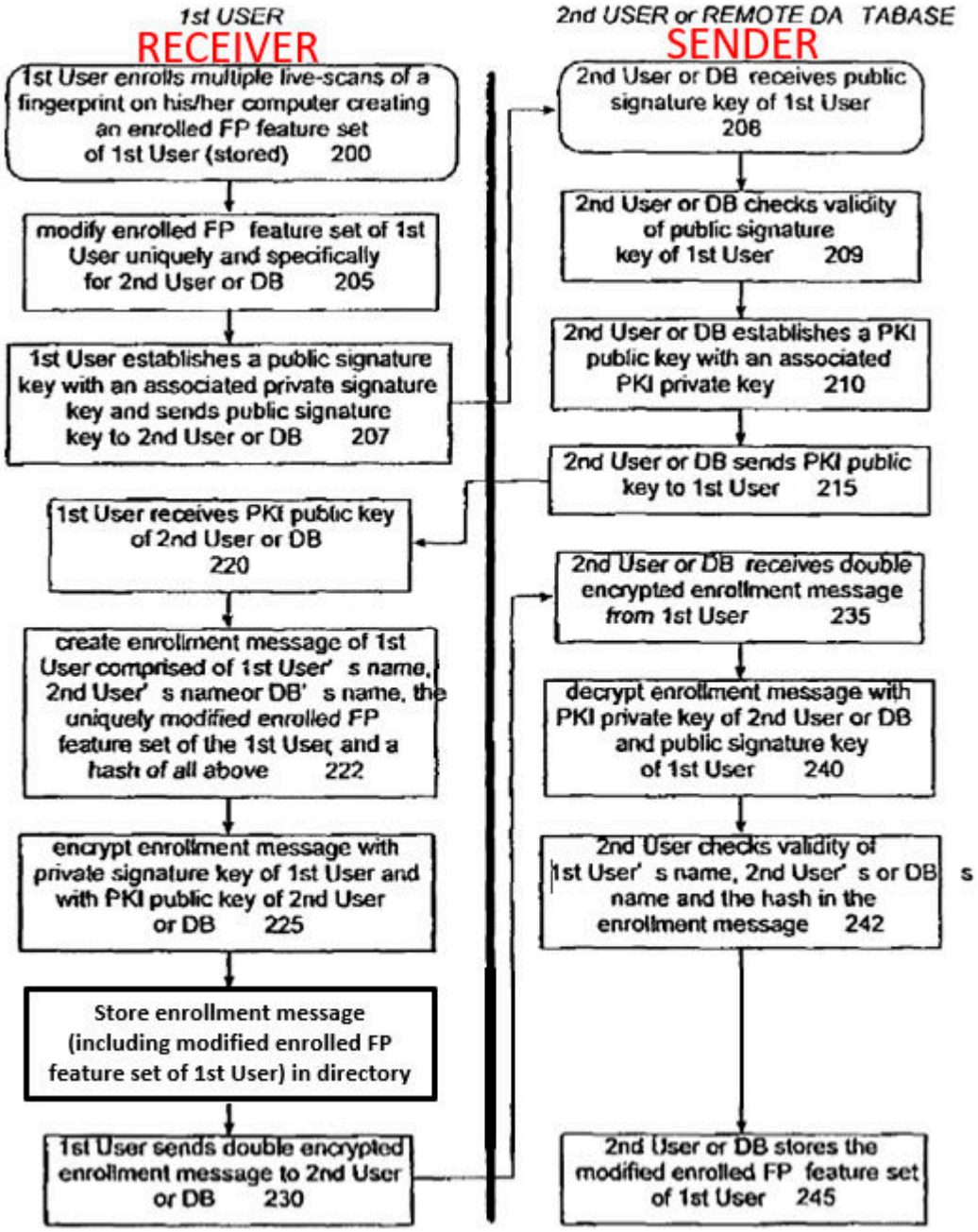


FIG. 2

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

84. Indeed, as discussed for [1.a.ii], Immega teaches securely storing modified enrolled feature sets that are "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 computing device to distinguish the receiver's various enrolled fingerprint feature sets from one another, it would have been obvious that each enrolled fingerprint feature set would be stored with an identifier that identifies the particular user for which the feature set facilitates secure communication. This information is already included in Immega's enrollment message (e.g., "the first user's name, the second user's name[,] the uniquely modified enrolled fingerprint feature set (that has been uniquely changed and assigned to the specific second user from whom messages will be received). USAA-1004, [0047]. Thus, it would been obvious to a POSITA that, in the Immega-Day-Tomko combination, during enrollment, the receiver's device stores the encrypted enrollment message for each user with whom messages will be exchanged. When the receiver's device later required use of the receiver's modified enrolled fingerprint feature set, the receiver's device would simply apply his/her fingerprint to retrieve the enrollment message/modified enrolled fingerprint feature set, per Immega, and decrypt the enrollment message "firstly with the private key of the [sender] and secondly with the public signature of the

[receiver]," both of which the receiver's device has in its possession (per steps 207, 220, 230). USAA-1004, [0009], [0050], [0045]-[0047].

85. A POSITA would have found obvious that enhancing Immega's method based on Tomko's teachings of encrypting a decryption key before storing it would introduce multiple advantages. Tomko explains that storing an encrypted version of the decryption key allows the decryption key to "be passed to the remote station on line 30" 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.*. 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-1005, 6:10-12.

86. For example, as Levy explains that, in known storage systems, "sensitive information stored on the storage medium 2 is freely accessible to anyone who may use the system." USAA-1008, 3:26-37. "Therefore a need existed to provide a system and method for ***securing sensitive data contained upon mass storage media***," and the "system and method must provide a low cost mechanism for securing media resident data that poses a minimum possible impact to the end user who is already familiar and comfortable with accepted peripheral types, operating systems, and off the shelf applications." USAA-1008, Abstract,

1:14-39 (emphasis added). Levy then describes "a rational standard for the selective encryption of sensitive data on a computer system." USAA-1008, 1:41-45.

87. As such, a POSITA would have been motivated to incorporate Tomko's teaching of encrypting decryption keys before storing them to Immega's authentication system at least because of the added security benefits of locally storing encrypted versions of sensitive information.

88. A POSITA would have found relevant solutions within Tomko and would have expected success in incorporating Tomko's solutions within Immega. For instance, Tomko describes various methods for "[d]eveloping an encrypted decryption key," and Immega similarly teaches encrypting its modified enrolled fingerprint feature sets. USAA-1004, [0047]; USAA-1005, 2:48-5:11.

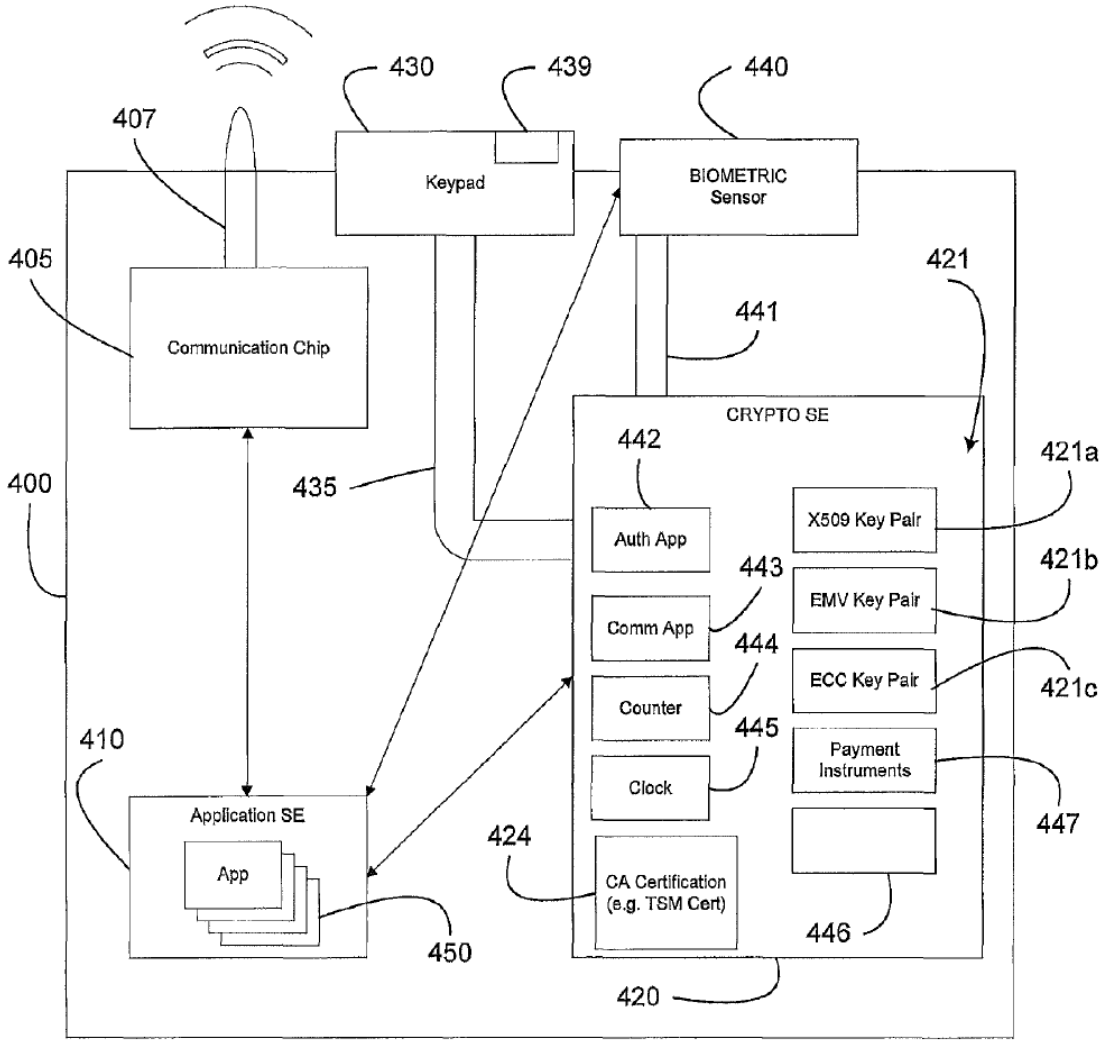
89. Moreover, configuring Immega's devices to leverage Tomko's teachings would have required only routine programming knowledge well within the skill of a POSITA prior to the earliest effective filing date. Indeed, the change would have amounted to nothing more than the use of a known technique to improve similar devices – in each instance a computing 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.

90. 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 modified enrolled fingerprint feature sets used to send and receive secure email but, as taught by Tomko, would store the modified enrolled fingerprint feature sets in an encrypted form for improved security. Accordingly, a POSITA would have naturally expected success when incorporating Tomko's teachings into Immega. *Id.*

F. U.S. Patent No. 8,108,318 ("Mardikar '318")

91. 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, FIGS. 4, 5a, 5b, 6a.

92. In more detail, Mardikar '318's FIG. 4 (reproduced below) "shows an example embodiment of … a client device 400 … such as a mobile phone" that "may include a communication chip 405, an antenna 407, secure elements 410, 420, a keypad 430 and a biometric sensor 440." USAA-1010, 6:43-49.



USAA-1010, FIG. 4

93. Mardikar '318 explains that a secure element (SE) "may be, for example, a smart card … embedded inside device 400," adding that a "smart card is a small, relatively tamper-proof computer" that "may contain a CPU and some non-volatile storage" that "makes it possible for the card to keep some secrets, such as the private keys associated with any certificates it holds." *Id.*, 7:45-57.

94. FIG. 4's "Application SE" 410, and "Crypto SE" 420 "may be pre-loaded with applications and/or may be capable of downloading … applications for facilitating financial transactions over a network, key pairs, payment instruments and/or a Certifying Authority (CA) certificate." *Id.*, 7:58-63. "Splitting the App SE from the Crypto SE may enable a single Trusted Service Manager to verify and authenticate the identity of a user for each of a number of various Service Providers." *Id.*, 9:48-59.

95. In more detail, the App SE 410 may, in an exemplary embodiment, "be designated for and arranged for storing various, resident financial transaction or payment applications 450, each of which may facilitate financial transactions for a different financial Service Provider," for example, "PayPal." *Id.* 8:62-9:3. In that regard, the App SE 410 may be a "SIM card" that "securely store[s] a service-subscriber key (IMSI) used to identify a subscriber," and that is loaded with "applications 450" that are "signed by a common Trusted Service Manager (TSM) public key." *Id.*, 9:4-23.

96. The Crypto SE 420 may, in an exemplary embodiment, "be designated for and arranged for loading and storing authentication data 446 (for example a PIN or biometric signature), payment instruments 447, certificates 424, crypto keys 421 and other security-related information, including, for example, unique biometric authentication information related to a specific user." *Id.*, 9:39-

43. The Crypto SE 420 may, for example, "provide verification and authentication for multiple applications stored in the App SE 410." *Id.*, 43-47.

97. In that regard, a biometric authentication application 442 "may reside on the Crypto SE 420 and may evaluate" biometric data received from biometric sensor 440 "and compare the data to data from a registered user, or may register the data where the data is being collected as part of a registration or certification procedure." *Id.*, 9:60-65, 10:42-11:7; FIGS. 4, 5a, 5b.

98. Mardikar '318's FIGS. 5a and 5b (reproduced below) "illustrate an exemplary system 500 for registering client device 400" with a "trusted service manager 505," for example, "to unlock a payment credential or CA certificate 424 (FIG. 4) pre-loaded on the device 400." *Id.*, 10:41-47.

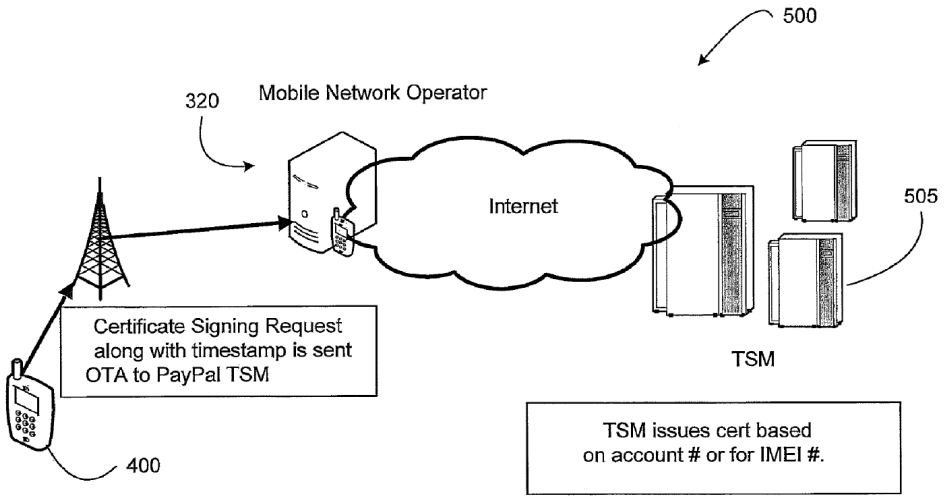


FIG. 5a

USAA-1010, FIG. 5a

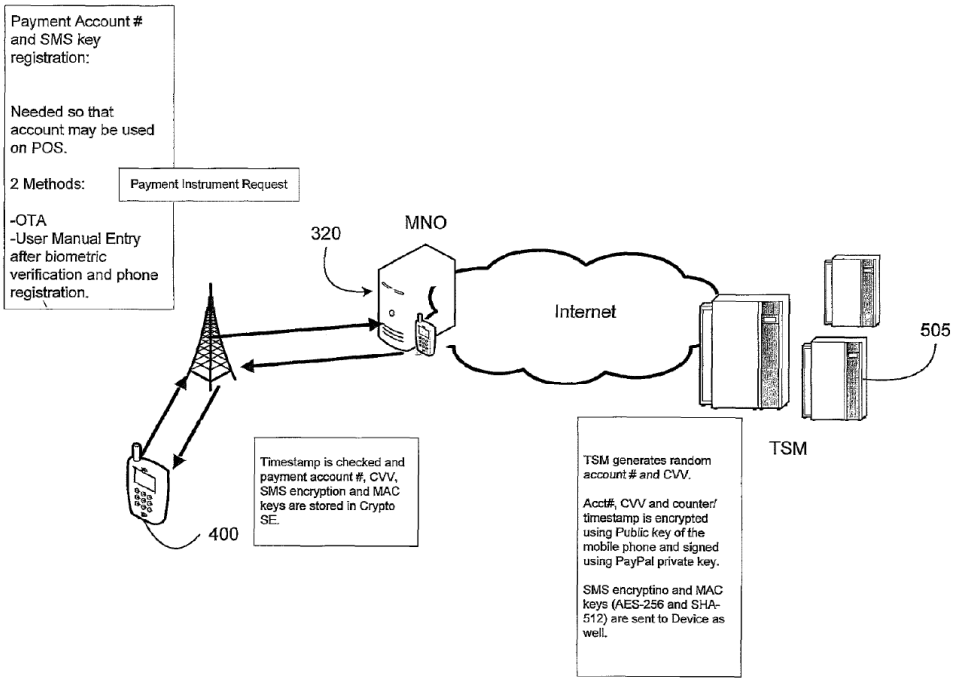


FIG. 5b

USAA-1010, FIG. 5b

99. "Registration may include registering a biometric attribute, for example a thumb-print or finger-print, to unlock payment," and "[a]ll applications on the device may be registered with and deployed via the trusted service manager." *Id.*, 10:47-54. For instance, "a payment credential 424 (FIG. 4) … may be unlocked by registering the user's unique biometric profile using the biometric sensor 440 (FIG. 4) … by registering a thumb-print twice …." *Id.*, 10:54-60.

100. In this context, Mardikar '318 further explains that "when a customer invokes pre-loaded app 450 (FIG. 4), SCEP/CRMF (Simple Certificate Enrolment Protocol/Certificate Request Message Format) is invoked," and a "user's TSM

credential or certificate 424" may be "entered and associated with the Service Provider's user account." *Id.*, 10:63-66. A "payment account number may be randomly generated by the Service Provider along with CVV (card verification value), and in an exemplary embodiment the "payment account number, CVV and counter/timestamp (to prevent replay attacks) may be encrypted using the Public key of the mobile phone and signed using the TSM's private key." *Id.*, 11:9-21. The "counter may be checked and payment account number and CVV may be stored in the Crypto SE." *Id.*, 11:17-19.

101. Mardikar '318's FIG. 6a (reproduced below) "illustrate[s] a method 600 of conducting a near-field communication (NFC) transaction at a point of sale (POS)" that is facilitated by a Service Provider (e.g., PayPal), and that involves unlocking the user's registered payment credentials through further biometric authentication. *Id.*, 11:29-13:36, FIGS. 6a, 6b, 6c.

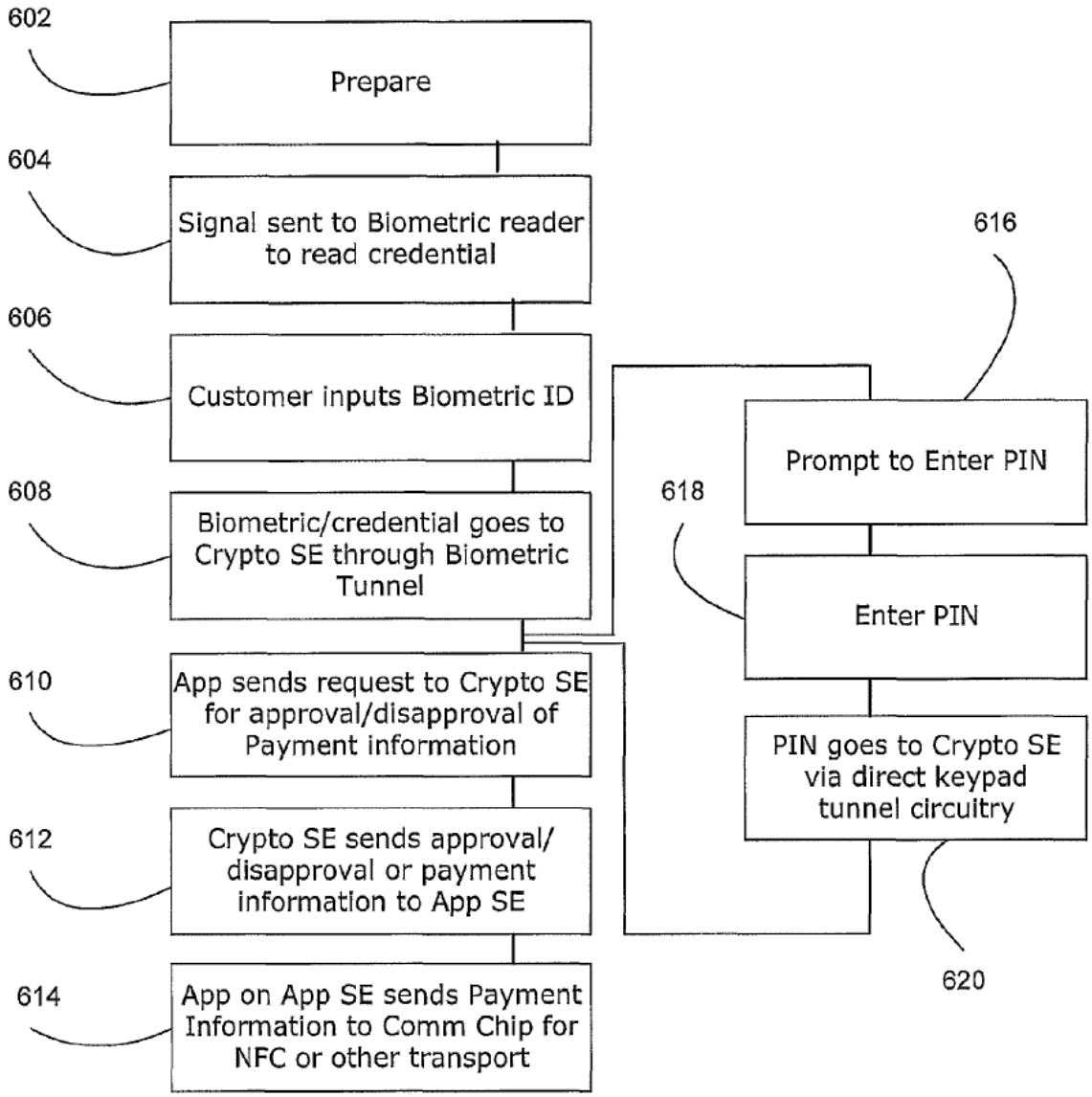


FIG. 6a

USAA-1010, FIG. 6a

102. In more detail, Mardikar '318 explains in the context of an exemplary embodiment involving a POS NFC transaction that "preparing the device for payment may prompt a payment application resident on the App SE 410 … to

check 604 the biometric sensor for biometric input," that a user may then input 606 their biometric identifying data (ID) or signature by placing or swiping a thumb or finger on biometric sensor 440," and that the "input biometric ID may be directly sent or tunnelled 608 to Crypto SE 420 … for authentication/unlocking." *Id.*, 11:44-51; *see also id.*, 9:60-65 ("a biometric authentication application … may evaluate the biometric data and compare the data to data from a registered user").

103. "Once a user's biometric identity is authenticated properly, the Crypto SE 420 may send 612 an approval/disapproval message and payment or other information to the App SE," which "may then send the payment information 614 to the communication chip 405 for further transmission or transport to a reader or other communication reception device located at the POS, for example a POS NFC reader located at a merchant/vendor's place of business." *Id.*, 11:62-12:3. "In other example embodiments, the Crypto SE 420 may establish a direct, secure transmission between the Crypto SE 410 and the POS." *Id.,* 12:4-21.

104. Either way, the transmitted "[p]ayment information may include payment information, such as amount and account number, and may include a CVV." *Id.*, 12:22-30. For example, "[w]hen a payment is made at a merchant POS 650 using Visa/MC/AmEx, the last four digits of the payment instrument may be sent to the TSM (using, for example, an application provided on the App SE by the TSM)," and "[t]his information may be correlated with signature information"

that is "collected by the TSM" and "used to identify the client device and its user."[3] *Id.*, 12:31-43.

105. Notably, Mardikar '318 expressly indicates that "the payment information may be transmitted by alternate methods of communication as desired or necessary in a particular embodiment or circumstance …." *Id.*, 12:22-30; *see also id.*, 3:11-33, 4:27-36 ("the system is not limited to NFC applications, but may also apply to other types of applications, for example, SMS, mobile internet or other forms of communication"), 13:37-14:19 (describing a secure SMS transaction).

106. For instance, Mardikar '318 explains that "TSM 325 may act as a payment provider system (PP), such as PayPal, and may provide payment

---

[3] Mardikar '318 explains that "[c]lient device 400 may further include one or more user identifiers that may be implemented, for example, as operating system registry entries, cookies associated with a browser application, identifiers associated with hardware of client device 400, or other appropriate identifiers … for example, the International Mobile Equipment Identity number (IMEI #) or the Secure Element ID number." *Id.*, 4:57-65. "[A] user identifier may be used by a payment service provider or TSM 240 to associate client device 400 or user 220 with a particular account maintained by payment service provider 240."

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.

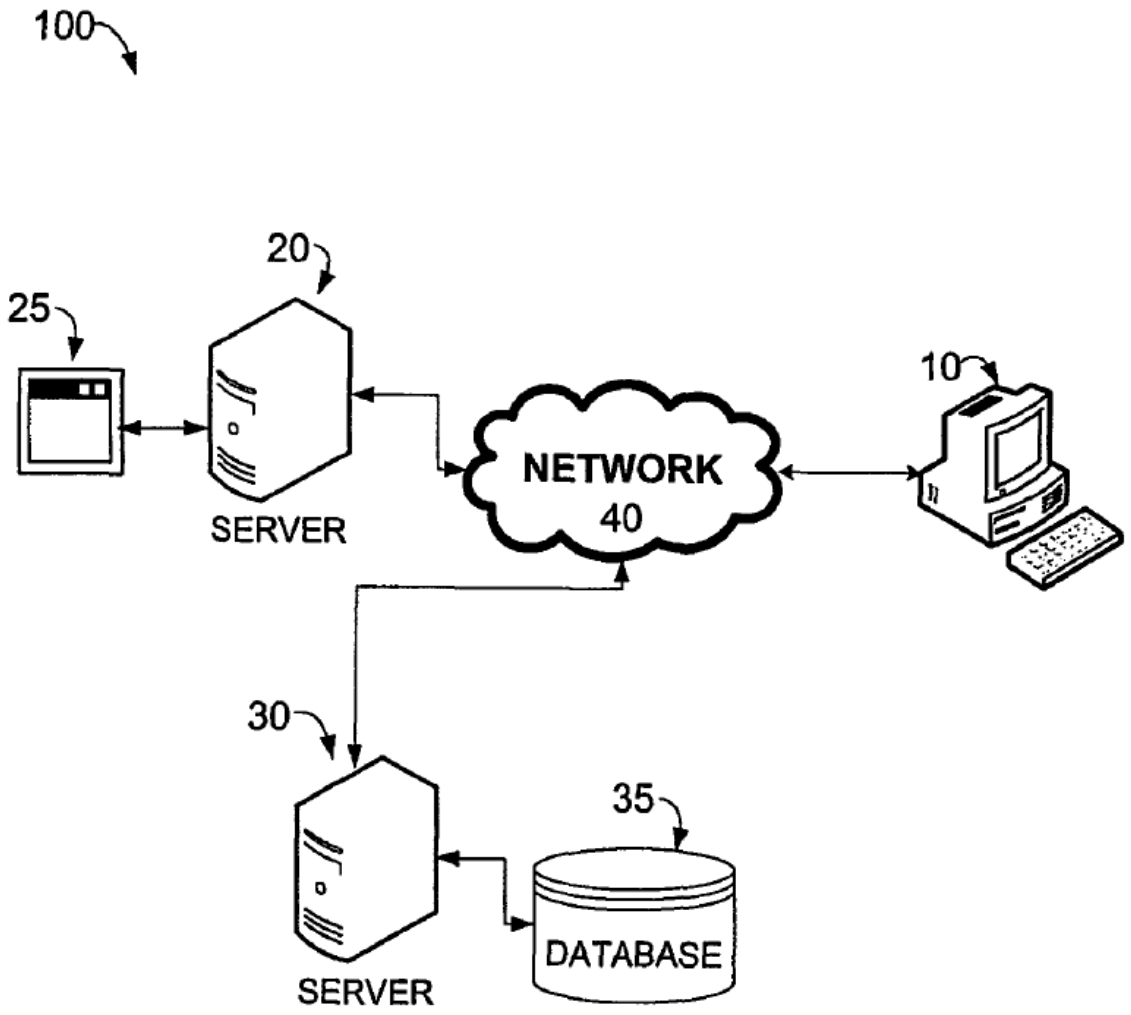
107. In that regard, "the customer may pre-register his account with the payment provider system, map the account to an email address, and then use the payment provider system to make purchases when redirected to the payment provider system from the merchant's site." *Id.* "After the financial transaction is authorized, the TSM 325 or payment provider system completes the transaction."

G. U.S. Patent No. 8,234,697 ("Chhabra")

108. 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.

109. In more detail, Chhabra's FIG. 1 (reproduced below) illustrates "a system for sending credentials securely to a remote server" 20 from a user computing platform 10, which "may be, for example, … a mobile computer" 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.

