

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ASKELADDEN, L.L.C.,

Petitioner

v.

JABAA, L.L.C.,

Patent Owner

IPR2024-00916

U.S. Patent No. 7,480,637

**Declaration of Dr. Henry Houh Under 37 C.F.R. § 1.68
In Support of Petition for *Inter Partes* Review of
U.S. Patent No. 7,480,637
(Claims 7-20)**

Table of Contents

I.	Introduction.....	4
II.	Background and Qualifications	7
III.	Understanding of Patent Law	14
IV.	The '637 Patent.....	17
V.	Prosecution History of the '637 Patent.....	20
VI.	Level of Ordinary Skill in the Pertinent Art.....	21
VII.	Claim Construction.....	22
VIII.	Detailed Unpatentability Analysis.....	23
A.	Ground 1: Claims 7-9 and 20 are rendered obvious over Rescorla in view of Mathiassen	25
1.	Overview of Rescorla	25
2.	Overview of Mathiassen	27
3.	Motivation to Combine Rescorla and Mathiassen.....	33
4.	Analysis	43
a)	Claim 7.....	43
b)	Claim 8.....	73
c)	Claim 9.....	74
B.	Ground 2: Claims 10-14 would have been obvious over Rescorla in view of Mathiassen and Ryan.	77
1.	Overview of Ryan.....	77
2.	Motivation to Combine Rescorla and Mathiassen with Ryan.....	81
3.	Analysis	86

Declaration of Dr. Henry Houh Under 37 C.F.R. § 1.68 in Support of
Petition for *Inter Partes* Review of Claims 7-20 of U.S. Patent No. 7,480,637

a)	Claim 10.....	86
b)	Claim 11.....	91
c)	Claim 12.....	94
d)	Claim 13.....	94
e)	Claim 14.....	96
C.	Ground 3: Claims 15-20 would have been obvious over Mathiassen in view of Rescorla and Ryan.	97
1.	Motivation to Combine Mathiassen with Rescorla	97
2.	Motivation to Combine Mathiassen and Rescorla with Ryan.	99
3.	Analysis	100
a)	Claim 15.....	100
b)	Claim 16.....	120
c)	Claim 17.....	120
d)	Claim 18.....	120
a)	Claim 19.....	121
b)	Claim 20.....	122
IX.	Availability for cross-examination	136
X.	Conclusion	136

Declaration of Dr. Henry Houh Under 37 C.F.R. § 1.68 in Support of
Petition for *Inter Partes* Review of Claims 7-20 of U.S. Patent No. 7,480,637

I, Henry Houh, do hereby declare as follows:

I. INTRODUCTION

1. I have been retained by counsel for Askeladden, L.L.C. (“Askeladden”) as an independent expert witness for the above-captioned Petition for *Inter Partes* Review (“IPR”) of U.S. Patent No. 7,480,637 (“the ’637 Patent”). I am being compensated at my usual and customary rate for the time I spend in connection with this IPR. My compensation is not affected by the outcome of this IPR.

2. I have been asked to provide my opinions regarding whether claims 7-20 (the “Challenged Claims”) of the ’637 Patent are unpatentable as they would have been obvious to a person having ordinary skill in the art (“POSITA”) as of the earliest claimed priority date. After reviewing the prior art discussed below, it is my opinion that the Challenged Claims would have been obvious to a POSITA.

3. In preparing this Declaration, I have reviewed:

- Ex.1001, the ’637 Patent;
- Ex.1002, the file history of the ’637 Patent;
- the prior art references discussed below:
 - Ex.1015, Eric Rescorla, “SSL and TLS: Designing and Building Secure Systems,” Addison-Wesley, (2001) (“Rescorla”);

Declaration of Dr. Henry Houh Under 37 C.F.R. § 1.68 in Support of
Petition for *Inter Partes* Review of Claims 7-20 of U.S. Patent No. 7,480,637

- Ex.1005, U.S. Patent Publication No. 2004/0123113 to
Mathiassen et al. (“Mathiassen”);
- Ex.1006, U.S. Patent Publication No. 2005/0109841 to
Ryan et al. (“Ryan”);
- the following materials:
 - Ex.1007, U.S. Patent Publication No. 2003/0005336 to
Poo et al. (“Lim”);
 - Ex.1017, U.S. Patent Publication No. 2005/0165700 to
Karthik (“Karthik”);
 - Ex.1018, U.S. Patent Publication No. 2006/0123465 to
Ziegler (“Ziegler”);
 - Ex.1021, U.S. Patent Publication No. 2005/0193198 to
Livowsky (“Livowsky”);
 - Ex.1022, U.S. Patent No. 7,725,717 to Roux et al.
 (“Roux”);
 - Ex.1023, U.S. Patent No. 7,975,139 to Coulier
 (“Coulier”); and
- any other document cited below.

Declaration of Dr. Henry Houh Under 37 C.F.R. § 1.68 in Support of
Petition for *Inter Partes* Review of Claims 7-20 of U.S. Patent No. 7,480,637

These cited documents are the types of materials that an expert in my field would reasonably rely on in forming an opinion on this subject.

4. I understand that the '637 Patent issued on January 20, 2009, from U.S. Patent Application No. 11/317,141 ("the '141 Application"), filed December 23, 2005. The face of the '637 Patent lists Douglas Kozlay as inventor. I have been informed by counsel that, according to assignment records, Jabaa, L.L.C. is the current assignee of the '637 Patent.

5. In forming the opinions expressed in this Declaration, I relied upon my education and experience in the relevant field of art, and have considered the viewpoint of a person of ordinary skill in the art ("POSITA"), as of December 23, 2005, the filing date of the '637 Patent.

6. In forming the opinions expressed in this Declaration, I have also considered:

- a) the documents listed above,
- b) any additional documents and references cited in the analysis below,
- c) the relevant legal standards, including the standard for obviousness, and
- d) my knowledge and experience based upon my work in this area as described below.

While I have organized the information presented in this declaration into various sections, my opinions are supported by the information in the declaration in its entirety.

II. BACKGROUND AND QUALIFICATIONS

7. My qualifications are set forth in my curriculum vitae, a copy of which is submitted as Exhibit 1004 in this proceeding. As set forth in my curriculum vitae:

8. I received a Ph.D. in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology (“MIT”) in 1998. Beforehand, I received a Master of Science degree in Electrical Engineering and Computer Science in 1991, a Bachelor of Science degree in Electrical Engineering and Computer Science in 1989, and a Bachelor of Science degree in Physics in 1990, all from MIT.

9. I am currently self-employed as an independent technical consultant. Until October 2022, I was also president of a company that provides supplemental science, technology, engineering, and mathematics (“STEM”) education to children of all ages.

10. I first worked in the field of telecommunications in 1987 as a summer intern at AT&T Bell Laboratories as part of a five-year dual degree program at MIT. I continued to work at AT&T Bell Laboratories as part of this MIT program. While at MIT, I was a teaching assistant (“TA”) in the Electrical Engineering and Computer Science Department’s core Computer Architectures course. My first TA post, during

my senior year, was to a role typically reserved for graduate students. I later became head TA. The course covered various topics in computer architectures. As a TA, I helped write homework assignments, lab assignments, and exams. I also taught in the recitation sections.

11. Later, as part of my doctoral research at MIT from 1991-1998, I was a research assistant in the Telemedia Network Systems (“TNS”) group at the Laboratory for Computer Science. The TNS group built a high-speed gigabit network and created applications that ran over the network. Example applications included ones for remote video capture, processing, and display of video on computer terminals. In addition to working on the design of core network components, I worked on designing and building high-speed links, and designing and writing device drivers for interface cards, and set up the group’s web server.

12. I also helped to build the web pages that initiated the above-mentioned video sessions via a web interface. Vice President Al Gore visited our group in 1996 and received a demonstration of—and remotely drove—a radio-controlled toy car with a wireless video camera mounted on it that was built by our group. This toy car device received commands transmitted over a network from a remote computer, and video data from the toy car was transmitted wirelessly then over a computer network back to the user controller. On occasion, we allowed users visiting our web site to drive the toy car from their remote computer while they watched the video on their

computer. The video stream was encoded by TNS-designed hardware, streamed over the TNS-designed network, and displayed using TNS-designed software.

13. In January 1998, I defended and submitted my Ph.D. thesis, titled “Designing Networks for Tomorrow’s Traffic.” As part of my thesis research, I analyzed local area and wide area flows to show a more efficient method for routing packets in a network, based on traffic patterns at the time. The traffic flow data included Ethernet, IP, TCP or UDP, and RTP header information, which I analyzed to reach the conclusions set forth in my thesis.

14. From 1997 to 1999, I was a Senior Scientist and Engineer at NBX Corporation, a start-up that made business telephone systems for streaming packetized audio over data networks instead of using traditional telephone lines. NBX was later acquired by 3Com Corporation and the phone system is still used today by numerous businesses.

15. As part of my work at NBX, I designed the core audio reconstruction algorithms for the telephones, as well as the packet transmission algorithms. I also designed and validated the core packet transport protocol used by the phone system. The protocol was used for all signaling in the phone system, including for the setup of conference calls.

16. The NBX system also featured a computer interface for initiating phone calls, which could also initiate conference calls. The NBX system also supported the

Telephony Application Programming Interface (“TAPI”) that allowed other computer programs to integrate with our system telephony features. We obtained U.S. Patent No. 6,967,963, entitled “Telecommunication method for ensuring on-time delivery of packets containing time-sensitive data,” as part of this work. I also programmed the first prototype of our phone which communicated using IP, and I demonstrated our IP phones working over the Internet when we attended a trade show in California. The phone connected over the Internet to our headquarters in Andover, MA. I also programmed a data capture and analysis system that provided data on the operation of the system.

17. From 1999-2004, I was employed by Empirix or its predecessor company, Teradyne. Empirix was a leader in test tools for telecommunications protocols and systems, providing functional testing tools as well as load testing tools. From 2000-2001, I conceived and built a test platform for testing Voice-over-IP (VoIP). The first application on this new test platform was a cloud emulator for simulating the effects of transmitting VoIP over a busy network. The test platform was based on a network processor chip, which could be programmed to cut-through packets while processing packet data such as various protocol layer headers including addresses included therein and even packet data contents. I also designed a protocol analyzer built on the same platform. The application captured and performed protocol decoding at various layers in the protocol stacks of captured packets,

including detailed Ethernet header decoding, IP header decoding, TCP header decoding, UDP header decoding, RTP header decoding, and many other specified protocols. The application was also designed to reconstruct entire conversations that spanned multiple packets.

18. At Empirix, I also redesigned the architecture of the Web Test division's core product, e-Test Suite. E-Test Suite was a software program designed to perform functional and load testing of web applications. I was technical lead on the project, and also worked on programming a Javascript interpreter for the product. Javascript is the flexible programming layer that allows users to interact with web pages through actions such as clicking and dragging that allows web page programmers to extend the functionality of a web page beyond clicking on links.

19. In 2006, as part of my role at BBN Technologies, I helped found PodZinger Inc., now known as RAMP Inc. PodZinger utilized BBN's speech recognition algorithms to search through the spoken words in audio and video segments. While I was Vice President of Operations and Technology, PodZinger followed its initial prototype with a full streaming audio and video search solution. I also created a social networking web site, which BBN sold to a venture-funded startup company. In the process of creating the web site, I designed and specified the authentication and authorization protocols.

20. At my educational company, Einstein's Workshop, I created the initial web site and integrated it with online payment solutions. I evaluated, sourced, and configured the point-of-sale system for the company, which involved integration with and setup of mobile shopping terminals. We also teach programming to children of all ages, starting with Scratch programming for young elementary students and advancing through programming in Python and for game development for high school students. I conceived many of the programming classes and have taught programming to novice and more advanced students. We also created an educational computer-aided design tool, called BlocksCAD. We received a grant, on which I was the principal investigator, to further develop BlocksCAD and successfully met our grant objectives. BlocksCAD was spun-off from Einstein's Workshop and has been part of various incubator/accelerator programs in education as well as at the MIT Media Lab. Today, BlocksCAD is used worldwide in makerspaces as well as in schools throughout the U.S.

21. I have been awarded several United States patents, and I have several patent applications pending including the following examples:

- U.S. Patent No. 7,975,296, "Automated security threat testing of web pages";
- U.S. Patent No. 7,877,736, "Computer language interpretation and optimization for server testing";

Declaration of Dr. Henry Houh Under 37 C.F.R. § 1.68 in Support of
Petition for *Inter Partes* Review of Claims 7-20 of U.S. Patent No. 7,480,637

- U.S. Patent No. 7,801,910, “Method and apparatus for timed tagging of media content”;
- U.S. Patent 7,590,542, “Method of generating test scripts using a voice-capable markup language”;
- U.S. Patent No. 6,967,963, “Telecommunication method for ensuring on-time delivery of packets containing time-sensitive data”;
- U.S. Patent Application Publication No. 20070106685, “Method and apparatus for updating speech recognition databases and reindexing audio and video content using the same”;
- U.S. Patent Application Publication No. 20070106693, “Methods and apparatus for providing virtual media channels based on media search”;
- U.S. Patent Application Publication No. 20070106760, “Methods and apparatus for dynamic presentation of advertising, factual, and informational content using enhanced metadata in search-driven media applications”;
- U.S. Patent Application Publication No. 20070112837, “Method and apparatus for timed tagging of media content”;

- U.S. Patent Application Publication No. 20070118873, “Methods and apparatus for merging media content”; and
- U.S. Patent Application Publication No. 20090222442, “User-directed navigation of multimedia search results.”

III. UNDERSTANDING OF PATENT LAW

22. I am not an attorney. For the purposes of this declaration, I have been informed about certain aspects of the law that are relevant to my opinions. My understanding of the law was provided to me by Petitioner’s attorneys.

23. I have been asked to provide my opinions regarding whether claims 7-20 of the ’637 Patent would have been obvious to a POSITA at the time of the alleged invention in light of the prior art.

24. I understand that prior art to the ’637 Patent includes patents and printed publications in the relevant art that predate the priority date of the ’637 Patent.

25. I understand that a claim is unpatentable if it would have been obvious. Obviousness of a claim requires that the claim would have been obvious from the perspective of a POSITA at the time the alleged invention was made. I understand that a claim could have been obvious from a single prior art reference or from a combination of two or more prior art references.

26. I understand that an obviousness analysis requires an understanding of the scope and content of the prior art, any differences between the alleged invention and the prior art, and the level of ordinary skill in evaluating the pertinent art.

27. I further understand that a claim would have been obvious if it unites old elements with no change to their respective functions, or alters prior art by mere substitution of one element for another known in the field and that combination yields predictable results. Also, I understand that obviousness does not require physical combination/bodily incorporation, but rather consideration of what the combined teachings would have suggested to persons of ordinary skill in the art at the time of the alleged invention. I 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.

28. As mentioned above, I understand that a claim would have been obvious if it unites old elements with no change to their respective functions, or alters prior art by mere substitution of one element for another known in the field and that combination yields predictable results. While it may be helpful to identify a reason for this combination, I understand that there is no rigid requirement of finding an express teaching, suggestion, or motivation to combine within the references. When a product is available, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a POSITA

can implement a predictable variation, obviousness likely bars its patentability. For the same reason, if a technique has been used to improve one device and a POSITA would recognize that it would improve similar devices in the same way, using the technique would have been obvious. I understand that a claim would have been obvious if common sense directs one to combine multiple prior art references or add missing features to reproduce the alleged invention recited in the claims.

29. I further understand that certain factors may support or rebut the obviousness of a claim. I understand that such secondary considerations include, among other things, commercial success of the patented invention, skepticism of those having ordinary skill in the art at the time of invention, unexpected results of the invention, any long-felt but unsolved need in the art that was satisfied by the alleged invention, the failure of others to make the alleged invention, praise of the alleged invention by those having ordinary skill in the art, and copying of the alleged invention by others in the field. I understand that there must be a nexus—a connection—between any such secondary considerations and the alleged invention. I also understand that contemporaneous and independent invention by others is a secondary consideration tending to show obviousness.

30. I am not aware of any allegations by the named inventors of the '637 Patent or any assignee of the '637 Patent that any secondary considerations tend to rebut the obviousness of the Challenged Claims of the '637 Patent.

31. I understand that in considering obviousness, it is important not to determine obviousness using the benefit of hindsight derived from the patent being considered.

32. I understand that other challenges to the validity of a patent, including patent ineligibility, enablement, written description, and definiteness, cannot be raised in *inter partes* review proceedings before the Board to challenge the unpatentability of the '637 Patent. Accordingly, I did not consider those other challenges.

33. I understand that Petitioner has the burden of proving unpatentability by a preponderance of evidence, which means that the claims are more likely than not unpatentable.

34. I understand that the claims are to be construed according to the same claim construction standard that district courts use wherein claim terms are given their ordinary and customary meaning from the perspective of a person of ordinary skill in the art at the time of the invention.

35. The analysis in this declaration is in accordance with the above-stated legal principles.

IV. THE '637 PATENT

36. The '637 Patent relates to a customer authentication apparatus. The '637 Patent describes the customer authentication apparatus as a USB dongle in one

embodiment and as a wireless card in another embodiment. Ex.1001, Abstract. The USB dongle embodiment is shown in Fig. 1A, shown below. The wireless card embodiment is shown in Fig. 1B, also shown below. Ex.1001, Abstract, 4:61-5:35, 6:49-58. The '637 Patent describes the customer authentication apparatus as an "Internet Transaction Authentication" (ITA) apparatus. Ex.1001, 1:9-14, 4:61-64, 6:48-54. The ITA apparatus purports to improve security of a transaction with a website by authenticating the user. Ex.1001, 3:36-39. The '637 Patent also alleges that the ITA apparatus also authenticates a website. Ex.1001, 5:31-35.