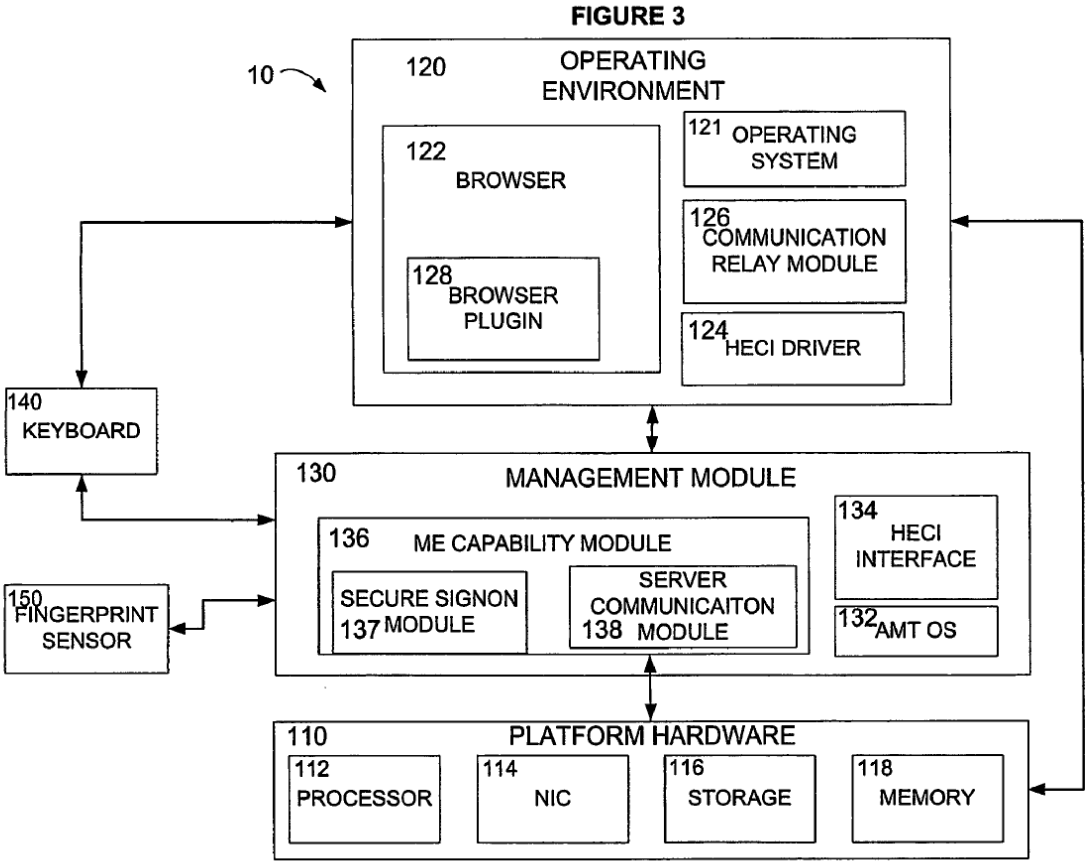
FIGURE 1



USAA-1013, FIG. 1

110. As further illustrated and described with respect to Chhabra's FIG. 3 (reproduced below), the user's computing platform 10 may further feature a "management module" 130 that (similar to Mardikar '318's Crypto SE) "may

request a user's input for authorization or authentication" in the context of a web-based financial transaction that is facilitated by the remote servers 20 and/or 30, which the user provides through "a sensor such as … fingerprint sensor 150 or other biometric device." *Id.*, 9:32-44.

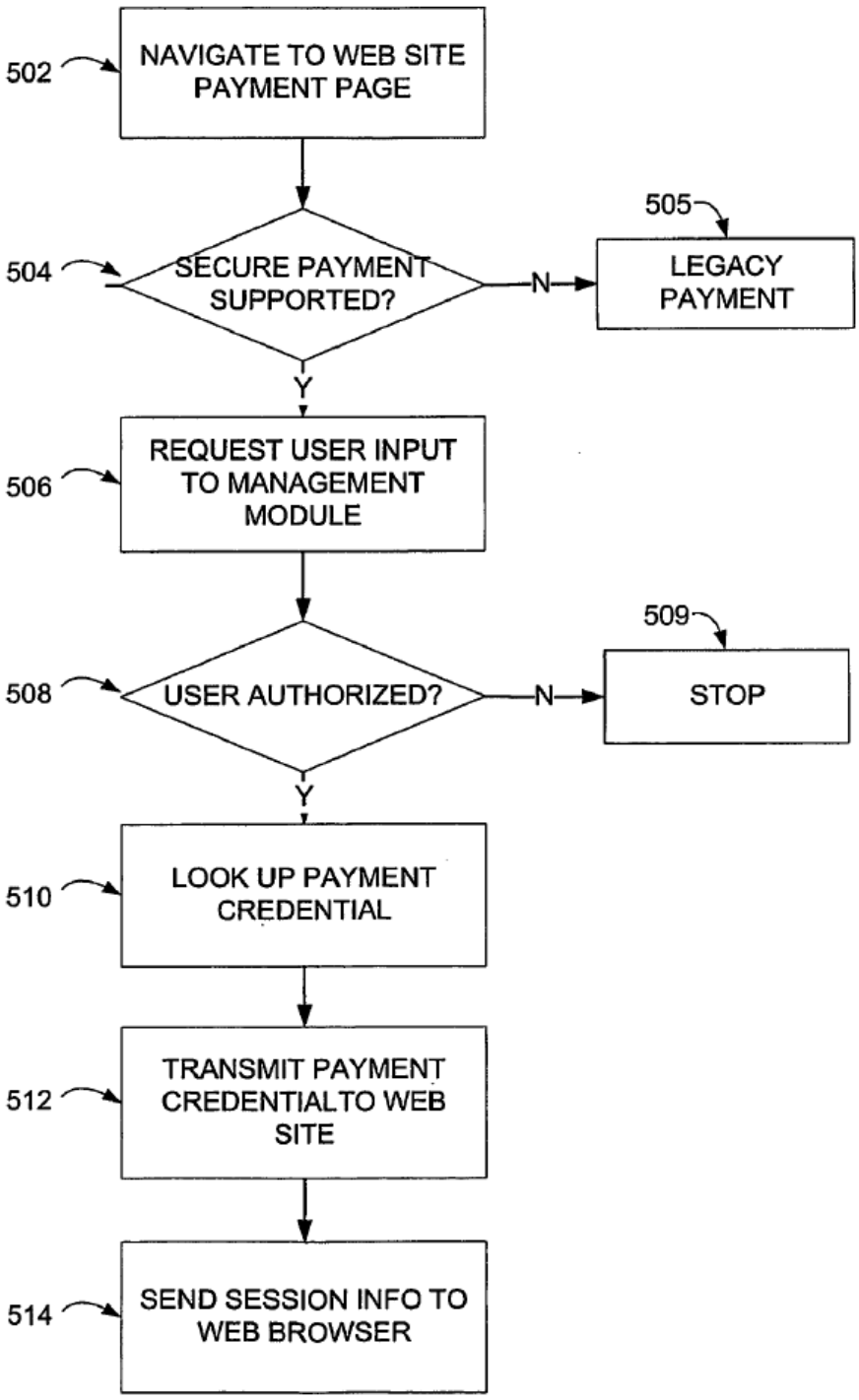


USAA-1013, FIG. 3

111. In more detail, Chhabra's FIG. 5 (reproduced 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 "may request the user to enter payment credentials … such as for

example, a credit card number, a credit card expiration date, a security code, and … payment account information such as for example bank account routing information and password, an on-line payment service (e.g. PayPal®) username and password, or other credentials that may identify or authorize a user and/or a financial account." *Id.*, 10:40-55.

FIGURE 5



USAA-1013, FIG. 5

112. For example, the "management module" 130 "may request user input for authorization to complete the financial transaction" in an operation 506 that is performed in response to a message that is communicated to computing platform 10 from "database server 30." *Id.*, 9:32-44[4], 6:45-48, 10:65-11:9, 13:58-14:24. Upon receiving the user's input from "keyboard 140 and/or fingerprint sensor 150," the "management module 130 may … verify or confirm that the user is authorized" through a process that "may include but is not limited to a table or database lookup, [and] fingerprint matching …." *Id.*, 9:45-64, 10:65-11:9. For example, "[f]ingerprint sensor 150 may be or include a sensor for capturing a representation of a user's fingerprint for authentication or identification of a user,"

---

[4] Chhabra expressly notes that "[i]n some embodiments, some operations described below in the method of FIG. 5 may be similar to like-named operations described above for the method FIG. 4," and that "embodiments of the method of FIG. 5 may be used by, or may be implemented by, the same elements or components as the method of FIG. 4 including for example an application 25 that may require a financial transaction, although the invention is not limited in this respect." USAA-1013, 10:31-39. From this and related description, a POSITA would have understood and found obvious that Chhabra's disclosures with respect to Chhabra's FIGS. 1, 3 and 4 are applicable as appropriate to Chhabra's FIG. 5.

and a "digital template may be derived from the captured representation and compared with one or more stored reference digital templates"; a "positive match may authenticate or identify a user." *Id.*, 7:44-56.

113. "If the user is authorized, management module 130 may look up in a table or database the appropriate identifier or credential needed," which "may be stored in any memory on computing platform 10 that is secure," and may "transmit a permission token, number or string such as an http post login string and/or other appropriate credential to application 25 over public network 40," where application 25 is hosted on remote server 20. *Id.*, 3:3-25, 9:55-10:3, 3:3-14, FIG. 2. For example, "in operation 510 management module may look up the appropriate payment credential needed to complete the transaction," and may in operation 512 "encrypt and transmit the requisite http request string and payment credential over the public network 40 to application 25." *Id.*, 11:10-29, 9:65-10:16.

H. Mardikar-Chhabra Combination

114. As independently and expressly suggested by both Mardikar '318 and Chhabra, a POSITA would have found it obvious to apply authentication techniques enabling a user to securely log in to a payment provider's site when redirected to that site from a merchant's site during a browser session, and/or to securely complete an associated financial transaction through the payment

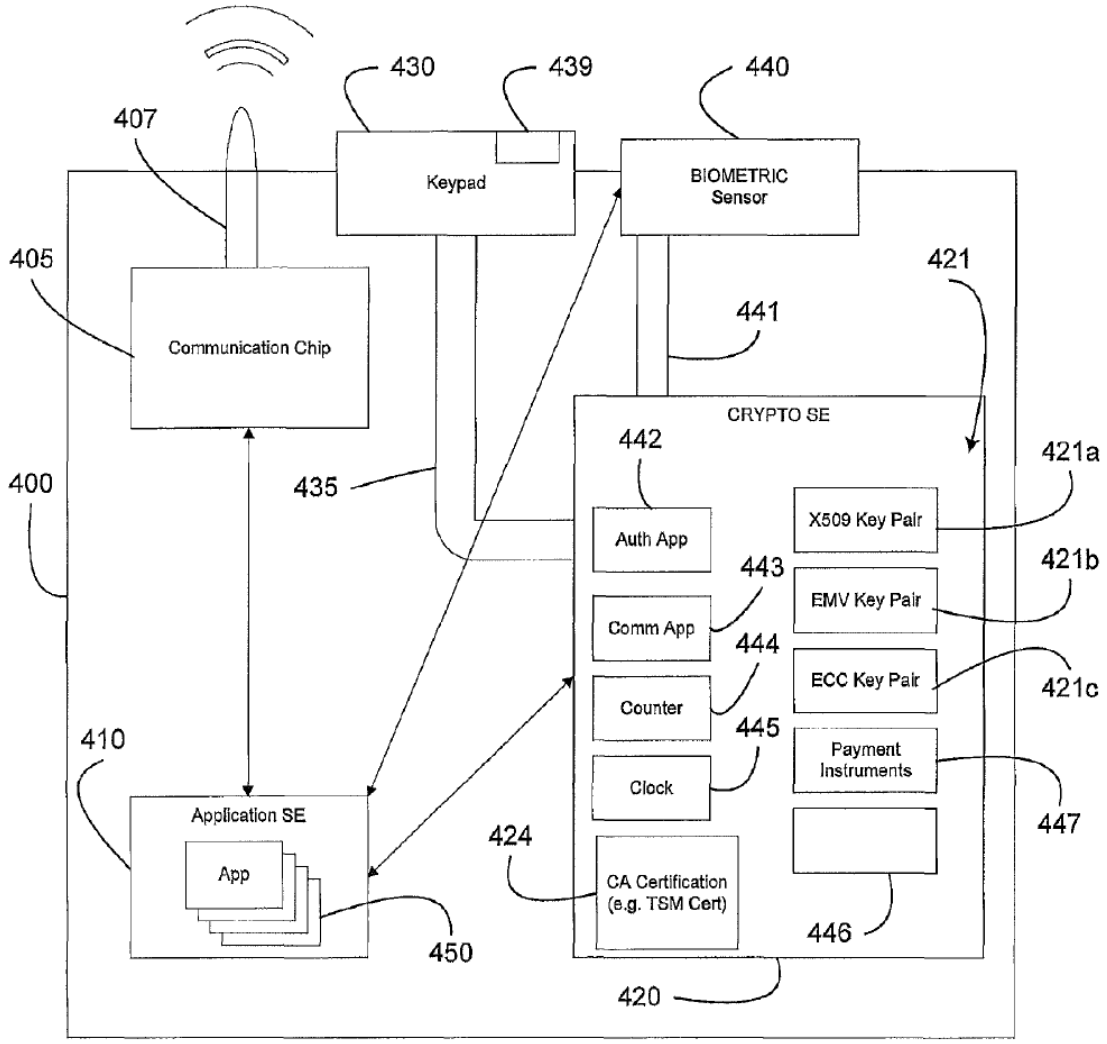
provider's site during that browser session. USAA-1010, 6:13-29, FIGS. 4, 5a, 5b; USAA-1013, 10:40-55, FIGS. 1, 3, 4, 5.

115. Mardikar '318, for instance, explains that "TSM 325 may act as a payment provider system (PP), such as PayPal, and 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.*, 6:19-23. In that context, Mardikar '318 further explains that "the customer may pre-register his account with the payment provider system, map the account to an email address, and then use the payment provider system to make purchases when redirected to the payment provider system from the merchant's site," adding that "[a]fter the financial transaction is authorized, the TSM 325 or payment provider system completes the transaction." USAA-1010, 6:24-29.

116. Chhabra similarly describes "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 "may request the user to enter payment credentials … such as for example, a credit card number, a credit card expiration date, a security code, and … payment account information such as … an on-line payment service (e.g. PayPal®) username and password, or other credentials that may identify or authorize a user and/or a financial account." USAA-1013, 10:40-55, FIGS. 1, 3, 4, 5.

117. Although Mardikar ’318 describes in detail an exemplary process for performing a secure NFC transaction at a merchant’s POS terminal using computing device 400, it offers fewer specific details with respect to web transactions. *See* USAA-1010, 6:13-29, 11:30-13:36, FIGS. 4, 6a, 6b, 6c. In that regard, a POSITA would have found it obvious to supplement Mardikar ’318’s teachings with Chhabra’s when implementing biometric authentication for web transactions facilitated by a payment provider’s remote server.

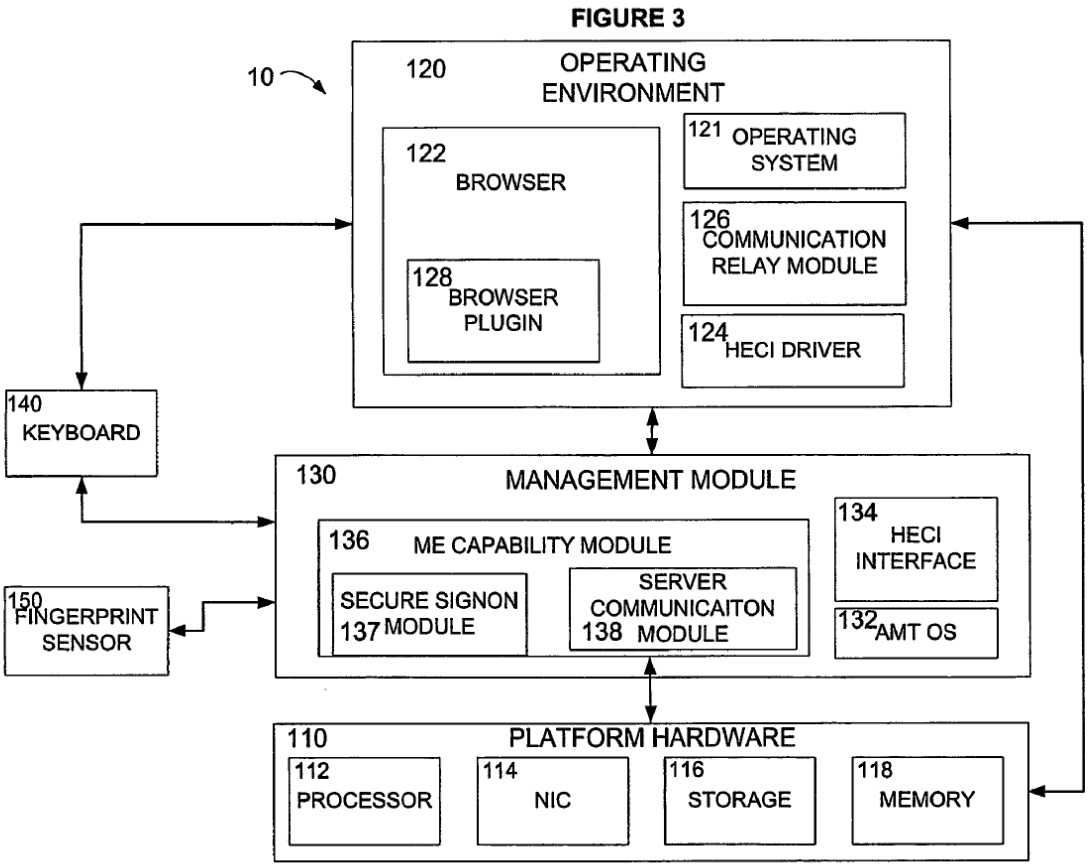
118. In more detail, a POSITA would have understood and found obvious that computing device 400 is, as described with respect to Mardikar ’318’s FIG. 4 (reproduced below), equipped with the hardware and software necessary to enable the customer to “pre-register his account with the payment provider system,” “map the account to an email address, and then use the payment provider system to make purchases when redirected to the payment provider system from the merchant’s site”; relatedly, the POSITA would have understood and found obvious that Chhabra’s additional teachings with respect to web transactions could be easily and advantageously implemented by that device and the payment provider’s remote server. USAA-1010, 6:19-29, 9:60-65, 10:42-11:7, FIG. 4.



USAA-1010, FIG. 4

119. For instance, similar to the computing platform 10 "management module" 130 and fingerprint sensor 150 that Chhabra describes with respect to Chhabra's FIG. 3 (reproduced below), Mardikar '318's computing device 400 features a biometric authentication application 442 that resides on Crypto SE 420, evaluates biometric data received from biometric sensor 440, and compares "the

data to data from a registered user" as part of a process of authenticating a transaction. 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.



USAA-1013, FIG. 3

120. And, similar to the computing platform 10 "operating environment" 120 and browser 122 that Chhabra describes with respect to Chhabra's FIG. 3, Mardikar '318's computing device 400 features Application SE 410, which "may be pre-loaded with applications and/or may be capable of downloading various

applications … for facilitating financial transactions over a network." USAA-1010, 7:58-9:3.

121. A POSITA would have understood and found obvious from Mardikar '318's descriptions that one such application residing on Application SE 410 would be a web browser. *See*, *e.g.*, USAA-1010, 4:58-62 (noting that "Client device 400 may further include … cookies associated with a browser application"), 6:19-29 ("the customer may pre-register his account with the payment provider system, map the account to an email address, and then use the payment provider system to make purchases when redirected to the payment provider system from the merchant's site").

122. In that regard, a POSITA would have further understood and found obvious that Mardikar '318's system, including both computer device 400 and the remote payment provider server with which it interacts, is readily adaptable to conveniently and securely enable authenticated web transactions along the lines that Mardikar '318 already suggests, and that Chhabra further details. USAA-1010, 6:13-29, FIG. 4; USAA-1013, USAA-1013, 6:45-48, 9:32-11:9, 13:58-14:24, FIGS. 1, 3, 4, 5.

123. For example, as described by Chhabra, "a user desiring to complete a financial transaction on a web site … may be automatically redirected to a payment page" that "may request the user to enter payment credentials … an on-line

payment service (e.g. PayPal®) username and password, or other credentials that may identify or authorize a user and/or a financial account." USAA-1013, 10:40-55.

124. In that context, a POSITA would have been motivated and would have found it obvious to implement Chhabra's related teachings using, for example, biometric authentication application 442 and/or another application residing on Crypto SE 420; in which case, the implementing application would "request user input for authorization to complete the financial transaction" in an operation performed in response to a message communicated to computer device 400 from the payment provider's remote server upon or after the user's redirection to the payment provider's site. *See* USAA-1013, 9:32-44, 6:45-48, 10:65-11:9, 13:58-14:24; USAA-1010, 6:24-29 ("the customer may … use the payment provider system to make purchases when redirected to the payment provider system from the merchant's site").

125. Upon receiving the user's input from "biometric sensor 440," the Crypto SE application would "verify or confirm that the user is authorized" through a process that "may include but is not limited to a table or database lookup, [and] fingerprint matching …." USAA-1013, 9:45-64, 10:65-11:9; USAA-1010, 11:44-51 ("preparing the device for payment may prompt a payment application … to check 604 the biometric sensor for biometric input"). For

example, biometric sensor 440 would capture a representation of the user's fingerprint," and a digital template "derived from the captured representation" would be "compared with one or more stored reference digital templates," with a "positive match" yielding identification and/or authentication. USAA-1013, 7:44-56; USAA-1010, 9:60-65 ("a biometric authentication application … may evaluate the biometric data and compare the data to data from a registered user").

126. Upon authorization, the Crypto SE application would "look up in a table or database the appropriate identifier or credential needed," and would "transmit a permission token, number or string such as an http post login string and/or other appropriate credential to" the payment provider's remote server. Id., 3:3-25, 9:55-10:3, 3:3-14, FIG. 2. For example, the Crypto SE application would "look up the appropriate payment credential needed to complete the transaction," and "encrypt and transmit the requisite http request string and payment credential over the public network" to the remote server. USAA-1013, 11:10-29, 9:65-10:16; USAA-1010, 11:62-12:21, 12:22-43 ("[p]ayment information may include … amount and account number, and may include a CVV … "[t]his information may be correlated with signature information" that is "used to identify the client device and its user").

127. A POSITA would have been motivated to enhance Mardikar '318's system based on Chhabra in this and other ways because they would have

understood that, consistent with the teachings of both references, doing so would provide the user with a more convenient and secure process for completing web-based financial transactions, among multiple additional advantages, including:

128. Enabling Mardikar '318's user computing device 400 to securely send authentication information and/or other user credentials to a payment provider's remote server for purposes of login, upon or after being redirected to the payment provider's site, so as to enhance user convenience and avoid exposing the credentials to a third party. USAA-1013, 1:31-33, 7:65-10:55, FIGS. 4, 5; USAA-1010, 4:9-11 ("the Customer expects convenient, friendly and secure services within a trusted environment"), 6:13-29, FIGS. 4, 5a, 5b.

129. Enabling Mardikar '318's user computing device 400 to "send[] credentials securely" to a payment provider's remote server, upon or after being redirected to the payment provider's site, so as to enhance user convenience, and "so that the customer does not expose payment information directly to the merchant." USAA-1010, 4:9-11, 6:19-23; USAA-1013, 1:31-33, FIG. 4.

130. Enabling "a payment provider system (PP), such as PayPal" to provide secure "payment processing for online transactions on behalf of the customer" when the customer initiates those transactions through a browsing session performed on Mardikar '318's user computing device 400, so as to enhance user convenience and transaction security in the context of web-based transactions,

and so as to enhance the overall utility of the payment provider system to the user. USAA-1010, 5:34-47 ("Customer 305 may desire to purchase or pay for goods or services provided by merchant/service provider"), 6:19-23, FIG. 3; USAA-1013, 1:34-45, 7:65-11:29, FIGS. 4, 5.

131. In these and other scenarios involving web based-transactions, providing strong second factor authentication to verify the authenticity of computing device 400 and its user, and to thereby further enhance the convenience and security of those transactions for all involved. USAA-1010, 4:7-17 ("although each player may have its own culture and expectations, they all have the same basic requirement—the need for security and confidentiality"), 5:34-61 ("a Trusted Service Manager (TSM) 325 may provide a single point of contact for Service Provider 315, or providers, to access their customers"), FIG.3; USAA-1013, 3:26-43; USAA-1012[5], ¶¶ [0005]-[0014] (emphasizing the importance of second factor authentication in a similar SMS context), [0020], [0030]-[0031].

---

[5] Mardikar '673 is a publication of a related application that was filed 3 days after Mardikar '318 and that, like Mardikar '318, was assigned to eBay Inc. USAA-1012, Cover Page. Mardikar '673 describes techniques for secure SMS transactions, but a POSITA would have understood and found obvious that the

132. These among other advantages would have amply motivated a POSITA to integrate Chhabra's teachings into Mardikar '318 in a manner enabling Mardikar '318's user computing device 400 to securely log in to a payment provider's site when redirected to that site from a merchant's site during a browser session, and/or to securely complete an associated financial transaction through the payment provider's site during that browser session. USAA-1010, 6:13-29, FIGS. 4, 5a, 5b; USAA-1013, 10:40-55, FIGS. 1, 3, 4, 5.

133. 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 prior to the earliest effective filing date. Indeed, the change would have amounted to nothing more than the use of a known technique to improve similar devices – in each instance a computing device equipped with hardware and software for performing biometric authentication and related cryptographic techniques in the context of securing financial transactions – in a similar way, and combining prior art elements according to known methods to

---

advantages ascribed by Mardikar '673 to biometric authentication in that context are similarly applicable to the web-based transactions enabled through integration of Chhabra's teachings into Mardikar '318. USAA-1012, ¶¶ [0005]-[0014], [0020], [0030]-[0031].

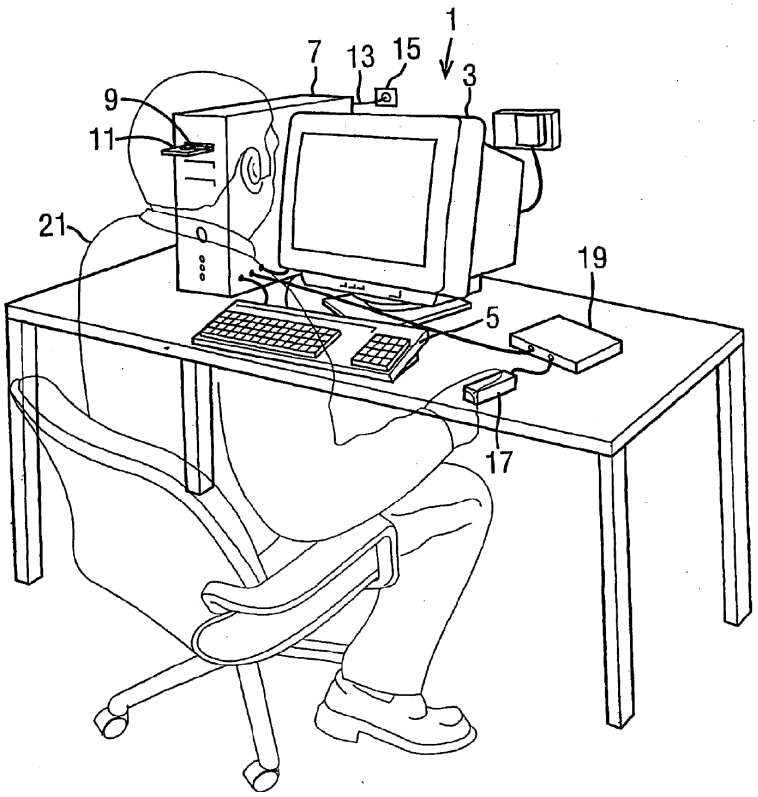
yield the predictable results described above. USAA-1010, 9:60-65, 10:42-12:43, FIG. 4; USAA-1013, 6:45-48, 9:32-44, 10:40-11:9, 13:58-14:24, FIGS. 3, 5. In addition, the elements of the resulting combination would each perform functions they had been known to perform prior to the combination. Accordingly, a POSITA would have had more than a reasonable expectation of success when incorporating Chhabra's teachings into Mardikar '318.

I. U.S. Patent App. Pub. No. 2004/0111625 ("Duffy")

134. Duffy is directed to "generating a cryptographic key using data representative of an analogue source" such as "using biometric data obtained by scanning a fingerprint, an iris, a retina or the like." USAA-1014, Abstract, [0001]. Duffy describes "a computer system including a fingerprint sensor and a cryptography unit" in one of the embodiments. USAA-1014, [0015], [0029] ("FIG. 1 shows a computer 1 having a display 3, a keyboard 5 and a computer tower 7 which includes a slot 9 for receiving a floppy disk 11. The computer tower 7 includes a modem (not shown) which is connected, via a cable 13, to a telephone socket 15 to allow access to the Internet. A fingerprint sensor 17, which in this embodiment includes an ATMEL thermal sensing chip, is connected to a cryptographic unit 19 which is in turn connected to the computer tower 7."), FIG. 1. Duffy explains, "[A] dedicated cryptography unit is used to process the biometric data and to perform cryptographic operations. However, these operations

could instead be performed by computer programs executed by a conventional computer." USAA-1014, [0088].

Fig. 1



USAA-1014, FIG. 1

135. In one aspect, Duffy tries to mitigate system vulnerabilities by associated with storage of the entire cryptographic keys. USAA-1014, [0003] ("It is important that the cryptographic key used in a symmetric encryption system or the private key used in an asymmetric encryption system is known only by authorized personnel or devices. However, the cryptographic keys employed are typically large numbers which are difficult for a person to memorise [*sic*] and

therefore a permanent record of the cryptographic key is generally made. This raises the problem of security of the permanent record.”).