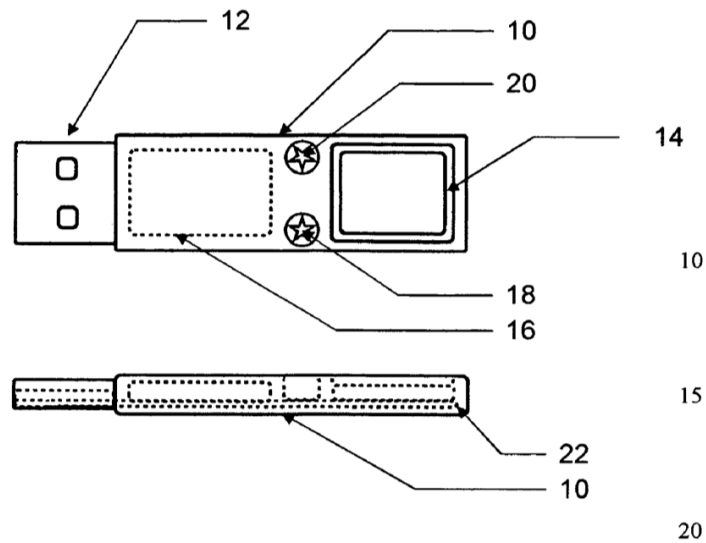


Figure 1A, Internet Transaction Authenticator in USB Dongle Form

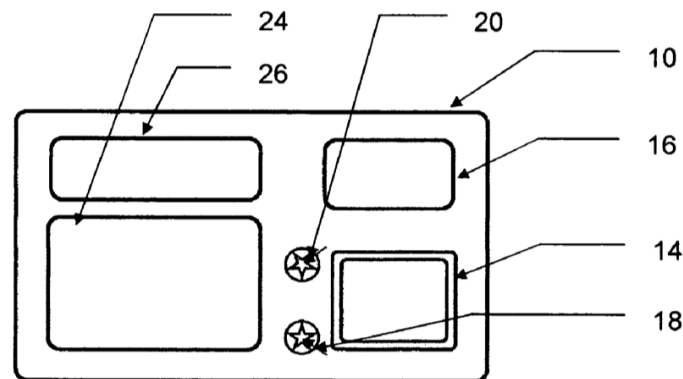


Figure 1B, Internet Transaction Authenticator in Wireless Card Form

Ex.1001, Figs. 1A and 1B

In both embodiments, the ITA apparatus includes a fingerprint sensor array 14 for user authentication. Ex.1001, 5:25-27 (“Additionally, a biometric fingerprint authentication component is provided, such as integrated fingerprint sensor array 14....”). In both embodiments, the ITA apparatus includes LED lights 18, 20 for

communicating whether a user has been authenticated. Ex.1001, 5:27-31 (“In the embodiment shown in FIG. 1, there are also a plurality of light emitting diodes, LED 18 and LED 20, which are coupled to the fingerprint sensor array 14, processor 16, and which are mounted on substrate 22.”). The ITA apparatus is inserted into a USB port. Ex.1001, 5:38-51 (“When an enrolled person is ready to initiate their transaction, they first insert the ITA USB connector 12 into an available USB port on a target machine.”). The user then places a finger on the fingerprint sensor array 14 to authenticate herself, and the LED 18 turns green if the user is authenticated or red if the user is not authenticated. Ex.1001, 5:38-55. If the user is authenticated, the apparatus sends an encrypted packet with the authentication results to the website. Ex.1001, 6:15-26. The user may then complete a transaction on the website. Ex.1001, 6:27-32. The ’637 Patent explains that the wireless card embodiment operates in the same way as the USB embodiment, except that the wireless card communicates wirelessly (e.g., via Bluetooth) instead of via a USB interface. Ex.1001, 6:48-57. The challenged claims, which I have analyzed in full, are included in an Appendix to this declaration.

V. PROSECUTION HISTORY OF THE ’637 PATENT

37. The U.S. Patent Application of the ’637 Patent (U.S. Patent No. 11/317,141 referred to herein as “the ’141 Application”) was filed on December 23, 2005. The United States Patent and Trademark Office issued a rejection rejecting all

claims as obvious over U.S. Patent Publication No. 2005/0165700 to Karthik, published on July 28, 2005, and U.S. Patent Publication No. 2006/0123465 to Ziegler, published on June 8, 2006. Ex.1002, 76-90. The inventor filed a response which was not recognized by the Patent Office and a notice of abandonment issued. The inventor assigned the application to Biometric Associates, LP, which filed a response with a petition to revive. In its response, the assignee did not amend claim 15. '637 Patent File History, 43-44. The assignee amended claims 7 and 20 to remove the terms "means of." '637 Patent File History, 41-42, 45-46. The assignee argued that the claims were allowable because "[w]ith the system architecture and methodology of the claimed invention, authentication resides within the apparatus and not in the user's or web host's system." '637 Patent File History, 47-49.

38. The petition to revive was granted, and a Notice of Allowance issued, allowing claims 1-24. The Notice of Allowance identified features of claim 1 of the '637 patent as the allowable features which rendered all claims allowable, despite those limitations of claim 1 not being included in claims 7-20. '637 Patent File History, 26. As shown in Section VI below, claims 7-20 are rendered obvious by prior art not considered by the Examiner.

VI. LEVEL OF ORDINARY SKILL IN THE PERTINENT ART

39. I understand there are multiple factors relevant to determining the level of ordinary skill in the pertinent art, including (1) the levels of education and

experience of persons working in the field at the time of the invention; (2) the sophistication of the technology; (3) the types of problems encountered in the field; and (4) the prior art solutions to those problems.

40. A person of ordinary skill in the art at and before the priority date of the '637 Patent (December 23, 2005) ("POSITA") would have had a bachelor's degree in electrical engineering, computer engineering, computer science, or a related subject, and one to two years of work experience in electronic device design, secure electronic communications, or a related field. Less experience may be necessary with additional education (e.g., a Master's degree), and likewise, less education may be necessary with additional work experience (e.g., 5-6 years).

VII. CLAIM CONSTRUCTION

41. It is my understanding that in order to properly evaluate the '637 Patent, the terms of the claims must first be interpreted. It is my understanding that the claims are to be construed according to the same claim construction standard that district courts use. Under the claim construction standard that district courts use (i.e., the so-called *Phillips* standard), claim terms are given their ordinary and customary meaning from the perspective of a person of ordinary skill in the art at the time of the invention. I have been informed that that the phrase "ordinary and customary meaning" in the so-called *Phillips* standard is often referred to as the "plain and ordinary meaning." I will use the phrase "plain and ordinary meaning" below.

42. In order to construe the Challenged Claims of the '637 Patent, I have reviewed the entirety of the '637 Patent along with portions of the prosecution history of the '637 Patent. Consistent with the '637 Patent disclosure, I have interpreted the terms in the Challenged Claims according to their plain and ordinary meaning as understood by a person of ordinary skill in the art, and considered any explicit definitions provided by the specification of the '637 Patent, where applicable.

43. In my opinion, all claim terms of the '637 Patent should be construed according to their plain and ordinary meaning and that no claim terms require explicit claim construction for the purposes of this proceeding. Below, I provide an explanation of the plain and ordinary meaning of the term “resident within” based on the disclosure of the '637 Patent and other contemporaneous prior art before the priority date of the '637 Patent.

VIII. DETAILED UNPATENTABILITY ANALYSIS

44. I have been asked to provide my opinion as to whether the Challenged Claims of the '637 Patent would have been obvious in view of the prior art. The discussion below provides a detailed analysis of how the prior art references I reviewed disclose, teach, or suggest the limitations of the Challenged Claims of the '637 Patent.

45. As part of my analysis, I have considered the scope and content of the prior art and any potential differences between the claimed subject matter and the prior art. I conducted my analysis as of the priority date of the '637 Patent: December 23, 2005. I have also considered the level of ordinary skill in the pertinent art as of that date.

46. I describe in detail below the scope and content of the prior art, as well as any differences between the claimed subject matter and the prior art, on an element-by-element basis for the Challenged Claims of the '637 Patent. This analysis supports my finding that the limitations of the Challenged Claims of the '637 Patent are disclosed in the prior art, or that the differences between the Challenged Claims of the '637 Patent and the prior art discussed herein are such that the subject matter as a whole would have been obvious at the time of the filing of the '637 Patent to a person having ordinary skill in the art to which the subject matter pertains.

47. As described in detail below, the claimed subject matter of the Challenged Claims would have been obvious in view of the teachings of the identified prior art references as well as the knowledge of a POSITA.

48. I will now describe, in the grounds below, on an element-by-element basis, how the prior art discloses or teaches all elements of the Challenged Claims.

Unless otherwise noted, all *italics* refers to claim language, and **bold** or ***bold italics*** is added for emphasis.

A. Ground 1: Claims 7-9 and 20 are rendered obvious over Rescorla in view of Mathiassen

49. It is my opinion that the combined teachings of Rescorla and Mathiassen disclose or render obvious, to a POSITA, the subject matter of each and every element of claims 7-9, 11-13, and 20 of the '637 Patent.

1. Overview of Rescorla

50. Rescorla describes the Secure Sockets Layer (SSL) and/or Transport Layer Security (TLS) protocol. At the time of the '637 Patent, the SSL/TLS protocol was one of the most commonly used protocols for authenticating websites and users, as explained by Rescorla:

The Secure Sockets Layer (SSL) is by far the most widely deployed security protocol in the world. Essentially every commercial Web browser and server supports secure Web transactions using SSL. When you buy online using “secure” Web pages (an estimated 20 billion dollars’ worth of such transactions will occur in 2000), you’re almost certainly using SSL.

Ex.1015, xvii.

51. Rescorla provides an overview of the SSL/TLS protocols. It was written to provide details of how to implement SSL/TLS protocols for authenticating online transactions in a wide variety of scenarios.

After reading this book, you should know most if not all of what you need to know in order to design secure systems using SSL/TLS. You'll know enough about SSL/TLS to understand what security features it can deliver and what it can't deliver. Further, you'll be familiar with the common design patterns for using SSL/TLS and be ready to apply them to new situations.

Ex.1015, xvii.

52. Chapters 2-3 of Rescorla provide an overview of SSL/TLS encryption.

Ex.1015, Chapters 2-3. Rescorla describes a number of embodiments of a handshake between a server, most commonly a website, and a client, most commonly a user.

Ex.1015, 58. In one common example, “[t]he server...sends...a certificate containing the server’s public key.” Ex.1015, 58. Then, “the client authenticates the server’s certificate and extracts the server’s public key.” Ex.1015, 58. The handshake protocols described in Rescorla may also be used to authenticate the user.

Ex.1015, 96.

SSL also provides a mechanism for cryptographically authenticating the client. This would be useful if a server wanted to restrict access to some services to only certain authorized clients and could use client authentication to do so. The idea here is that the client uses its private key to sign something, thus proving that it has possession of the private key corresponding to the certificate.

Ex.1015, 96-97.

53. Rescorla also contemplates biometrically authenticating a user.

Biometric authentication measures such as fingerprint identification and retinal scans are often used as secure access control measures. Although there is some doubt as to whether they can be securely implemented, they are nevertheless fairly widely used for access to secure environments and computers.

Ex.1015, 153.

54. A POSITA at the time would have been familiar with the SSL/TLS protocols described in Rescorla and would likely have encountered them in academic study or professional experience.

2. Overview of Mathiassen

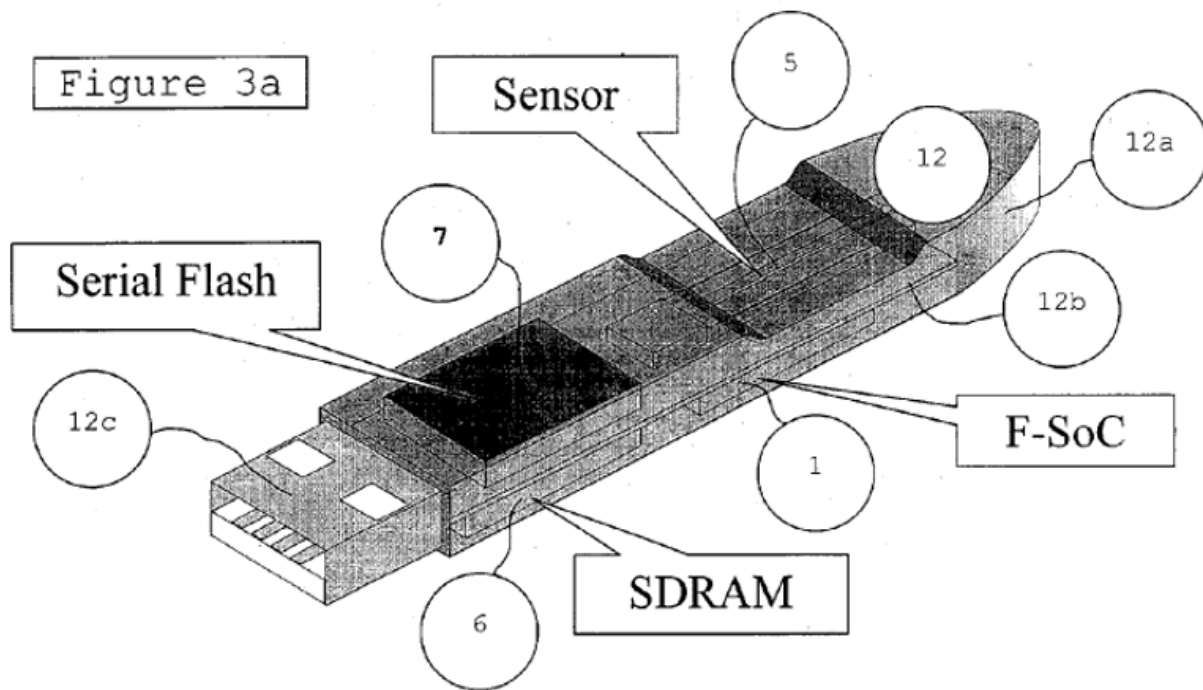
55. Mathiassen describes “[a] portable or embedded access device.”

Ex.1005, Abstract.

A portable or embedded access device is provided for being coupled to, and for allowing only authorized users access to, an access-limited apparatus, device, network or system, e.g. a computer terminal, an internet bank or a corporate or government intranet.

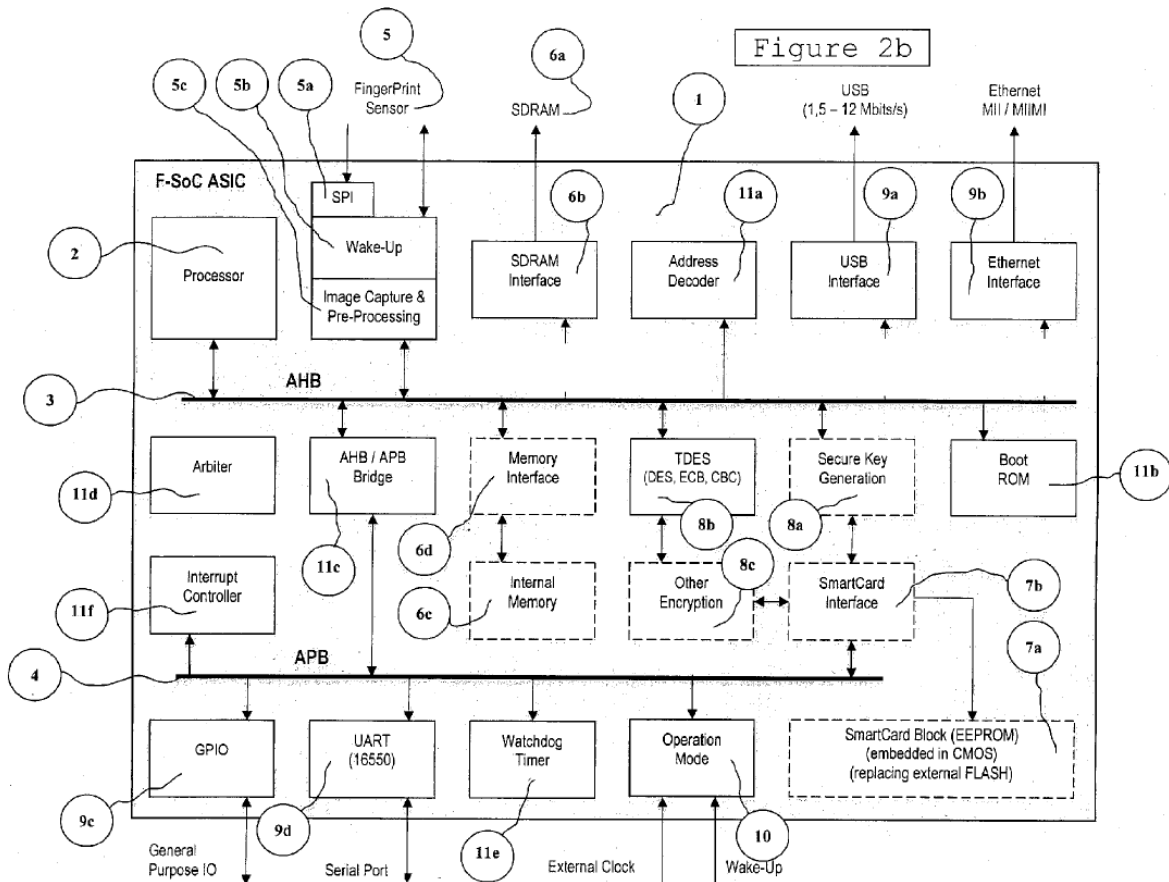
Ex.1005, Abstract.

Mathiassen’s portable device improves communication security by biometrically authenticating a user. Ex.1005, Abstract, [0047]. One embodiment of Mathiassen’s portable device is shown in Fig. 3a, below.



Ex.1005, Fig. 3a

The portable device includes a USB connector referred to as a USB mechanical interface 12C. Ex.1005, [0054]. The portable device also includes a fingerprint sensor 5. Ex.1005, [0048]. Mathiassen explains that the “biometrics sensor in the form of a fingerprint sensor (5) is coupled with a biometrics processor in the form of an integrated circuit—IC (1).” Ex.1005, [0047]-[0048]. The IC 1 of the portable device is illustrated in Fig. 2b, shown below. Ex.1005, [0048] (“Two versions of the IC are shown in FIGS. 2A and 2B.”).



Ex.1005, Fig. 2b

56. The IC 1 is used to obtain a fingerprint from a user and compare it to a master fingerprint stored in the memory of the portable device. Ex.1005, [0049]-[0050]. If the obtained fingerprint matches the master fingerprint, the user is authenticated and a secure output is generated and transmitted to an external system showing that the user was successfully biometrically authenticated. Ex.1005, [0050]-[0050], [0073]-[0083]. More specifically, Mathiassen describes administrative software stored in the non-volatile memory 7a of the portable device

that is configured for biometrically authenticating the user and cryptographically encapsulating¹ communications sent to external systems. Ex.1005, [0050].

57. To use Mathiassen's portable device for authenticating users for allowing access to secure locations or networks, the user must first be enrolled. Mathiassen explains this process.

The network administrator, or persons he has delegated authority to, will then enroll the user who will be the "owner" of the portable device (12 or 13).

...

Enrolment of a new user, by the administrator or a sub-administrator, will be performed on a terminal connected to the server (30). The administrator (or a sub-administrator) will perform the enrolment procedure of a new user, including capturing one or more fingerprints of the new user, and issuing a seed for the SKG algorithm to such new user. Eventually the administrator, or sub-administrator, will complete this procedure by counter-signing with his fingerprint. If the counter-signature fingerprint matches that of an authorized administrator, or sub-administrator, the enrolment procedure is deemed valid, and the personalized data downloaded to the portable device (12 or 13) connected to the terminal.

Ex.1005, [0061]-[0062].

¹ The term cryptographically encapsulating is a term sometimes used to describe encryption.

58. After the user is enrolled, she may use the portable device to biometrically authenticate herself. To do so, “[t]he user will insert the portable device (12 or 13) into the USB port.” Ex.1005, [0065]. After the user places her finger on the sensor 5, the portable device acquires a fingerprint image. Ex.1005, [0049], [0066]. The device then compares the acquired fingerprint image to a prestored fingerprint image, called a “master minutia.” Ex.1005, [0050], [0071]. If the acquired fingerprint matches the prestored fingerprint, the user is authenticated. Ex.1005, [0073]. (“If the matching is positive, the connection process will automatically continue.”). Mathiassen’s portable device then compiles and encrypts a message conveying that the user is authenticated, which may include a username and password of the user or other identification data, and transmits the message to a network or system in communication with the portable device. This process is explained by Mathiassen in detail.

Thereby the IC (1) is designed as a multi-purpose tool that can service a fingerprint sensor (5) in a stand-alone mode, but it can also communicate with external devices and networks (N) by bridging the biometrics from the sensor (5) to a non-biometrics representation into the network (N) and onto its server(s) (30). The IC (1) transforms the fingerprint, under prevailing secure communication rules, to a regular representation by e.g. password and User ID on a server (30).
Ex.1005, [0051].

59. In some embodiments, Mathiassen's encrypted message may also include an IP address stored in the portable device.

One result of the occurrence of a positive match could be that the release of an IP address from the SmartCard block (7C) or from the external SmartCard chip (7E).

Ex.1005, [0074].

60. Encryption of the contents of the message is also described as occurring after the user is biometrically authenticated.

When the central processor (2) has established a positive match between the access attempt minutiae and the resident master minutiae, the administrative software stored in the non-volatile memory (7, 7A or 7E) will calculate a secure key. The secure key will either be calculated by an algorithm executed on the central processor (2) (in case of FIG. 2A), or alternatively by a dedicated hardware block (8A) in case of FIG. 2B). The general algorithm will generate the secure key, and the particular key or password will be generated as a result of the seed being inputted to the algorithm. This seed will either be scrambled and stored in scrambled format in non-volatile memory (7) in the alternative of FIG. 2a, or be securely stored in a SmartCard environment (7A) in case of the alternative IC architecture outlined in FIG. 2b.

The secure key will be input to the encryption block (8,8B or 8C) for encryption of a message/communication. The message will comprise the following elements,

The device number of the USB Dongle or the PCMCIA card (12 or 13)
and the SKG key number (not the key itself) in non-encrypted format.

The IP address of the device (12 or 13) in encrypted format.

The secure key number (in encrypted format).

The user ID, in encrypted format.

Optionally PKI verification in encrypted format, in case of
authentication of the user holding the electronic certificate.

Other encrypted information required by the particular requirements for
secure communication, of the prevailing Intranet.

The calculated communication response is thus a result depending on
the above comparison of fingerprints. This message/communication is
encrypted to form a secure output in a predefined format and sequence
(e.g. handshake procedures) and transferred to an external unit, network
or system through one of the communication interfaces.

Ex.1005, [0076]-[0084].

3. Motivation to Combine Rescorla and Mathiassen

61. A person of skill in the art at the time tasked with designing a portable
electronic device for establishing secure communication between a user and a

website would have referenced Rescorla for information. Rescorla describes SSL protocols which was “by far the most widely deployed security protocol in the world” at the time, making it a clear choice regarding two-way secure communication. Ex.1015, xvii. In addition, a POSITA would have executed the client-side protocol of the SSL handshake described by Rescorla with a portable device that enables biometric authentication, such as the one described by Mathiassen, because “biometrics add valuable security.” Ex.1015, 153. Thus, a POSITA familiar with portable devices used for biometrically authenticating users for online transactions, like Mathiassen’s portable device, would have been motivated to implement the SSL/TLS handshake protocols described by Rescorla with a portable device to enable that portable device to perform SSL/TLS handshakes with online websites because SSL/TLS handshakes were the most common type of handshake for online transaction security at the time. *See* Ex.1015, xvii.

62. Rescorla provides an in-depth review of SSL protocols. SSL protocols were well known and widely adopted long before the ’637 patent. Ex.1015, xvii. SSL protocols were commonly used to secure two-way communication for many years prior to the priority date of the ’637 patent.

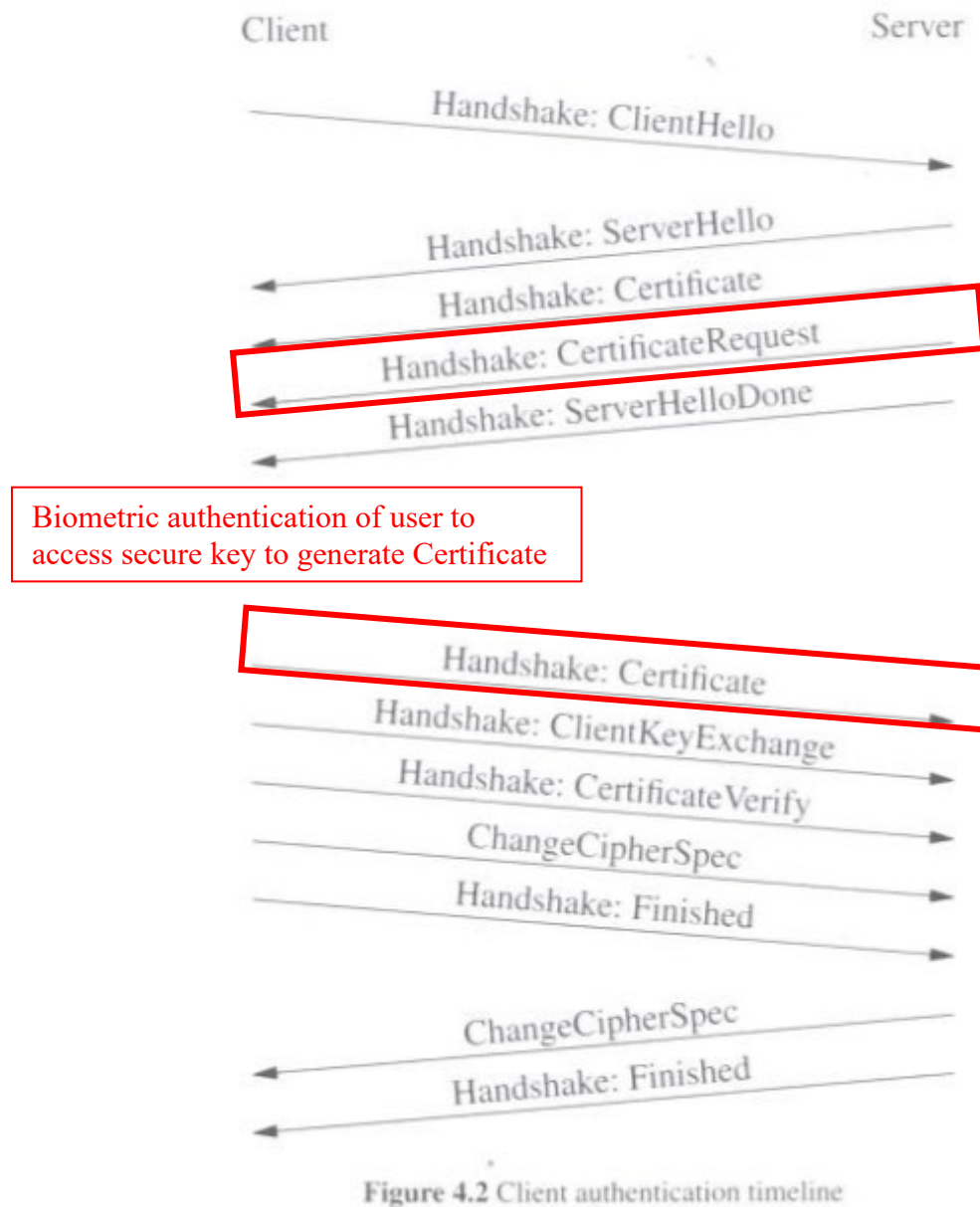
63. Rescorla explains how SSL protocols may be combined with biometric authentication. Ex.1015, 153. Rescorla explains that biometric authentication is not

suitable for generating an encryption key because “the characteristic being measured is not identical every time.” Ex.1015, 153. Due to this variation, which is caused by different portions of the finger being read by the sensor each time, “it’s difficult if not impossible to recreate the same encryption key from the biometric each time.” Ex.1015, 153. However, a POSITA would have understood, and Rescorla explains, that biometrics may be used in conjunction with SSL protocols if they are used to access resources for secure key or certificate generation, not to generate that information itself. For example, Rescorla explains that biometric authentication may be used to gain access to the encryption key “stored in trusted tamper-resistant hardware.” Ex.1015, 153.

64. Mathiassen explains using biometric authentication in exactly the same way as Rescorla. Ex.1005, [0050] (“If a positive match is established, the chip may proceed with generating a secure key...based on a seed pre-stored in the non-volatile memory.”). Thus, claims 7-20 of the ’637 patent merely recite well-known SSL protocol steps executed by a portable device incorporating biometric authentication exactly as Rescorla anticipates.

65. A POSITA would have easily recognized that the combination of Rescorla and Mathiassen simply implements the steps of biometric authentication described by Mathiassen after the client receives the Handshake: CertificateRequest

message and prior to sending the Handshake: Certificate message, as shown in Rescorla, Figure 4.2, illustrated below. *See* Ex.1015, 98.



Ex.1015, Fig. 4.2 (annotated)

66. A POSITA at the time would not have considered any of these concepts as new at the priority date of the '637 patent. In fact, the '637 patent itself

acknowledges that a variety of handshake protocols had already been developed. [cite]. Those handshake protocols included transmitting various requests and acknowledgments between the parties using any number of cryptographic techniques. Portable devices with processing capabilities for authentication were also well known prior to the '637 patent. Ex.1005, (...); Ex.1006; (...).

67. Rescorla is similar to the '637 patent. The '637 patent relates to increasing online transaction security by biometrically authenticating a user and authenticating a website. '637 Patent, Abstract. Rescorla is within the same field of endeavor because it pertains to handshake protocols to authenticate both sides of an online transaction. Ex.1015, 96 (“authenticat[ing]...the server” and “cryptographically authenticating the client.”). Rescorla indicates that its techniques are highly versatile and applicable to a wide variety of online transaction environments.

Although its most common use is for securing Web traffic, SSL is actually **quite a general protocol** suitable for securing a **wide variety** of kinds of traffic.

...

These techniques can often be applied to a new application protocol **with minimal modification**. In essence, we've developed a set of design patterns for securing protocols. Much of the work of securing a system is in recognizing which pattern most closely matches the system you're working with and then using the appropriate techniques.

Ex.1015, xvii.

68. Given the admitted versality and ready modification of the SSL/TLS protocols, a POSITA would have been encouraged to implement those protocols in a portable device, such as Mathiassen's portable device. A POSITA would have been further encouraged based on Rescorla's specific contemplation of using SSL/TLS protocols with biometric authentication. Ex.1015, 153 ("Biometric authentication measures such as fingerprint identification and retinal scans are often used as secure access control measures."). Therefore, Rescorla is in the same technological field of improving online transaction security by biometrically authenticating a user and authenticating a website. Rescorla is also relevant to the problem the inventor sought to solve, namely performing mutual authentication of a user and a website. Ex.1015, 96.

69. Mathiassen also describes a comparable technology to the '637 patent. The '637 patent describes using a portable device for biometrically authenticating users. '637 Patent, Abstract. Mathiassen is within the same field of "allowing only authorized users access to" a network through biometric authentication. Ex.1005, Abstract. Thus, Mathiassen is in a similar field of improving online transaction security by biometric authentication and is also relevant to the problem the inventor allegedly solved, namely implementing biometric authentication in a portable device for improving online transaction security. Ex.1005, Abstract.

70. A POSITA would have naturally implemented the handshake protocols described in Rescorla to be performed in Mathiassen's portable device for reasons provided by both references themselves. Mathiassen says that using biometrics is a more secure way of authenticating the user than passwords because "passwords...may intentionally be passed away to a third person, or unintentionally and illegally acquired by such third person." Ex.1005, [0004]. Similarly, Mathiassen explains that "there is a general consensus that biometrics access control is far more secure, and convenient, than password-based or token-based access control." Ex.1005, [0015]. However, the adoption of biometric authentication was inhibited by issues of interoperability and a lack of a uniform standard. Ex.1005, [0012]. SSL, as described Rescorla, is both highly adaptable, and widely adopted and would address these issues. Ex.1015, xvii. A POSITA would have recognized the advantages of biometric authentication and would have implemented Mathiassen's teachings regarding biometric authentication by a portable device to provide this increased level of security with Rescorla's SSL protocols for increased interoperability.

71. Mathiassen's implementation of biometric authentication entirely within a portable device would also have motivated a POSITA to adopt Mathiassen's teachings to implement handshake protocols described in Rescorla. Mathiassen's portable device includes all the necessary software and processing capabilities to

perform biometric authentication. As a result, “the supplier of the network system architecture” does not have to modify their system at all to be compatible with Mathiassen’s device. Ex.1005, [0048]. More specifically, Mathiassen explains that the supplier does not have to “make[] any decision on which biometrics standard will evolve in the future” because “the biometrics processor can transform the biometrics from the sensor (B) to general communication security measures in a network.” Ex.1005, [0048]. This results in increased security, convenience, and adoptability of biometric authentication. Ex.1005, [0048].

72. In addition, because Mathiassen’s portable device is portable and universal, it offers multiple additional advantages. For example, a user of Mathiassen’s portable device would use biometric authentication with any number of standard devices (i.e., devices with a standard USB port) for authentication. The user would not need to purchase specialized equipment for biometric authentication. Mathiassen’s device allows biometric authentication of a user even using public terminals. For example, Mathiassen describes using its device for biometric authentication at a computer in “an Internet Café or a Business Center at a hotel.” Ex.1005, [0065]. Similarly, Mathiassen’s portable device is configured to perform “handshake sequences according to the rules of secure communication of the device, network or system (N)” with which it communicates, but is not limited to any specific protocol. Ex.1005, [0095].

73. The combination of Rescorla and Mathiassen would have been a straightforward combination of commonly known technology at the time. Specifically, the device described in the '637 patent, as well as the steps of the handshake between the device and an external server is a rudimentary combination of SSL/TLS handshake protocols, as taught by Rescorla, with a portable device that biometrically authenticates a user, as taught by Mathiassen. The techniques required to successfully make this combination would have been common knowledge to a POSITA at the time because implementing SSL handshake protocols “to a new application protocol” was done “with minimal modification,” as taught by Rescorla. Ex.1015, xvii. The combination would result predictably in a portable device used both for biometrically authenticating a user and for cryptographically authenticating a website.

74. A POSITA would have easily recognized the feasibility of such a combination. Both Rescorla and Mathiassen describe handshake protocols. Mathiassen explains that the message generated by its portable device as a result of successful biometrics could be implemented “in a predefined format and sequence (e.g., **handshake procedures**).” Ex.1005, [0084]. Rescorla’s entire purpose is to provide implementation details of handshake procedures, specifically SSL/TLS handshake protocols. Ex.1015, xvii. Mathiassen explicitly anticipates modifying the handshake sequences implemented by the portable device “according to the rules of

secure communication of the...network or system (N).” Ex.1015, [0095]. Rescorla discloses that “[t]he *Secure Sockets Layer* (SSL) is by far the most widely deployed security protocol in the world.” Ex.1015, xvii. One of Mathiassen’s explicitly stated goals is to promote interoperability with a wide variety of standard systems and protocols. Ex.1005, [0006] (on overcoming the issue of “gain[ing] wide public acceptance.”).

75. Similarly, Rescorla explains that modifying the SSL protocols to fit any suitable application would have involved routine skill in the art:

These techniques can often be applied to a new application protocol with minimal modification. In essence, we’ve developed a set of design patterns for securing protocols. Much of the work of securing a system is in **recognizing which pattern most closely matches the system** you’re working with and then **using the appropriate technique**.

Ex.1015, xvii.

76. Accordingly, a POSITA would have easily understood that Rescorla’s handshake protocols would be combined with Mathiassen’s portable device for all the reasons listed above.