136. Responsive to these concerns, Duffy describes storing a subset of a cryptographic key[6]. Duffy describes a cryptographic key that is combination of (1) an intermediate key (reflecting a post-enrollment biometric capture) with (2) a mapping key stored in NVRAM (generated during biometric enrollment). Duffy notes that “a biometric value is calculated using image data representative of the fingerprint of a user. This biometric value forms an intermediate key linking a mapping key with a cryptographic key.” *See e.g.*, USAA-1014, [0113], Abstract, [0008], [0031], [0044].

137. The “mapping key” is generated during the ENROL_USER[7], i.e., user enrollment, and is a combination of the private key (used for encryption and/or decryption) and the biometric value, and is “stored in a mapping key store 1013,” e.g., in a NVRAM 41 of the cryptography unit 19. USAA-1014, [0043] (“The CPU 35 then processes, in step S7, the private key K_{pri} and the biometric value K_{bio} to generate the mapping key K_{map}. In this embodiment, the private key K_{pri} is a 128-bit binary number and the mapping key K_{map} is generated by subtracting the

---

[6] In some cases, this is referred to as a “Triple Key Cryptography.”

[7] ENROL_USER (user enrollment) is described in at least [37]-[44].

biometric value K_{bio} from the private key K_{pri} as shown in equation 1. $K_{map}=K_{pri}-K_{bio}$ (1)"), FIG. 2 (showing generation of the mapping key K_{map} from combining the biometric value K_{bio} with the private key K_{pri}, by the "mapping key generator 1009" and storage of the generated mapping key in a mapping key store 1013), [0031], [0034] (cryptography unit 19 having "a non-volatile random access memory (NVRAM)"), [0037] (FIG. 5 showing "NVRAM 41 stores the mapping key 61"), [0044], FIGS. 5, 6 (step S7 "process private key and biometric value to generate mapping key").

138. Duffy explains that "[i]n this way, it is not necessary to maintain a permanent record of the cryptographic key. Although the mapping key is stored, by itself the mapping key gives no information about the cryptographic key." USAA-1014, [0008]. That is, while Duffy describes storing K_{map}, the entire cryptographic key need not be stored. See, e.g., [81] (noting that private key $K_{pri}= K_{map} + K_{bio}$).

139. Duffy explains "[i]n the first embodiment, the mapping function which is applied to the intermediate key (i.e. the biometric value K_{bio}) and the mapping key K_{map} is a simple addition. However, any mapping function which is monotonic, i.e. each set of input variables generates a unique output, could be used. For example, the mapping function could be a simple subtraction. It can be shown that the mapping function used does not affect the security of the system. A bit-wise exclusive-OR function could also be used both to combine the

intermediate key and the cryptographic key to generate the mapping key, and subsequently to combine the intermediate key and the mapping key to generate the private key." USAA-1014, [0117].

140. To avoid having a permanent record of the private key (or "cryptographic key"), Duffy describes a method where the private key, subsequent to an initial enrollment process (the "ENROL_USER routine"), "can only be regenerated when new biometric data corresponding to the fingerprint of the user 21 is received and processed to regenerate the biometric value K_{bio}" through a "RECOVER_PRIVATE_KEY routine." USAA-1014, [0044] ("The ENROL-_USER routine then concludes by deleting, in step S13, the private key K_{pri}, the biometric value K_{bio}, and the biometric data. Therefore, after the ENROL_USER routine has been completed, the private key K_{pri} is not stored anywhere in the cryptography unit 19 and can only be regenerated when new biometric data corresponding to the fingerprint of the user 21 is received and processed to regenerate the biometric value K_{bio}. The mapping key K_{map}, which is stored in the cryptography unit 19, by itself gives no information concerning the private key K_{pri}."); *see also id.*, [0034] (describing the "main components of the cryptography unit 19" including "central processing unit (CPU) 35, a read only memory (ROM) 37, a random access memory (RAM) 39, a non-volatile random access memory (NVRAM) 41," and "a cryptography processor 45, which is configured to perform

any required cryptographic operations."), [0035] ("In this embodiment, the cryptography processor 45 is capable of generating the private key K_{pri} and the public key K_{pub}, pair using [an] RSA algorithm.").

141. In more detail, Duffy describes an "ENROL_USER routine 51" for enrolling a new user, where a "biometric value K_{bio}," a "private key K_{pri}," and a "mapping key K_{map}" are generated and linked together through a mapping function. USAA-1014, [0031], [0036] ("The ROM 37 stores a number of routines which are used during operation of the cryptography unit 19, four of which are shown in FIG. 4. An ENROL USER routine 51 is used to process image data corresponding to the fingerprint of a new user 21 to generate the biometric value K_{bio}, and subsequently to generate a mapping key K_{map} which when combined with the generated biometric value K_{bio} using a mapping function generates the private key K_{pri} for the user 21."), FIGS. 2, 4, 6. "When enrolling a new user, the number generator 1003 processes one or more feature templates representative of the fingerprint of the new user and determines processing instructions and process variables which improve the repeatability of a generated biometric value K_{bio}. These processing instructions and process variables are stored as an ambiguity resolution vector 1005. A switch 1007 then directs the biometric value K_{bio} to a mapping key generator 1009, and a cryptographic key generator 1011 generates a private key K_{pri} and public key K_{pub} pair, of which the public key K_{pub} is sent to a certifying

authority and the private K_{pri} is input to the mapping key generator 1009. The biometric value K_{bio} and the private key K_{pri} are used by the mapping key generator 1009 to generate a mapping key K_{map}, using a monotonic mapping function, and the mapping key K_{map} is stored in a mapping key store 1013." *Id.*, [0031]. *See also id.*, [0039]-[0073] (detailed description of the "ENROL USER routine 51").

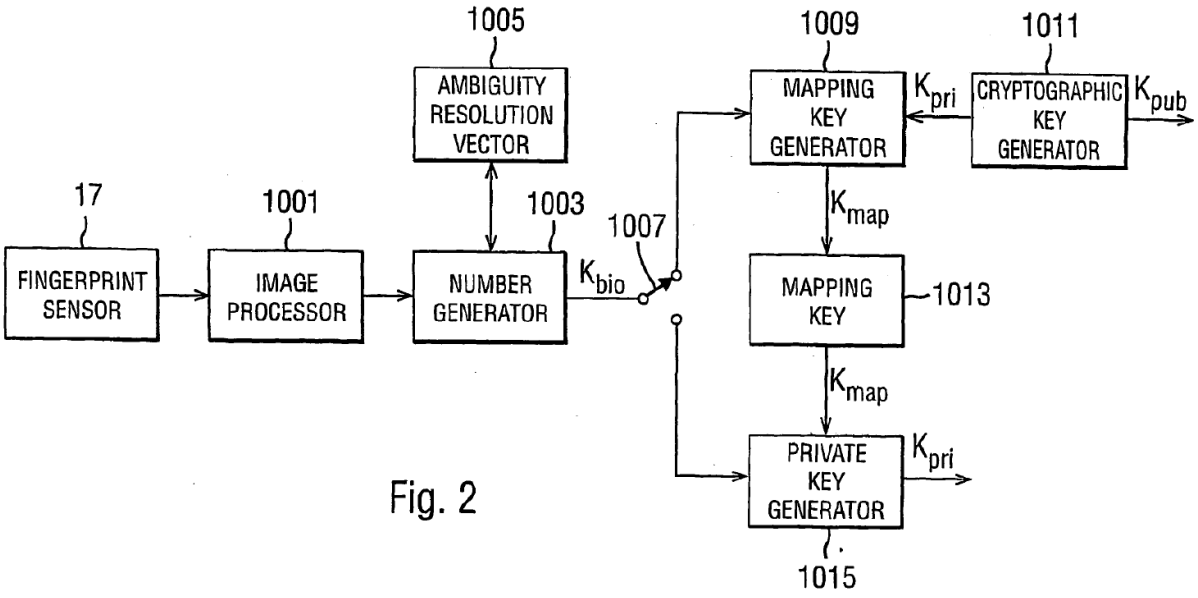
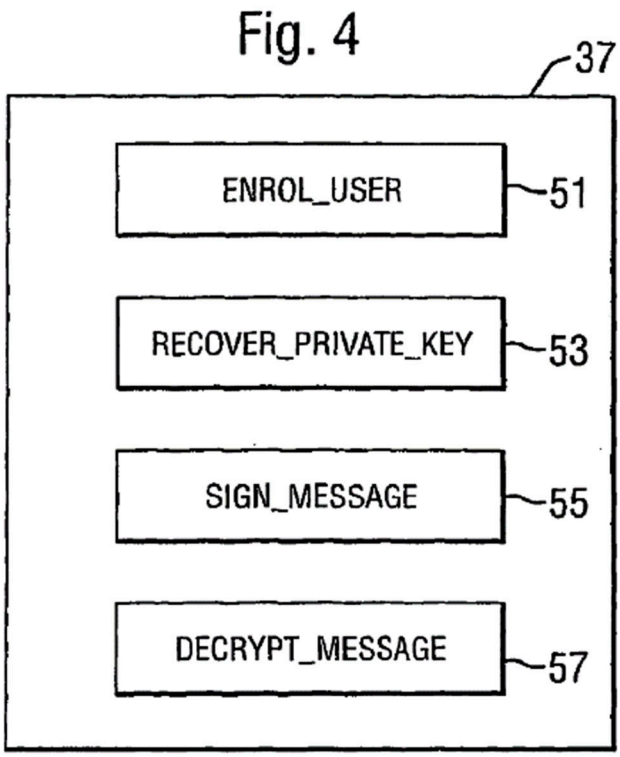


Fig. 2

USAA-1014, FIG. 2



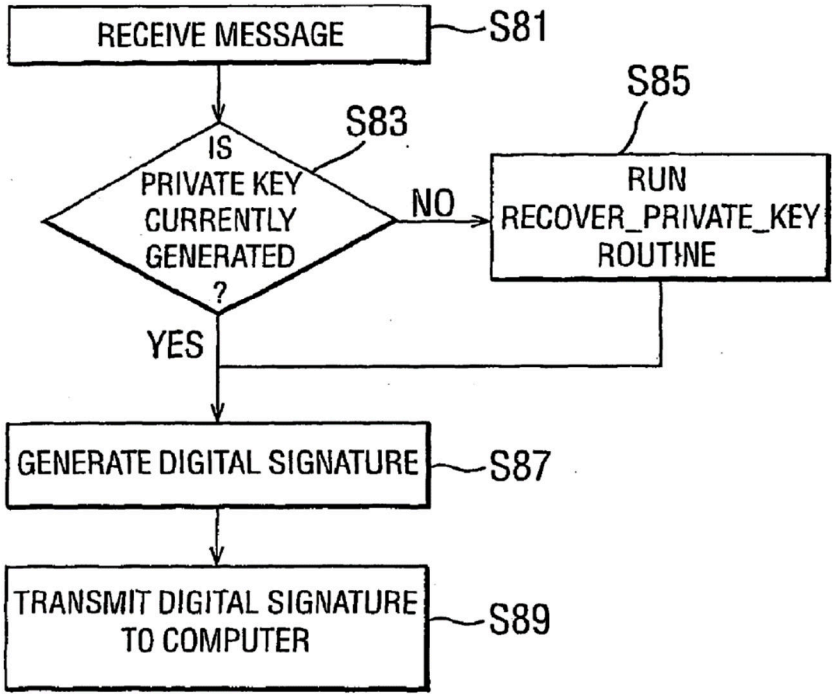
USAA-1014, FIG. 4

142. Duffy then describes a "RECOVER_PRIVATE_KEY routine 53," "[a]fter enrollment, when a user wishes to generate the private key K_{pri}, the fingerprint sensor 17 scans the fingerprint of the user and sends image data to the image processor 1001, which generates one or more feature templates. The number generator 1003 processes the one or more generated feature templates, using the processing instructions stored in the ambiguity resolution vector store 1005, to generate the biometric value K_{bio} and the switch 1007 directs the biometric value K_{bio} to a private key generator 1015. The biometric value K_{bio} and the mapping key K_{map} are combined by the private key generator 1015, using the monotonic mapping function, to generate the private key K_{pri}." USAA-1014, [0032], [0036]

("A RECOVER PRIVATE KEY routine 53 enables the private key K_{pri} associated with a user to be recovered by applying a mapping function to the biometric value K_{bio} generated from the image data for the fingerprint of the user 21 and the mapping key K_{map}."), FIG. 10; *see also id.*, [0074]-[0080] (detailed description of the RECOVER_PRIVATE_KEY routine 53"), FIG. 9.

143. Duffy further describes a "SIGN_MESSAGE routine 55 [that] is used to generate a digital signature, using the private key K_{pri} generated for a user, in order to authenticate the source and integrity of a message." USAA-1014, [0036], [0033] ("The cryptographic unit 19 is then able, for example, to create a digital signature using the private key K_{pri}"); *see also id.*, [0083]-[0085] (detailed description of the "SIGN_MESSAGE routine 55" "using the generated private key K_{pri} to generate the digital signature" for an outgoing communication). Duffy explains, [t]he digital signature is then transmitted, in step S89, to the computer 1, which attaches the digital signature to the original message to form a signed message and transmits the signed message to a desired recipient." *Id.*, [0085].

Fig. 10

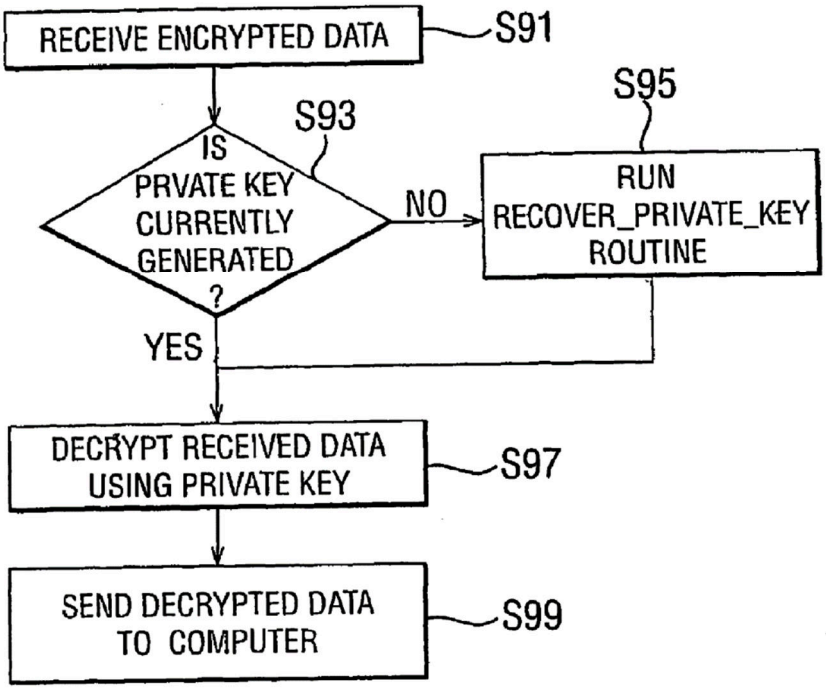


USAA-1014, FIG. 10

144. Duffy also describes a "DECRYPT_MESSAGE routine 57 [] used to decrypt, using the private key K_{pri} for the user 21, messages encoded with the associated public key K_{pub}." USAA-1014, [0036], [0033] ("The crypto unit 19 is then able, for example, to … decrypt a message received from the computer 1 using private key K_{pri}."), [0086]-[0087] (detailed description of the "DECRYPT_MESSAGE routine 57"). Upon receiving an encrypted communication (step S91), the cryptography unit "checks, in step S93, if the private key K_{pri} is currently generated." *Id.*, [0086]. "If the private key is not

currently generated, the cryptography unit 19 runs, in step S95, the RECOVER-_PRIVATE KEY routine to generate the private key K_{pri}." *Id.*, [0087].

Fig. 11



USAA-1014, FIG. 11

145. Duffy's "public key K_{pub} and a private key K_{pri} pair using the RSA algorithm is [] performed, in step S3, using the cryptography processor 45. The generated public key K_{pub} is transmitted, in step S5, to the certification authority by transmitting the public key K_{pub}, via the computer I/O port 47, to the computer 1 which in turn transmits the public key K_{pub}, via the Internet, to the certification

authority. In this way, third parties have access to the public key K_{pub}." USAA-1014, [0042].

146. Duffy's explains that the private key (as well as the public key) is used for both decrypting and encrypting messages between a sender and a recipient, "[a]s those skilled in the art will appreciate, messages encrypted with a private key K_{pri} generated using the RSA algorithm can only be decrypted using the corresponding public key K_{pub}, and similarly messages encrypted with a public key K_{pub} generated using the RSA algorithm can only be decrypted using the corresponding private key K_{pri}. These properties are put to two main uses, to create digital signatures authenticating the source and integrity of a message and to encrypt a message so that only the desired recipient can decrypt the message." USAA-1014, [0082].

J. Mardikar-Chhabra-Duffy Combination

147. A POSITA would have found obvious integration of Duffy's technology[8], and the use of K_{map} into Mardikar-Chhabra's system, thereby further enhancing Mardikar-Chhabra's security. USAA-1014, [0088]. As explained below, the result is a system with added functionality ("the Mardikar-Chhabra-Duffy system"), capable of improving the security associated with a user's private

[8] This may include the use of Duffy's Triple Encryption.

keys, by regenerating the entire key whenever needed while only storing a portion of it, K_{map} that was generated during the enrollment process. *Id*.

148. For example, the Mardikar-Chhabra-Duffy system would leverage Duffy's technology of generating a "mapping key" from a combination of a biometric value (e.g., Mardikar-Chhabra's original biometric signature/profile) with a private key, storing the mapping key locally (e.g., Crypto SE), increasing the security of the private key used on the client device afterwards, which reduces the ability of malicious actors to compromise the user's cryptographic engine. That is, the user device in Mardikar-Chhabra-Duffy only forms the entire private key whenever needed, based on the mapping key (K_{map}) and the biometric value. USAA-1014, Abstract, [0008], [0031]-[0036], [0043]-[0044], [0113], [0117]. This mapping key is thus a modified biometric signature/profile of the user.

149. In greater detail, Mardikar-Chhabra generates a biometric value (e.g., "biometric signature" or "biometric profile") from a user's biometric data, such as fingerprint, retina scan or voice data, obtained via a biometric sensor 440, and stores this biometric value in a directory of the client device. USAA-1010, 7:26-43, 10:54-62; USAA-1013, 2:22-28, 5:60-64, 7:44-64; *supra*, Mardikar-Chhabra ground. Similarly, Duffy generates a biometric value (e.g., "biometric value K_{bio}") from "biometric data obtained by scanning a fingerprint, an iris, a retina or the like," for example, "from the image data representative of the fingerprint of the

user 21" obtained from a fingerprint sensor 17. USAA-1014, Abstract, [0001], [0030]. Thus, Duffy's particular biometric techniques can be implemented in the Mardikar-Chhabra described above in Ground 2A.

150. The Mardikar-Chhabra combination operates by accessing local cryptographic keys (including private keys) on the client device, along with "unique biometric authentication information related to a specific user." USAA-1010, 7:45-63 (client device storing "private keys associated with any certificates it holds"), 9:37-43 ("In an example embodiment, the Crypto SE 420 may be designated for and arranged for loading and storing authentication data 446 (for example a PIN or biometric signature), payment instruments 447, certificates 424, crypto keys 421 and other security-related information, including, for example, unique biometric authentication information related to a specific user."), FIG. 4. Duffy provides the ability to dynamically generate a local cryptographic key, which can then readily interface with the Mardikar-Chhabra protocol.

151. A POSITA would have been motivated to implement Duffy's "Triple Key Cryptography" technology for Mardikar-Chhabra, to further enhance security, such that the **entire** private keys are no longer stored on the client device, and instead, each private key is regenerated whenever needed by processing a new biometric value in combination with the already stored mapping key, in accordance with Duffy. In the resulting system, Mardikar-Chhabra-Duffy's key relies upon

the biometric-based key (K_{map}) as taught by Duffy with the infrastructure and protocol taught by Mardikar-Chhabra.

152. A POSITA would also have been motivated to look to Duffy for implementation details to generate a "biometric signature" or "biometric profile" from "raw biometric data." USAA-1010, 7:27-43 (Mardikar '318 describing biometric sensor 440 generating "a data signal or signals representative of the user's biometric signature" from "raw biometric data" without providing implementation details); USAA-1013, 7:44-51 ("digital template" and "reference digital templates" generated using "[f]ingerprint sensor 150" without implementation details); USAA-1014, [0031], [0036], [0039]-[0073] (detailed description of generating a "biometric value K_{bio}" from raw biometric data), FIGS. 2, 6 (step S1 "receive and process biometric data to generate biometric value and ambiguity resolution vector"), 7A, 7B, 8.

153. Moreover, configuring Mardikar-Chhabra's system (e.g., modifying the Authentication Application to perform certain computer programs) to leverage Duffy's teachings would have required only routine programming knowledge that was well within the skill of a POSITA prior to the earliest effective filing date. Indeed, the change would have amounted to nothing more than the use of a known technique (Duffy's "Triple Key Cryptography" technique performed using computer programs) to improve similar devices (in each instance a computing

device equipped with hardware and software, employing encryption/decryption systems relying upon one or more cryptographic keys, for performing biometric data processing and related cryptographic operations in the context of secure information exchange with a remote party) in a similar way, and combining prior art elements according to known methods to yield the predictable results described above. *E.g.*, USAA-1010, 4:37-5:1 (client device 400), 7:27-8:47 (biometric sensor and secure elements), 10:25-11:7 (public key infrastructure and registration process), 11:11-14:28 (NFC transaction and secure SMS transaction); USAA-1013, 5:59-7:21 (computing platform 10), 7:44-64 (fingerprint sensor), 7:65-10:24 (sending credentials securely to a remote server for a transaction), 10:25-11:29 (secure transaction through a remote web site); USAA-1014, [0029] (computer 1 having fingerprint sensor 17 and other components), [0030-[0044] (generation and use of various keys including cryptographic keys), [0088] ("In the first embodiment, a dedicated cryptography unit is used to process the biometric data and to perform cryptographic operations. However, these operations could instead be performed by computer programs executed by a conventional computer.").

154. Furthermore, the elements of the resulting combination would each perform functions they had been known to perform prior to the combination. Accordingly, a POSITA would have had a reasonable expectation of success when incorporating Duffy's teachings into Mardikar-Chhabra.

IX. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '689 CLAIMS UNPATENTABLE

A. Ground 1A: Combination of Immega and Day Renders Obvious Claims 1-4 and 6-8

[1.pre] A method, comprising:

155. 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"). 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.

[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

156. Immega-Day renders obvious [1.a.i]. USAA-1004, [0008], [0041], [0043]-[0044], FIG. 3A; *supra,* §VIII.C, §V.E (Technology Overview). Preliminarily, Immega explains that the "receiver" device can comprise a "computer or any device equipped to execute the steps" described in Immega, including, for example, "cellular telephones, personal digital assistants and the like" ("a mobile device"). USAA-1004, [0041]. Moreover, as discussed above in §VIII.C, the secret is generated in Immega-Day by the device's secure email utility ("an application running on a mobile phone"), which performs the enrollment process, including receiving user fingerprints. USAA-1006, [0014], [0020].

157. Next, the receiver's device ("mobile phone") receives the receiver's fingerprint(s) ("unique user input) and generates the receiver's modified enrolled fingerprint feature set ("secret") upon receipt of and based on the receiver's live-scan fingerprint ("unique user input"). USAA-1004, [0008], [0041], [0044], FIG. 3A. In particular, during a cross-enrollment process, a user enrolls one or more fingerprints at the receiver's device ("receiving … 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, the receiver's device ("mobile phone") processes the enrolled fingerprint feature set of the user and generates the receiver's modified enrolled fingerprint feature set ("secret") based on the receiver's live-scan fingerprint ("unique user input"). USAA-1004, [0008], [0041], [0044], FIG. 3A. Immega requires "both the sender and the receiver to cross-enroll biometric feature sets," where a "fingerprint sensor" on the device generates a "biometric identifier file … uniquely modified for each recipient so that only the designated individual can employ it for messaging." USAA-1004, [0008].

158. A POSITA would have understood that the live-scan fingerprint is a unique user input since Immega explains that the "fingerprint sensor provides a biometric input, unique to each individual." USAA-1004, [0042]. Immega's teachings are analogous to the description in the '689 patent, which explains that a "security application for a computing device, e.g., a mobile phone, allows generation of a secret according to a unique user input (e.g., user credentials)." USAA-1001, Abstract. Further, it was well-known as of the Critical Date to use fingerprints as credentials. For example, Johnson's "identity credential verification subsystem 103 uses ***digital representations of fingerprints as the identity credential***;" Poo explains that fingerprints "have been legally and universally accepted for verifying identity for over a century;" and Kuhlman explains that

"other credentials, such as biometrics, have become a preferred method of authentication." USAA-1030, [0047]; USAA-1028, [0007]; USAA-1029, [0003]. Immega further 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 for each recipient so that only the designated individual can employ it for messaging." USAA-1004, [0008]. A POSITA would have understood that a modified enrolled fingerprint feature set is a "secret," especially given that it is used as an encryption key. USAA-1004, [0009], [0012]-[0014], [0018]-[0019], [0064]-[0067]. For example, Phoha defines a secret as a "quantity known only to the principals that can be used for AUTHENTICATION and encryption of information flow between them." USAA-1031, 3 (emphasis in the original). In Immega, the modified enrolled fingerprint feature sets are known only to the principals (sender and receiver) and are used for encryption of information flow between them. Further, Immega explains that "FIG. 3B shows a sample algorithm flow chart for generating a ***secret 'difference key'*** which is derived from two fingerprints and is used to encrypt and decrypt messages." USAA-1004, [0034]. Therefore, from the disclosure in Immega (e.g., "secret 'difference key'") and Phoha's definition, a POSITA would have

understood that a modified enrolled fingerprint feature set is a secret. USAA-1031, 3; USAA-1004, [0009], [0012]-[0014], [0018]-[0019], [0034], [0044], [0064]-[0067], FIG. 3A (illustrating generating a modified enrolled fingerprint feature set).

159. With respect to FIG. 3A, Immega describes generating the modified enrolled fingerprint feature set of a user:

> Starting with step 300, the centroid of the fingerprint is determined from the relative positions of the features of the fingerprint in the image. 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). The modified enrolled fingerprint feature set is then assigned to a specific person with whom messages will be exchanged (step 308).

USAA-1004, [0044].

[1.a.ii] storing said secret at said mobile device, said secret being stored with an identifier

160. Immega-Day renders obvious [1.a.ii]. USAA-1004, [0008], [0010], [0012], [0013], [0044], [0047], [0059], [0066]. In particular, the receiver's computing device ("mobile device") stores the receiver's modified enrolled

fingerprint feature set ("secret") with an identification of the "person with whom messages will be exchanged" (e.g., email address) ("identifier"). USAA-1004, [0008], [0044], [0047]. Immega first explains that, after generating the modified enrolled feature sets, they are "securely stored" and "assigned to a specific person with whom messages will be exchanged." USAA-1004, [0044]. Immega further specifically explains that a user stores his/her own modified enrolled fingerprint feature set. USAA-1004, [0009] ("The stored modified enrolled fingerprint feature set of the sender (which was previously sent to the receiver during cross-enrollment) is then retrieved"), [0010] ("In the preferred embodiments, the 'difference key' is derived from the live-scan (real-time) fingerprint feature set of the sender and the stored modified enrolled fingerprint feature set of the sender."), [0012] ("The sender's live-scan fingerprint feature set is then matched against the stored modified enrolled fingerprint feature set of the sender (which was previously sent to the receiver during cross-enrollment), validating the identity of the sender."), [0044], [0059] ("Not shown in FIG. 5, the decrypted modified enrolled fingerprint feature set of the receiver can be optionally compared to the stored modified enrolled fingerprint feature set of the receiver (which was previously sent to the specific sender during cross-enrollment)"), FIG. 2 ("creating an enrolled FP feature set of 1st User (stored)" and "modify enrolled FP feature set of 1st User…"). Thus, Immega discloses or at least suggests securely storing, at

the receiver's device, a modified enrolled fingerprint feature set of the receiver that is "assigned to [the] specific person with whom messages will be exchanged." USAA-1004, [0009], [0010], [0012], [0044], [0059].

161. As discussed in §VIII.C, in Immega-Day, the receiver's modified enrolled fingerprint feature set is securely stored in a Contacts address book located in a directory and that includes the "[m]any uniquely modified enrolled feature sets, one (or more) for each person with whom messages will be exchanged." 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]. In this way, the receiver's modified enrolled fingerprint feature set ("secret") is stored with an identification of the person with whom the Contacts entry is associated (e.g., email address) ("identifier"). Additionally, because Day's systems run on a conventional operating system such as Windows, a POSITA would have understood and found obvious that the Contacts list that stores the identifier and secret would be stored in a directory. USAA-1006, [0098]. For example, Padwick states that "C/W Outlook can access information about items

stored in your *Personal Address Book* (PAB)" (emphasis in the original) which is stored in a Windows directory such as "local settings." USAA-1023, 298, 337.