4. Analysis

a) Claim 7

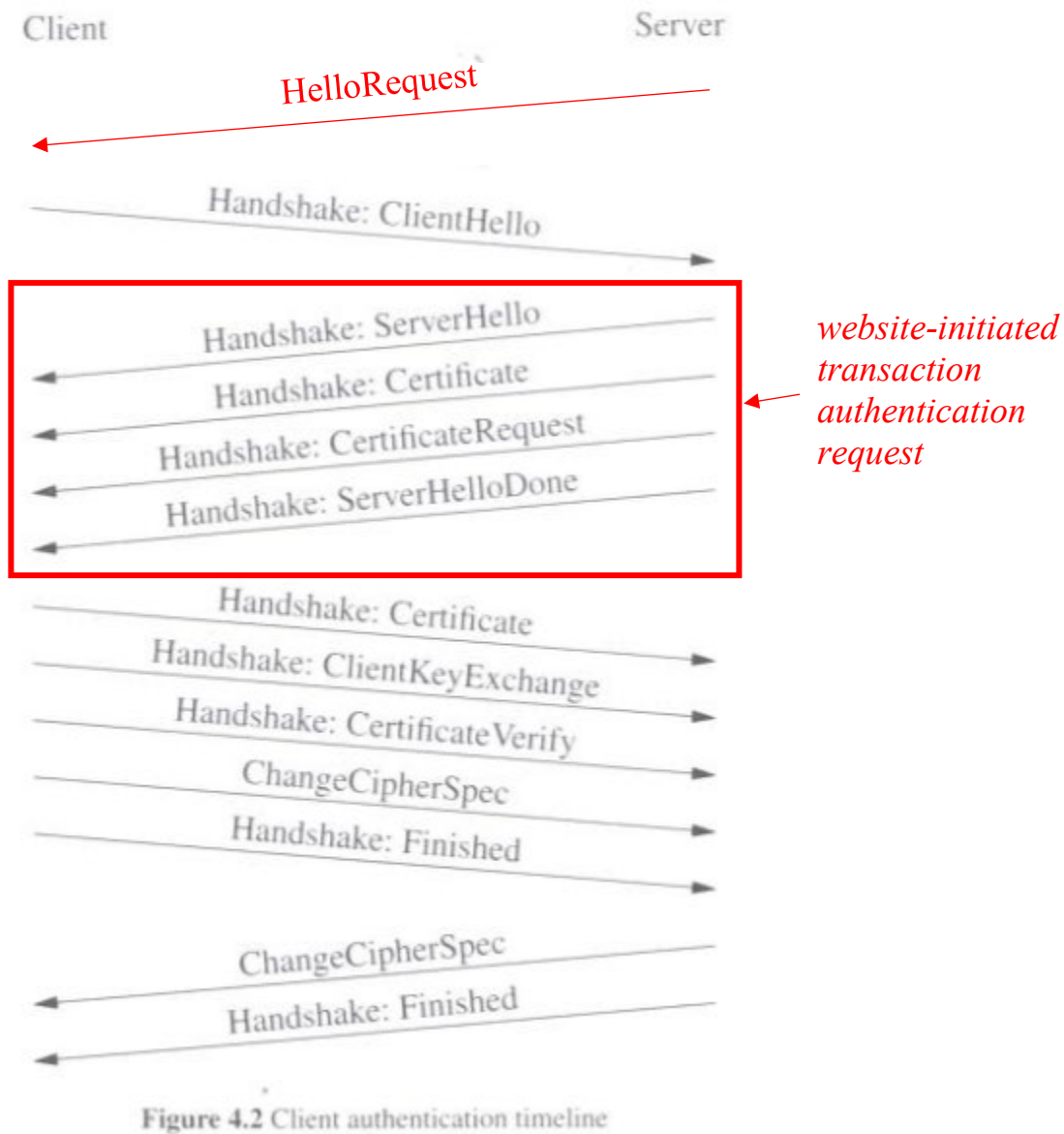
[7.0] A method for securely processing and responding to a website-initiated transaction authentication request, comprising the steps of:

77. I have been informed that the preamble of claim 7 is not limiting. To the extent the preamble is limiting, Rescorla describes a *method for securely processing and responding to a website-initiated transaction authentication request*.

78. As an initial matter, it is important to understand what is meant by a *website-initiated transaction authentication request*. According to the '637 patent, a website may initiate a transaction, but even when the website initiates the transaction, it always does so in response to some activity from the user. For example, the user first navigates to the websites and attempts to make a transaction or perform some other activity. The '637 patent explains that the website first “detect[s] that the customer is attempting to use the website.” '637 Patent, 5:57-6:2. The website then informs the user that the user must be authenticated. This was and is commonly done when websites request that a user, for example, logs into an account. The '637 patent explains that user's activity “caus[es] the website to initiate a request for authentication.” '637 Patent, 5:57-6:2. Thus, when the '637 patent refers to a website-initiated transaction, it does not necessarily mean that the website

sends the first request to the user. Rather, the website initiates authentication in response to the user's attempt to access a resource.

79. Rescorla describes this same scenario. Specifically, Rescorla describes that after a user accesses a website and the website's server "determines that the resource being requested requires client authentication," the server sends a HelloRequest message to the client. Ex.1015, 326. "The HelloRequest causes the client to initiate a new handshake." Ex.1015, 326. The handshake protocols begin with the client sending a ClientHello to the website. Ex.1015, 60 ("Step 1"), Fig. 3.2, Fig. 4.2. After receiving the ClientHello, the website compiles and sends multiple messages, including the ServerHello, Certificate, and ServerHelloDone messages. Ex.1015, 60 ("Step 2"), Fig. 4.2. These messages from the server to the client are illustrated in Fig. 4.2.



Ex.1015, Fig. 4.2 (annotated)

80. Even though the first message shown in Fig. 4.2 is the “ClientHello” message from the client, the HelloRequest message, which is not pictured but added above, is described in Rescorla. It would be sent before the ClientHello message, and as explained above, initiates the authentication process. Ex.1015, 134. The

ServerHello, Certificate, CertificateRequest, and ServerHelloDone messages disclose a *transaction authentication request* because they provide the information necessary to authenticate the website and the client. All these messages are *receiv[ed]* by the client. The Certificate message is *for cryptographically confirming the web site's identity*. See Section VIII.A.4.a (limitation [7.1.2]). The CertificateRequest message is *for requesting said apparatus provide a corroborating response...to prove that said response originates from a legitimate customer*. See Section VIII.A.4.a (limitations [7.1.3], [7.1.4]). Because this handshake protocol is initiated by the website first sending the HelloRequest message to the client, this *transaction authentication request* is *website-initiated*.

81. Rescorla similarly discloses securely processing and responding to the ServerHello, Certificate, CertificateRequest, and ServerHelloDone messages (*website-initiated transaction authentication request*) received from the server.

82. Regarding the Certificate message, Rescorla explains how the client processes and responds. Specifically, “[t]he client verifies the server’s certificate and extracts the server’s public key. The client then generates a random secret string called the *pre_master_secret* and encrypts it using the server’s public key. It sends the encrypted *pre_master_secret* to the server.” Ex.1015, 58. Extracting the public key and generating and encrypting the *pre_master_secret* discloses *securely processing* the Certificate message which is part of the *website-initiated transaction*

authentication request because extracting a public key is performed to verify that the sender encrypting the response similarly secures the communication. Ex.1015, 58, 9 (“[T]he receiver uses your public key to *verify* your signature.”). Sending the encrypted `pre_master_secret` discloses *securely...responding to* the Certificate message, which is part of the *website-initiated transaction authentication request*, because it is sent in response to the Certificate message. Ex.1015, 58.

83. The client also *securely process[es] and respond[s]* to the CertificateRequest message which is part of the *website-initiated transaction authentication request* by providing its own certificate via the Certificate and CertificateVerify messages. *See* Ex.1015, Fig. 4.2.

84. Thus, Rescorla describes a method in which the server sends the ServerHello, Certificate, CertificateRequest, and ServerHelloDone messages (*a website-initiated transaction authentication request*) and, after receiving these messages, the client extracts public keys, and generates, encrypts, and sends a `pre_master_secret` in response (*securely processing and responding*) to the server.

[7.1.1] (1) receiving in a customer authentication apparatus said website-initiated transaction authentication message

85. Rescorla and Mathiassen describe *receiving in a customer authentication apparatus said website-initiated transaction authentication message*.

86. As explained above at [7.0], Rescorla explains that each of the ServerHello, Certificate, CertificateRequest, and ServerHelloDone messages are received by the client.

87. Rescorla explains that the ServerHello, Certificate, CertificateRequest, and ServerHelloDone messages are received by the client (a portable device such as the one described by Mathiassen in the proposed combination), as illustrated in Figure 4.2 below.

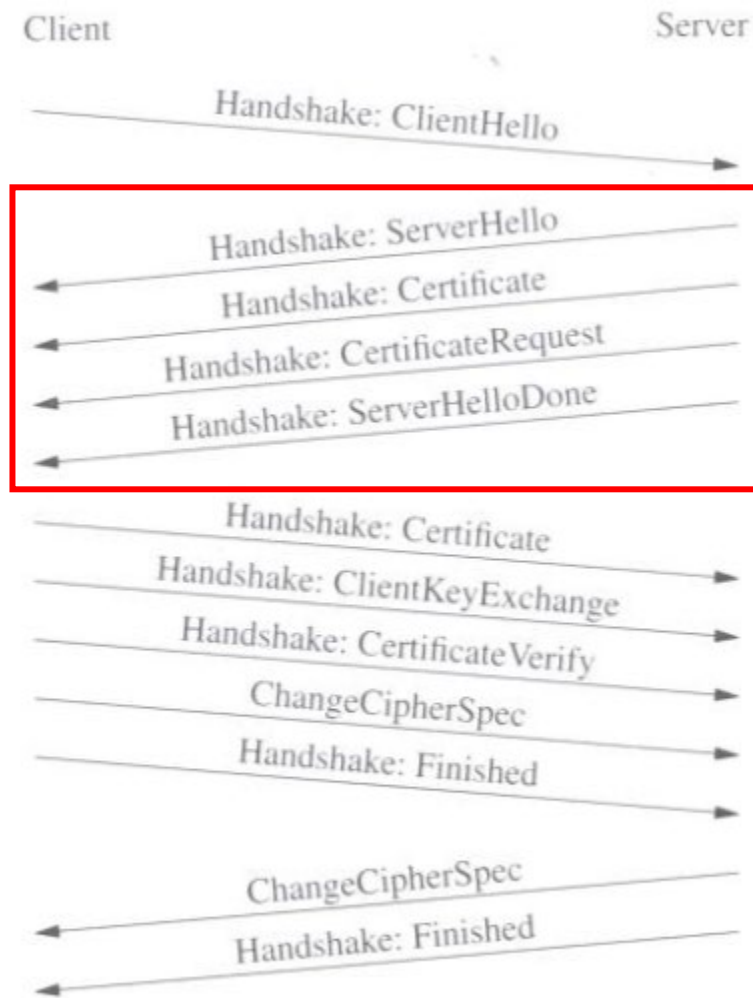


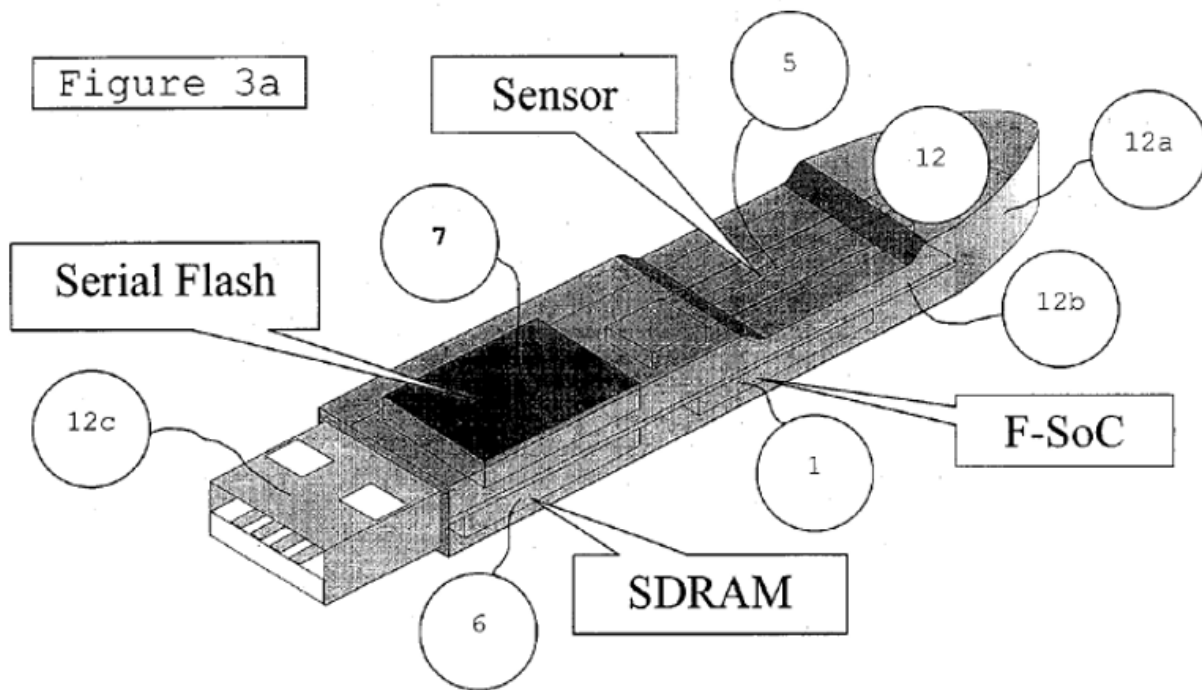
Figure 4.2 Client authentication timeline

Ex.1015, Fig. 4.2 (annotated)

88. The client receives the ServerHello, Certificate, CertificateRequest, and ServerHelloDone messages (*website-initiated transaction authentication message*).

89. It would have been obvious to a POSITA at the time that the functions performed by the client described in Rescorla would be performed by a portable device, such as the device described in Mathiassen. More specifically, as described above in Section VIII.A.3, a POSITA would have been motivated, based on the

teachings of Mathiassen, to implement the handshake protocols described in Rescorla on a portable device. Mathiassen's portable device is a *customer authentication apparatus* because it is used to biometrically authenticate a user, which in the context of an online transaction as described by Rescorla and Mathiassen, is also commonly a customer. Specifically, Mathiassen describes a "portable or embedded access device," which is often referred to as a "portable device." Ex.1005, Abstract. Mathiassen's portable device is depicted in Fig. 3a, below.



Ex.1005, Fig. 3a

90. Mathiassen's portable device includes a "fingerprint sensor (5)." Ex.1005, [0048]. Mathiassen's portable device authenticates a user based on

readings from the sensor. Ex.1005, [0048], [0050] (“fingerprint representations...are compared...with master fingerprint representations” to identify “a positive match.”). Further, as described above in Section VIII.A.3, a POSITA would have been motivated to implement the SSL/TLS handshake protocols described by Rescorla in Mathiassen’s portable device.

91. Mathiassen doesn’t limit its portable device to specific handshake protocols or sequences. Instead, Mathiassen explains that it could implement the particular handshake protocols or sequences of the external system it is intended to communicate with. For example, in describing the administrative software of the portable device, Mathiassen describes “tailoring handshake sequences.” Ex.1005, [0095].

tailoring handshake sequences according to the rules of secure communication **of the device, network or system (N)**. The pre-loaded subset of the administrative software is preferably also adapted to perform sequencing of the operation of the respective functionality blocks of the chip/IC (1) in order to produce secured output data which is **suitable for transmission in the targeted network (C) and for processing by receiving units connected to the network (C)**. Ex.1005, [0095].

92. Given this wide applicability of Mathiassen’s portable device to implement any suitable handshake protocols, a POSITA would have at the very least

expected it could implement SSL handshake protocols because they are “the most widely deployed security protocol in the world.” Ex.1015, xvii. Therefore, a POSITA would have readily understood that Mathiassen’s portable device would perform SSL handshake sequences as explained by Rescorla.

93. Therefore, Rescorla and Mathiassen describe receiving the ServerHello, Certificate, CertificateRequest, and ServerHelloDone messages (*website-initiated transaction authentication message*) by a portable device (*customer authentication apparatus*).

[7.1.2] for cryptographically confirming the web site’s identity and

94. Rescorla and Mathiassen describe *cryptographically confirming the web site’s identity*.

95. Rescorla describes SSL handshake procedures which are used for cryptographically verifying the validity of a website (*cryptographically confirming the web site’s identity*). This is accomplished when the server sends the Certificate message shown in Fig. 4.2, below.

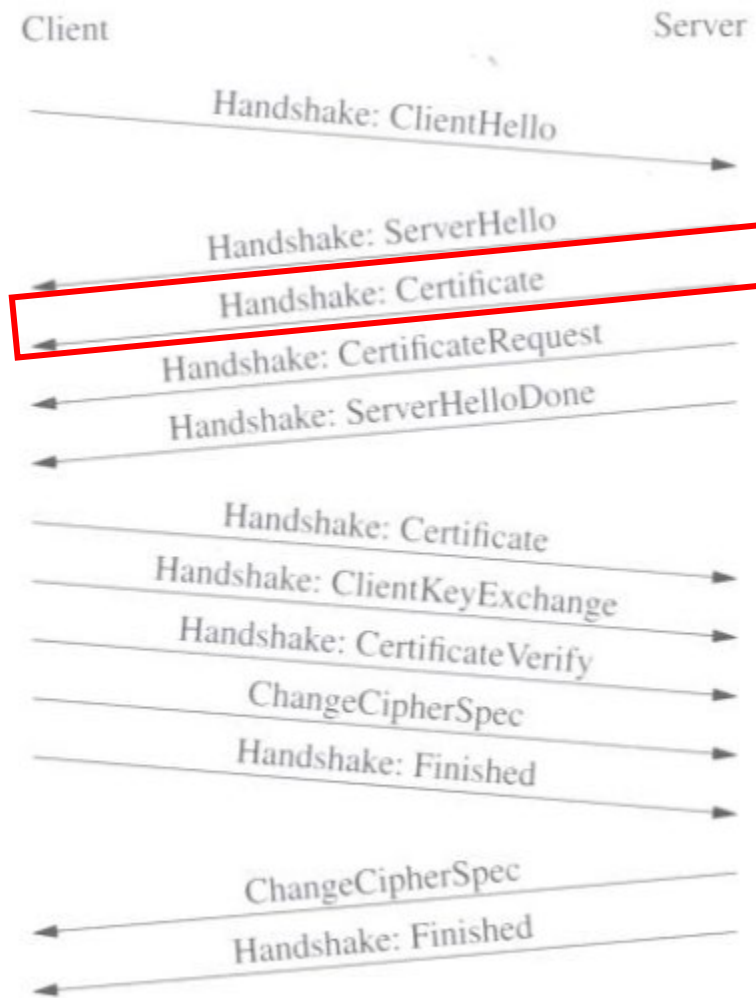


Figure 4.2 Client authentication timeline

Ex.1015, Fig. 4.2 (annotated)

96. Rescorla’s server’s “certificate contain[s] the server’s public key [and] provides the server’s identity for authentication purposes.” Ex.1015, 58. The server “sends its certificate in the Certificate message.” Ex.1015, 60. Rescorla explains verifying the server’s identity based on the received certificate as follows:

As we discussed earlier, **the certificate presented by the server must contain an identity** which is somehow connected to the expected

identity of the server. The expected identity can't be carried over the wire, but must **already be known to the client at the time the connection is initiated.**

In most cases, when a client wants to connect to an SSL server, the destination is specified by a DNS domain name (see [Mockapetris 1987a, Mockapetris1987bJ) such as foo.example.com or by a *Uniform Resource Locator* (URL) [Berners-Lee 1994] that contains a domain name. Thus, **the expected identity of the server is the domain name and that must match the identity in the certificate.**

Ex.1015, 156.

97. Rescorla explains that the Certificate message from the server to the client, which is part of the *website-initiated transaction authentication message* is for *cryptographically confirming the web site's identity*.

98. A POSITA would have used a portable device, such as the device described in Mathiassen, to implement website authentication. Mathiassen describes using its portable device for PKI (public key infrastructure) verification. Ex.1005, [0082]. For example, Mathiassen explains accessing a “PKI system with electronic certificates.” Ex.1005, [0012]; *see also* [0050] (describing “PKI biometrics verification and hand-shake sequences”). The use of “electronic certificates” such as certificates used in PKI verification was suitable for mutual authentication of two parties (i.e., a website and a user). Mathiassen also specifically describes “PKI

biometrics verification and hand-shake sequences” and “PKI keys.” Ex.1005, [0050]. PKI verification was a commonly used method of exchanging digital certificates to confirm users’ identities such as the certificate exchange protocols described by Rescorla. *See* Ex.1015, Fig. 4.2.

99. In addition, authenticating a website’s identity with a portable device was well within the processing capabilities of the time. For example, Ryan describes using a portable device, called a “smart fob” to prevent “viruses, worm, spam and Internet ‘phishing’ fraud.” Ex.1006, [0249]. An internet phishing fraud is an attack where a fraudulent website is created to mimic a legitimate website in order to get sensitive information from an unsuspecting user (e.g., usernames and passwords, credit card info, etc.). A POSITA would have understood that preventing phishing fraud using a portable device as described in Ryan included at least authenticating a website to ensure that it is not fraudulent. Livowsky similarly describes a portable device, referred to as “a personal authentication token” for “mutually authenticat[ing] senders and/or recipients of electronic transactions.” Ex.1021, Abstract, [0033]. It was, therefore, well understood at the time that a portable device could authenticate a website.

100. Therefore, Rescorla and Mathiassen describe a portable device that verifies an encrypted certificate for authentication (*cryptographically confirming the web site’s identity*).

[7.1.3] for requesting said apparatus provide a corroborating response including a biometric authentication of an enrolled customer and

101. Rescorla and Mathiassen describe *requesting said apparatus provide a corroborating response including a biometric authentication of an enrolled customer*.

102. Rescorla explains that the CertificateRequest message *requests...a corroborating response* (the Certificate and CertificateVerify messages) from the client to authenticate the client, as shown in Fig. 4.2 below.

103. Rescorla explains an embodiment for “cryptographically authenticating the client” in Fig. 4.2. Ex.1015, 96, 98.



Figure 4.2 Client authentication timeline

Ex.1015, Fig. 4.2 (annotated)

104. The CertificateRequest message is sent with the Certificate message and prior to the ServerHelloDone message. In this case, the ServerHelloDone message signifies the end of the contents of the set of messages sent from the server to the client when a handshake procedure is initiated. Specifically, “the ServerHelloDone is needed” to signify that “no...other messages will be” sent. Ex.1015, 60.

105. Rescorla explains that “[c]lient authentication is initiated by the server sending a CertificateRequest message to the client.” Ex.1015, 97. “The client responds by sending a Certificate message...and a CertificateVerify message.” Ex.1015, 97. These response messages are also shown in Fig. 4.2.

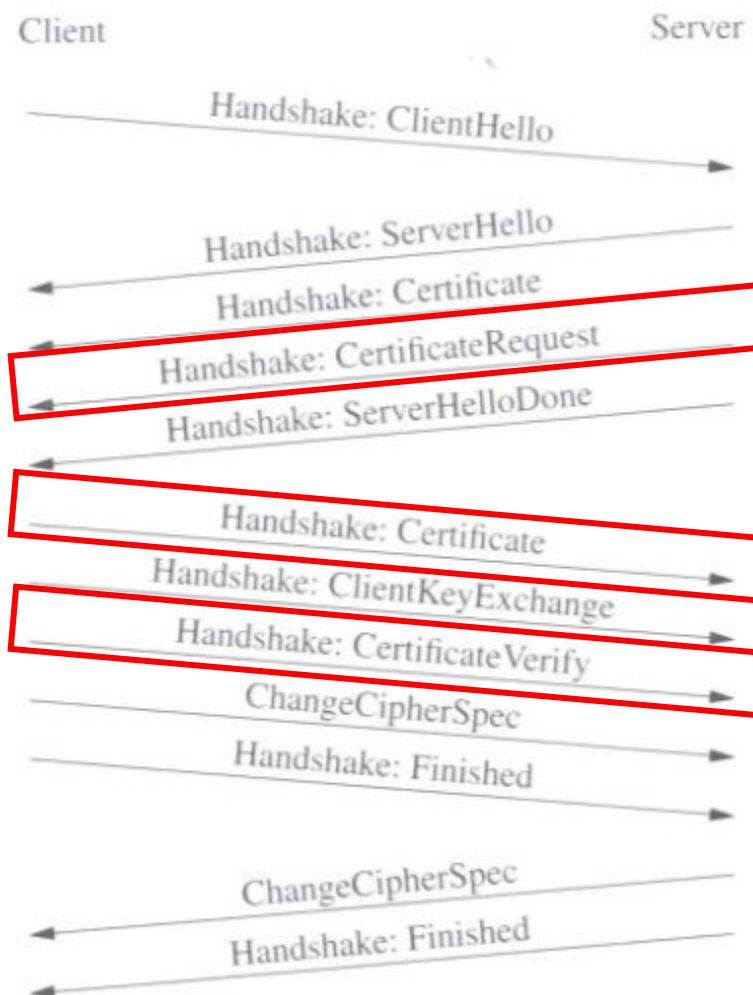


Figure 4.2 Client authentication timeline

Ex.1015, Fig. 4.2 (annotated)

106. Thus, the Certificate Request message of the “Step 2” set of messages *requests a corroborating response* in the form of the Certificate and/or CertificateVerify messages.

107. The Certificate and CertificateVerify messages are used for *authentication of an enrolled customer*.

The CertificateVerify does all the actual work of client authentication. It contains a digest of the handshake messages signed by the client’s private key (the one that corresponds to the certificate in the client’s Certificatemessage). This is what the digitally-signed operator means. Because **only the holder of the private key corresponding to the certificate could sign this message, the server can conclude that the entity named in the certificate is connecting.** Ex.1015, 111; *see also* 108.

The idea here is that **the client uses its private key to sign something, thus proving that it has possession of the private key corresponding to the certificate.** Client authentication is initiated by the server sending a CertificateRequest message to the client. The client responds by sending a Certificate message (the same message that the server uses to transmit its certificate) and a CertificateVerify message. The CertificateVerify message is **a string signed with the private key associated with the certificate that it transmitted.** Ex.1015, 97.

108. A POSITA would have configured the system such that the Certificate and CertificateVerify messages are sent by the portable device as a result of biometric authentication. For example, Rescorla contemplates the use of biometrics in conjunction with its system: “[b]iometric authentication measures such as fingerprint identification and retinal scans are often used as secure access control measures.” Ex.1015, 153. A POSITA would not have been discouraged by the limitations of biometric authentication mentioned in Rescorla.

However, biometrics are singularly inappropriate for protecting private keying material. The measures we’ve talked about so far all depend on encrypting the private key based on some piece of data the user inputs. This piece of data must be identical each time because it is used to create an encryption key and encryption algorithms are specifically designed so that tiny errors in the key cause large errors in decryption.

However, biometrics cannot be easily used for this purpose because the characteristic being measured is not identical every time. Therefore, it’s difficult if not impossible to recreate the same encryption key from the biometric each time. Biometric systems therefore have to keep the key in the clear and **simply use the biometric to control access**. This is inferior if the device containing the key is ever compromised, because the attacker doesn’t need to decrypt the key. If the key is stored on disk somewhere, this is catastrophic.

There are two exceptions to this general rule. First, **if the key is stored in trusted tamper-resistant hardware, then a biometric is safe** because the hardware will zeroize the key before allowing it to be recovered. This requires having a lot of faith in your tamper resistance! Second, if a passphrase is used in conjunction with a biometric, then the key can still be encrypted using the passphrase and biometrics can be used as a secondary piece of **access control. In this case, biometrics add valuable security.**

Ex.1015, 153.

109. Mathiassen teaches using a biometric to authenticate the user in exactly the same way Rescorla encourages, namely to control access, and storing the key in a secure memory. For example, Mathiassen explains that the “second memory interface block...is typically used for storing...secret information like seed and key number(s) for the encryption” and that the “secure key (SKG)” is generated “based on a seed pre-stored in the non-volatile memory.” Ex.1005, [0050]; *see also* [0076]. In addition, Mathiassen describes capturing a fingerprint and comparing it “with master fingerprint representations” to biometrically authenticate the user and “control access” to encryption software and keys. Ex.1005, [0050] (“[a]ccess to...extended encryption will be given to the user **pending a positive match** of his fingerprint **with an authorized fingerprint.**” Ex.1005, [0050]. Thus, Rescorla and Mathiassen disclose or render obvious *a biometric authentication of an enrolled customer.*

110. In the combination of Rescorla and Mathiassen, the corroborating response to the CertificateRequest described at Step 2 of Rescorla would include a biometric authentication of the user. For example, Mathiassen describes the contents of the message sent from its portable device to the external server indicating user authentication. Ex.1005, [0078]-[0083]. This response includes, among other things, “[t]he secure key number,” and “PKI verification in encrypted format.” Ex.1005, [0080], [0083]. This message is generated only “if a positive match of the captured fingerprint with the fingerprint representation...is obtained.” Ex.1005, [0085]. The receiving server then “retrieve[s] the particular seed issued to the user, during enrolment” and inputs it into the “secure key generation algorithm SKG on the server” to verify the user. Ex.1005, [0087].

111. A POSITA would have been motivated to use biometrics to control access to the secure key using Mathiassen’s portable device and then use the key to authenticate the user to the server, for the reasons presented above in Section VIII.A.4. Rescorla expressly contemplates the use of biometrics in this way.

112. Therefore, Rescorla and Mathiassen describe sending Certificate and CertificateVerify messages (*provid[ing] a corroborating response*) from a portable device (*said apparatus*) including biometric authentication of the user of the device (*including a biometric authentication of an enrolled customer*).

[7.1.4] further including a cryptographic encapsulation of said response in order to prove that said response originates from a legitimate customer;

113. Rescorla and Mathiassen describe *further including a cryptographic encapsulation of said response in order to prove that said response originates from a legitimate customer.*

114. Mathiassen's response, referred to as a "message/communication," indicates biometric authentication (Ex.1005, [0077]-[0083]) and is cryptographically encapsulated. Regarding cryptographic encapsulation of the response or message/communication, Mathiassen explains as follows.

When the central processor (2) has established a positive match between the access attempt minutiae and the resident master minutiae, the administrative software stored in the non-volatile memory (7, 7A or 7E) will **calculate a secure key**. The secure key will either be calculated by an algorithm executed on the central processor (2) (in case of FIG. 2A), or alternatively by a dedicated hardware block (8A) in case of FIG. 2B). The general algorithm will generate the secure key, and the particular key or password will be generated as a result of the seed being inputted to the algorithm. This seed will either be scrambled and stored in scrambled format in non-volatile memory (7) in the alternative of FIG. 2a, or be securely stored in a SmartCard environment (7A) in case of the alternative IC architecture outlined in FIG. 2b.

The secure key will be input to the encryption block (8,8B or 8C) for encryption of a message/communication.

Ex.1005, [0076]-[0077].

115. As explained at [7.1.3], it would have been obvious for the Certificate and/or CertificateVerify messages of Rescorla to be generated in response to biometric authentication of the user. Rescorla further explains that the Certificate and/or CertificateVerify messages are used to verify the identity of the client. *See* VIII.A.4.a, [7.1.3]. Similarly, Mathiassen explains that its message/communication is used by the server to verify the identity of the user.

116. Therefore, a POSITA would have configured the portable device of the combination to cryptographically encapsulate the Certificate and/or CertificateVerify messages, as Mathiassen explains cryptographically encapsulating the message/communication. *See* Ex.1005, [0077]-[0083] (Mathiassen teaching that the response indicating biometric authentication of the user is cryptographically encapsulated).

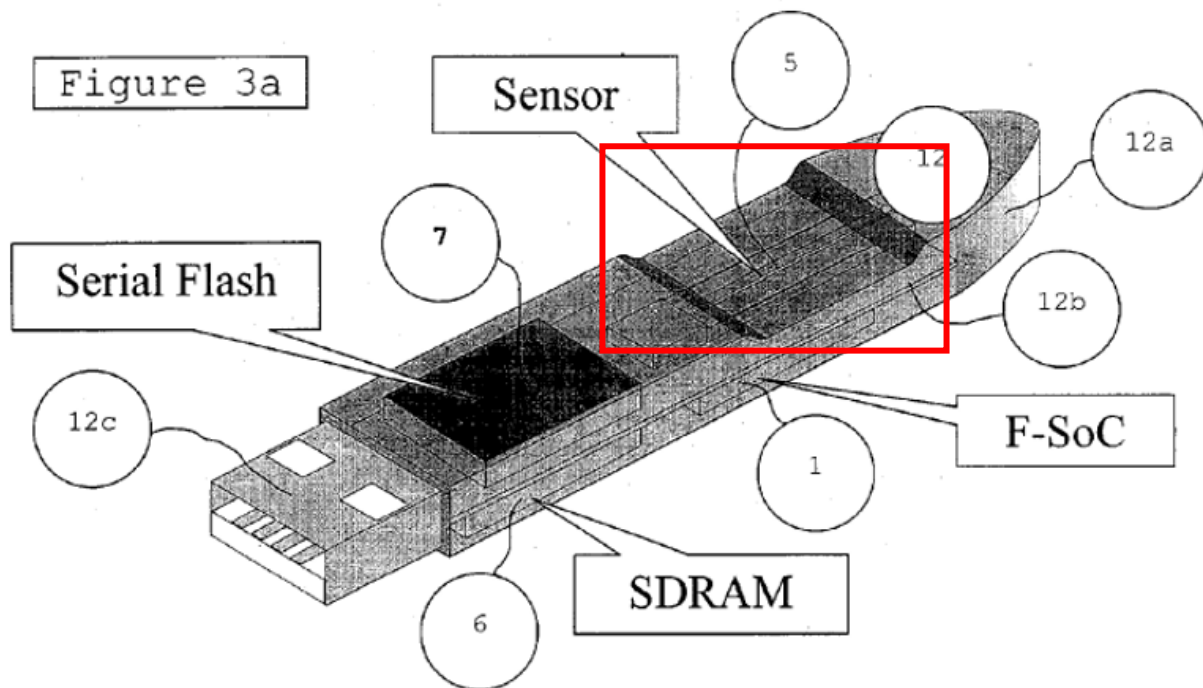
117. Therefore, Rescorla and Mathiassen describe encrypting the Certificate and/or CertificateVerify messages (*including a cryptographic encapsulation of said response*) to verify the identity of the user (*in order to prove that said response originates from a legitimate customer*).

[7.2] (2) biometrically authenticating said customer by said customer authentication apparatus prior to transmitting said response to said request;

118. Rescorla and Mathiassen describe *biometrically authenticating said customer by said customer authentication apparatus prior to transmitting said response to said request*.

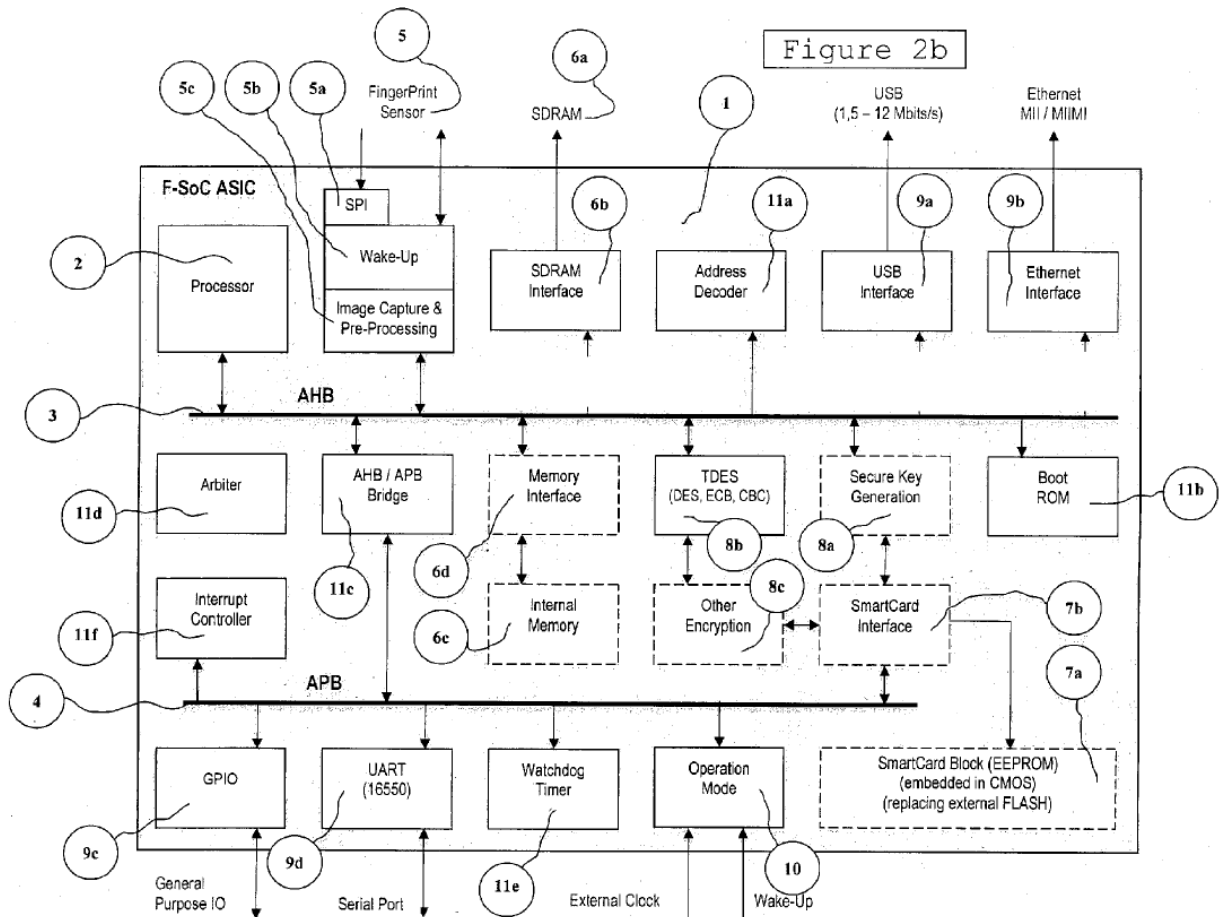
119. As explained at [7.1.3], Rescorla discloses the use of biometric verification to “control access” to keys. Ex.1015, 153. Mathiassen explains additional implementation details regarding biometric authentication, specifically in a portable device.