162. A POSITA would have found obvious for the receiver's modified enrolled fingerprint feature set to be securely stored in a directory that includes the "[m]any uniquely modified enrolled feature sets, one (or more) for each person with whom messages will be exchanged." USAA-1004, [0044]. Specifically, because Immega teaches that the "modified enrolled feature sets" for multiple people are stored and that each is "assigned to a specific person with whom messages will be exchanged," a POSITA would have further found obvious that each "modified enrolled fingerprint feature set" would be stored with an identifier (e.g., email address) that identifies the particular person with whom the modified enrolled feature set is associated. Storing the "modified enrolled fingerprint feature set" with a particular person would allow the computing device to identify who each "modified enrolled fingerprint feature set" is associated with for purposes of later retrieval and use. A POSITA would have further understood and found obvious that, stored in that directory, would be the receiver's own modified fingerprint feature set. USAA-1004, [0059] ("The receiver then provides a live-scan of a fingerprint and extracts an associated live-scan fingerprint feature set (step 510). The live-scan fingerprint feature set of the receiver is then compared to the stored enrolled feature set of the receiver (step 515)."), [0066] ("When the

receiver receives transmission, the receiver provides a second live-scan fingerprint (step 638) and extracts a second live-scan fingerprint feature set, 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) (step 640)."), [0013] ("Once the sender's identity is confirmed, the 'difference key' is reconstructed by subtracting the sender's live-scan fingerprint feature set from the sender's modified enrolled fingerprint feature set. The 'difference key' is then used to decrypt the receiver's modified enrolled fingerprint feature set (which was received with the message—not the original unmodified version stored on the receiver's hard drive).").

163. Moreover, Immega explains, with respect to an alternative embodiment, the use of an "Identity Server" with "databases for names and numbers, public keys of network users, and fingerprint data of network users," where the "information in the Identity Server databases allow cellular telephone users to verify identity without storing any direct biometric information in the cell phone." USAA-1004, [0021]. A POSITA would have thus understood that this alternative embodiment involving the Identity Server alleviates the need for any device to store "any direct biometric information in the cell phone." In other words, other embodiments that do not involve the Identity Server must store all biometric information on the cell phone, including, "names, numbers, public keys

of network users, and fingerprint data of network users." *Id.* In this way, fingerprint data is associated with public keys, names, and numbers—all of which a POSITA would have understood to be "identifiers." *Id.*

164. It would have been obvious to a POSITA that the receiver's own modified enrolled fingerprint feature set ("secret") would be stored in the directory at least with an identification of the person with whom messages are sent using that modified enrolled fingerprint feature set. USAA-1004, [0008] ("a user's 'enrolled fingerprint feature set' (typically a minutiae file) that has been uniquely modified for each recipient so that only the designated individual can employ it for messaging"). That is, if the receiver has cross-enrolled with Alice and Bob, two separate modified enrolled fingerprint feature sets would be stored in the receiver's directory, one uniquely modified for communications with Alice, and one uniquely modified for communications with Bob. In order for the receiver's computing device to distinguish the receiver's various enrolled fingerprint feature sets from one another, it would have been obvious that each enrolled fingerprint feature set would be stored with an identifier that identifies the particular user for which the feature set facilitates secure communication (e.g., Alice, Bob, or, generally, the user of a "remote computer-based station").

165. Moreover, because Immega contemplates communications via email, a POSITA would have further found obvious that the identifier would be the email

address, or derived from the email address, of the particular message recipient, which is what the receiver would use to communicate with each of the individuals. USAA-1004, [0006] ("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").

166. For example, Day explains that encryption keys are stored in a Contact List. USAA-1006, [0014]. Day further explains that "[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]. Since Day teaches creating a new contact that includes (among other fields) the sender's certificate after determining that the sender of the email is not within the contact list, and in the context of email, a sender is identified by the sender's email address, a POSITA would have understood that the identifier used in the contact list comprises the sender's email address.

[1.a.iii] so as to be retrievable when the unique user input is again received at the mobile device;

167. Immega-Day renders obvious [1.a.iii]. USAA-1004, [0009], [0050], [0065]. In particular, the receiver's modified enrolled fingerprint feature set ("secret") is retrievable when the receiver ("user") applies his/her fingerprint ("unique user input"). USAA-1004, [0009], [0050], [0065]. Immega explains that

when a user applies "a live-scan of the [user's] fingerprint," the "stored modified enrolled fingerprint feature set of the [user] … is then retrieved."[9] USAA-1004, [0009], [0050] ("The sender next provides a live-scan fingerprint (of a finger that has been previously enrolled) and extracts a new live-scan fingerprint feature set (step 405). The sender next retrieves his/her modified enrolled fingerprint feature set, which has been previously modified for the specific receiver (and cross-enrolled with the specific receiver) (step 410)."), [0065] ("The sender then provides a second live-scan fingerprint and extracts the second live-scan fingerprint feature set of the sender (step 628). The sender then retrieves the modified enrolled fingerprint feature set of the sender that was previously modified for the specific receiver (and cross-enrolled with the receiver) (step 630).").

[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;

168. Immega-Day renders obvious [1.b]. USAA-1004, [0009], [0041], [0042], [0062], [0065], FIG. 6. In particular, FIG. 6 of Immega shows "an algorithm flow chart for sending and receiving a biometrically certified message

---

[9] Note that the sender/receiver can be interchanged in Immega because messages are sent back-and-forth. USAA-1004, [0009], [0041].

with higher security protection," which "requires cross-enrollment of modified enrolled feature sets" of both users. USAA-1004, [0062].

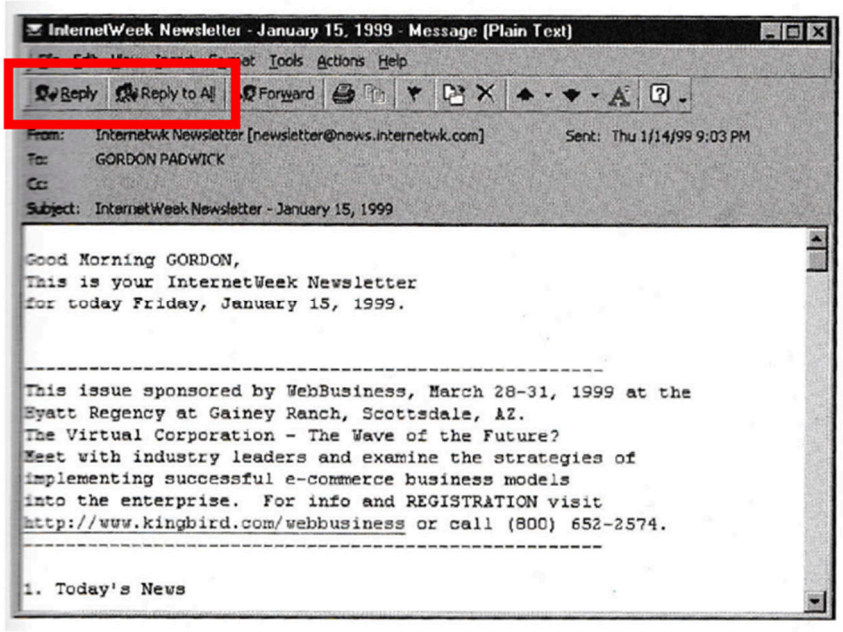
169. As shown in FIG. 6, the receiver device ("mobile device") receives from a sender's device ("remote computer-based station") a communication ("first communication"). USAA-1004, [0041] (explaining that the term "sender" as used in Immega "refers to the individual or to his/her computer or any device equipped to execute the steps described"), [0042] ("computer work stations 100-150"), [0065], FIG. 1. Immega explains that 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), 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].

170. With respect to 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 this obvious. More 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]; *see also id.*, [0020] ("An optional process allows for the sender to be given direct confirmation that the correct person has received the message, thus providing a kind of electronic "registered mail." To provide affirmative acknowledgement of reception, the receiver's second live-scan fingerprint feature set is encrypted, preferably with the "difference key" of the sender, and transmitted to the sender. "). 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 offering the user an opportunity to respond to the sender's message. *Id.*

171. Email programs commonly provided (and continue to provide) the ability for users to respond to messages. For example, Padwick explains that, in Outlook 2000, "[t]o reply to a message, select that message in the Inbox Information viewer, then choose Reply in the viewer's Standard tool bar," and "[a]lternatively, if you want to send a reply to everyone to whom the original

message was addressed (including those people on the Cc list), choose Reply to All." USAA-1023, 227; Figure 3.55.



USAA-1023, Figure 3.55 (annotated).

172. 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-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] in response to the providing, authenticating the user at the mobile device by receiving a candidate user input; and

173. Immega-Day renders obvious [1.c.i]. USAA-1004, [0008], [0019], [0042], [0066], FIG. 6. 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]. In particular, Immega states that, "[u]pon receiving the encrypted message and feature sets, the receiver provides a second live-scan fingerprint." *Id.*, [0019]. Immega further 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].

174. 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].

[1.c.ii] said mobile device verifying said user to the remote computing device in a second communication encoded using said secret.

175. Immega-Day renders obvious [1.c.ii]. USAA-1004, [0064]-[0065], [0067], FIG. 6. 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]. 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].

176. While Immega says the "direct confirmation message" is "preferably" encrypted with the sender's difference key, it would have been an obvious design choice to encrypt the confirmation message using the receiver's difference key rather than the sender's. Immega states that the message is "preferably" encrypted with the difference key of the sender, but Immega is not so limited. It would have been an obvious design choice to encrypt it with the difference key of the receiver because the sender is already in possession of the difference key of the receiver

(see step 620), which the sender would use for decrypting the message. USAA-1004, [0065]. Immega also provides a second embodiment in which the receiver's difference key is used to encrypt a response to the sender. USAA-1004, [0016]-[0018]. A POSITA would have understood that using the receiver's difference key to encrypt the response to the sender could be applied to other embodiments for many reasons. The receiver and sender would already be in possession of the difference key of the receiver (see step 612). USAA-1004, [0064]. Thus, use of the receiver's difference key would require no additional transmissions or exhcanges by either party. USAA-1004, [0064]-[0065]. A POSITA would have further understood that use of either key is equally secure at least because Immega states that "[e]ach 'difference key' is unique and can be calculated only at the point of origin and at the point of reception of the message, and can be made invisible to both sender and receiver," and that the "'difference key' is also specific to the message being sent and thus is usable one time only." USAA-1004, [0011]. Therefore, a POSITA would have understood and found obvious that both the sender's key and the receiver's key are equally secure, and either key can be used without altering the security properties of the system, and the choice of key is a simple design choice.

177. Moreover, because the "difference key" that is used to encode the second communication is "reconstructed by subtracting the first live-scan

fingerprint feature set of the receiver from the stored modified enrolled fingerprint feature set of the receiver," a POSITA would have understood and found obvious that the second communication would be encoded using the receiver's stored modified enrolled fingerprint feature set ("secret"). USAA-1004, [0065].

[2] The method of claim 1, wherein the secret comprises an encryption key.

178. Immega-Day renders obvious [2]. USAA-1004, [0009]; §VIII.C. As I explained in §VIII.A, §VIII.C, and in reference to claim 1, the process used for encrypting the communication uses information derived from the modified enrolled fingerprint feature set. Therefore, a POSITA would have understood and found obvious that the modified enrolled fingerprint feature set is an encryption key. Specifically, Immega teaches that messages are encrypted using a "difference key," which is derived from a user's live-scan fingerprint feature set and the user's modified enrolled fingerprint feature set ("secret"). USAA-1004, [0009]. Because the receiver's modified enrolled fingerprint feature set ("secret") is used directly to derive the "difference key" (which is used for encryption), a POSITA would have found obvious that the modified enrolled fingerprint feature set is an encryption key.

[3] The method of claim 1, wherein the secret comprises a static portion and a dynamic portion.

179. Immega-Day renders obvious [3]. USAA-1004, [0044], FIG. 3A. Immega describes how the modified enrolled fingerprint feature set ("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 the modified enrolled fingerprint feature set." *Id.* Thus, a POSITA would have understood that the the modified enrolled fingerprint feature set ("secret") comprises an enrolled fingerprint feature set ("static portion"), which is constant (e.g., based on the unique fingerprint feature of the user), and a displacement vector generated from a random number ("dynamic portion"), which, by its random nature, is dynamic. Indeed, as Immega teaches, the same enrolled fingerprint feature set is used to generate each the modified enrolled fingerprint feature set (and thus is static), while a different displacement vector is used for each communication partner (and thus is dynamic).

[4] The method of claim 1, wherein the first communication comprises a request for user credentials of the user of the mobile device.

180. Immega-Day renders obvious [4]. 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 live-scan fingerprint feature set." USAA-1004, [0067]. "When 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, 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.

181. The '689 Patent lists "a username and password" as examples of "user credentials" and indicates that "[o]ther forms of user credentials may be used." USAA-1001, 13:17-24. Thus, a POSITA would have understood that the receiver's live-scan fingerprint (included in a live-scan fingerprint feature set) comprises user credentials. USAA-1004, Abstract, [0042]; *infra*, Ground 1A, analysis of Claim [6]. A POSITA would have understood that any message sent by the sender that triggers the receiver's direct confirmation (which comprises the receiver's live-scan fingerprint) to be a request for user credentials of the user of the computing device. *Id.* More specifically, 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.

[6] The method of claim 1, wherein the unique user input comprises user credentials.

182. Immega-Day renders obvious [6]. USAA-1004, [0008], [0044], FIG. 3A. The receiver's live-scan fingerprint ("unique user input") comprises user credentials. USAA-1004, Abstract; *see supra*, Ground 1B, analysis of Claim [5].

The live-scan fingerprint is received via a fingerprint sensor ("user interface") of the computing device. USAA-1004, [0008]. From this and related description, a POSITA would have understood and found obvious that the user's live-scan fingerprint is/includes user credentials. For example, as I explained in §IX.A.[1.a.i], a POSITA would have understood that the live-scan fingerprint is unique user input since Immega explains that the "fingerprint sensor 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,'" and further explains that "[b]iometric certification can also be used to augment other known security means such as encryption using public key/private key systems." USAA-1004, [0042]. The purpose of the exchange of messages in Immega is to establish that messages are received by authorized parties. "An optional process allows for the sender to be given direct confirmation that the correct person has received the message, thus providing a kind of electronic 'registered mail.'" USAA-1004, [0015]. As I also explained in §IX.A.[1.a.i], it was well-known as of the Critical Date to use fingerprints as credentials. For example, Johnson's "identity credential verification subsystem 103 uses ***digital representations of fingerprints as the identity credential***;" Poo explains that fingerprints "have been legally and universally accepted for verifying identity for over a century;" and Kuhlman explains that "other credentials, such as biometrics, have become a preferred

method of authentication." USAA-1030, [0047]; USAA-1028, [0007]; USAA-1029, [0003].

[7] The method of claim 1, wherein the first and second communications comprise two related communications of a communication session.

183. Immega-Day renders obvious [7]. USAA-1004, [0067]. 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).

[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.

184. Immega-Day renders obvious [8]. First, Immega teaches generating a live-scan fingerprint feature set ("candidate identifier") using the sender's live-scan fingerprint ("received candidate user input"). 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].

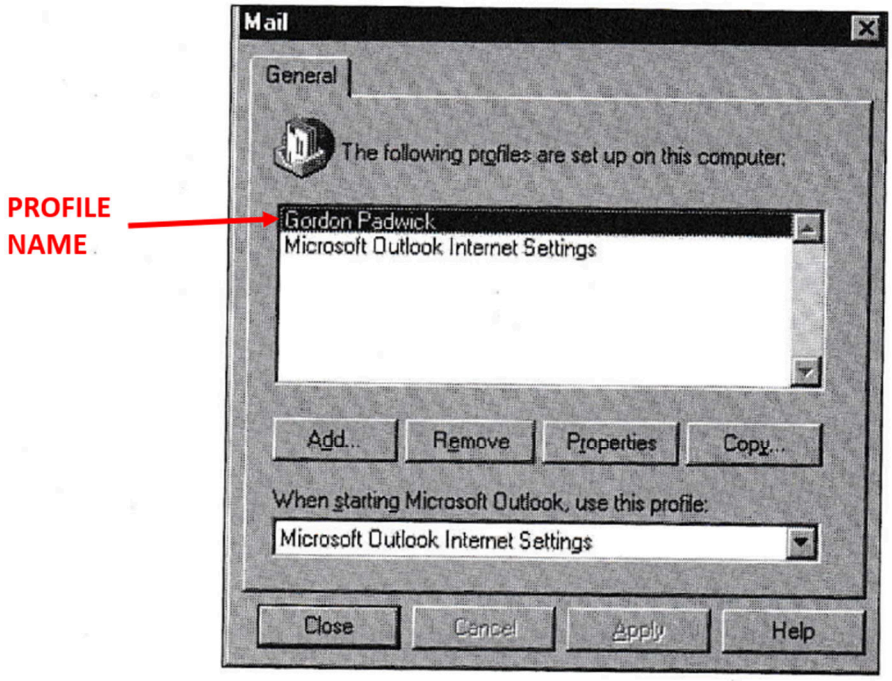
185. Next, Immega teaches determining if the live-scan fingerprint feature set ("candidate identifier") matches the identifier. For example, Immega describes

determining "[i]f the receiver's second live-scan fingerprint feature set is valid" by "extract[ing] a second live-scan fingerprint feature set, 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 §VIII.C, in Immega-Day, the receiver's modified enrolled fingerprint feature set is securely stored in a Contacts address book that includes the "[m]any uniquely modified enrolled fingerprint feature set, one (or more) for each person with whom messages will be exchanged." USAA-1004, [0044], USAA-1006, [0119]-[0120]. Thus, a POSITA would have understood and found obvious that the modified enrolled fingerprint feature set ("secret") is stored with both an identification of "person with whom messages will be exchanged" (e.g., the person's email address), as discussed for [1.a.ii] (Ground 1A), and further with an identification of the receiver. *Id.*; *supra*, Ground 1A, analysis of Element [1.a.ii]. Specifically, a POSITA would have understood and found the latter obvious at least because the modified enrolled fingerprint feature set 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).

186. For example, Outlook supports multiple profiles, which contain "information that defines how Outlook works for you." USAA-1023, 152. For

example, the profile provides access to the Outlook Contacts and the "location to which new e-mail should be delivered." USAA-1023, 152, 155. Each profile is named (as shown in FIG. 5.2 below), which enables multiple profiles on the same device, for example, when a user "share[s] a computer with other people." USAA-1023, 153-154.

Figure 5.2
Only one profile is listed if you haven't previously used Outlook or Windows Messaging.



USAA-1023, FIG. 5.2 (annotated)

187. Since a profile is associated with a user (e.g., when the computing device is shared) and provides access to the Contacts (including the senders's email address), a POSITA would have understood and found obvious that the modified enrolled fingerprint feature set is stored with an identifier that collectively includes an identifier of the sender (e.g., email address) and an

identifier of the receiver (e.g., the profile name). In this way, a POSITA would have understood and found obvious that, in matching the receiver's second live-scan fingerprint feature set against the stored fingerprint feature set of the receiver (thus matching the receiver's live-scan fingerprint feature set with the receiver), the receiver's second live-scan fingerprint feature set ("candidate identifier") is matched with the receiver (which the "identifier" comprises).

188. If the receiver's live-scan fingerprint feature set matches the identifier, Immega teaches retrieving the modified enrolled fingerprint feature set so that the receiver can "reconstruct" the difference key for decryption. USAA-1004, [0066]. Specifically, Immega explains that "the 'difference key' of the [receiver] is then reconstructed by subtracting the [receiver's second live-scan fingerprint feature set from the receiver's stored modified enrolled fingerprint feature set." USAA-1004, [0019], [0066]. That is, since the modified enrolled fingerprint feature set ("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 modified enrolled fingerprint feature set ("secret") when decoding the message. USAA-1004, [0019].

B. Ground 1B – Combination of Immega, Day, and Tomko Renders Obvious Claims 5 and 9-21

[5] The method of claim 1, wherein the secret is stored in an encrypted format.

189. Immega-Day-Tomko renders obvious [5]. USAA-1004, [0047]; USAA-1005, Abstract, 2:42-5:11. As discussed in §VIII.E, in the Immega-Day-Tomko combination, 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 in the directory. *Supra*, §VIII.E. Specifically, Tomko teaches generating "an encrypted version of a message decryption key" that 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.

[9.pre] A mobile device, comprising

190. Immega-Day-Tomko renders obvious [9.pre]. USAA-1004, [0041]; *supra*, §V.E (Technology Overview). 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*, Ground 1A, analysis of Claim [1].

[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:

191. 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. *Supra*, §§V.E (Technology Overview), 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] 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,

192. Immega-Day-Tomko renders obvious [9.b]. USAA-1004, [0041]. As discussed above in §VIII.C, §VIII.E, 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-1006, [0014], [0020]; *supra*, Ground 1A, analysis of Element [1.a.i]. The secure email utility communicates with a user via a user interface to receive a unique user input. *Supra*, Ground 1A, analysis of Element [1.a.i]. 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-1004, [0041] ("any device equipped to execute the steps described").

[9.c.i] upon receipt of said unique user input, generating a secret,

193. *Supra*, Ground 1A, analysis of Element [1.a.i].

[9.c.ii] storing said secret in said storage device, said secret being stored with an identifier

194. Immega-Day-Tomko renders obvious [9.c.ii]. *Supra*, Ground 1A, analysis of Element [1.a.ii], §V.E (Technology Overview). 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, which the '689 Patent explains can be a hard disk. USAA-1001, 27:1-8.

195. As I described in §VIII.C, Immega-Day stores its Contacts database on a hard disk. For example, Padwick explains that Outlook Contacts can be stored in a Personal Address Book, which is typically stored on a hard disk (or other storage device) in a subfolder within the "\WINDOWS\Local Setting" folder. USAA-1023, 298, 337.

196. In fact, storing application data on a storage device was (and is) a conventional technique, e.g., so application data survives with the device is powered off then on again. As one example, Chu explains that the "hard disk 1732 stores program and data files for each software component, including files distributed by the vendor as well as ***files created or updated by operation of the software after it is installed***." USAA-1035, [0161] (emphasis added). A hard disk's persistent storage is in contrast to RAM (an example of "memory" in the

’689 Patent), which “comprises volatile memory devices such as DRAM or SDRAM memory chips that do not retain their stored contents when power is removed.” USAA-1001, 27:3; USAA-1058, [0158].

[9.c.iii] so as to be retrievable when the unique user input is again received;

197. *Supra*, Ground 1A, analysis of Element [1.a.iii].

[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;

198. *Supra*, Ground 1A, analysis of Element [1.b].

[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

199. *Supra*, Ground 1A, analysis of Element [1.c.i].

[9.e.ii] recovering the secret from said storage device if the candidate identifier matches the identifier; and

200. *Supra*, Ground 1A, analysis of Claim [8] and Ground 1B, analysis of Element [9.c.ii].

[9.f] verifying said user to the remote computing device in a second communication encoded using said secret.

201. *Supra*, Ground 1A, analysis of Element [1.c.ii].

[10] The mobile device of claim 9, wherein the secret comprises an encryption key.

202. *Supra*, Ground 1A, analysis of Claim [2].

[11] The mobile device of claim 9, wherein the secret comprises a static portion and a dynamic portion.

203. *Supra*, Ground 1A, analysis of Claim [3].

[12] The mobile device of claim 9, wherein the first communication comprises a request for user credentials of the user of the mobile device.

204. *Supra*, Ground 1A, analysis of Claim [4].

[13] The mobile device of claim 9, wherein the secret is stored in an encrypted format.

205. *Supra*, Ground 1B, analysis of Claim [5].

[14] The mobile device of claim 9, wherein the proffered user input comprises user credentials.

206. *Supra*, Ground 1A, analysis of Claim [6].

[15] The mobile device of claim 9, wherein the first and second communications comprise two related communications of a communication session.

207. *Supra*, Ground 1A, analysis of Claim [7].

[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:

208. To the extent the preamble is limiting, Immega-Day-Tomko renders obvious [16.pre]. *Supra*, Ground 1B, analysis of Element [9.a]; §§V.E (Technology Overview), VIII.E.i.

[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,

209. Immega-Day-Tomko renders obvious [16.a]. USAA-1004, [0041]; *supra*, §V.E (Technology Overview).

210. As discussed above in §VIII.c, §VIII.E, the Immega-Day-Tomko device's secure email utility is an application running on a processor-based

platform. 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. For example, Jobs's "device has a touch-sensitive display (also known as a "touch screen") with a graphical user interface (GUI), ***one or more processors***, memory and one or more modules, programs or sets of instructions stored in the memory for performing multiple functions." USAA-1032, [0008]. The "***processors 120 run or execute various software programs and/or sets of instructions stored in memory*** 102 to perform various functions for the device 100 and to process data." USAA-1032, [0098]. A POSITA would have understood that the Immega-Day-Tomko device's secure email utility is an example of an application as described by Jobs. Similarly, Granito's "***computing device 1000 includes a processor*** 1005, a memory 1010, an input/output controller 1015, a GPS receiver 1020, a network adapter 1025, and a storage device 1030," and the "***processor 1005 is capable of processing instructions for execution*** within the computing device 1000." USAA-1034, [0075]-[0076]. More generally, processor-based mobile devices were well-known as of the Critical Date.

211. The processor-based platform executes instructions for communication with at least one remote computer-based station, e.g., the sender.

Supra, Ground 1A, analysis of Element [1.b]. Further, note that, as described above, both Jobs's and Granito's devices execute instructions. USAA-1032, [0098]; USAA-1034, [0075]-[0076].

212. The secure email utility is configured to receive a unique user input. *Supra*, Ground 1B, analysis of Element [9.b].

[16.b.i] upon receipt of said unique user input, generating a secret,

213. *Supra*, Ground 1A, analysis of Element [1.a.i].

[16.b.ii] storing said secret in a memory of said processor-based platform, said secret being stored with an identifier

214. *Supra*, Ground 1A, analyses of Elements [1.a.ii] and [9.c.ii].

215. 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. *Supra*, §V.E (Technology Overview).

216. As I described with respect to [9.c.ii], the secret is stored in the Contacts database, which is stored on a persistent media such as a hard drive so the data survives when the device reboots. §IX.B.[9.c.ii].

217. However, a POSITA would have understood and found obvious that to use the secret (i.e., to make the data available to the processor), the secret would be stored in memory since such operation (i.e., loading data from persistent storage, e.g., a hard drive, into volatile storage, e.g., RAM), is how most computing devices operated (and continue to operate). For example, Chu explains

that "the CPU 1710 executes instructions and ***manipulates data stored in the system memor***y." USAA-1035, [0148]. Note that both Chu and the '689 patent explains can be RAM. USAA-1001, 27:3; USAA-1035, [0158].

218. Therefore, in Immega-Day, the secret is stored in a Contacts database on a hard drive so that the data survive when the device reboots, and loaded to memory (RAM) when needed by the processor, e.g., to encrypt and/or decrypt data.

[16.b.iii] so as to be retrievable when the unique user input is again received;

219. *Supra*, Ground 1A, analysis of Element [1.a.iii].

[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;

220. *Supra*, Ground 1A, analysis of Element [1.b].

[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

221. *Supra*, Ground 1A, analysis of Element [1.c.i].

[16.d.ii] recovering the secret from said memory if the candidate identifier matches the identifier; and

222. *Supra*, Ground 1A, analysis of Claim [8].

[16.e] verifying said user to the remote computing device in a second communication encoded using said secret.

223. *Supra*, Ground 1A, analysis of Element [1.c.ii].

[17] The non-transitory computer-readable medium of claim 16, wherein the secret comprises an encryption key.

224. *Supra*, Ground 1A, analysis of Claim [2].

[18] The non-transitory computer-readable medium of claim 16, wherein the secret comprises a static portion and a dynamic portion.

225. *Supra*, Ground 1A, analysis of Claim [3].

[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.

226. *Supra*, Ground 1A, analysis of Claim [4].

[20] The non-transitory computer-readable medium of claim 16, wherein the secret is stored in an encrypted format.

227. *Supra*, Ground 1B, analysis of Claim [5].

[21] The non-transitory computer-readable medium of claim 16, wherein the proffered user input comprises user credentials.

228. *Supra*, Ground 1A, analysis of Claim [6].

C. Ground 2A: Combination of Mardikar '318 and Chhabra Renders Obvious Claims 1-4 and 6-7

[1.pre] A method, comprising:

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

230. For example, 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.

[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

231. Mardikar-Chhabra renders obvious [1.a.i]. Mardikar '318 explains that "[c]lient device 400 may be implemented using any appropriate combination of hardware and/or software configured for wired and/or wireless communication over a network," adding 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.