120. Specifically, Mathiassen’s portable device includes a subset of administrative software including “matching algorithm” software for fingerprint authentication. Ex.1005, [0072]. The fingerprint sensor 5 of the portable device, shown in Fig. 3a below, captures “raw images” of a fingerprint. Ex.1005, [0049]-[0050].



Ex.1005, Fig. 3a (annotated)

121. The portable device includes an integrated circuit (1) illustrated in Fig. 2b, shown below, which processes the received fingerprint to authenticate the user.



Ex.1005, Fig. 2b

122. The pre-processing block 5C processes the received fingerprint into “intermediate results” and compares them “with master fingerprint representations stored in non-volatile memory (7, 7A or 7C).” Ex.1005, [0049]-[0050]. In this way, the processor 2 biometrically authenticates a user.

123. Mathiassen explains that this biometric authentication occurs before sending the response to the external server. Specifically, “[a]ccess to such extended encryption will be given to the user **pending a positive match** of his fingerprint **with an authorized fingerprint.**” Ex.1005, [0050].

124. In addition, Mathiassen provides an example in which “a user [is] traveling” and “want[s] to connect to the Intranet server (30) of the network (N) from an Internet Café or a Business Center at a hotel.” Ex.1005, [0065]. Mathiassen walks through the process in chronological order at paragraphs [0065]-[0090]. At paragraphs [0066]-[0070], Mathiassen describes acquiring a fingerprint image from the user and processing the image. At paragraphs [0071]-[0073], Mathiassen describes comparing the received fingerprint with a master fingerprint. At paragraphs [0074]-[0077], Mathiassen describes generating a secure output, called the “message/communication” if the fingerprint matches the master fingerprint. Paragraphs [0078]-[0083] list the contents of the message and paragraphs [0084]-[0086] describing sending the message/communication to the external system or server. This sequence of events shows that the user is biometrically authenticated (*see* Ex.1005, [0065]-[0077]) before transmitting the message/communication (*see* Ex.1005, [0078]-[0086]).

125. Thus, Rescorla and Mathiassen describe *biometrically authenticating said customer by said customer authentication apparatus prior to transmitting said response to said request.*

[7.3] (3) performing said cryptographic encapsulation of said response by said customer authentication apparatus only after successful completion of said biometric authentication of said customer using fingerprint biometrics;

126. Rescorla and Mathiassen describe *performing said cryptographic encapsulation of said response by said customer authentication apparatus only after successful completion of said biometric authentication of said customer using fingerprint biometrics.*

127. Mathiassen explains that the output generated by its portable device indicating successful biometric authentication is generated after authentication:

Thus if a **positive match** of the **captured fingerprint** with the **fingerprint representation of an authorized user** is obtained, an output signal from the IC/chip (1) including target IP address and encrypted communication is generated.

Ex.1005, [0085].

128. As explained at [7.2], the example provided by Mathiassen shows that the user is first biometrically authenticated (*see* Ex.1005, [0065]-[0073]) before the messages/communication is cryptographically encapsulated (*see* Ex.1005, [0074]-[0083]).

129. Thus, Rescorla and Mathiassen describe this limitation.

[7.4] transmitting said response to said request; and

130. Rescorla and Mathiassen describe *transmitting said response to said request.*

131. Rescorla explains that the Certificate and CertificateVerify messages are transmitted from the client to the server, as shown in Fig. 4.2 below.

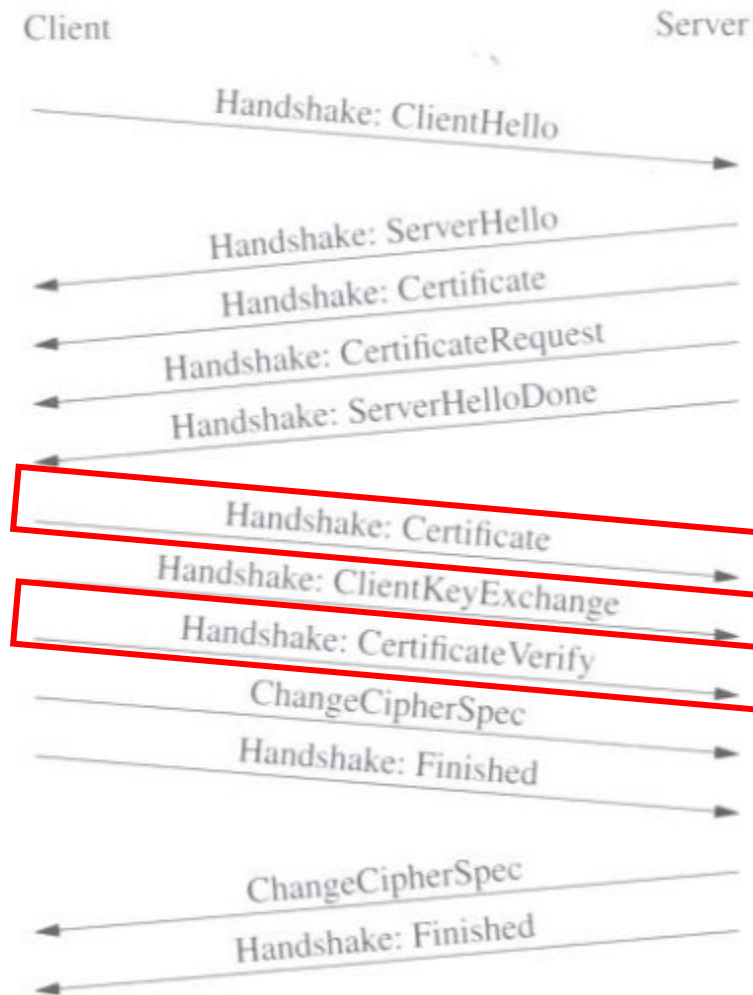


Figure 4.2 Client authentication timeline

Ex.1015, Fig. 4.2 (annotated)

132. Similarly, Mathiassen discloses “transferr[ing]” the message/communication. Ex.1005, [0084]. Similarly, Mathiassen describes receiving the message/communication by the server:

When this information is **received by e.g. the target server (30)** of the network (N) the receiving server (30) will look up the non-encrypted serial number, or IP address of the device (12 or 13) in the privilege subset of the data repository on the server (30).

Ex.1005, [0086].

133. Thus, Rescorla and Mathiassen describe sending the Certificate and CertificateVerify messages to the server, which teaches *transmitting said response to said request*.

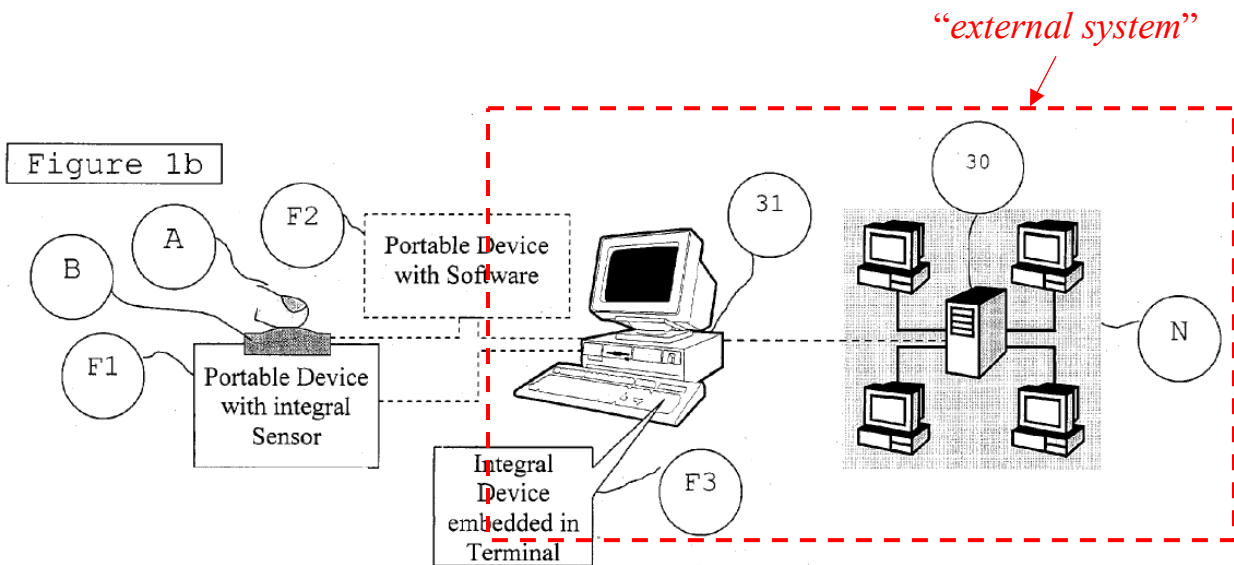
[7.5] verifying by at least one of said website and at least one external system that said response satisfactorily authenticates said customer.

134. Rescorla and Mathiassen describes *verifying by at least one of said website and at least one external system that said response satisfactorily authenticates said customer*.

135. As explained at limitation [7.1.4], the Certificate and CertificateVerify messages are used for *authentication of an enrolled customer*. See Section VIII.A.4.a, [7.1.4]. Rescorla explains that “sending the Certificate message...and the Certificate Verify message” is how the client “authenticate[s] itself.” Ex.1015, 108; *see also* 111 (“The CertificateVerify does all the actual work of client authentication.”). Thus, Rescorla explains *verifying...that said response satisfactorily authenticates said customer*.

136. Rescorla also explains that this verification is performed *by at least one of said website and at least one external system*. Specifically, “**the server...conclude[s]** that the entity named in the certificate is connecting.” Ex.1015, 111. The server described in Rescorla includes a *website*. For example, Rescorla describes “Servers under Load” as a “Web site when a large number of people decide to request a page at more or less the same time” Ex.1015, 202. Similarly, Rescorla explains that a server may be a “secure site”). Ex.1015, 232.

137. A POSITA would also have understood that a website is part of *at least one external system* based on Mathiassen’s teachings. For example, Mathiassen’s Fig. 1b illustrates how a portable device communicates with a “network (N)” that includes multiple “server(s) (30).” Ex.1005, [0051].



Ex.1005, Fig. 1b (annotated)

138. Mathiassen's network (N) provides internet access. Ex.1005, [0064] ("The user may...access the server (30) of the network (N)...by Internet."). Thus, a POSITA would have understood that Rescorla's server hosts a *website* and is part of a network of servers that correspond to an *external system*.

139. Thus, Rescorla and Mathiassen describe *verifying by at least one of said website and at least one external system that said response satisfactorily authenticates said customer*.

b) Claim 8

[8.0] The method of claim 7, wherein said step of performing cryptographic encapsulation of said transaction authentication response by said customer authentication apparatus also includes the step of explicitly identifying said customer authentication apparatus.

140. Rescorla and Mathiassen describe *explicitly identifying said customer authentication apparatus*.

141. As explained at [7.3], Mathiassen discloses *performing cryptographic encapsulation of said transaction authentication response by said customer authentication apparatus*. See Section VIII.A.4.a, [7.3]. Mathiassen further explains that the transaction authentication response sent to the server includes an identification of the portable device (*customer authentication apparatus*).

142. In particular, Mathiassen describes several "elements" that may be included in the "message/communication" sent to the server, including "[t]he device

number of the USB Dongle” (Ex.1005, [0078]), “[t]he IP address of the device (12 or 13)” (Ex.1005, [0079]), and “[t]he user ID” (Ex.1005, [0081]). Any of these elements would *explicitly identify* the portable device as claimed.

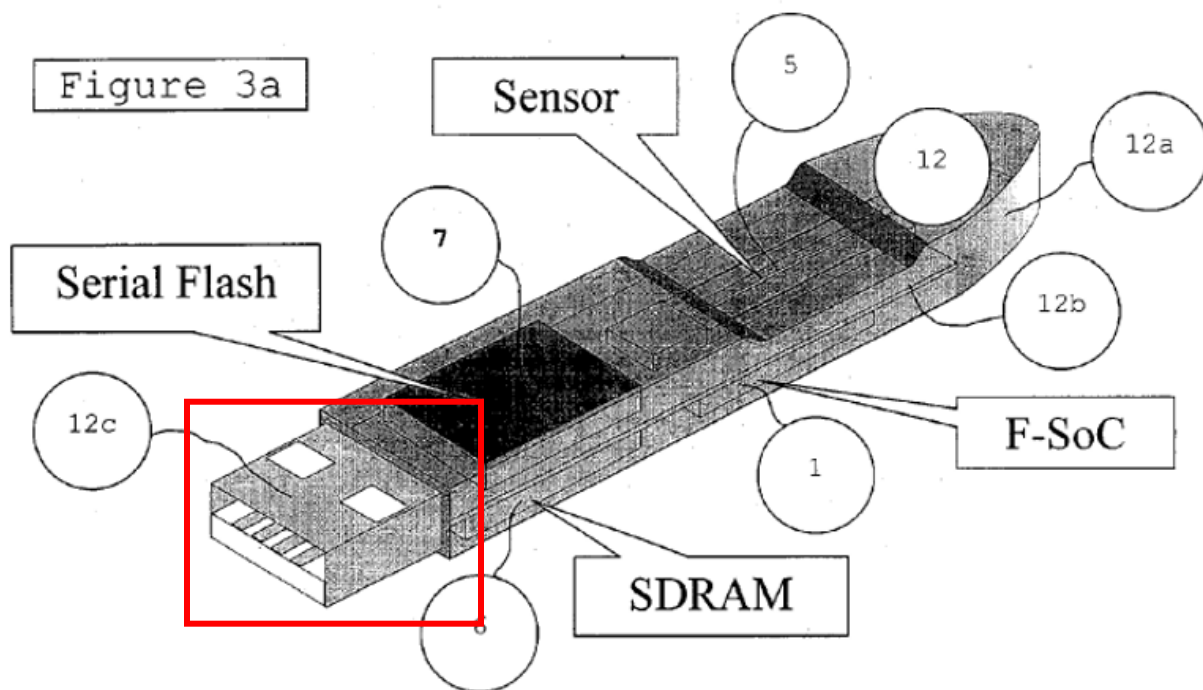
143. Thus, Rescorla and Mathiassen describe *explicitly identifying said customer authentication apparatus*.

c) Claim 9

[9.0] The method of claim 7, wherein said step of transmitting said transaction authentication response further comprises transmitting said cryptographically encapsulated secure data message by an external communications interface comprising an external interface connector disposed upon said customer authentication apparatus after said external interface connector has been inserted into an external interface port on an external system.

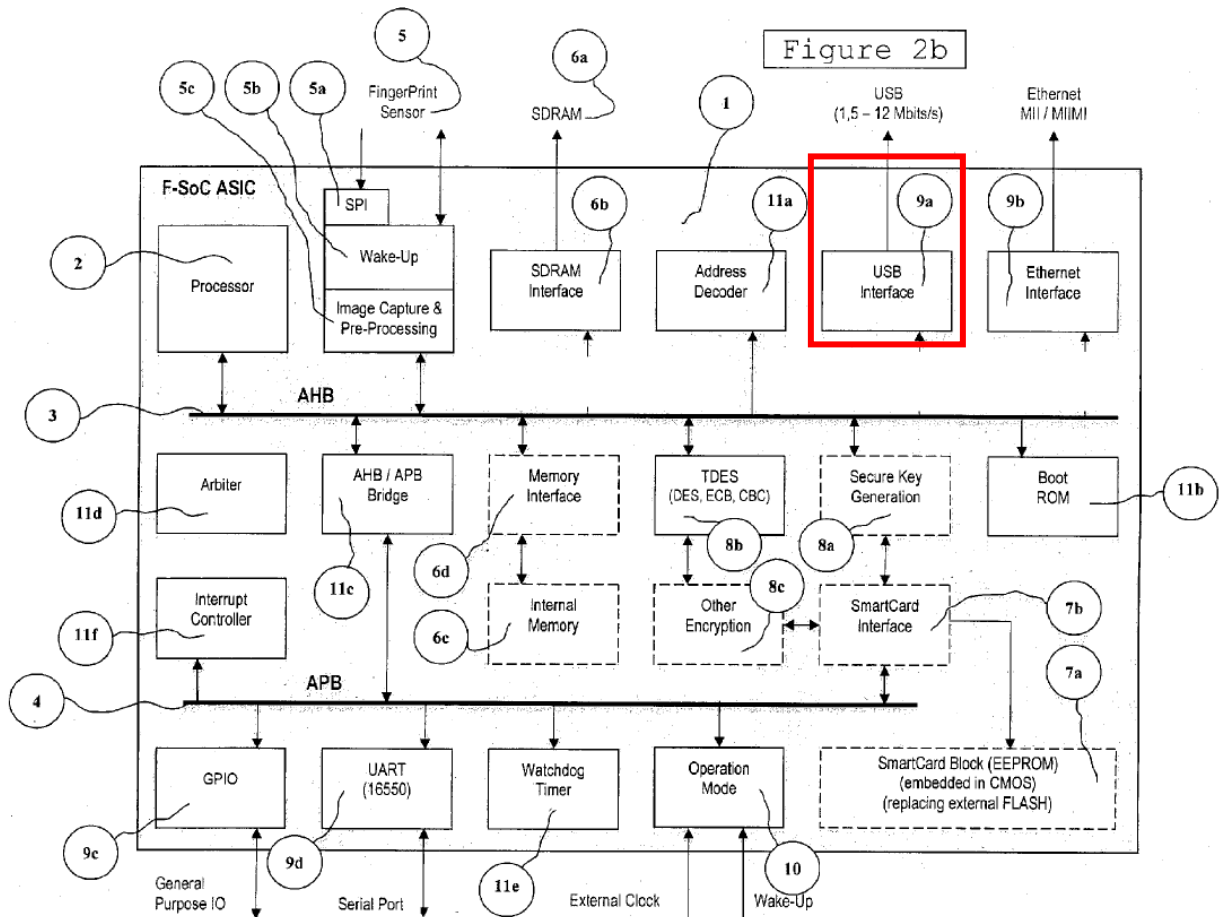
144. Rescorla and Mathiassen describe *transmitting said cryptographically encapsulated secure data message by an external communications interface comprising an external interface connector disposed upon said customer authentication apparatus after said external interface connector has been inserted into an external interface port on an external system*.

145. Mathiassen discloses *an external communication interface comprising an external interface connector*. Mathiassen’s device includes a physical USB connector described as the “USB interface (12C)” shown in Fig. 3a. Ex.1005, [0054].



Ex.1005, Fig. 3a (annotated)

146. In addition to the physical USB plug illustrated in Fig. 3a, “[e]lectronic surface components...support...the USB interface (12C).” Ex.1005, [0054]. These components include, for example, “second interface blocks (9A, 9B, 9C, or 9D).” Ex.1005, [0050], Fig. 2b.



Ex.1005, Fig. 2b (annotated)

147. Interface block 9A facilitates “transferring data to other devices and networks (N) external to the IC (1).” Ex.1005, [0050]. Thus, Mathiassen discloses an *external communications interface* (USB interface 9a and USB interface 12C) comprising an *external interface connector* (USB interface 12C) disposed upon said customer authentication apparatus.

148. Mathiassen also explains that the encrypted transaction authentication response is transmitted via the USB interface 12C (*transmitting said cryptographically encapsulated secure data message by an external*

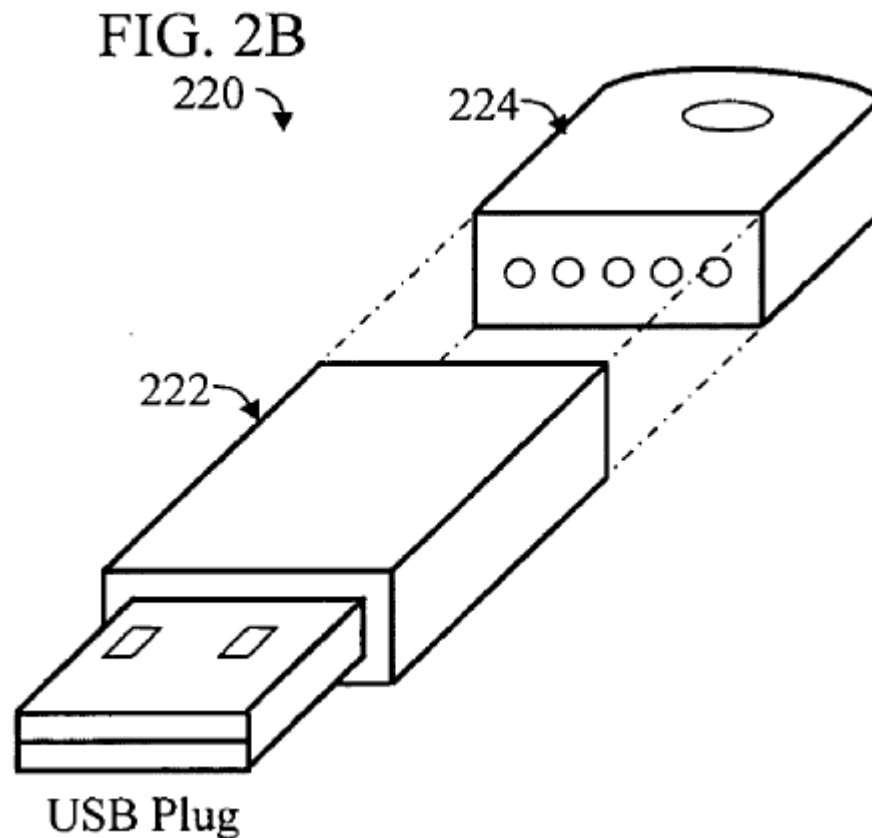
communications interface) after the portable device is inserted into a USB port of a computer (*after said external interface connector has been inserted into an external interface port on an external system*). For example, Mathiassen describes a scenario in which a “user will insert the portable device (12 or 13) into the USB port” of a computer in an “Internet Café or a Business Center at a hotel.” Ex.1005, [0065]. After the user is biometrically authenticated, a response is generated, encrypted, and “transferred to an external unit, network or system through one of the communication interfaces,” such as the USB interface 12C and interface block 9A. Ex.1005, [0084], [0050], [0054].

149. Therefore, Mathiassen also discloses this limitation.

B. Ground 2: Claims 10-14 would have been obvious over Rescorla in view of Mathiassen and Ryan.

1. Overview of Ryan

150. Ryan describes “[a] compact personal token apparatus, suitably resembling a conventional USB memory fob in size, shape, and form which can be plugged into a PC and interfaced with the virtual world of the Internet.” Ex.1006, Abstract. Ryan’s compact personal token apparatus both resembles and performs similar functions as Mathiassen’s portable device and the ’637 Patent’s ITA apparatus. Ryan describes multiple embodiments of its compact personal token, one of which is shown in Fig. 2B below.



Ex.1006, Fig. 2B

The embodiment shown in Fig. 2B includes two modules.

FIG. 2B illustrates another exemplary embodiment 220 of the smart fob, again in the general form of a USB memory fob. But in this case, the smart fob has a first physical module 222 (left, as viewed) which contains the input module (e.g., 102, USB plug, cf. 212) and translation module (e.g., 104), and a second physical module 224 (right, as viewed) which contains the processor module (e.g., 106, dual-interface chip) and output module (e.g., 108, RF antenna and modulator).

Ex.1006, [0203].

151. Ryan's apparatus may authenticate a user with a "biometric—such as fingerprint...." Ex.1006, [0229]. Ryan's apparatus also "may comprise an LCD screen" to display a variety of indicators, images, or symbols. Ex.1006, [0132], [0219], [0250], [0264].

152. Ryan's compact personal token apparatus is used to improve communication security for a wide variety of transactions. Ryan lists several exemplary transactions.

In use, for example, the user plugs the smart fob into his PC, or other Internet capable device (appliance), connects to the Internet, and interacts with a service or content provider to upload and/or download information. For example, downloading a ticket. Then, the user takes the smart fob to the event where it connects wirelessly with a reader at the venue to allow entrance and stamp the ticket (e.g., set a flag indicating that the ticket was used).

In another example, a consumer can use the smart fob to store "e-coupons" on the smart fob—loaded via the Internet. Then taking the Smart fob to a participating merchant, use the coupons to receive a savings or price reduction on the product.

In another example, a consumer could load cash value to the smart fob via the Internet and use the cash in the real world—at participating merchants—to buy a meal, newspaper, etc.

In another example, which can be called “kids fob” (also, without prejudice to potential trademark rights)—parents can provide their young children with a smart fob loaded with a preset amount of cash and send them off to the mall or participating theatre and know that the money will be used as intended.

In another example, a consumer could use the smart fob to load cash via the internet—and while still connected to the PC use the stored value to pay cash for products or services on the internet. This addresses the concern that consumers still have some reservations about giving out their credit card information over the Internet.

...

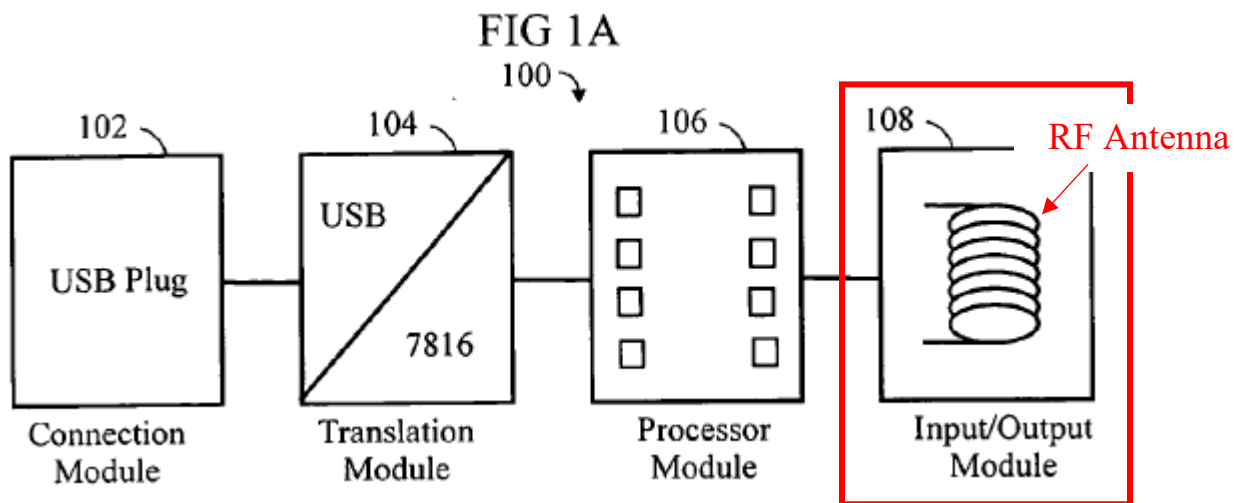
In another example, a consumer can load cash to the electronic purse of the smart fob device via Internet banking, and while still connected to the PC use the stored value to pay for online products or services.

Ex.1006, [0223]-[0227], [0236].

153. Ryan’s apparatus enhances the security of transactions by encrypting “packets of data” sent and received as part of these transactions. Ex.1006, [0241]. As a specific example, Ryan explains that “[p]ersonal data, frequency flyer miles as well as credit card details can be encrypted and stored in the smart fob.” Ex.1006, [0249]. Similarly, “digital content could be encrypted for limited time use or conditional access.” Ex.1006, [0367]. In addition, “all coupons are encrypted as a security feature reducing or eliminating the likelihood that coupon values could be

counterfeited or altered in any way.” Ex.1006, [0368]. Ryan’s compact personal token apparatus may authenticate a user with a “biometric—such as fingerprint, iris scan etc.” Ex.1006, [0229].

154. In addition, Ryan’s compact personal token apparatus communicates wirelessly with an RF antenna within the second physical module 224 shown in Fig. 2B. Ryan explains that the “second physical module 224...contains the processor module (e.g., 106, dual interface chip) and output module (e.g., 108, RF antenna and modulator.” Ex.1006, [0203]. The output module 108 within the second physical module 224 is shown in more detail in Fig. 1A, shown below.



“The output module 108 comprises an RF antenna.” Ex.1006, [0182].

2. Motivation to Combine Rescorla and Mathiassen with Ryan

155. A POSITA would have been motivated to modify the combination of Rescorla and Mathiassen by modifying Mathiassen’s portable device to conduct

transactions with a wireless interface, as taught by Ryan. Doing so would enable Mathiassen's portable device to communicate wirelessly with external devices. In addition, a POSITA would have been motivated to modify Mathiassen's portable device to implement an LCD screen, as described by Ryan.

156. Ryan relates to a similar technological field as the '637 patent. Ryan relates to "[a] compact personal token apparatus" for conducting transactions online and biometrically authenticating a user. Ex.1006, Abstract, [0229]. Ryan is in the same field and is relevant to the problem with which the inventor was involved.

157. A POSITA would have modified Mathiassen's portable device to include a wireless interface, as taught by Ryan, to configure Mathiassen's portable device to communicate wirelessly with external devices, in addition to the wired communication techniques that Mathiassen's portable device utilizes to communicate with external devices. Ryan's wireless interface allows the personal token apparatus to interact "via its wireless interface in the real world" (Ex.1006, [0151]) with a wider variety of systems and devices, such as ticket kiosks at venues or similar settings (Ex.1006, [0223] ("the user takes the smart fob to the event where it connects wirelessly with a reader at the venue,") [0235] (a user can "wave the device in close proximity to a turnstile equipped with a wireless reader at the entrance.")). Implementing wireless communication as taught by Ryan, "eliminate[s] the need to tender cash." Ex.1006, [0248]. In view of these advantages,

a POSITA would see the benefit in modifying Mathiassen's portable device to include a wireless interface as taught by Ryan. Doing so would enable Mathiassen's portable device to more fully perform its stated purpose of facilitating and improving security for online transactions, such as transactions with "an internet bank or a corporate or government intranet" by facilitating a wider variety of transactions and settings, such as any of the transactions described in Ryan, including wirelessly presenting a ticket at a venue, redeeming coupons, and paying for purchases. Ex.1005, Abstract; Ex.1006, [0223], [0235], [0224], [0225].

158. A POSITA would also implement an LCD screen, as described by Ryan, in Mathiassen's portable device. For example, Ryan explains that its LCD screen is capable of displaying a wide variety of images or text, including "messages regarding status or other relevant information to the user." Ex.1006, [0219]. In addition, text, such as a "seat reservation number" may be displayed (Ex.1006, [0250]), "[i]nformation, news or special offers," and "discounts...in barcode format" may be displayed as well (Ex.1006, [0264]). In contrast, Mathiassen's indicators are limited to colored LEDs (Ex.1005, [0124], [0135], [0138]) and a "beeper" (Ex.1005, [0120]). These functions require the user to learn and remember predetermined meaning attached to each indicator. For example, the user must remember that a flashing "red LED" signifies that "the user ID does not match any of the pre-stored authenticated users the process is aborted." Ex.1005, [0138]. A POSITA at the time

would have been motivated to implement an LCD, as described by Ryan, within the portable device to increase the flexibility and specificity of the messages the portable device is able to provide to the user. For example, error messages could be displayed on the LCD screen explaining specifically why the user was not authenticated, such as insufficient quality of captured fingerprint image as opposed to an incorrect fingerprint, etc. The provision of an LCD screen within Mathiassen's portable device would also enable Mathiassen's portable device to perform any number of the functions described by Ryan leading to increased adoptability and functionality. *See* Ex.1006, [0132], [0219], [0250], [0264].

159. Accordingly, the combination of Rescorla and Mathiassen with Ryan would have merely been the combination of well-known elements: a combination of Mathiassen's portable device with Ryan's wireless interface and LCD screen. The combination would be achieved by well-known methods, including implementing Mathiassen's encryption software to encrypt authentication data with Ryan's wireless interface for securing transaction data and LCD screen for displaying messages and symbols. Predictably, the combination would result in a portable device capable of interfacing with other devices, networks, and/or systems through wired and wireless connections and reporting, to the user, the status of transaction or functions via an LCD display.

160. Further, both Mathiassen and Ryan disclose a portable device that authenticates a user biometrically. Ex.1005, Fig. 3a, [0048]-[0050]; Ex.1006, [0222]-[0229], [0236]. Both Mathiassen and Ryan encrypt data sent from portable devices. Ex.1005, [0075]-[0098]; Ex.1006, [0249], [0367]-[0368]. The devices of both Mathiassen and Ryan interact with external devices, networks, and/or systems via communications interfaces. Ex.1005, [0053]; Ex.1006, [0124]. Mathiassen and Ryan each disclose portable devices for authenticating a user. Ex.1005, Abstract; Ex.1006, [0229]. Ryan's apparatus includes a wireless transceiver interface (Ex.1006, Fig. 1A (Input/Output Module 108)).

161. In addition, Mathiassen's wired interface perform essentially the same functions as a wireless interface as taught by Ryan and would be a simple substitution. Mathiassen describes a number of wired communications interfaces by which its portable device communicates with external systems. Ex.1005, [0050], Fig. 2b (interfaces blocks 9A, 9B, 9C, and 9D). Ryan describes a wired communications interface as well as a wireless communications interface that performs the same function of transmitting data to an external device. Ex.1006, [0175] (listing wired interfaces and wireless interfaces equally suitable for communicating "between an external memory/processing apparatus and a personal computer."). Ryan explains that both its wired communications interface and wireless communications interface perform the same function of transferring data to

and from the compact personal token apparatus. Ex.1006, [0223], [0235]. Similarly, the '637 patent itself explains that its wired interface and wireless interface are interchangeable equivalents. '637 Patent, 6:50-54 (Fig. 1B is “the same as the USB model in FIG. 1A except for a change in physical form from that of a stick-type enclosure to a card or similar, and the replacement of the USB interface with a radio circuit such as a Bluetooth or ZigBee chip with antenna 26.”). For all these reasons, a POSITA at the time would have been motivated to modify Mathiassen to include a wireless interface and authenticate transactions, as taught by Ryan.

162. Therefore, a POSITA at the time would have been encouraged to modify Mathiassen to include a wireless interface and an LCD display, as taught by Ryan.