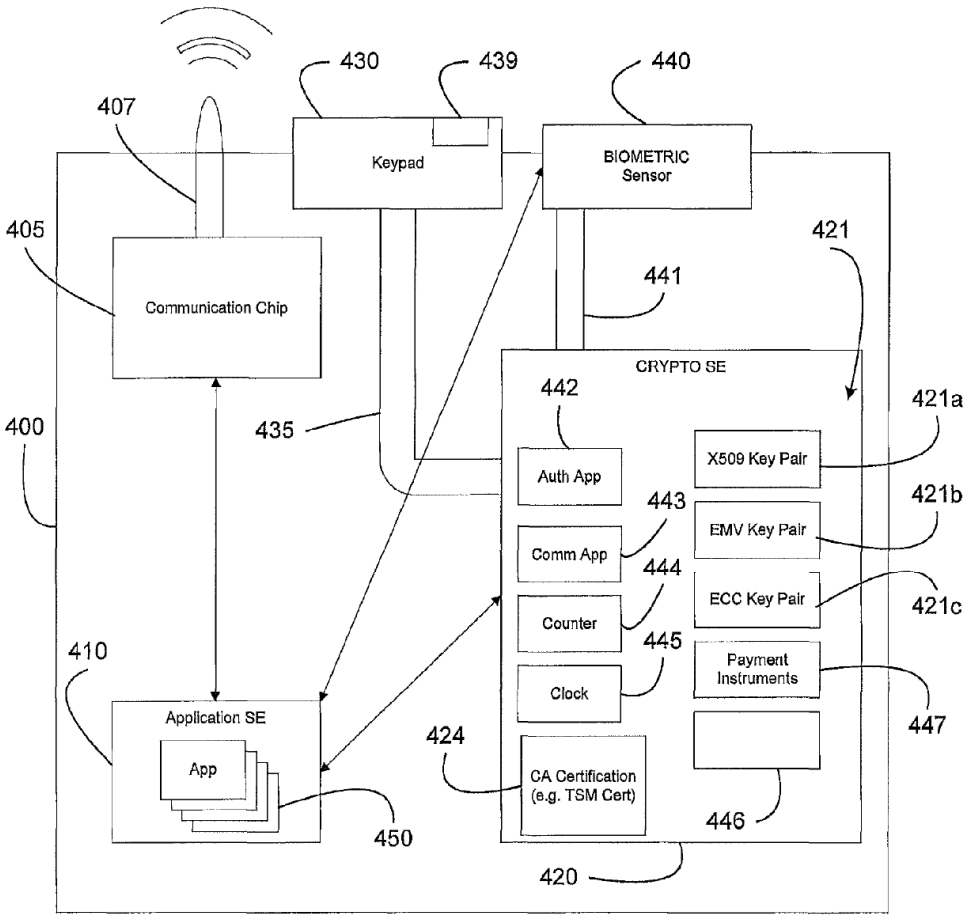


FIG. 4

USAA-1010, FIG. 4

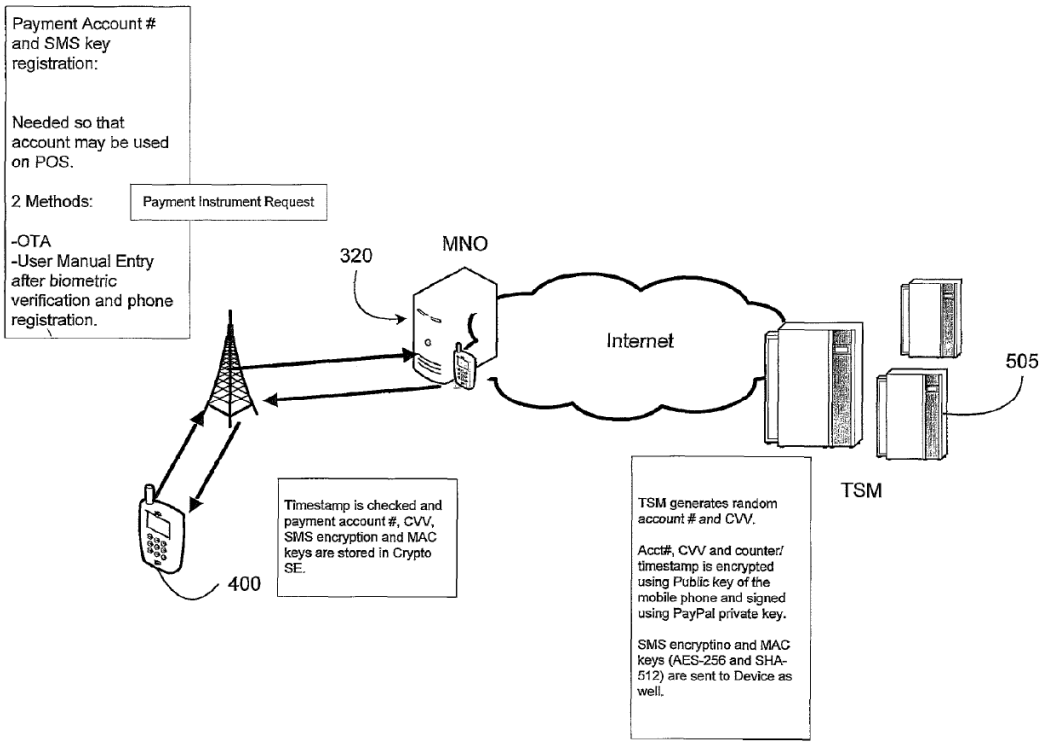


FIG. 5b

USAA-1010, FIG. 5b

232. For at least these reasons, a POSITA would have understood and found obvious that client device 400 is a mobile computing and communication device. USAA-1010, 1:60-64, 4:7-49, FIGS. 3, 4, 5a, 5b.

233. A POSITA would have further understood and found obvious that client device 400 includes as a component another mobile device: Crypto SE 421, which Mardikar '318 describes as a "small, relatively tamper-proof" "smart card" computer that itself "contain[s] a CPU and some non-volatile storage," and that in at least some embodiments further includes "a communication application" and/or other means to "establish a direct, secure transmission between the Crypto SE 410"

and other devices "using technologies like Secure Socket Layer (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.

234. A POSITA would have understood and found obvious that an application running on Crypto SE 420 generates a secret based upon a unique user input, at least insofar as Mardikar '318 explains that a biometric authentication application 442 "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.

235. Mardikar '318 explains, for example, that "[r]egistration may include" unlocking "a payment credential 424 (FIG. 4) … 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 (describing "biometric sensor 440," "for example a finger/thumb-print sensor, retina scan or voice identifier" that "sense, measure, evaluate and generate a data signal or signals representative of the user's biometric signature" which is "stored as authentication data 446 on the Crypto SE 420"), 15:54-16:45. And Chhabra similarly discloses

that its "[f]ingerprint sensor 150 may be or include a sensor for capturing a representation of a user's fingerprint for authentication or identification of a user," and that "[a] digital template may be derived from the captured representation and compared with one or more stored reference digital templates," with a "positive match" providing a basis for authenticating or identifying a user. USAA-1013, 7:44-51, 7:57-64, 8:33-35, 9:31-39, 9:45-50, 11:2-7, FIG. 4.

236. From this and related description, a POSITA would have understood and found obvious that the biometric authorization application 442 running on Mardikar-Chhabra's client device 400, via the biometric sensor 440 ("user interface"), communicates with the user of the client device to receive one or more unique user inputs (for example, two thumbprints), that the sensor captures and sends those inputs to Crypto SE 420, and that the biometric authorization application 442 generates and stores the user's unique biometric profile/signature based upon the received inputs, for purposes of enabling user authentication in the context of financial transactions involving the associated payment credential. USAA-1010, USAA-1010, 2:58-59, 7:28-42, 9:60-65, 10:42-11:7, FIGS. 4, 5a, 5b,

15:54-16:45; USAA-1013, Abstract, 7:44-51, 7:57-64, 8:33-40, 9:31-39, 9:45-50, 11:2-7, FIG. 4; *see also* USAA-1011[10], [0040]-[0046], FIGS. 4, 5.

237. More, a POSITA would have understood and found obvious that Mardikar-Chhabra's "biometric profile"/"biometric signature" is a "secret", both because Mardikar '318 and Chhabra each independently emphasize the importance of maintaining the security/secrecy of the user's biometric data, and because sensitive data was commonly understood to be a type of "secret." *See* USAA-1010, 7:28-42 (explaining that the secure elements may be smart cards featuring "tamper-proof" "non-volatile storage," which "makes it possible for the card to keep some secrets, such as the private keys associated with any certificates it holds"), 7:27-9:23, FIG. 4; USAA-1013, 5:59-7:64, FIG. 3; *see also* USAA-1017, 136 (explaining basic concepts of "Practical Cryptography", including that "we have two types of secrets: the keys and the data"), 347-362 (describing techniques

---

[10] Mardikar '140 is a publication of a related application that was filed 2 months before Mardikar '318 and that, like Mardikar '318, was assigned to eBay Inc. USAA-1011, Cover Page. Mardikar '140 provides additional description of systems and methods that are strongly similar to those disclosed by Mardikar '318, and a POSITA would have understood that those additional descriptions are relevant to Mardikar '318's teachings.

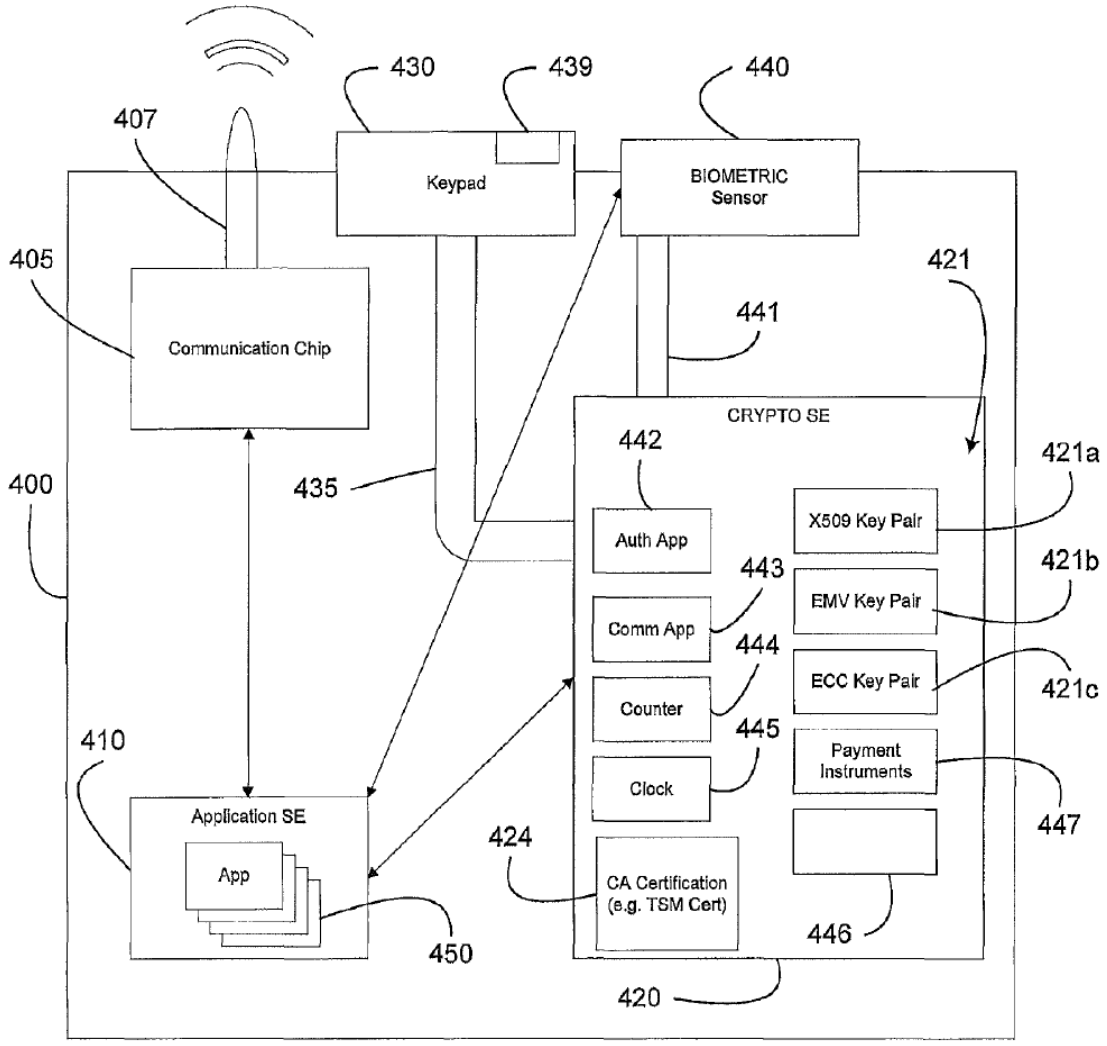
for storing "long-term secrets, such as passwords and private keys," including the use of a secure token such as a "smart card").

[1.a.ii] storing said secret at said mobile device, said secret being stored with an identifier

238. Mardikar-Chhabra renders obvious [1.a.ii]. A POSITA would have understood and found obvious that Mardikar-Chhabra stores the user's generated "biometric profile"/"biometric signature" ("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 ("The biometric signature may be stored as authentication data 446 on the Crypto SE 420"), 7:44-57 (example implementation of a "Secure Element" such as a "smart card" including "some non-volatile storage"), 9:36-47, 9:60-65, 10:42-11:7, FIGS. 4, 5a, 5b, 15:54-16:45.

239. As explained above, and as shown in Mardikar '318's FIG. 4 (reproduced below), "authentication application 442 … may evaluate … biometric data and compare the data to data from a registered user, or may register the data where the data is being collected as part of a registration or certification procedure." USAA-1010, 9:60-65, 11:44-51. In that regard, Crypto SE 420 is "arranged for loading and storing authentication data 446 (for example a PIN or biometric signature), payment instruments 447, certificates 424, crypto keys 421 and other security-related information, including, for example, unique biometric

authentication information related to a specific user." USAA-1010, 9:36-47; *see also* USAA-1011, [0041]-[0046], FIG. 4.



USAA-1010, FIG. 4

240. From this and related description, a POSITA would have understood and found obvious that biometric authentication application 442 stores "unique biometric authentication information related to a specific user" in Crypto SE 421's

memory[11] with an identifier so as to be retrievable for comparison when the user again applies their unique user input to client device 400 through biometric sensor 440 during the course of a transaction. USAA-1010, 9:60-65, 10:42-11:7, FIGS. 4, 5a, 5b; *see also* USAA-1013, 9:45-11:9 (similarly describing that "management module 130 may … verify or confirm that the user is authorized" through a process that "may include but is not limited to a table or database lookup, [and] fingerprint

---

[11] Mardikar '318 explains that a secure element (SE) "may be, for example, a smart card … embedded inside device 400," including "a CPU and some non-volatile storage" that "makes it possible for the card to keep some secrets, such as the private keys associated with any certificates it holds," adding that "Crypto SE" 420 "may be pre-loaded with applications … for facilitating financial transactions over a network, key pairs, payment instruments and/or a Certifying Authority (CA) certificate." USAA-1010, 7:45-63, 9:48-59; *see also* USAA-1011, [0031] ("a SE … is a combination of hardware, software, interfaces and protocols that enable secure storage and the use of credentials for payments, authentication and other services"), FIG. 5; USAA-1017, 347-362.

matching"), 7:44-56 ("a "digital template may be derived from the captured representation and compared with one or more stored reference digital templates").

241. In that regard, Mardikar and Chhabra describe a multitude of identifiers[12] 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 when the user again submits their unique biometric input through biometric sensor 440 during the course of a transaction. USAA-1010, 4:58-5:2 ("Client device 400 may further include one or more user identifiers that may be implemented, for example, as operating system registry entries, cookies associated with a browser application, identifiers associated with hardware of client device 400, or other appropriate identifiers. Identifiers associated with hardware of the client device 400 may be, for example, the International Mobile Equipment

---

[12] As Chhabra explains, "a credential may be a password, username, fingerprint, biometric identifier, user identification (ID) number, or other identifier, digital string, template, or other digitally encoded identifier as needed to confirm a user's authority for access to for example a software application or account," and "may also be or include a digital identifier required to authorize the completion of a transaction." USAA-1013, 2:22-34.

Identity num ber (IMEI #) or the Secure Element ID number. In one embodiment, a user identifier may be used by a payment service provider or TSM 240 to associate client device 400 or user 220 with a particular account maintained by payment service provider 240"), 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.

242. In more detail, Mardikar '318 describes the "biometric profile" as being "related to" the user, and as being generated as part of the larger registration system illustrated in Mardikar '318's FIGS. 5a and 5b (reproduced below), which yields registration of the client device 400 (e.g., with a trusted service manager 505), 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 Service Provider's user account." USAA-1010, 10:5-11:7, FIGS. 5a, 5b.

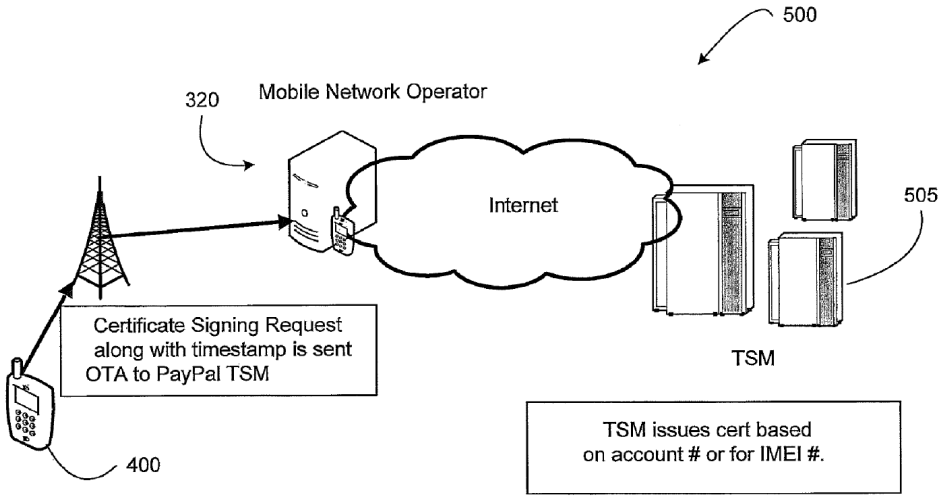


FIG. 5a

USAA-1010, FIG. 5a

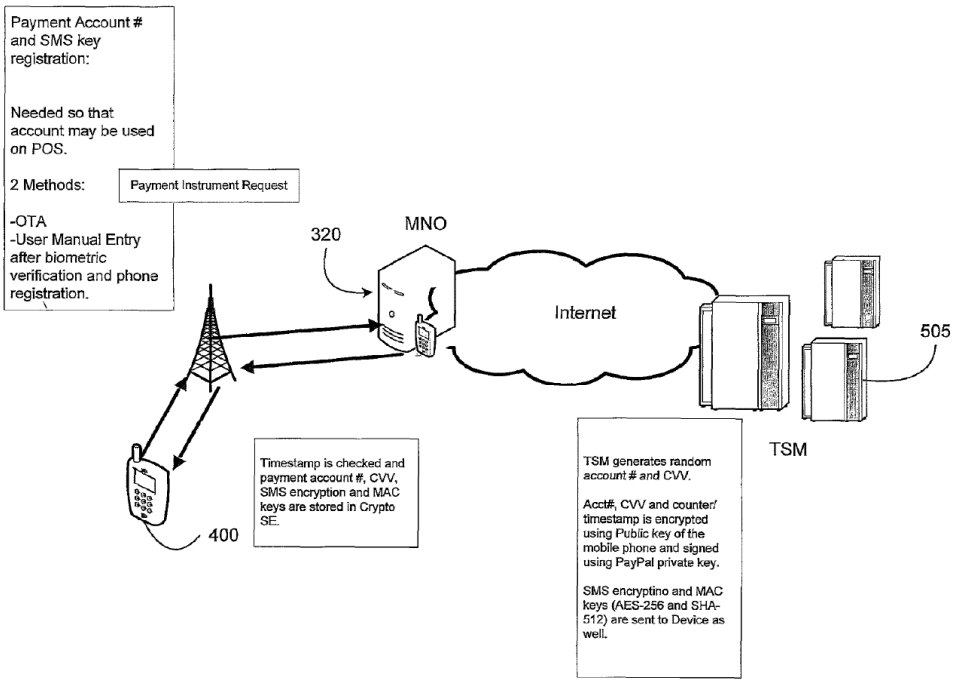


FIG. 5b

USAA-1010, FIG. 5b

243. For example, "a payment credential or CA certificate 424" may "be unlocked by registering the user's unique biometric profile using the biometric sensor 440"; the "certificate 424 is entered and associated with the Service Provider's user account," and a certificate "based on" the associated account number or IMEI device number is issued to device 400, which stores the "account #, CVV, SMS encryption and MAC keys ... in Crypto SE." USAA-1010, 10:42-11:7, FIGS. 5a, 5b.

[1.a.iii] so as to be retrievable when the unique user input is again received at the mobile device;

244. Mardikar-Chhabra renders obvious [1.a.iii]. As explained both above with respect to [1.a.ii] and in further detail below with respect to [1.b] and [1.c.i], a POSITA would have understood and found obvious that the account number, IMEI device number, server name, server domain, encryption keys, and MAC keys, etc., that are associated through Mardikar '318's registration process 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 the biometric sensor 440 in the course of a login or financial transaction. 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 ("a credential may be a password, username, fingerprint, biometric identifier, user identification (ID) number, or

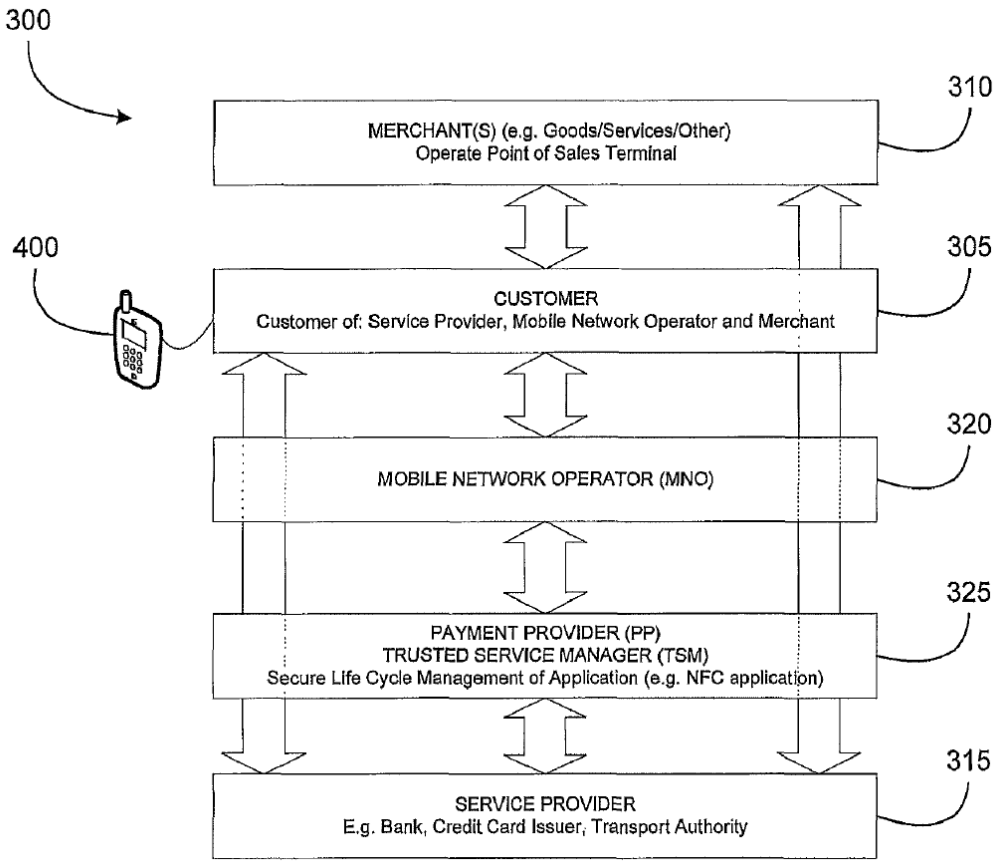
other identifier, digital string, template, or other digitally encoded identifier as needed to confirm a user's authority for access to for example a software application or account"), 4:18-21, 8:22-43, 10:8-14; USAA-1016, 10, 11-17.

245. In that regard, Mardikar-Chhabra's Crypto SE application verifies "that the user is authorized" to complete a given transaction through a process including but "not limited to 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, 11:44-51, 13:16-21. For instance, Mardikar '318 explains that "a biometric authentication application … may evaluate the biometric data and compare the data to data from a registered user." USAA-1010, 9:45-64.

246. From this and related description, 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 Service Provider account. USAA-1010, 4:20-26, 10:42-11:7 (explaining that a "CA certificate 424" may "be unlocked by registering the user's unique biometric profile using the biometric sensor 440," that the "certificate 424 is entered and associated with the Service Provider's user account," and that a certificate "based on" the associated account number is issued to device 400, which stores the "account # ... in Crypto SE"), FIGS. 5a, 5b.

247. Mardikar ’318 further explains that a user may maintain separate accounts with each of several service providers, and that Crypto SE may “register[] and verify[] various applications 450 separately for each Service Provider” based on unique user biometric data. USAA-1010, 2:2-3 (“each payment application has its own, separate security registration and verification procedures”), 2:11-14 (“unique biometric identifying information, for example a thumb or finger-print … may be captured by any of the several applications”), 9:53-65, 10:25-11:7, FIGS. 3, 5b.

248. In that regard, Mardikar ’318’s FIG. 3 (reproduced below) illustrates various service providers with whom the user of client device 400 may maintain accounts, and a POSITA would have understood and found obvious that Crypto SE would, in each separate registration procedure for each separate service provider, generate a unique “biometric profile”/“biometric signature” that would thereafter be stored in the Crypto SE with associated identifiers (e.g., a service provider account number and additional identifiers included in the associated certificate), so as to be retrievable when the user’s biometric data is again applied to client device 400 in the course of a transaction with the corresponding service provider. 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] 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;

249. Mardikar-Chhabra renders obvious [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-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.

250. As explained above, Mardikar '318's device 400 is equipped with the hardware and software necessary to enable the customer to "pre-register his account with the payment provider system," "map the account to an email address, and then use the payment provider system to make purchases when redirected to the payment provider system from the merchant's site," and a POSITA would have implemented Chhabra's additional teachings with respect to web transactions with that device and the payment provider's remote server. USAA-1010, 6:19-29, 9:60-65, 10:42-11:7, FIG. 4.

251. For example, as described by Chhabra, "a user desiring to complete a financial transaction on a web site … may be automatically redirected to a payment page" that "may request the user to enter payment credentials … an on-line payment service (e.g. PayPal®) username and password, or other credentials that may identify or authorize a user and/or a financial account." USAA-1013, 10:40-55.

252. Chhabra further explains that "the communication between computing platform 10 and remote server 20 may utilize a secure connection such as for example secure socket layer (SSL) and/or transfer layer security (TLS)," and that the computing platform 10's management module may "encrypt and transmit a …

http post login string including the [user's] credential using for example a TLS or an SSL cryptographic protocol." USAA-1013, 4:18-21, 8:22-43, 10:8-14.

253. In that regard, and as a first step toward completing the transaction through a secure connection upon being redirected to the payment service provider's remote server, a POSITA would have understood and found obvious that the Mardikar-Chhabra client device 400 and the remote server would engage in a SSL "handshake", during which the client device would send a message to the server, and then receive a message ("first communication") from the server including the server's certificate and a chain of certificates up to a Root CA. *See* USAA-1010, 12:4-21 ("Crypto SE 420 may establish a direct, secure transmission … using technologies like Secure Socket Layer (SSL)"), 10:65-67 ("A user's TSM credential or certificate 424 is entered and associated with the Service Provider's user account."); USAA-1013, 4:18-21, 8:22-43, 10:8-14; USAA-1016, 10 ("An SSL transaction … starts with the client sending a handshake to the server. In the server's response, it sends its certificate"), 10-12, 17.

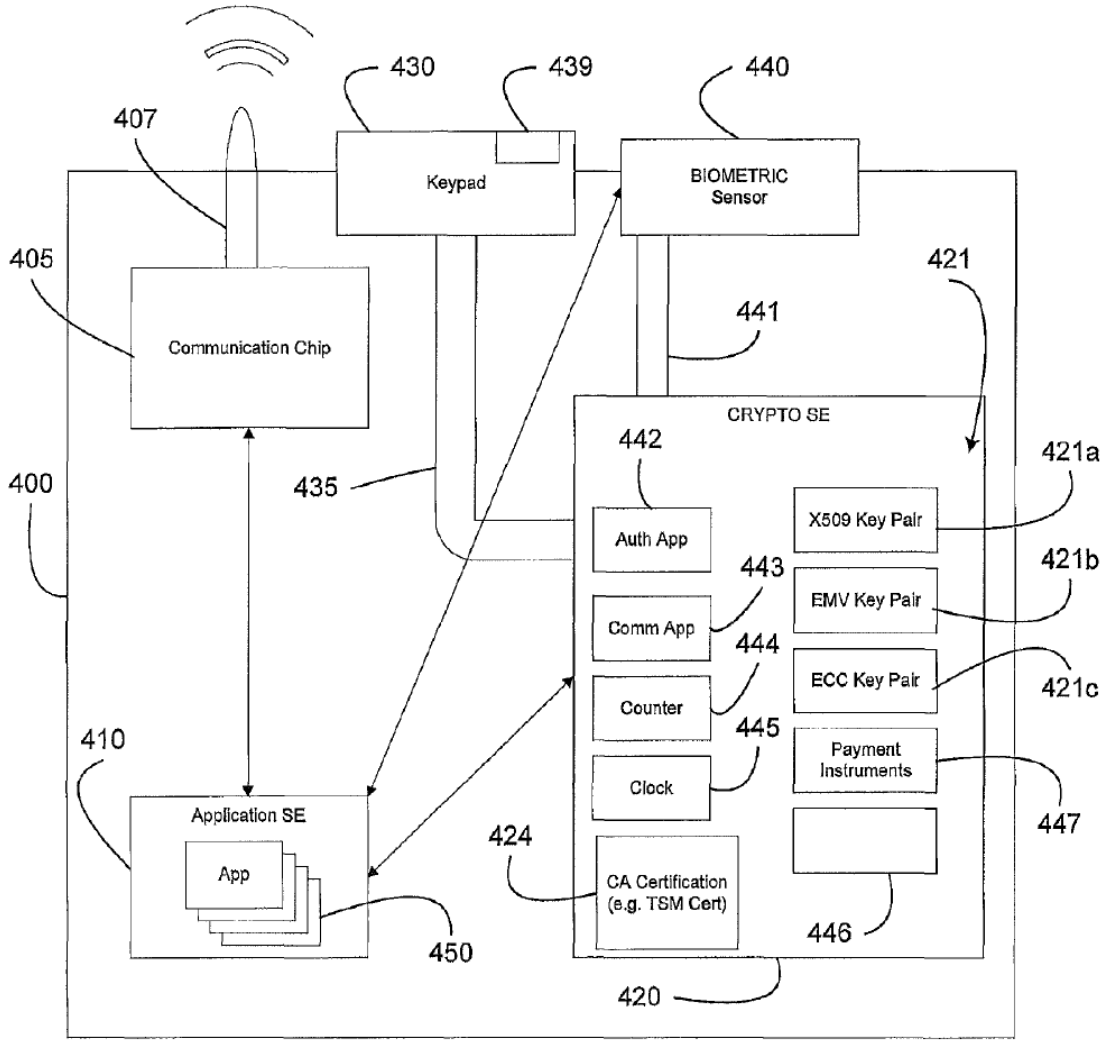
254. Furthermore, a POSITA would have understood and found obvious that the user, via the mobile device, is provided an opportunity to respond to the message from the server containing the server's certificate, by verifying the received certificate against the CA certificate already stored in device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

1010, 12:4-21 ("[i]f SSL or IPSec is used, a known Root CA may be stored in Crypto SE … [d]uring the SSL or IPSec handshake, the certificate chain containing POS's certificate and Root CA is sent by POS to crypto SE directly … [t]he Crypto SE may verify the POS's certificate against the Root CA that it already has. If the certificate matches, it may give payment information using an SSL/IPSec/secure channel"); USAA-1013, 4:18-21, 8:22-43, 10:8-14; USAA-1016, 10 ("a certificate is a piece of data that includes a public key associated with the server and other interesting information, such as the owner of the certificate, its expiration date, and the fully qualified domain name* associated with the server"), 11-17 ("for SSL to work at all, the client must be able to extract the public key from a presented certificate").

[1.c.i] in response to the providing, authenticating the user at the mobile device by receiving a candidate user input; and

255. Mardikar-Chhabra renders obvious [1.c.i]. A POSITA would have understood and found obvious that, in response to receiving the message from the payment provider's remote server, Mardikar-Chhabra's device 400 would prompt the user to again provide their unique biometric input ("a candidate user input") through biometric sensor 440, in order 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-1010, 9:60-65, 11:44-51; USAA-1013, 3:3-25, 7:44-56, 9:55-10:16, 11:10-29.

256. For example, and as shown in Mardikar ’318’s FIG. 4 (reproduced below), Crypto SE 420’s biometric authentication application 442 is configured to evaluate biometric data received from biometric sensor 440 and to “compare the data to data from a registered user,” or to register the data when it “is being collected as part of a registration or certification procedure.” USAA-1010, 9:60-65, 10:42-11:7, FIGS. 4, 5a, 5b. “Registration may include registering a biometric attribute, for example a thumb-print or finger-print, to unlock payment”; for instance, “a payment credential 424 (FIG. 4) … may be unlocked 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; 15:54-16:45.



USAA-1010, FIG. 4

257. In the context of an exemplary POS NFC transaction, Mardikar '318 further explains that "preparing the device for payment may prompt a payment application resident on the App SE 410 … to check 604 the biometric sensor for biometric input," that a user may then input 606 their biometric identifying data (ID) or signature by placing or swiping a thumb or finger on biometric sensor

440," and that the "input biometric ID may be directly sent or tunnelled 608 to Crypto SE 420 … for authentication/unlocking." USAA-1010, 11:44-51; *see also id*., 9:60-65 ("a biometric authentication application … may evaluate the biometric data and compare the data to data from a registered user"). "Once a user's biometric identity is authenticated properly, the Crypto SE 420 may send 612 an approval/disapproval message and payment or other information" for purposes of completing the transaction. USAA-1010, 11:62-12:21.

258. In at least this way, Mardikar-Chhabra renders obvious authenticating a user at the mobile device by receiving a candidate user input. USAA-1010, Abstract, 1:15-17, 3:11-33, 7:28-42, 9:60-65, 10:42-11:7, 11:44-51, 11:62-12:21, 15:54-16:45, FIGS. 4, 5a, 5b, 6a; USAA-1013, 2:22-34, 8:22-40, 9:31-10:16, 11:2-16, FIGS. 4, 5.

259. Notably, Mardikar '318 expressly indicates that "the payment information may be transmitted by alternate methods of communication," adding that "TSM 325 may act as a payment provider system (PP), such as PayPal, and 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." USAA-1010, 12:22-30, 3:11-33, 4:27-36, 6:13-29, 13:37-14:19.

260. In that regard, "the customer may pre-register his account with the payment provider system, map the account to an email address, and then use the

payment provider system to make purchases when redirected to the payment provider system from the merchant's site." *Id.*, 6:13-29. "After the financial transaction is authorized, the TSM 325 or payment provider system completes the transaction." *Id.*

261. In at least this additional way, Mardikar-Chhabra renders obvious authenticating a user at the mobile device. USAA-1010, 3:11-33, 4:27-36, 6:13-29, 12:22-30, 13:37-14:19.

262. And, as explained in more detail above with respect to the Mardikar-Chhabra combination, a POSITA would have been motivated to further enhance Mardikar '318's system, including both computer device 400 and the remote payment provider server with which it interacts, by adapting it to conveniently and securely enable authenticated web transactions along the lines that Mardikar '318 already suggests, and that Chhabra further details. USAA-1010, 6:13-29, FIG. 4; USAA-1013, 6:45-48, 9:32-11:9, 13:58-14:24, FIGS. 1, 3, 4, 5.

263. In the resulting Mardikar-Chhabra system, biometric authentication application 442 and/or another application running on Crypto SE 420 would "request user input for authorization to complete the financial transaction" in an operation performed in response to a message communicated to computer device 400 from the payment provider's remote server, and upon receiving the user's input from "biometric sensor 440," the Crypto SE application would "verify or

confirm that the user is authorized" through a process that "may include but is not limited to a table or database lookup, [and] fingerprint matching …." USAA-1013, 6:45-48, 9:32-64, 10:65-11:9, 13:58-14:24; USAA-1010, 6:24-29, 11:44-51, FIG. 4, 15:54-16:45.

264. For example, biometric sensor 440 would capture a representation of the user's fingerprint," and a digital template "derived from the captured representation" would be "compared with one or more stored reference digital templates," with a "positive match" yielding identification and/or authentication. USAA-1013, 7:44-56; USAA-1010, 9:60-65, FIG. 4.

265. Upon authorization, the Crypto SE application would "look up in a table or database the appropriate identifier or credential needed," and would "transmit a permission token, number or string such as an http post login string and/or other appropriate credential to" the payment provider's remote server. USAA-1013, 3:3-25, 9:55-10:3, 3:3-14, FIG. 2. For example, the Crypto SE application would "look up the appropriate payment credential needed to complete the transaction," and "encrypt and transmit the requisite http request string and payment credential over the public network" to the remote server. USAA-1013, 11:10-29, 9:65-10:16; USAA-1010, 11:62-12:21, 12:22-43 ("[p]ayment information may include… amount and account number, and may include a CVV

… "[t]his information may be correlated with signature information" that is "used to identify the client device and its user").

266. In at least these ways, and as explained in more detail below with respect to the remaining claim 1 features, Mardikar-Chhabra renders obvious authenticating the user at the mobile device by receiving a candidate user input. USAA-1010, Abstract, 1:15-17, 3:11-33, 4:27-36, 6:13-29, 7:28-42, 9:60-65, 10:42-11:7, 11:44-51, 11:62-12:43, 13:37-14:19, 15:54-16:45, FIGS. 4, 5a, 5b, 6a; USAA-1013, 2:22-34, 3:3-25, 6:45-48, 7:44-56, 8:22-40, 9:31-11:29, 13:58-14:24, FIGS. 3, 4, 5.

[1.c.ii] said mobile device verifying said user to the remote computing device in a second communication encoded using said secret.

267. Mardikar-Chhabra renders obvious [1.c.ii]. A POSITA would have understood and found obvious that in at least some of the transactions facilitated by Mardikar-Chhabra's system, 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-1010, 4:20-21 ("The TSM role includes providing a single point of contact for the SPs"), 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.

268. Regarding the payment provider's server, Mardikar '318 expressly describes scenarios in which "the duties or roles of one or more involved parties may be combined and preformed by a single entity." USAA-1010, 6:13-15. For example, in the specific context of a web-based financial transaction, Mardikar '318 explains that a trusted service manager may additionally "act as a payment provider system (PP), such as PayPal, and 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." USAA-1010, 6:13-29, 4:20-21, 5:48-51, 5:65-6:1, FIG. 3.

269. In that scenario, "the customer may pre-register his account with the payment provider system, map the account to an email address, and then use the payment provider system to make purchases when redirected to the payment provider system from the merchant's site," with the payment provider system completing the transaction after it is authorized. USAA-1010, 6:13-29.

270. From this and related a description, a POSITA would have understood and found obvious that a single remote server operated by a trusted service manager that simultaneously performs the role of payment provider (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." *See* 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.

271. More, a POSITA would have understood and found obvious that, in order to complete the desired financial transaction through a secure SSL connection with client device 400, the client device and the payment provider's remote server would first establish the secure SSL connection through the handshake protocol described above with respect to [1.b]. *See* 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; USAA-1018, 33-63. And, for at least that additional reason, a POSITA would have found obvious that a remote server that sends a first communication including one or more identifiers associated with the user's biometric profile would be the same remote server that receives a second communication that is sent by device 400, and that is encoded using the biometric profile, directly and indirectly, as I describe further below.

272. 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-1013, 8:33-49 ("This management module may prompt the user to confirm his identity by for example a fingerprint match or other process. If the management module verifies the identified user is authorized … then the management module may retrieve a … credential and possibly encrypt and transmit a … string including the credential using for example a TLS or an SSL cryptographic protocol"), 9:65-10:16, 11:10-29, FIGS. 4, 5; USAA-1010, 11:62-12:43, 16:33-40.

273. In that regard, and as I describe further below in relation to "indirect usage," 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 payment provider's remote server that the user has been authorized to proceed with the requested transaction based on the biometric profile. USAA-1010, 11:62-12:43, 16:33-40 ("generating a secure payment information message in response to an authentication including a match of the biometric data with the stored biometric signature"); USAA-1013, 8:33-49, 9:65-10:16, 11:10-29, FIGS. 4, 5.

274. Mardikar '318 further describes enabling a service provider's 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: "When a payment is made … the last four digits of the payment instrument may be sent to the TSM"; "[t]his information may be correlated with signature information" that is "used to identify the client device and its user." USAA-1010, 12:22-43; *see also* USAA-1013, 7:44-56.

275. 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 (as it uniquely identifies the user to the TSM as the biometric signature stored in the Crypto SE does). USAA-1010, 11:62-14:19; USAA-1012, Abstract, FIG. 2, [0029]-[0033]; USAA-1014, [0036], [0082]-[0085].

276. Indeed, Mardikar '318 interchangeably refers to the user authentication data that Crypto SE stores as a result of the registration process 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. USAA-1010, 7:28-43, 10:5-11:7, 12:31-43, 15:54-16:50 ("the client device is

registered with the TSM for authentication by registering a biometric signature using a biometric sensor of the client device"), FIGS. 5a, 5b; USAA-1012, Abstract, FIG. 2, [0029]-[0033][13]; USAA-1013, 7:44-56; USAA-1014, [0036], [0082]-[0085].

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

---

[13] In a highly similar context, Mardikar '673 explains that "a strong second factor authentication may be provided to verify the authenticity of the client device or user," adding that "[t]he encryption and processing of the SMS message or data may include applying an HMAC to a timestamp or counter along with pre-registered identification information for a particular user." USAA-1012, [0031]. For instance, "Crypto block 130 encrypts the SMS message or data by processing it through, for example, a keyed-Hash Message Authentication Code (HMAC) using an RSA algorithm or Elliptic Curve Cryptography (ECC), and applying it to a combination of a timestamp and/or counter along with second factor authentication information … for example, biometrics may be used for identification purposes such as a fingerprint or retinal pattern." USAA-1012, [0029]; *See also* USAA-1010, 14:3-19.

because[14] information about (i.e., an encoding of) the biometric profile (i.e., the secret) is included in the second communication.

278. Regarding the second communication being "encoded using the secret," the scope of the term "using" is unclear. A POSITA would have certainly understood that "using" includes transforming the bits encoding a first message into an encoded second message using the bits that encode the secret. For example, while the details of secure encryption algorithms (e.g., DES) are complex (and were complex as of the Critical Date) and beyond the scope of this

---

[14] 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 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 client device's successful authentication check using the biometric profile, and in view of that message at least implicitly conveying to the payment provider's remote server that the user has been authorized to proceed with the requested transaction based on the biometric profile. USAA-1010, 11:62-12:43, 16:33-40; USAA-1013, 8:33-49, 9:65-10:16, 11:10-29, FIGS. 4, 5.

declaration, such algorithms can include, e.g., performing an "exclusive-or" (XOR) function between the bits of the message being encoded and the bits of the secret. In an illustrative (but unrealistically simple) example, each bit of a message can be encoded can be XORed with a corresponding bit of the key to produce an encoded bit in the encoded message. As I noted above, such operations would have been understood by a POSITA as encoding a message using the secret. For the purpose of this declaration, I will call such usage "direct."

279. Embodiments within the '689 disclose this "direct" use of encoding a message using the secret. For example, as illustrated in the flowchart of FIG. 3, secrets are used at step 243 to first generate message digests, which are then used to assemble cryptographic keys for encrypting/decrypting communications among members at step 245. In this way, the secret has a direct influence on the bits that comprise the cryptographic keys used for encrypting or decrypting (encoding or decoding) communications. Therefore, a POSITA would have understood that such embodiments in the '689 directly encode a message using the secret, as the secret is used as an input to a function (i.e., the "n-bit generator" shown in step 243 of FIG. 3) which produces the cryptographic keys used to encode the message.

280. Returning to the Mardikar-Chhabra combination, 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" to the remote server only after verifying/authenticating the user based on the registered biometric profile to which the payment credential relates. USAA-1013, 11:10-29, 9:65-10:16; USAA-1010, 11:62-12:43. As such, the second communication is encoded both as an immediate consequence of verification of the user's unique biometric input against the biometric profile, and in a way that at least implicitly conveys to the payment provider's remote server that the user has been authorized with respect to that biometric profile. USAA-1010, 11:62-12:43. For the purpose of this declaration, I will call such usage "indirect."

281. To the extent that a POSITA would have understood the '689 patent's reciting "a second communication encoded using said secret" language to encompass indirect use of the secret, Mardkar-Chhabra renders that language obvious in at least two additional ways.

282. First, the state of whether the user has been verified or has not been verified determines whether the message will be encoded. Put differently, the message will be encoded if and only if the user had been verified. Further, since that determination is based on a comparison of one or more biometric inputs against the biometric profile, and the biometric profile is the secret, the secret is used to determine whether the encoding process occurs. Moreover, that determination is both necessary and sufficient – that is, the message is encoded if

and only if the biometric input has been verified. Therefore, to the extent that the "a second communication encoded using said secret" language encompasses such indirect use of the secret, a POSITA would have understood and found obvious that Mardkar-Chhabra renders it obvious for that additional reason.

283. Second, as I describe above, since the second communication is encoded and received as an immediateconsequence of the client device's successful authentication check using the biometric profile (and occurs only upon successful authentication), the successful authentication at least implicitly conveys to the payment provider's remote server that the user has been authorized to proceed with the requested transaction based on the biometric profile.

284. Consider the analogy of a "signal fire," where the mere presence of a fire set by one party signals information to another party, which can be deemed encoding that information by setting the fire. In more detail, whether the fire exists or not conveys a specific meaning to the person perceiving it, assuming that the person who perceives the fire and the person who sent the message by setting the fire previously established the message's meaning. That is, the person perceiving the fire is able to recognize the encoded meaning conveyed by the mere presence of the fire, as previously established between the parties.

285. The Revolutionary War's use of "one if by land, two if by sea" is a second analogous example: the mere presence of lit lanterns indicates an attack

(encodes the information that an attack is occurring or is imminent), and the number of laterns lit further encodes the type of attack.

286. Since the authentication uses the secret (biometric profile), the second communication is encoded (indirectly) using the secret. Therefore, to the extent that the "a second communication encoded using said secret" language encompasses this second indirect use of the secret, a POSITA would have understood and found obvious that Mardkar-Chhabra renders it obvious.

[2] The method of claim 1, wherein the secret comprises an encryption key.

287. Mardikar-Chhabra renders obvious [2]. Mardikar '318 describes, for example, 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. Notably, the "user identity must be unique for each CA," and "[i]n an example embodiment, a Trusted Service Manager (TSM) may act as the CA and may … preload the Root Certificate of Authority (CA) 424 on a client device 400, for example on the Crypto SE 420 of the device." USAA-1010, 10:26-40.

288. As explained in more detail above, Mardikar '318 further describes registering a user's biometric signature/profile with the CA "as part of a

registration or certification procedure" that yields unlocking of a preloaded "payment credential or CA certificate 424," and association of the certificate 424 "with the Service Provider's user account." USAA-1010, 9:60-65, 10:5-11:7, FIGS. 5a, 5b. For example, "a payment credential or CA certificate 424" may "be unlocked by registering the user's unique biometric profile using the biometric sensor 440," in which case the "certificate 424 is entered and associated with the Service Provider's user account," and a certificate "based on" the associated account number or IMEI device 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.

289. In that regard, a POSITA would have understood and found it obvious to bind the user's public key with their unique user identity based on the user's unique biometric profile, which is already generated by the client device and registered with the CA as part of the same registration process. USAA-1010, 10:26-11:7, FIGS. 5a, 5b.

290. More, in view of Mardikar '318's further description of local generation of keys by the client device, a POSITA would have found it obvious to generate the user's key-pair based on the user's unique biometric profile, and to store the same together, as doing so would provide an efficient, secure, and convenient means of implementing related teachings. USAA-1010, 13:56-59,

10:26-14:19, FIGS. 5a, 5b; USAA-1014, [0033], [0035], [0036], [0081]-[0085], FIG. 10, USAA-1015, [0016] (noting that "the terms 'authentication information,' and 'authentication key'" are interchangeable), [0007]-[0009], [0017], [0024], FIGS. 1, 1A, 3; USAA-1019, §7.1; USAA-1014, [0035] (describing local generation of a key pair); USAA-1004, [0009] (describing a key derived from a user's live-scan fingerprint feature set and the user's modified enrolled fingerprint feature set); USAA-1014, [0008], [0043], [0117], FIG. 2 (describing generation of a key based on a biometric value), FIG. 6.

291. Mardikar '318 describes, for example, generation by the client device of encryption keys including "a symmetric key and a MAC key" that are used to encrypt messages transmitted by the client device. USAA-1010, 13:56-59 ("A client application … may generate a symmetric key and a MAC key" and "may then encrypt payload with the symmetric key and MAC key"). Mardikar '318 further describes "one or several key-pairs" that, like the user's biometric profile, are stored in Crypto SE 420. USAA-1010, 10:18-40, 13:56-59; USAA-1019, §20, §3.3.39, §3.3.45; USAA-1014, [0082].

292. In that regard, a POSITA would have found it obvious to generate one or more encryption keys based on the user's biometric profile during the registration process for a given service provider, and to store the generated keys in the Crypto SE with the corresponding biometric profile and identifiers (e.g., a

service provider account number and additional identifiers included in the associated certificate). *Supra*, Ground 2A, analysis of Element [1.a.ii]; USAA-1010, 7:28-42 (explaining that the secure elements may be smart cards featuring "tamper-proof" "non-volatile storage," which "makes it possible for the card to keep some secrets, such as the private keys associated with any certificates it holds"), 9:37-46, 10:25-40, 13:56-59; USAA-1013, 9:45-61 ("a table or database lookup"); USAA-1017, 347-362; USAA-1015, [0016]; USAA-1004, [0009]; USAA-1014, [0008], [0043], [0117], FIG. 2 (describing generation of a key based on a biometric value), FIG. 6.

293. The resulting stored secret would include both the biometric profile and the key-pairs generated based on the biometric profile, both of which also individually be considered secrets. USAA-1010, 7:28-9:23, FIG. 4; USAA-1013, 5:59-7:64, FIG. 3; USAA-1017, 136 ("we have two types of secrets: the keys and the data").

[3] The method of claim 1, wherein the secret comprises a static portion and a dynamic portion.

294. Mardikar-Chhabra renders obvious [3]. As discussed *supra* Ground 2A, analysis of Claim [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-1010, 10:2-4 ("A counter 444 and a clock 445 may be used to identify and/or timestamp particular communications to prevent against replays."), 10:65-11:16 ("A random counter may be generated by counter 444 (FIG. 4) on the Crypto SE and stored in the Crypto SE for counter based replay protection. In an alternative embodiment, clock 426 445 (FIG. 4) may generate a timestamp for timestamp-based replay protection. In an example embodiment, this information, for example a tuple, may be sent along with the SCEP…"), 14:17-19.

295. As explained above at Ground 2A, analysis of Element [1.c.ii], the second communication (message from device 400 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 part of the secret, where the biometric profile comprises a static portion, and the counter/timestamp/rotating keys comprises a dynamic portion. USAA-1012, Abstract ("encrypting the SMS data by processing the SMS data with a Message Authentication Code (MAC) and a timestamp and/or counter along with second factor authentication information"), [0011]-[0013], [0029], [0031]-[0033], [0039]-[0041], FIG. 2.

[4] The method of claim 1, wherein the first communication comprises a request for user credentials of the user of the mobile device.

296. Mardikar-Chhabra renders obvious [4]. For example, 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 protocol and, after establishing a secure SSL channel, the client sends a second communication to the server including payment information, among other user credentials. 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; USAA-1018, 33-63.

297. A POSITA would have understood and found obvious that the first communication sent by the server to the client device 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, with all of its included credentials; 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 such as account number and CVV. 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 such as for example, a credit card number, a credit card expiration date, a security code, and

the like." USAA-1013, 10:40-55, Abstract, 2:22-34, 3:3-14, 3:26-31, 11:11-16, FIGS. 4, 5.

[6] The method of claim 1, wherein the unique user input comprises user credentials.

298. Mardikar-Chhabra renders obvious [6]. As explained above, and as for example shown in Mardikar '318's FIG. 6a (reproduced below), Mardikar '318 describes receiving, via "a biometric sensor" on the client device "biometric information" or "raw biometric data" ("unique user input") prior to generating the "biometric profile"/"biometric signature" ("secret"). USAA-1010, 3:19-22, 6:42-49 ("a biometric sensor 440" on a "client device 400"), 7:27-43, 10:57, FIG. 4.

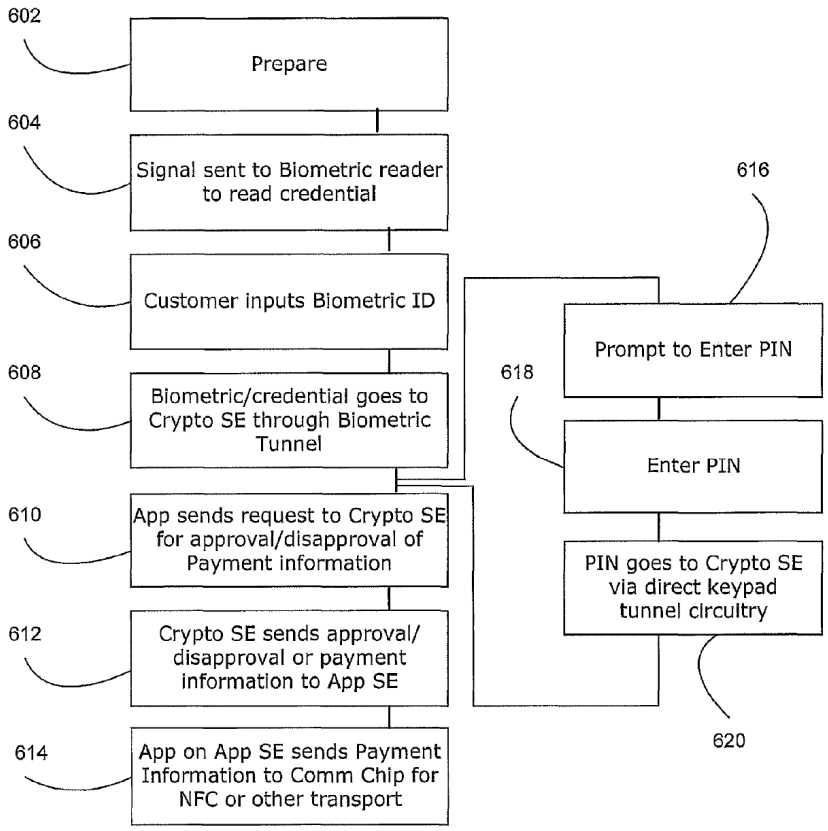


FIG. 6a

USAA-1010, FIG. 6a

299. From this and related description, A POSITA would have understood and obvious that the user's unique biometric input is/includes user credentials. USAA-1010, FIG. 6b ("Biometric/credential goes to Crypto SE" at step 608), 11:44-55 ("A user may then input 606 their biometric identifying data (ID) or signature by placing or swiping a thumb or finger on biometric sensor 440. The input biometric ID may be directly sent or tunnelled 608 to Crypto SE"); USAA-

1013, 2:22-28 ("a credential may be …, fingerprint, biometric identifier"), 5:60-64, 6:38-45, 7:44-48, 7:57-64, 9:31-39, 11:2-9, FIG. 3.

[7] The method of claim 1, wherein the first and second communications comprise two related communications of a communication session.

300. Mardikar-Chhabra renders obvious [7]. As explained above with respect to [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 with the client device sends the second communication, with both communications occurring in the context of the same web-based transaction between the client device and the remote server. 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. For at least that reason, a POSITA would have understood and found obvious that the first second and communications comprise two related communications of a communication session.

D. Ground 2B: Combination of Mardikar '318, Chhabra, and Duffy Renders obvious Claims 1-21

301. As explained above, Mardikar-Chhabra renders obvious those claims addressed by Ground 2A, based at least on a mapping of Mardikar '318's "biometric profile" to the recited "secret." *See* Ground 2A, analysis of Element [1.a.1] (referencing USAA-1010, 9:60-65, 10:42-11:7, FIGS. 4, 5a, 5b).

302. As explained in more detail below, Mardikar-Chhabra-Duffy further renders obvious the same and additional claims, based additionally on Duffy's disclosure of a "mapping key," a mathematical XOR combination of a biometric value (the biometric signature/profile) and a private key.

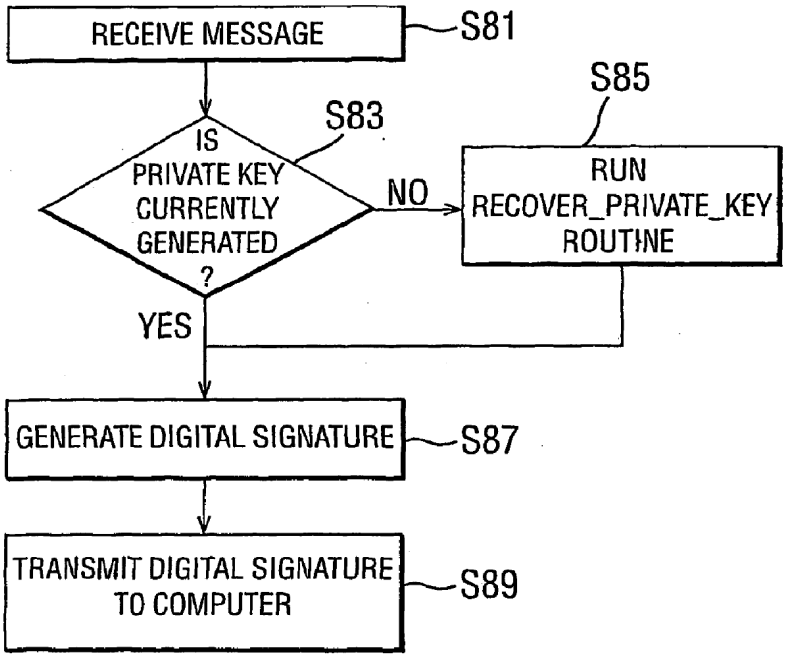
[1]

303. 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. However, if the Board were to require the recited "secret" appearing in [1.a.i] and [1.c.ii] to represent a cryptographic key, then Mardikar-Chhabra-Duffy also renders obvious this limitation. The Mardikar-Chhabra-Duffy described above relies upon the modified biometric signature/profile ("secret"), that is, a mapping key. This mapping key is a combination of a biometric value (the biometric signature/profile) and a private key, in accordance with Duffy. *Supra*, §VIII.J, Mardikar-Chhabra-Duffy Combination.

304. Further, the combination also renders obvious the limitation reciting, "said mobile device verifying said user to the remote computing device in a second communication encoded using said secret" as recited in [1.c.ii]. Specifically, Duffy describes a "SIGN_MESSAGE routine 55 [that] is used to generate a digital signature, using the private key K_{pri} generated for a user, in order to authenticate

the source and integrity of a message" to the remote computing device. USAA-1014, [0036], [0033] ("The cryptographic unit 19 is then able, for example, to create a digital signature using the private key K_{pri}"); *see also id.*, [0083]-[0085] (detailed description of the "SIGN_MESSAGE routine 55" "using the generated private key K_{pri} to generate the digital signature" for an outgoing communication). Duffy further explains in referring to FIG. 10 (reproduced below), [t]he digital signature is then transmitted, in step S89, to the computer 1, which attaches the digital signature to the original message to form a signed message and transmits the signed message to a desired recipient." USAA-1014, [0085]. This allows the server to in fact execute any underlying transaction.

Fig. 10



USAA-1014, FIG. 10

305. A POSITA would have found it obvious that the Mardikar-Chhabra-Duffy system signs the original message (e.g., message with payment credential to complete a transaction) with a digital signature to form a signed message, in accordance with Duffy, and the private key used to create the digital signature of the signed message ("a second communication encoded") is regenerated using the modified biometric signature/profile of the user ("using said secret"). This encoding of the second communication provides enhanced security through authentication of the user (of the client device) ("verifying said user to the remote computing device") and the integrity of the message to the remote computing device (e.g., the TSM facilitating a web-based transaction).

[2] The method of claim 1, wherein the secret comprises an encryption key.

306. Mardikar-Chhabra-Duffy renders obvious [2] for additional reasons. For example, as discussed *supra* Mardikar-Chhabra-Duffy Combination, Mardikar-Chhabra-Duffy's 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"), per Duffy. *Supra*, §VIII.J, §VIII.I, Duffy Overview; USAA-1014, [0008], [0043], FIG. 2 (showing generation of the mapping key K_{map} from combining the biometric value K_{bio} with the private key K_{pri}, by the "mapping key generator 1009"), FIG. 6 (step S7 "process private key and biometric value to generate mapping key"), [0117] ("In the first embodiment, the mapping function

which is applied to the intermediate key (i.e. the biometric value K_{bio}) and the mapping key K_{map} is a simple addition. However, any mapping function which is monotonic, i.e. each set of input variables generates a unique output, could be used. For example, the mapping function could be a simple subtraction. It can be shown that the mapping function used does not affect the security of the system. A bit-wise exclusive-OR function could also be used both to combine the intermediate key and the cryptographic key to generate the mapping key, and subsequently to combine the intermediate key and the mapping key to generate the private key.”).

307. The private key (as well as a public key) is used for encryption (“encryption key”) and/or decryption of data, for example, messages between a sender and a remote recipient. USAA-1014, [0002] (brief description of “[e]ncryption/decryption systems,” “private key” and “public key”), [0082] (“As those skilled in the art will appreciate, messages encrypted with a private key K_{pri} generated using the RSA algorithm can only be decrypted using the corresponding public key K, and similarly messages encrypted with a public key K_{pub} generated using the RSA algorithm can only be decrypted using the corresponding private key K_{pri}. These properties are put to two main uses, to create digital signatures authenticating the source and integrity of a message and to encrypt a message so

that only the desired recipient can decrypt the message."); *supra*, Ground 2A, analysis of Claim [2].

[3] The method of claim 1, wherein the secret comprises a static portion and a dynamic portion.

308. In addition to the reasons explained *supra* Ground 2A, Mardikar-Chhabra-Duffy also renders obvious [3]. For example, Mardikar-Chhabra-Duffy's secret is a modified biometric profile/signature, which is a "mapping key" comprising a private key, per Duffy. *Supra*, Ground 2B, analyses of Claims [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.

309. 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. *Supra*, §VIII.J, Mardikar-Chhabra-Duffy Combination.

[5] The method of claim 1, wherein the secret is stored in an encrypted format.

310. Mardikar-Chhabra-Duffy renders obvious [5]. For example, Mardikar '318 describes encrypting its "keys." USAA-1010, 13:54-61 ("The TSM may preload a public key inside a Crypto SE, for example an SIM/SE. A client application on the App SE of a client device, with help of the Crypto SE, may generate a symmetric key and a MAC key. The application may then encrypt payload with the symmetric key and MAC key. **The keys will be encrypted using the TSM's public key** that can be then used to create a digital envelope."); USAA-1012 (corroborating reference), [0040] ("Secure SMS service provider 330 may have a public key inside Crypto block 130 of client device 110. … Crypto block 130 may generate a MAC key and encrypt a message or data with such MAC key. **The keys may be encrypted** using secure SMS service provider's 330 public key that may then be used to create a digital envelope."). Mardikar further notes that the "MAC keys are **stored** in Crypto SE" with other keys. USAA-1010, FIG. 5b.

311. A POSITA would have understood and found obvious that Mardikar-Chhabra-Duffy's mapping key (the modified biometric signature/profile comprising a private key) ("secret"), like the other "keys," is also encrypted, for

example, using the TSM's public key, prior to being stored in the Crypto SE, to achieve further enhanced security. *Supra*, Grounds 2A and 2B, analysis of Element [1.a.ii]; USAA-1010, 13:54-61, FIG. 5b; Tomko Overview; USAA-1005, Abstract, 2:42-5:11 (Tomko teaching 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"), 4:60-65 (the finger-print based key is "stored in memory 24" as an "encrypted version").

[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.

312. Mardikar-Chhabra-Duffy renders obvious [8]. As discussed above in the analysis of Element [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-1010, 7:28-43, 16:25-35; USAA-1013, 7:44-49.

313. Also discussed above under the Mardikar-Chhabra-Duffy Combination and analysis of Claim [1], in the Mardikar-Chhabra-Duffy system,

the modified biometric profile/signature is a mapping key ("secret") that is recovered each time for regenerating the private key when needed (e.g., by running a "RECOVER_PRIVATE_KEY" routine"), such as in signing the message ("second communication" recited in claim [1]) 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}." *Supra*, §VIII.J; Grounds 2A and 2B, analysis of Claim [1]; USAA-1014, [0030]-[0036], [0074]-[0085], FIG. 9.

314. 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-1010, 7:28-43, 16:25-35; USAA-1013, 7:44-49 ("A digital template may be derived from the captured representation [of a user's fingerprint] and

compared with one or more stored reference digital templates. A positive match may authenticate or identify a user."); USAA-1014, [0030]-[0044], [0074]-[0087], FIGS. 9-11.

[9.pre] A mobile device, comprising

315. *Supra*, Ground 2A, analysis of Element [1.a.i].

[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:

316. Mardikar-Chhabra-Duffy renders obvious [9.a]. For example, 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, in at least some embodiments, also includes means to "establish a direct, secure transmission between the Crypto SE" and other devices "using technologies like Secure Socket Layer (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.

317. For example, Mardikar '318's FIG. 4 (reproduced 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.

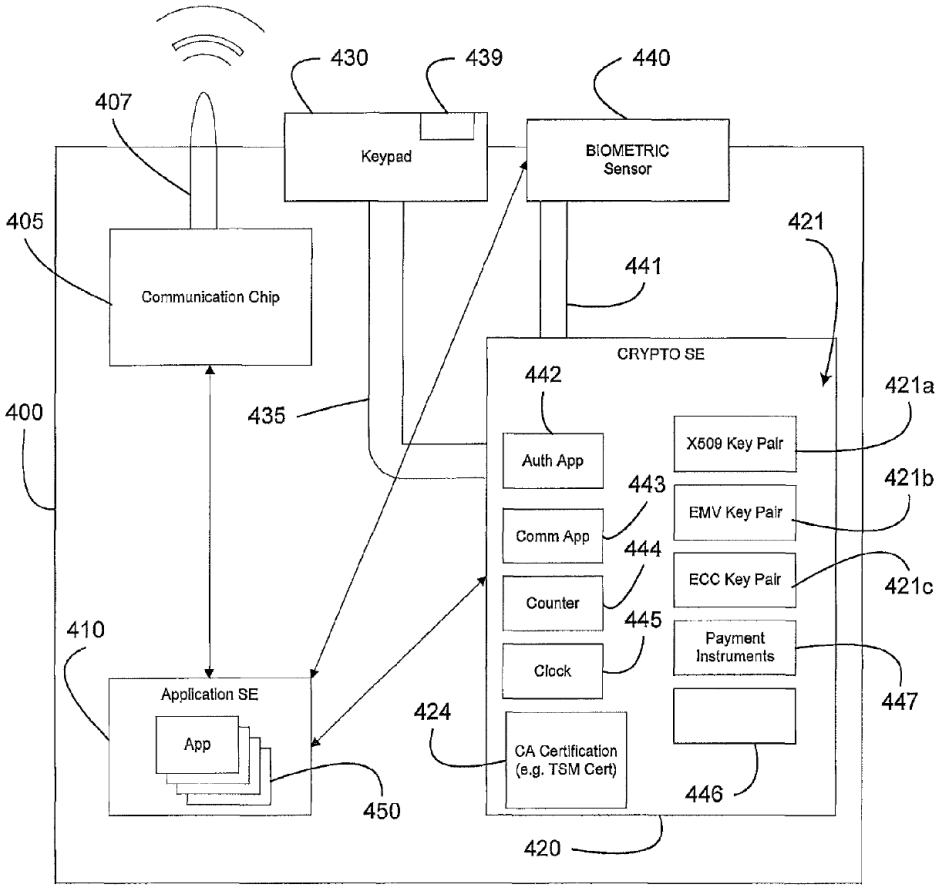


FIG. 4

USAA-1010, FIG. 4

318. From this and related description, 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-1010, Abstract (Crypto SE comprising a "computer-readable medium having a security key, a payment instrument, stored authentication data and instructions for generating a secure payment information message"), 2:37-41, 14:51-15:41 ("Logic may be encoded in a computer readable medium, which may refer to any medium that participates in providing instructions to the processor for execution. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. ... Some common forms of computer readable media includes, for example, floppy disk, flexible disk, hard disk, magnetic tape, any other magnetic medium, CD-ROM, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, RAM, PROM, EPROM, FLASH-EPROM, any other memory chip or cartridge, carrier wave, or any other medium from which a computer is adapted, … the various hardware components and/or software components set forth herein may be combined into composite components comprising software, hardware, and/or both … the various hardware components and/or software components set forth herein may be separated into sub-components comprising software, hardware, or both"), FIG. 4; USAA-1012, [0037]; USAA-1013, 4:41-5:9, 12:30-37 ("[e]mbodiments … may include a computer or processor readable storage

medium, such as for example a memory, a disk drive, or a USB or other flash memory, including instructions which when executed by a processor or controller, carry out or perform methods disclosed herein. … may also include other systems for performing the operations herein such as for example mobile computing platforms"), 14:29-15:41 (describing various processors, memories, and "processor [] executing one or more sequences of one or more instructions contained in a system memory component. Such instructions may be read into the system memory component from another computer readable medium, such as static storage component or disk drive component"), FIG. 3 (illustrating a security "management module" including both a "secure signon module" and a "server communication module"); USAA-1014, FIG. 6 (storing mapping key "in non-volatile memory"), [0017] ("a read only memory forming part of the cryptographic unit"), [0018] ("a non-volatile random access memory"), [0034] (cryptography unit including "a central processing unit (CPU) 35, a read only memory (ROM)37, a random access memory (RAM) 39, a non-volatile random access memory (NVRAM) 41").

[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,

319. Mardikar-Chhabra-Duffy renders obvious [9.b]. *Supra*, Grounds 2A and 2B, analyses of Elements [1.a.i], [1b], [1.c]. 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 user interface (e.g., biometric sensor) and with at least one remote computer-based station (e.g., remote server(s) of one or more service providers or a TSM), e.g., in registering the user's biometric profile/signature with the at least one remote computer-based station, and in conducting a transaction with/through the remote computer-based station upon authenticating the user's biometric input. USAA-1010, 9:60-65.

[9.c.i] upon receipt of said unique user input, generating a secret,

320. *Supra*, Grounds 2A and 2B, analysis of Element [1.a.i].

[9.c.ii] storing said secret in said storage device, said secret being stored with an identifier

321. *Supra*, Grounds 2A and 2B, analysis of Element [1.a.ii].

[9.c.iii] so as to be retrievable when the unique user input is again received;

322. *Supra*, Grounds 2A and 2B, analysis of Element [1.a.iii].

[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;

323. *Supra*, Grounds 2A and 2B, analysis of Element [1.b].

[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

324. *Supra*, Grounds 2A and 2B, analysis of Element [1.c.i], and Ground 2B, analysis of Claim [8].

[9.e.ii] recovering the secret from said storage device if the candidate identifier matches the identifier; and

325. *Supra*, Ground 2B, analysis of Claim [8].

[9.f] verifying said user to the remote computing device in a second communication encoded using said secret.

326. *Supra*, Grounds 2A and 2B, analysis of Element [1.c.ii].

[10] The mobile device of claim 9, wherein the secret comprises an encryption key.

327. *Supra*, Grounds 2A and 2B, analysis of Claim [2], and Ground 2B, analysis of Claim [9].

[11] The mobile device of claim 9, wherein the secret comprises a static portion and a dynamic portion.

328. *Supra*, Grounds 2A and 2B, analysis of Claim [3], and Ground 2B, analysis of Claim [9].

[12] The mobile device of claim 9, wherein the first communication comprises a request for user credentials of the user of the mobile device.

329. *Supra*, Ground 2A, analysis of Claim [4], and Ground 2B, analysis of Claim [9].

[13] The mobile device of claim 9, wherein the secret is stored in an encrypted format.

330. *Supra*, Ground 2B, analyses of Claims [5] and [9].

[14] The mobile device of claim 9, wherein the proffered user input comprises user credentials.

331. *Supra*, Ground 2A, analysis of Claim [6], and Ground 2B, analysis of Claim [9].

[15] The mobile device of claim 9, wherein the first and second communications comprise two related communications of a communication session.

332. *Supra*, Ground 2A, analysis of Claim [7], and Ground 2B, analysis of Claim [9].

[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:

333. To the extent the preamble is limiting, Mardikar-Chhabra-Duffy renders obvious [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 a security key, a payment instrument, stored authentication data and 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 ("[e]mbodiments … may include a computer or processor readable storage medium, such as for example a memory, a disk drive, or a USB or other flash memory, including instructions which when executed by a processor or controller, carry out or perform methods disclosed herein. … may also include other systems for performing the operations

herein such as for example mobile computing platforms"), 14:29-15:41 (describing various processors, memories, and "processor [] executing one or more sequences of one or more instructions contained in a system memory component. Such instructions may be read into the system memory component from another computer readable medium, such as static storage component or disk drive component"), FIG. 3; USAA-1014, FIG. 6, [0017], [0018], [0034]; *supra*, Ground 2B, analysis of Element [9.a].

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. *Supra*, Ground 2B, analysis of Element [9.a].

[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,

335. Mardikar-Chhabra-Duffy renders obvious [16.a]. *Supra*, Ground 2B, analyses of Elements [9.a]-[9.b] and [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. *Supra*, Ground 2B, analysis of Element [9.a].

[16.b.i] upon receipt of said unique user input, generating a secret,

336. *Supra*, Grounds 2A and 2B, analysis of Element [1.a.i].

[16.b.ii] storing said secret in a memory of said processor-based platform, said secret being stored with an identifier

337. *Supra*, Grounds 2A and 2B, analyses of Elements [1.a.ii], Ground 2B, analyses of Elements [9.a], and [16.pre]-[16.a].

[16.b.iii] so as to be retrievable when the unique user input is again received;

338. *Supra*, Grounds 2A and 2B, analysis of Element [1.a.iii].

[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;

339. *Supra*, Grounds 2A and 2B, analysis of Element [1.b].

[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

340. *Supra*, Grounds 2A and 2B, analysis of Element [1.c.i].

[16.d.ii] recovering the secret from said memory if the candidate identifier matches the identifier; and

341. *Supra*, Ground 2B, analysis of Claim [8].

[16.e] verifying said user to the remote computing device in a second communication encoded using said secret.

342. *Supra*, Grounds 2A and 2B, analysis of Element [1.c.ii].

[17] The non-transitory computer-readable medium of claim 16, wherein the secret comprises an encryption key.

343. *Supra*, Grounds 2A and 2B, analysis of Claim [2], and Ground 2B, analysis of Claim [16].

[18] The non-transitory computer-readable medium of claim 16, wherein the secret comprises a static portion and a dynamic portion.

344. *Supra*, Grounds 2A and 2B, analysis of Claim [3], and Ground 2B, analysis of Claim [16].

[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.

345. *Supra*, Ground 2A, analysis of Claim [4], and Ground 2B, analysis of Claim [16].

[20] The non-transitory computer-readable medium of claim 16, wherein the secret is stored in an encrypted format.

346. *Supra*, Ground 2B, analyses of Claims [5] and [16].

[21] The non-transitory computer-readable medium of claim 16, wherein the proffered user input comprises user credentials.

347. *Supra*, Ground 2A, analysis of Claim [6], and Ground 2B, analysis of Claim [16].

X. CONCLUSION

348. For all the reasons I have noted in the foregoing paragraphs, claims 1-21 of the '689 Patent are obvious in view of the references discussed above.

349. I currently hold the opinions set expressed in this declaration. But my analysis may continue, and I may acquire additional information and/or attain supplemental insights that may result in added observations.

Appendix A

Seth James Nielson's Vita

(512) 387-4310
seth@crimsonvista.com
March 2025

Academic Degrees

2009	**Ph.D. Computer Science,** Rice University, Houston, TX
2004	**M.S. Computer Science,** Brigham Young University, Provo, UT
2000	**B.S. Computer Science,** Brigham Young University, Provo, UT

Certifications

CISSP

Current Appointments

President and Chief Scientist	Crimson Vista, Inc.
Director of Cybersecurity Research	Curuvar LLC
Adjunct Assistant Professor	University of Texas at Austin Law School
Senior Fellow	Robert Strauss Center for International Security and Law

Professional Advising

2019-2024	Advisory Board	Syccure Inc.

Non-profit and Community Engagement

2021-Present	Founding Director	The Crypto Done Right Foundation
2019-2021	Cyberlab Advisory Board	The SEED School of Maryland

Grants and Research Awards

Decentralizing Zero-Trust Infrastructure to Combat Advanced Persistent Threats and Malicious Insiders (Senior Personnel), NSF 2020 SBIR solicitation. Award number 2051989, Curuvar LLC.

Mitigation of Ransomware, DoD 2018.B STTR solicitation (Army), Topic: A18B-T010, Crimson Vista, $150,000 (2019)

An Enabling Repository of Cryptographic Knowledge (Co-PI), Cisco Grant, Johns Hopkins University Information Security Institute, $150,000 (2017-2021)

University Research Funding

Sel4 Security Appliance Capstone, funded by Crimson Vista to Brigham Young University Department of Computer Science. 2021

Academic Awards

Brown Fellowship
John and Eileen Tietze Fellowship

Professional Service

International Cryptographic Module Conference, 2018-2025 Program Committee

Subject Matter Expertise and Selected Projects

Forensic Analysis (e.g., Code/IP Theft)

Trusted images research (UT Austin, 2024)

Investigation of email transmissions, reception (Crimson Vista, 2024-)

Investigation of stolen digital documents, provenance, handling (Crimson Vista, 2023-)

Investigation of cryptocurrency transfers and fraud (Crimson Vista, 2023-)

Investigation of website content development and provenance (Crimson Vista, 2023-2024)

Investigation of server, laptop, and hard drives for indica of tampering (Crimson Vista, 2023)

Investigation of voting machine software for vulnerabilities (Crimson Vista, 2022-)

Investigation of altered/forged emails (Crimson Vista, 2022)

CLE training related to source code analysis/trade secrets (Source Code Discovery, 2021)

Investigation of IP/code theft related to MTA, spear-phishing, and email (Crimson Vista, 2019-2021)

Investigation of code theft related to housing and rental software (Crimson Vista, 2019-2022)

Investigation of code development for security vulnerabilities/intrusion (Crimson Vista, 2020)

Investigation of code theft related to digital mobile radios (Crimson Vista, 2017-2021)

Investigation of code theft related to financial trading software (Crimson Vista, 2016-2017)

Investigation of code theft related to e-commerce (Harbor Labs, 2015)

Investigation of IP theft related to domain anti-abuse (Harbor Labs, 2015)

Investigation of IP theft related to high-frequency trading (Harbor Labs, 2010-2011)

Applied Cryptography

Cryptography training modules (UT Austin, 2022-2024)

Analysis of compromised password hashes (Crimson Vista, 2020)

“Crypto Done Right”, Cryptographic Knowledge Base Non Profit (2020-2024)

“Crypto Done Right”, Cryptographic Knowledge Base with Cisco (Johns Hopkins, 2017-2020)

Simulated implementation of Vehicle-to-Vehicle authentication (Crimson Vista, 2018-2019)

Cryptographic protocol analysis and design for Syccure Inc. (Crimson Vista, 2017-2023)

Timing attacks on Hardware Security Modules with Diamond Key Security (Johns Hopkins, 2018)

Technical consulting for U.S. Dpt. of Justice (Antitrust Division, Transportation, Energy & Agriculture) (Crimson Vista, 2018)

Aircraft/drone anti-collision protocol security with OnBoard Security (Johns Hopkins, 2017)

Cryptographic communication library for Security First Corp (ISE, 2010-2011)

Encryption library, file system encryption, GPU for Security First Corp (ISE, 2005-2011)

Security Operations, Compliance, Oversight

Corporate board advisory (Crimson Vista, 2025-)

Risk Assessment (Crimson Vista, 2024-)

Penetration Testing (Crimson Vista, 2024-)

AI Governance (Crimson Vista, 2024-)

SEC cybersecurity disclosures (Crimson Vista, 2024-)

GDPR, Privacy, PII analysis (Crimson Vista, 2024-)

Security analysis of Twitter cybersecurity operations/practices (Crimson Vista, 2022)

Virtual Chief Information Security Officer for IperionX (Crimson Vista, 2022-2023)

IoT Devices and IoT Security

Medical implant analysis (Crimson Vista, 2024-)

Robotic automation system (Crimson Vista, 2024-)

Traffic lights and systems software analysis (Crimson Vista, 2023-2024)

Vulnerability and exploitation analysis of voting machine hardware (Crimson Vista, 2023-)

High-security appliance based on formal methods (Crimson Vista, BYU, 2021)

Hadoop security research (Crimson Vista, 2021-2022)

IoT data sensors for agricultural operations (Crimson Vista, 2020-2023)

Contributor, reviewer for the Institute of Assured Autonomy (Johns Hopkins, 2019)

IoT data aggregation security with Armored Things (Johns Hopkins, 2018-2019)

Automated IoT device profiling with the Physics Lab (Johns Hopkins, 2018)

Physical forensics from IoT devices (Johns Hopkins 2017)

Network Security

MPLS/VRF analysis (Crimson Vista, 2025-)

Bluetooth-enabled alert system security analysis (Crimson Vista, 2024)

Web security, cookies, XSS, XSRF training modules (UT Austin, 2023-2024)

Phishing samples analysis (Crimson Vista, 2022-2023)

WiFi transmission analysis, packet capture (Crimson Vista, 2023-2024)

Security-Focused Data Discovery Methods and Practice (Crimson Vista, 2022-2023)

Analysis of weaknesses in two-factor authentication (Crimson Vista, 2022-2023)

Analysis of bots on Twitter in terms of prevalence, stealth, and impact (Crimson Vista, 2022)

Secure distributed computing (Curuvar, 2021-2023)

Hadoop deployment and security considerations (Crimson Vista, 2021-2022)

SSO technology evaluation and test (UT Austin, Crimson Vista, 2021-2022)

Information risk assessment with respect to data breach (Crimson Vista, 2020-2021)

Data breach analysis with respect to password authentication (Crimson Vista, 2020-2021)

Network security curriculum design for Law and Policy (University of Texas at Austin, 2020-2024)

Network security curriculum design for undergraduates (University of Texas at Austin, 2020-2021)

Network security curriculum design (Johns Hopkins, 2013-2019)

Security analysis of financial services vendor for Fortune-100 client (Crimson Vista, 2018-2019)

Analysis of secure e-mail transmission for confidential client (Crimson Vista, 2018-2019)

Cloud storage system security evaluation for confidential client (Harbor Labs, 2015)

Secure gateway security and compliance evaluation for SecurityFirst Corp (Harbor Labs, 2015)

Gateway caching security/privacy engineering (Google, 2005)

Malware and Viruses

Ransomware training modules (UT Austin, 2022-2023)

Ransomware recovery research and development (Crimson Vista, 2018-2019)

Advanced malware and malware defenses analysis (Johns Hopkins, 2018)

Malware Analysis for Confidential Client (Crimson Vista, 2016)

Privacy

Investigation of biometric tracking in commercial systems (Crimson Vista, 2024-)

Investigation of location tracking in mobile devices (Crimson Vista, 2021-)

Investigation of biometric tracking/transmission in devices and systems (Crimson Vista, 2021-)

Development of an auditing tool for cookies and other web tracking (Crimson Vista, 2020, 2024)

Audit of a large hospital network for cookies and web tracking (Confidential client, 2020)

Development of a privacy curriculum for data architects (Crimson Vista, 2019)

Anonymization of threat indicators with the Applied Physics Lab (Johns Hopkins, 2017)

Analysis of anti-piracy vendor for Center for Copyright Information (Harbor Labs, 2013-2014)

Machine Learning and AI

AI Agent Analysis/Engineering (Crimson Vista, 2025-)

AI Governance (Crimson Vista, 2024-)

LLM red team testing (Crimson Vista, 2024-)

Investigation of use of unauthorized data in AI training (Crimson Vista, 2024)

Miscellaneous Security Technologies

Distributed ledger technology for secure state replication (Curuvar, 2021-2023)

Blockchain technology for sale and/or licensing of intellectual property (Crimson Vista, 2021-2022)

Blockchain technology analysis for a start-up (Crimson Vista, 2019-2020)

Analysis of cyber security norms for a confidential Fortune 100 client (Crimson Vista, 2018-2019)

Analysis of vulnerabilities in portable chemical manufacturing system (Johns Hopkins, 2018)

Open-Source Contribution and Sponsorship for The PyPy Project (Crimson Vista, 2018-2019)

Blockchain and smart contract design for confidential start-up (Crimson Vista, 2018)

Medical device system security evaluation for confidential client (Harbor Labs, 2015)

Software Engineering and Software Analysis

Automotive source code analysis (Crimson Vista, 2024-)

Medical implant source code analysis (Crimson Vista, 2024-)

Automated least-privilege compilation/language research (UT Austin 2024-)

Review of failed software project, root cause analysis, attribution (Crimson Vista, 2024-)

Review of development practices, error handling, and robustness (Crimson Vista, 2023-)

Open-source licensing analysis, build, and test (Crimson Vista, 2023-)

GitHub analysis and statistics for effort estimation (Crimson Vista, 2022)

Software theft analysis and tool design for various clients (Crimson Vista, 2018-)

Cyber insurance investigations for Clyde & Co (Crimson Vista, 2018-2019)

Distributed code coverage analysis tool for a confidential Fortune 100 client (ISE, 2011)

Software engineering for Metrowerks Inc. (2001-2003, formerly Lineo Inc.)

Code Languages: C, C++, Java, Python, Ruby, Scala, RTL/VHDL/Verilog, JavaScript, Go

Publications

Books

Seth James Nielson, *Discovering Cybersecurity: A Technical Introduction for the Absolute Beginner*. (December 2023).

Seth James Nielson, Christopher K. Monson, *Practical Cryptography in Python, Learning Correct Cryptography by Example*. (October 2019).

Refereed Publications

Joseph Kosturko, Eric Schlieber, Sean Futch, Seth James Nielson, *Cracking a Continuous Flow Reactor: A Vulnerability Assessment for Chemical Additive Manufacturing Devices*. In *Proceedings of the 2018 IEEE International Symposium on Technologies for Homeland Security*. (September 2018)

Chanyang Shin, Prerit Chandok, Ran Liu, Seth James Nielson, Timothy Leschke, *Potential Forensic Analysis of IoT Data: An Overview of Amazon Echo, Z-wave, and Home Router Data Extraction and Analysis*. In *Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings)*, Exeter, UK, pp. 705-710 (June 2017).

Seth James Nielson, *PLAYGROUND: Preparing Students for the Cyber Battleground*. *Computer Science Education*, volume 26, issue 4, pp. 255-276, (January 2017).

Seth James Nielson and Charles D. Knutson, *Design Dysphasia and the Design Patterns Maintenance Cycle*. *Information & Software Technology,* volume 48, number 8, pp. 660- 675, (August 2006)

Seth James Nielson, Scott S. Crosby, and Dan S. Wallach, *A Taxonomy of Rational Attacks*. In *Proceedings of the Fourth International Workshop on Peer-to-Peer Systems (IPTPS '05)*, Ithaca, New York, (February 2005)

Seth J. Nielson and Charles D. Knutson. *OO++: Exploring the Multiparadigm Shift*. *Proceedings of the Workshop on Multiparadigm Programming with Object-Oriented Languages* (MPOOL 2004), Oslo, Norway, (June 2004)

Rob Kunz, Seth Nielson, Mark Clement, Quinn Snell, *Effective Bandwidth for Traffic Engineering*, *Proceedings of the IEEE Workshop on High Performance Switching and Routing (HPSR 2001),* Dallas, TX, (May 2001)

Testimony Before Government Bodies

Testimony in support of *Maryland SB 151/HB 211 Criminal Law - Crimes Involving Computers – Ransomware*. Testimony given to the Judicial Proceedings Committee of the Maryland Senate and the Judiciary Committee of the Maryland House of Delegates (January/February 2019)

Invited Talks, Panels, and Technical Training

Seth James Nielson and Maria Jose Castro Landaeta, *Psychology & Incentives: How Social Engineering Exploits Privacy & Behavior*, RSAC 365 Webinar (January 2024).

Seth James Nielson, *Data Security: Four Approaches to a Better Defensive Posture*, 2023 Enterprise Data World, Anaheim, CA (September 2023)

[**CANCELED DUE TO VENUE CHANGE**] Seth James Nielson, *Maintaining Data Security and Data Privacy in the 21st Century*, 2022 Enterprise Data World, San Diego, CA (March 2022)

Seth James Nielson, *Securing Your Data Assets Against Hackers*, 2021 Enterprise Data World, Boston, MA. (April 2021)

Seth James Nielson, *The Cybersecurity of IP*, 2020 Essential Cybersecurity Law, Austin, TX (Virtual). (July 2020)

[**CANCELED DUE TO COVID 19**] Seth James Nielson and Ellie Daw, *Correct Cryptography in Python*, a Tutorial for Cryptography Beginners, PyCon 2020, Philadelphia, PA. (April 2020)

[**CANCELED DUE TO COVID 19**] Seth James Nielson, *Protecting Your Data Assets*, 2020 Enterprise Data World, Boston, MA. (March 2020)

Seth James Nielson, *Security and Privacy for Data Architects*, 2019 Data Architecture Summit, Chicago, IL (October 2019)

Seth James Nielson, Crypto Done Right, One Year In. Lessons Learned and Next Steps. Presented in the International Cryptographic Knowledge Base 2019 (ICMC 2019), Vancouver, Canada (May 2019)

Panel Discussion, *Hardening US Unmanned Systems Against Enemy Counter Measures*. Accepted invitation to 7th Annual DoD Unmanned Systems Summit, Alexandria, VA (April 2019).

Seth James Nielson, *A Gentle Introduction to Blockchain*. 2019 Enterprise Data World, Boston, MA (March 2019).

Seth James Nielson, *A Gentle Introduction to Blockchain*. 2018 Data Architecture Summit, Chicago, IL (October 2018).

Seth James Nielson, *Detecting Malicious Sandboxes*. Workshop on Defensive Deception and

Trust in Autonomy, San Diego, CA (August 2018).

Seth James Nielson and Debra Baker, *Towards a Crowd-Sourced Cryptographic Knowledge Base*. Presented in the International Cryptographic Knowledge Base 2018 (ICMC18), Ottawa, Canada (May 2018).

Seth James Nielson, *The PyPy Sandbox*. Presented in the National Centers of Academic Excellence Tech Talk, Online (March 2018).

Theses

PhD Thesis: Designing Incentives for Peer-to-Peer Systems (defended 10/2009)
Master's Thesis: OO++ Design Patterns, GOF Revisited (defended 8/2004)

Technical Reports

Seth James Nielson and Dan S. Wallach, The BitTorrent Anonymity Marketplace, arXiv Technical Report 1108.2718, (August 2011)

Seth James Nielson, Caleb E. Spare, and Dan S. Wallach, Building Better Incentives for Robustness in BitTorrent, arXiv Technical Report 1108.2716, (August 2011)

Seth James Nielson, Seth J. Fogarty, and Dan S. Wallach, *Attacks on Local Searching Tools*, arXiv Technical Report 1108.2704 (Originally produced in December, 2004, available on arXiv as of August 2011)

White Papers and Trade Publications

Seth James Nielson, *Techniques for Discovering Unauthorized Copying in Software*, Crimson Vista White Paper, (January 2022)

Aviel D. Rubin, Seth J. Nielson, Christopher K. Monson, *Evaluation of the MarkMonitor AntiPiracy System*, Produced for the Center for Copyright Information (December 2013)

Aviel D. Rubin, Seth J. Nielson, Sam Small, Christopher K. Monson, *Guidelines for Source Code Review in Hi-Tech Litigation*, Harbor Labs White Paper (September 2013)

Undergraduate Advising

Independent Research and Capstones (University of Texas Austin)

Charlotte White, *Automated Partitioning of Software During Compilation,* CS 370, Independent Study, Summer 2024

Nishaanth Saaketh Joopelli, *Automated Patching of Unsafe C Functions,* CS 370, Independent Study, Summer 2024

Tanuj Tekkale, *Analysis of Image Provenance Techniques,* CS 370, Independent Study, Summer 2024

Andrew Dang, *Individual Voice Recognition using Machine Learning*, CS 370, Independent Study, Summer 2023

Monique Tran, *Malware Classification with SVM*, CS 370, Independent Study, Summer 2023

Gonzalo Tamariz-Martel Sánchez, *SMART CONTRACTS: Different approaches to introduce external (off-chain*) data (June 2022)

Graduate Advising

Capstones for Masters of Science in Security Informatics (Johns Hopkins)

Weizhou Wang, Runjie Zhang, *Research on defense next-generation malware on the Windows platform* (December 2018)

Yu-Tsern Jou, Ying Liu, Menghan Bai, *Open Source HSM Side Channel Analysis* (December 2018)

Bowen Shi, Hong Ma, Mengqi Qin, *Side Channel Attack on HSM Based on Machine Learning* (December 2018)

Dylan Richmond, Matthew Shonman, Jingcheng Yang, *An Exploration of the Usability of HTTPS* (December 2018)

Steven Cheng, Venkata Aditya Bollapragada, and Antara Sargam, *Using Selective RAM Journaling to Fight Ransomware* (December 2018)

Yongqiang Fan, Haiwen Sun*, Fault Tolerance System for IoT* (December 2018)

Weike Chen, Harry Luo, Prashanth Venkateswaran, *IoT Discovery* (August 2018)

Joseph "Jay" Kosturko, Eric Schlieber, Sean Futch, *Cracking a Continuous Flow Reactor: A Vulnerability Assessment for Chemical Additive Manufacturing Devices* (May 2018)

Chao Lei, Wenjun Li, *Anti-Honeypot Detection in Advanced Botnet Attacks* (December 2017)

Ritvik Sachdev, Purushottam Kulkarni, Praveen Malhan, *Securing ADS-B Based Airborne Collision Avoidance Systems* (December 2017)

Ningyuan Bao, Mengying Hu, *Security-Testing-Orientated Internet of Things(IoT) Simulator* (December 2017)

Zehuan Li, Shanshan Yang, Liangjia Fu, *AIS Data De-anonymization* (December 2017)

Chanyang Shin, Prerit Chandok, Aurin Chakravarty, *Forensic Data Collection from IoT Devices* (December 2017)

Kevin Manzotti, Kashif Memon, Rahul Durgad, *Replication of CryptoDrop* (December 2016)

Harshneel More, Jingmiao Wang, Yuanqi Zhu, *Detecting XSS attacks using BRO IDS* (December 2016)

Asmaa Aljohani, Gyan Namdhari, Yue Zhu, *Feasibility, Security and Privacy Analysis of EMVCo*

Payment Tokenization Technology for Identity Enabled Transactions (December 2016)

Richard Eaton, *The Emperor Has No Friends: Identifying Botnet Customers and Mapping Out Botnets on Twitter* (May 2015)

Jingru Chen, Yaning Liu, Yifan Yu, Zhiyue Zu, *Investigating the Heartbleed Vulnerability* (2015)

Kartik Thapar, *Security Techniques for Developing iOS Applications* (February 2015)

Jie Feng, Jianxiang Peng, Likai Zhang, *De-anonymizing BitCoin* (January 2014)

Teaching

University of Texas at Austin

Cybersecurity Tech/Law Policy (2020-)
Network Security and Privacy (2020-2021)

Johns Hopkins University

Advanced Network Security (2017 - 2019)
Network Security (2014 – 2019)

Rice University

Data Structures and Algorithms (Spring 2008)

Patents

Co-inventor: Nielson, S. 2021. Distributed Authentication Between Network Nodes. U.S. Patent 11,032,252 filed January 2, 2019 and issued June 8, 2021.

Co-inventor: Orsini, R. 2014. Systems and methods for security data in motion. U.S. Patent 8,745,372 filed November 24, 2010 and issued June 3, 2014.

Co-inventor: Orsini, R. 2014. Systems and methods for security data in motion. U.S. Patent 8,745,379 filed August 20, 2012 and issued June 3, 2014.

Co-inventor: O'Hare, R. 2014. Systems and methods for security data. U.S. Patent 8,677,148 filed January 27, 2012 and issued March 18, 2014.

In the News

"Johns Hopkins Researchers and OnBoard Security Team Up to Protect Drones," *Robotics Tomorrow*, 3/16/2018

"Rice University Computer Scientists Find a Flaw in Google's New Desktop Search Program." *New York Times*, 12/20/2004

Employment History

University of Texas at Austin
2020- **Adjunct Assistant Professor**

Source Code Discovery, LLC.

2019-2021 **Founder and Partner**

Crimson Vista, Inc.
2016-Present **Founder and Chief Scientist**

Johns Hopkins Applied Physics Lab
2018-2019 **Senior Professional Staff (Temp/On-Call)**

Johns Hopkins University
2016-2019 **Director of Advanced Research Projects**
2015-2019 **Adjunct Associate Research Scientist**
2014 **Lecturer**

Harbor Labs, LLC
2014-2015 **Principal**
2011-2014 **Research Scientist**

Independent Security Evaluators
2010-2011 **Senior Security Analyst**
2005-2009 **Security Analyst**

Google, Inc.
2005 **Summer Intern**

Metrowerks (Formerly Lineo, Inc.)
2001-2003 **Software Engineer II**

Expert Testimony

On behalf of the State of Texas in State of Texas v. Google

Counsel:	Norton Rose Fulbright
Venue:	District Court of Victoria County Texas
Subject Matter:	Biometric Data Storage
Reports:	1 report, February 2025

On behalf of OAN in Dominion Voting Systems v. OAN

Counsel:	Jackson Walker
Venue:	United States District Court for the District of Columbia
Subject Matter:	Voting machine security including forensic investigation
Reports:	3 Reports: December 2024, February 2025, March 2025

On behalf of Proofpoint in Proofpoint Inc. v. Abnormal Security

Counsel:	McDermott Will & Emery, LLP
Venue:	Case No. CGC-21-597059 (Superior Court of California, County of San Francisco)
Subject Matter:	Email Machine Learning
Reports:	1 report submitted October 2024
Deposition:	1 deposition October 2024

On behalf of LG Electronics in TOT Power Control v LG Electronics; C.A No. 21-1304-MN

Counsel:	DLA Piper
Venue:	District of Delaware
Subject Matter:	Outer loop power control, source code
Reports:	1 report September 2024
Deposition	1 deposition November 2024

On behalf of Dexcom in Dexcom v Abbott Diabetes Care; C.A. No. 22-605-KAJ

Counsel:	Quinn Emanuel
Venue:	District of Delaware
Subject Matter:	Glucose alerts source code
Reports:	1 report September 2024

On behalf of Axonics in In the Matter of Certain Video Processing Devices and Components Thereof; Investigation No. 337-TA-1396

Counsel:	Tensegrity
Venue:	ITC
Subject Matter:	Medical implant wireless transmission source code
Reports:	2 reports September 2024
Deposition:	1 deposition October 2024
Trial:	1 trial December 2024

On behalf of Apple in Carbyne v. Apple; Civil Action No. 1:23-cv-00324

Counsel:	Ropes and Gray
Venue:	West District of Texas, Austin Division
Subject Matter:	Authentication, Secure Storage, Secure Processing, Access
Reports:	1 report August 2024, 1 report September 2024
Deposition:	1 deposition October 2024
Trial:	1 evidentiary hearing November 2024

On behalf of Commure in Commure v. Canopy Works; Case No. 3:24-cv-02592-AMO

Counsel:	Quinn Emanuel
Venue:	Norther District of California
Subject Matter:	Security norms and customs related to wireless security
Reports:	1 declaration August 2024, 1 report March 2025
Deposition:	1 deposition September 2024

On behalf of Samsara In the Matter of Certain Vehicle Telematics, Fleet Management, and Video-based Safety Systems, Devices, and Components Thereof, Investigation No. 337-TA-1393

Counsel:	Kirkland and Ellis
Venue:	ITC
Subject Matter:	Automotive tracking, safety, analysis source code
Reports:	1 report August 2024, 1 report September 2024, 1 report November 2024
Deposition:	1 deposition September 2024
Trial:	1 trial March 2025

In support of Unified's Request for Ex Parte Reexamination of 10,601,780

Counsel:	Unified Patents

Venue: PTAB
Subject Matter: Network security and data filtering
Reports: 1 declaration, August 2024

On behalf of BOKF in Dynapass v BOKF
Counsel: Fish and Richardson
Venue: Eastern District of Texas, Marshall Division
Subject Matter: Multifactor Authentication, Financial Systems
Reports: 1 report May 2024

On behalf of Samsung in Samsung v Maxell
Counsel: DLA Piper
Venue: PTAB; Eastern District of Texas Texarkana Division
Subject Matter: Biometrics
Reports: 1 declaration April 2024, 1 report December 2024
Deposition: 1 deposition December 2024, 1 deposition February 2025

On behalf of Forescout Technologies in Fortinet v Forescout Technologies
Counsel: Winston & Strawn
Venue: Northern District of California
Subject Matter: Network security architecture and devices
Reports: 1 report March 2024
Deposition: 1 deposition May 2024

On behalf of Threat Modeler Software in Iriusrisk v Threat Modeler Software
Counsel: Rimon
Venue: PTAB
Subject Matter: Threat modeling
Reports: 1 declaration January 2024, 1 declaration February 2024
Deposition: 1 deposition March 2024, 1 deposition April 2024

On behalf of Motorola Solutions in Motorola Solutions v. Hytera Communications
Counsel: Kirkland and Ellis
Venue: Northern District of Illinois, Eastern Division
Subject Matter: Source code forensics
Reports: 1 declaration January 2024
Deposition: 1 deposition February 2024

In support of Unified's Request for Ex Parte Reexamination of U.S. Patent 7,586,871
Counsel: Univied Patents
Venue: PTAB
Subject Matter: Network security and data filtering
Reports: 1 declaration, February 2024

On behalf of the State of Texas in State of Texas v. Google
Counsel: Norton Rose Fulbright
Venue: District Court of Victoria County Texas
Subject Matter: Location tracking
Reports: 1 report, January 2024

Deposition: 1 deposition May 2024

In support of Unified's Request for Ex Parte Reexamination of U.S. Patent 9,264,441

Counsel: Rothwell, Figg, Ernst, and Manbeck
Venue: PTAB
Subject Matter: Network security devices and operations
Reports: 1 declaration, January 2024

On behalf of Dennis Zeedyk in the United States vs. Dennis Zeedyk (2023-Present)

Counsel: Saul Euwing
Venue: Northern District of Indiana South Bend Division
Subject Matter: Website forensics
Reports: 1 report November 2023

On behalf of OpenAI in OpenAI v Open Artificial Intelligence and Guy Ravine (2023-Present)

Counsel: Quinn Emanuel
Venue Northern District of California
Subject Matter: Forensic investigation of website and related assets
Reports: 3 reports issued October 2023, January 2025, February 2025
Deposition: 1 deposition March 2025

On behalf of Palo Alto Networks in Centripetal Networks v Palo Alto Networks (2021-Present)

Counsel: Norton Rose Fulbright and Ropes & Gray
Venue: Eastern District of Virginia
Subject Matter: Network security devices
Reports: 3 reports issued August 2023, September 2023, and October 2023
2 related declarations for EPR submitted July 2024
Deposition: 1 deposition October 2023
In Court: January 2024

On behalf of Anchor Semiconductor in Elite v. Anchor (2022-Present)

Counsel: Vennable
Venue: Norther District of California
Subject Matter: Forensic investigation of alleged sabotage and data destruction
Reports 1 report July 2023

In support of Unified Patents in Ex Parte Reexamination of U.S. Patent 9,438,614

Counsel: Unified Patents
Venue: PTAB
Subject Matter: Machine learning and intrusion detection systems
Reports 1 declaration Apr 2023

On behalf of Trend Micro in Trend Micro v. TaaSera Licensing (2022-Present)

Counsel: Marbury Law Group
Venue: PTAB
Subject Matter: Security technologies and devices (various)
Reports: 4 declarations Apr 2023

On behalf of Salesforce in WSOU Investments v. Salesforce (2022-Present)

Counsel: Quinn Emanuel
Venue: Western District of Texas
Subject Matter: Source code related to transmission of marketing emails
Reports: 1 report March 2023
Deposition: 1 deposition August 2023

On behalf of Trend Micro in Trend Micro v. Webroot (2022-Present)
Counsel: Marbury Law Group
Venue: PTAB
Subject Matter: Security technologies and devices (various)
Reports: 5 declarations Feb-Mar 2023, 5 declarations September 2023

On behalf of Fox News in Dominion Voting Systems v. Fox News (2022-2023)
Counsel: Winston and Strawn
Venue: Superior Court of the State of Delaware
Subject Matter: Voting machine security including forensic investigation
Reports: 1 Report December 2022
Deposition: 1 deposition February 2023

On behalf of Public Storage in Estch v. Public Storage (2022-2023)
Counsel: Orrick
Venue: Eastern District of Texas
Subject Matter: VoIP, authentication, authorization
Reports: 1 Report January 2023
Deposition: 1 deposition January 2023

On behalf of Lenovo/Motorola Mobiliy in Maxell Ltd v. Lenovo/Motorola Mobility (2022-2023)
Counsel: Kirkland and Ellis
Venue: ITC
Subject Matter: Authentication
Reports: 1 Declaration November 2022
2 Reports February 2023
Deposition: 1 deposition March 2023

On behalf of Elon R Musk in Twitter Inc v. Elon R Musk (2022)
Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Court of Chancery of the State of Delaware
Subject Matter: Evaluation of Security in light of Whistleblower Report
Reports: 1 Report October 2022

On behalf of Bissell, Inc. in Bissell Inc. v. Tineco Intelligent Technology Co. Ltd., (2022)
Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: ITC
Subject Matter: Forensic evaluation of source code
Reports: 1 Report submitted September 2022
Deposition: 1 deposition November 2022
In Court: December 2022

On behalf of Hakkasan USA in Hakkasan USA v Endurance American Specialty Insurance (2022)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: District of Nevada (Clark County)
Subject Matter: Forensic evaluation of emails
Reports: 1 Report submitted May 2022
Deposition: 1 deposition July 2022

On behalf of JTC in Seimens vs JTC (2021-2022)
Counsel: Peckar and Abramson, PC
Venue: American Arbitration Association
Subject Matter: Software Engineering Efforts
Reports: 1 Report submitted in July 2021
1 Report submitted in September 2021
Deposition: 1 deposition October 2021
In Court: March 2022 (arbitration)

On behalf of Samsung in Samsung v. Proxense (2021-2022)
Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Western District of Texas (Waco)
Subject Matter: Authentication, Authorization, Device-to-device
Reports: 1 declaration submitted October 2021
Deposition: 1 deposition October 2022

On behalf of Bitglass in Netskope, Inc. v. Bitglass Inc. (2021-2022)
Counsel: Irell and Manela, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Authentication, Single-Sign-On
Reports: 1 declaration submitted September 2021
1 declaration submitted March 2021

On behalf of The State of Arizona in Arizona v. Google (2021-2022)
Counsel: Ruttenberg IP Law
Venue: Superior Court of the State of Arizona (Maricopa)
Subject Matter: Privacy, Location tracking, Data collection
Reports: 1 declaration submitted August 2021

On behalf of TLC in TLC v. Koninklijke Philips N.V., US Philips Corporation (2019-2021)
Counsel: Perkins Coie LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Cryptographic protocols
Reports: 1 declaration submitted February 2021

On behalf of Magic Micro in Monsoon v. Magic Micro (2020-2021)
Counsel: Gutnicki, LLP
Venue: International Centre for Dispute Resolution
Subject Matter: Blockchain, file storage
Reports: 1 declaration submitted October 2020
1 declaration submitted November 2020
In Court: In arbitration December 2020

On behalf of Juniper in Juniper Networks Inc. v. Huawei Digital Technologies Co. (2020-2021)

Counsel:	Irell and Manella, LLP
Venue	PTAB Petition for Inter Partes Review
Subject Matter:	Network perimeter defense against malware
Reports:	1 declaration submitted June 2020
	1 declaration submitted July 2021
Deposition:	1 deposition April 2021

On behalf of DivX in Netflix v. DivX (2020-2023)

Counsel:	Lowenstein & Weatherwax, LLP
Venue:	PTAB Petition for Inter Partes Review
Subject Matter:	Encryption of streaming media
Reports:	1 declaration submitted May 2020
	1 declaration submitted December 2020
	1 declaration submitted April 2021
Deposition	1 deposition January 2021, 1 deposition February 2021

On behalf of Juniper in Juniper Networks Inc. v. Implicit LLC (2019-2020)

Counsel:	Irell and Manella, LLP
Venue:	PTAB Petition for Inter Partes Review
Subject Matter:	Packet classification
Reports:	1 declaration submitted February 2020

On behalf of the Dealership class in Dealer Management Systems Antitrust Litigation (2019-Present)

Counsel:	Milberg Phillips Grossman LLP
Venue:	Case No. 18-cv-00864 (Northern District of Illinois)
Subject Matter:	Cybersecurity, risk assessment, third-party access
Reports:	1 report submitted November 2019
Deposition:	1 deposition January 2020

On behalf of Symantec in the Trustees of Columbia University in the City of New York v. Symantec Corporation. (2018-2022)

Counsel:	Quinn Emanuel Urquhart & Sullivan, LLP
Venue:	Case No. Civil Action No. 3:13-cv-00808-JRS (Eastern District of Virginia)
Subject Matter:	Deception technologies, Honeypots
Reports:	1 report submitted October 2019
Deposition:	1 deposition January 2020
In Court:	April 2022

On behalf of Proofpoint in Proofpoint Inc. v. Vade Secure (2019-2021)

Counsel:	Quinn Emanuel Urquhart & Sullivan, LLP
Venue:	Case No. 3:19-cv-04238 (Northern District of California)
Subject Matter:	Cloud-based email, malware detection, AI
Reports:	1 report submitted September 2019, 1 report submitted December 2019
	1 report submitted February 2021, 1 report submitted April 2021
Deposition:	1 deposition April 2021
In Court:	Expert testimony August 2021

On behalf of Bitdefender in Finjan Inc. v. BitDefender Inc. (2018-2021)

Counsel:	Susman Godfrey LLP
Venue:	Case No. 4:17-cv-4790-HSG (Northern District of California)
Subject Matter:	Web threat detection, malware, gateways
Reports:	1 report submitted July 2019, 1 report submitted August 2019
Deposition:	1 deposition October 2019

On behalf of HTC in Koninklijke Philips N.V., US Philips Corporation v. HTC Corp., HTC America Inc. (2019-2020)

Counsel:	Perkins Coie LLP
Venue:	Case No. 4:18-cv-01887-HSG (Northern District of California)
Subject Matter:	Cryptographic protocols
Reports:	1 report submitted May 2019, 1 report submitted June 2019
Deposition:	1 deposition August 2019

On behalf of Juniper in Juniper Networks Inc. v. Finjan Inc. (2018-2019)

Counsel:	Irell and Manella, LLP
Venue:	PTAB Petition for Inter Partes Review
Subject Matter:	Malware, firewall/gateway, network security
Reports:	4 declarations submitted October 2018
Deposition:	1 deposition June 2019

On behalf of Redbox in Disney Enterprises, Inc., LucasFilm Ltd, LLC, and MVL Film Finance LLC v. Redbox Automated Retail, LLC. (2018)

Counsel:	Robins Kaplan LLP
Venue:	Case No. 2:17-cv-08655-DDP (AGRx) (Central District of California, Western Division)
Subject Matter:	DRM, cloud security, media streaming
Reports:	1 declaration submitted May 2018

On behalf of Trend Micro in Trend Micro, Inc. v. Security Profiling, LLC (2017-2018)

Counsel:	The Marbury Law Group, PLLC
Venue:	Inter Partes Review Case No. IPR2017-02191 and IPR2017-02192
Subject Matter:	Automated security patches
Reports:	2 declarations submitted September 2017
Deposition:	1 deposition June 2018

On behalf of TeleSign in Twilio Inc. v. TeleSign Corporation (2016-2021, multiple cases)

Counsel:	Shook, Hardy & Bacon LLP
Venue:	Inter Partes Review Case No. IPR2016-01688, IPR2016-00360, IPR2017-01976 IPR2017-01977, IPR2017-01978 Case No. 5:16-cv-6925-LHK (Nor. District of California, San Jose Div.)
Subject Matter:	Telecommunications security
Reports:	1 declaration submitted August 2016, May 2017, and July 2017
Deposition:	1 deposition November 2016, 1 deposition July 2017, 1 deposition August 2017

On behalf of Blue Coat in Finjan Inc. v. Blue Coat Systems LLC (2017-2018)

Counsel:	Originally Wilson, Sonsini, Goodrich and Rosati PC; later Morrison &

Foerster LLP
Venue: Case No. 15-cv-03295-BLF-SVK (Nor. District of California, San Div.)
Subject Matter: Firewalls, gateway, security devices, malware
Reports: 1 report submitted April 2017
Deposition: 1 deposition April 2017
In Court: Tech tutorial February 2017, expert testimony November 2017

On behalf of Sedosoft in Sedosoft Inc. v Mark Burchett LTD and NFSx9 LLC (2016)
Counsel: McInnes and McLane LLP
Venue: Case No. Civil Action No. 1:15-cv-10244-RGS (District of Massachusetts)
Subject Matter: Code theft
Reports: 1 report submitted May 2016 and August 2016

On behalf of USAA in Asghari-Kamrani, et al. v. United Services Automobile Association, Inc.
Counsel: Fish and Richardson PC
Venue: Inter Partes Review Case No. IPR2015-01842, and CBM2016-00063, CBM2016-00064
Subject Matter: Applied cryptography, authentication
Reports: 1 report submitted September 2015, 1 report submitted April 2016
Deposition: 1 deposition March 2017

On behalf of WTS Paradigm in WTS PARADIGM, LLC v EDGEAQ, LLC (2015-2016)
Counsel: Quarles & Brady LLP
Venue: Case No. 3:15-CV-330 (Western District of Wisconsin)
Subject Matter: Software-assisted product configuration, presentation, and ordering
Reports: 1 report submitted March 2016
Deposition: 1 deposition April 2016

On behalf of Mr Leon Stambler in Mr. Leon Stambler v Mastercard IPR (2015-2016)
Counsel: Flachsbart & Greenspoon, LLC
Venue: CBM2015-00044
Subject Matter: Authentication, authentication codes
Reports: 1 declaration submitted October 2015
Deposition: 1 deposition December 2015

On behalf of Trusteer/IBM in Trusted Knight Corporation v. International Business Machines Corporation and Trusteer, Inc. (2015)
Counsel: Quinn Emanuel Urquhart & Sullivan LLP
Venue: C.A. No. 14-1063 LPS-CJB (District of Delaware)
Subject Matter: Key logging, protections against
Reports: 1 declaration submitted July 2015

On behalf of Sensus in Sensus USA, Inc. v. Certified Measurement, LLC (2015)
Counsel: Feldman Gale PA
Venue: Inter Partes Review Case No. IPR2015-01262, IPR2015-01311, IPR2015-01439, IPR2015-01454
Case number 3:14-cv-01069 (District of Connecticut)
Subject Matter: Applied cryptography, certification of data
Reports: 1 declaration submitted June 2015, 4 declarations submitted July 2015

On behalf of Chad Eichenberger in Chad Eichenberger v. ESPN (2015)

Counsel:	Edelson PC
Venue:	Case No. 2:14-cv-00463 (Western District of Washington)
Subject Matter:	Consumer privacy
Reports:	1 declaration submitted January 2015

On behalf of Microsoft Corporation in Microsoft Corporation v. Optimum Content Protection LLC. (2014)

Counsel:	Sidley Austin LLP
Venue:	Inter Partes Review No. IPR2015-00048
Subject Matter:	DRM, data streaming, protection
Reports:	1 declaration submitted October 2014

On behalf of Fortinet in Fortinet v. Sophos (2014-2015, multiple cases)

Counsel:	Quinn Emanuel Urquhart & Sullivan LLP
Venue:	Inter Partes Review No. IPR2015-00618
	Case No. 3:13-cv-05831-EMC (DMR) (Nor. District of California, SF div.)
	Case No. 1:14-cv-00100-GMS (District of Delware)
Subject Matter:	Antivirus, anti-malware
Reports:	2 declarations submitted September 2014, 1 submitted September 2015
	1 report submitted October 2015, November 2015
Deposition:	1 deposition October 2014, 1 deposition October 2015
In Court:	Tech tutorial December 2015

On behalf of Afilias in Afilias PLC v Architelos Inc and Alexa Raad (2015)

Counsel:	Haynes Boone LLP
Venue:	Case No. 1:15-cv-00014-LMB-JFA (Eastern District of Virginia)
Subject Matter:	Domain name system anti-abuse
Reports:	1 report submitted April 2015, May 2015
Deposition:	1 deposition June 2015
In Court:	Expert testimony August 2015

On behalf of Telit in M2M v. Motorola, Telit (2015-2016)

Counsel:	Pearl Cohen Zedek Latzer Baratz LLP
Venue:	Case No. 12-033-RGA (District of Delaware)
Subject Matter:	Authentication
Reports:	1 declaration submitted May 2014,
	1 report submitted July 2014, August 2014
Deposition:	1 deposition June 2015

On behalf of Rmail/Rpost in Rmail Limited, v. Amazon.com, Inc., and Paypal and Rmail Limited, Rpost Communications Limited, and Rpost Holdings Inc., v.Docusign, Inc. (2013-2014)

Counsel:	Hudnell Law Group PC
Venue:	Case No. 2:10-CV-258-JRG (Lead Case)
	Case No. 2:11-CV-299-JRG (Member Case) (E.D. Texas)
Subject Matter:	Email security
Reports:	2 reports April 2013, 1 declaration June 2013
Depositions	1 deposition May 2013 (2 days)

On behalf of Via Vadis in Via Vadis v. Skype (2012-2014)

Counsel:	WTP Law
Venue:	Via Vadis v. Skype, Case No. 11-507 (RGA) (District of Delaware)
Subject Matter:	P2P communications
Reports:	1 affidavit December 2012