3. Analysis

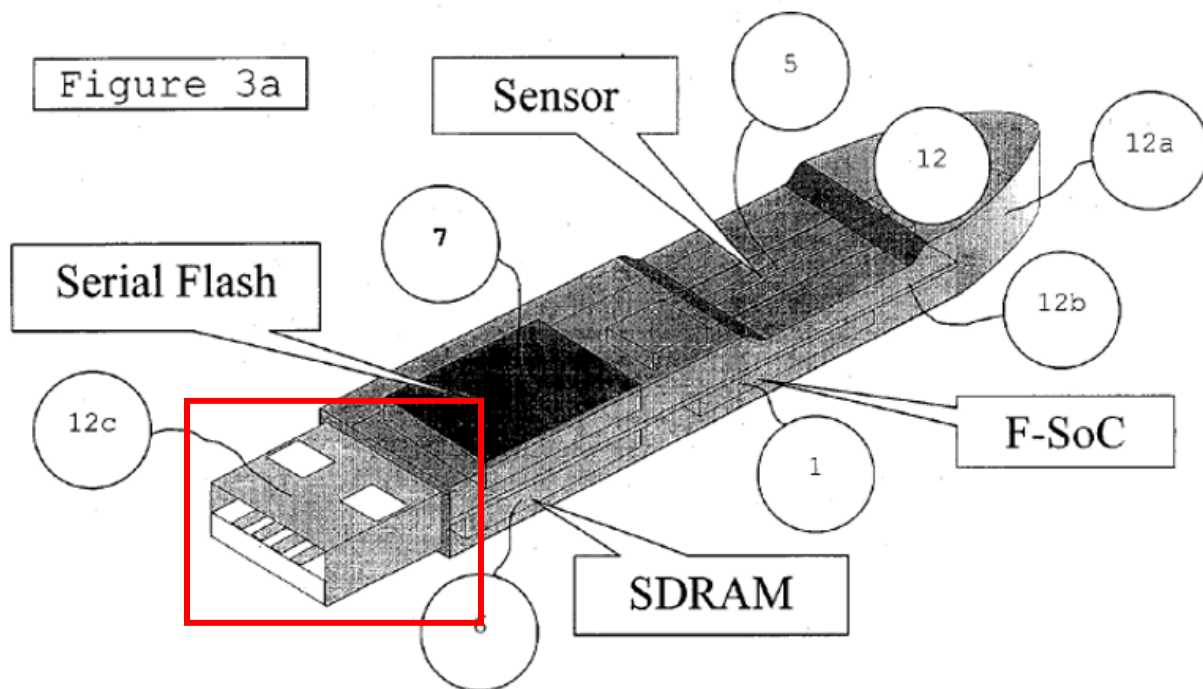
a) Claim 10

[10.0] The method of claim 7, wherein said step of transmitting said transaction authentication response further comprises transmitting said cryptographically encapsulated secure data message by an external communications interface comprising a wireless transceiver comprised within said customer authentication apparatus after said apparatus is within range of an external system having a wireless transceiver communications interface.

163. Rescorla, Mathiassen, and Ryan describe *transmitting said cryptographically encapsulated secure data message by an external communications interface comprising a wireless transceiver comprised within said*

customer authentication apparatus after said apparatus is within range of an external system having a wireless transceiver communications interface.

164. Specifically, Mathiassen's portable device includes *an external communications interface*, which, in the embodiment shown in Fig. 3a below, is a physical USB connector or USB plug described as a "USB interface (12C)." Ex.1005, [0054].



Ex.1005, Fig. 3a (annotated)

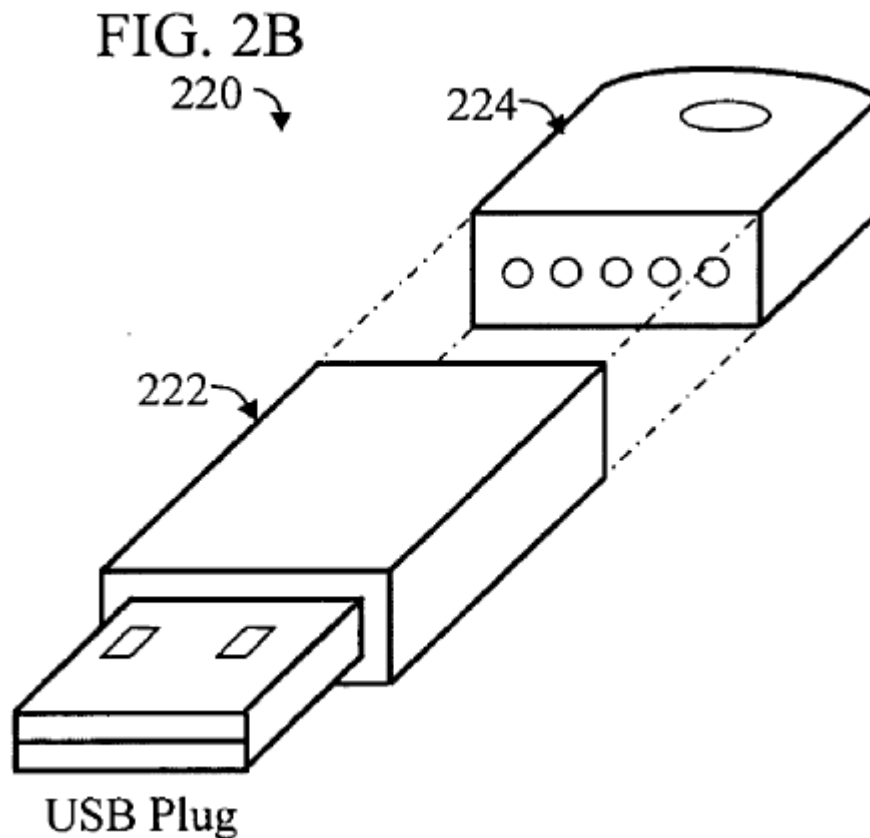
165. The USB interface 12C works in conjunction with "[e]lectronic surface components [which] support...the USB mechanical interface (12C)...mounted on the PCB (12B)." Ex.1005, [0054], Fig. 2b. In other embodiments, Mathiassen contemplates multiple other types of communications interfaces, including "a

number of second interface blocks (9A, 9B, 9C or 9D).” Ex.1005, [0050]. These interface blocks facilitate data communication via “USB (9A), Ethernet (9B), GPIO (9C), PCMCIA/UART (9D) and/or SmartCard (7C).” Ex.1005, [0050].

166. Mathiassen explains that the message/communication is transmitted via the external communications interface. Ex.1005, [0084] (“transferr[ing] to an external unit, network or system through one of the communication interfaces.”).

167. While Mathiassen does not explicitly disclose a wireless interface, given the multiple types of interfaces contemplated, a POSITA at the time would have understood that Mathiassen’s portable device would be readily modified to include a wireless interface, as taught by Ryan. *See* Section VIII.B.2.

168. Ryan’s “compact personal token apparatus comprises a wireless interface.” Ex.1006, [0124]. This token is shown in Fig. 2B.



Ex.1006, Fig. 2B

169. As shown in Fig. 2B, Ryan’s compact personal token apparatus includes a “first physical module 222” that contains the USB plug, also referred to as “the input module,” and a “second physical module 224” referred to as an “output module.” Ex.1006, [0203]. The output module within the second physical module 224 includes an “RF antenna and modulator.” Ex.1006, [0203]; Fig. 1A. Ryan’s wireless interface “enabl[es] communication with a personal device” external to the personal token apparatus. Ex.1006, [0038]. Thus, Ryan discloses or renders obvious *a wireless transceiver comprised within said customer authentication apparatus.*

170. In addition, Ryan specifically describes ranges of different wireless protocols. *See* Ex.1006, [0045] (“a 30-foot range” for “Bluetooth” communication), [0080] (“up to 50 inches distance” for “RF-ID tags”), [0089] (“short-range communication” for “NFC...wireless connectivity”), [0121] (“range of a Wi-Fi access point”). Ryan also explains that its token apparatus is “present[ed] to the point of sale (POS) contactless reader terminal” (Ex.1006, [0335]) as well as “communicat[ing] with contactless readers” (Ex.1006, [0370]). Based on this disclosure, a POSITA would have understood that the message/communication described in Mathiassen would be transmitted wirelessly, as described in Ryan, after the portable device was *within range of an external system having a wireless transceiver communications interface*.

171. Thus, Mathiassen and Ryan render obvious *transmitting said cryptographically encapsulated secure data message by an external communications interface comprising a wireless transceiver comprised within said customer authentication apparatus after said apparatus is within range of an external system having a wireless transceiver communications interface*.

b) Claim 11

[11.0] The method of claim 7, wherein said step 1 of cryptographically authenticating that said request originates from a legitimate customer and step 2 of biometrically authenticating said customer is indicated by means of at least one of a visual indicator cue and an audible indicator cue and a displayed indicator cue.

172. Rescorla and Mathiassen describe *wherein said step 1 of cryptographically authenticating that said request originates from a legitimate customer and step 2 of biometrically authenticating said customer is indicated by means of at least one of a visual indicator cue and an audible indicator cue and a displayed indicator cue.*

173. The '637 patent provides little details regarding if or how the ITA apparatus implements each of a visual indicator cue, audible indicator cue, and displayed indicator cue within the same device and whether these indicators are to be engaged simultaneously. Mathiassen describes an embodiment in which the same architecture as the portable device described above (*see* Section VIII.A.4.a, [7.1.1]) may be implemented in other forms, such as a medicine cabinet. Ex.1005, [0124]. In the context of this embodiment, Mathiassen explains that the device may include “3 LEDs (Light Emitting Diodes; green, yellow and red).” Ex.1005, [0124]. These LEDs are used to indicate whether the user has been authenticated. For example, “[i]f the user ID does not match any of the pre-stored authenticated users, the process is aborted and the red LED will flash.” Ex.1005, [0138]. A POSITA would have

understood that when the user was authenticated, the green LED would be used to indicate successful authentication. For example, other prior art at the time similarly employs LEDs to visually indicate that a user is authenticated. *See, e.g.*, Ex.1006, [0312] (“LEDs can be incorporated into the device...to alert a user that certain functions are occurring.”), [0220] (“LEDs (light-emitting diodes) 514, could readily be added to the device.”), [0132] (“The apparatus may comprise at least one LED.”), Ex.1007, [0035] (“LED 73 lights up to indicate that an authentication process is underway.”).

174. Mathiassen also discloses a “beeper” (*an audible indicator cue*). Ex.1005, [0120]. Mathiassen’s beeper “will beep for a pre-set period of say 10,0 seconds” when registering a new fingerprint. Ex.1005, [0119]-[0120]. Using this audible indicator cue to indicate various functions, including that the request originated from a legitimate customer, that it is verified through cryptographic authentication, and/or that the user was successful biometrically authenticated, would have been obvious to a POSITA at the time. A POSITA would have included an audible indicator to communicate information where the visual cue would be insufficient.

175. Ryan’s apparatus also includes “an LCD screen” (*a displayed indicator cue*). The LCD screen displays messages “regarding status or other relevant information.” Ex.1006, [0219]. Using an LCD screen as described by Ryan to

indicate that a user has been successful cryptographic authentication of the request or biometric authentication of the user would have similarly been obvious to a POSITA, and a POSITA would have been motivated to include an LCD screen to display status messages, as discussed in Section VIII.B.2.

176. In addition, any of these indicators could readily “be incorporated into the device...to alert a user that certain functions are occurring.” Ex.1006, [0312], [0219], [0250], [0264] (describing LED and LCD indicators used for displaying seat reservations and barcodes), and a POSITA would have expected success in doing so. There is nothing novel about adding simple indicators for the functions the claims recite.

177. Based on these disclosures, a POSITA would have understood that the red, yellow, and green LEDs and/or the beeper described in Mathiassen, as well as the LCD screen described by Ryan, may be implemented in the portable device to indicate when a customer is successfully authenticated (*step 1 of cryptographically authenticating that said request originates from a legitimate customer and step 2 of biometrically authenticating said customer is indicated by means of at least one of a visual indicator cue and an audible indicator cue and a displayed indicator cue*).

c) Claim 12

[12.0] The method of claim 11, wherein said visual indicator cue comprises at least one of lighting a light emitting diode and lighting a general purpose indicator light and displaying a visual indicator cue on a display.

178. Rescorla, Mathiassen, and Ryan describe *wherein said visual indicator cue comprises at least one of lighting a light emitting diode and lighting a general purpose indicator light and displaying a visual indicator cue on a display.*

179. As explained with reference to [11.0] above, Mathiassen discloses “3 LEDs (Light Emitting Diodes; green, yellow and red).” Ex.1005, [0124]. An LED is a general purpose light indicator because it is one of the most common and inexpensive forms of light emission for small electronic devices. Ryan discloses an LCD screen, which would be used to display an indicator that showed that the user was successfully authenticated. *See* Ex.1006, [0219], [0250], [0264]. Therefore, Ryan renders obvious *displaying a visual indicator cue on a display.*

180. Thus, Mathiassen discloses *said visual indicator cue comprises at least one of lighting a light emitting diode.*

d) Claim 13

[13.0] The method of claim 11, wherein said audible indicator cue comprises the sounding of at least one of a beep tone and a chime tone.

181. Rescorla and Mathiassen describe *wherein said audible indicator cue comprises the sounding of at least one of a beep tone and a chime tone.*

182. Mathiassen describes an embodiment in which the same architecture as the portable device described above (*see* Section VIII.A.4.a, [7.1.1]) may be implemented in a “hotel safe.” Ex.1005, [0119]. Mathiassen explains that its device could include “a beeper.” Ex.1005, [0120]. While Mathiassen explains that the beeper “will beep for a pre-set period of say 10,0 second” when registering a new fingerprint, using the beeper to similarly indicate any other functions would have been obvious to a POSITA at the time. For example, a POSITA, familiar with other prior art at the time would understand that any suitable indicators could readily “be incorporated into the device...to alert a user that certain functions are occurring.” Ex.1006, [0312]. It would be obvious to a POSITA that the same sound generating components, such as a speaker driver of any suitable type, used to generate a beep tone would also be used to generate a chime tone to indicate the same status.

183. Thus, Mathiassen discloses or renders obvious using a beep tone to indicate *cryptographically authenticating that said request originates from a legitimate customer and...biometrically authenticating said customer.*

e) **Claim 14**

[14.0] The method of claim 11, wherein said displayed indicator cue further comprises at least one of a predetermined indicator legend cue and a predetermined symbol cue and a predetermined image cue.

184. Rescorla, Mathiassen and Ryan describe *wherein said displayed indicator cue further comprises at least one of a predetermined indicator legend cue and a predetermined symbol cue and a predetermined image cue.*

185. As explained with reference to limitation [11.0], Mathiassen describes using “3 LEDs (Light Emitting Diodes; green, yellow and red)” to indicate the status of the portable device. Ex.1005, [0124]; *see* Section VIII.B.3.b.

186. Ryan’s apparatus similarly describes displaying various information related to the status of on-board functions and explains that its “apparatus may comprise an LCD screen.” Ex.1006, [0132]. Ryan’s LCD screen may be used for “displaying messages regarding status or other relevant information to the user.” Ex.1006, [0214]. Ryan explains that its LCD screen is capable of displaying a wide variety of symbols, including for example, “one or two line[s]” of text (Ex.1006, [0250]), or a “barcode” (Ex.1006, [0264]). Any of these display elements correspond to *a predetermined symbol cue or a predetermined image cue*, as claimed.

187. Thus, Mathiassen and Ryan disclose or render obvious *wherein said displayed indicator cue further comprises at least one of a predetermined indicator legend cue and a predetermined symbol cue and a predetermined image cue.*

**C. Ground 3: Claims 15-20 would have been obvious over
Mathiassen in view of Rescorla and Ryan.**

1. Motivation to Combine Mathiassen with Rescorla

188. As explained previously, a POSITA would have been motivated to implement the SSL/TLS handshake protocols described by Rescorla with Mathiassen's portable device. *See* Section VIII.A.3. In addition, a POSITA would have been additionally motivated to configure Mathiassen's portable device to perform aspects of the SSL/TLS handshake protocols described by Rescorla for the reasons below.

189. Given that Mathiassen does not limit its portable device to one specific handshake protocol, a POSITA would have understood that it could implement any suitable protocol. In addition, given that SSL/TLS is the most widely used handshake protocol, a POSITA would have been motivated to configure Mathiassen's portable device to perform the SSL/TLS handshake protocols described in Rescorla to increase compatibility of its device with web applications. Rescorla's handshake protocols describe mutual authentication (i.e., authentication of the client and server to each other). Ex.1015, 96 (describing "authenticat[ing] the server" and "cryptographically authenticating the client"). A POSITA would have recognized that allowing Mathiassen's portable device to authenticate the website with which the user connects would significantly increase communication security, which is one

of Mathiassen's stated objectives. *See* Ex.1005, Abstract ("providing increased security"), [0002] ("obtain[ing] a high level of security").

190. Authenticating the website to a user of Mathiassen's device prevents phishing attacks, thus keeping the user's confidential information, such as a payment information, out of the hands of unintended recipients. This mitigates the risk of identity theft or fraudulent activities. Authenticating the website to the user also increases trust of the user in using a particular website. Authenticating the website to the user by Mathiassen's portable device also allows the user to verify websites regardless of the particular terminal the user uses to access the website, thus providing all of the benefits of website authentication in a mobile application the user can take with her which greatly enhances convenience.

191. The combination of Mathiassen and Rescorla is a simple combination of well-known elements. It would simply combine Mathiassen's portable device for biometrically authenticating a user with commonly used and versatile SSL/TLS protocols for website authentication, as taught by Rescorla. Implementing SSL handshake protocols was well known, as explained by Rescorla, requiring "minimal modification." Ex.1015, xvii. The combination would predictably yield a portable device for both biometrically authenticating a user and cryptographically authenticating a website.

192. A POSITA would have understood how to successfully configure Mathiassen's portable device to perform the handshake protocols described by Rescorla. Mathiassen specifically contemplates that the portable device will implement handshake protocols. Ex.1005, [0084] (explaining that the message generated by Mathiassen's portable device as a result of successful biometrics could be implemented "in a predefined format and sequence (e.g., **handshake procedures**)."), [0091] ("output secure response" is compiled according to a "pre-defined format and sequence including **handshake sequences**"), [0095] ("tailoring **handshake sequences** according to the rules of secure communication" of the external system"), [0157], [0161].

193. Rescorla's handshake protocols are described as "by far the most widely deployed security protocol in the world" and highly compatible with a wide variety of applications. Ex.1015, xvii ("These techniques can often be applied to a new application protocol with minimal modification.").

194. Accordingly, a POSITA would have been recognized the benefits of modifying Mathiassen's portable device to perform the handshake sequences described by Rescorla and made such a modification.

2. Motivation to Combine Mathiassen and Rescorla with Ryan

195. As explained previously, a POSITA would have been motivated to modify Mathiassen's portable device to implement an LCD screen, as described by

Ryan. *See* Section VIII.D.2. This same reasoning applies to the combination of Mathiassen and Rescorla with Ryan with regards to claims 15-20.

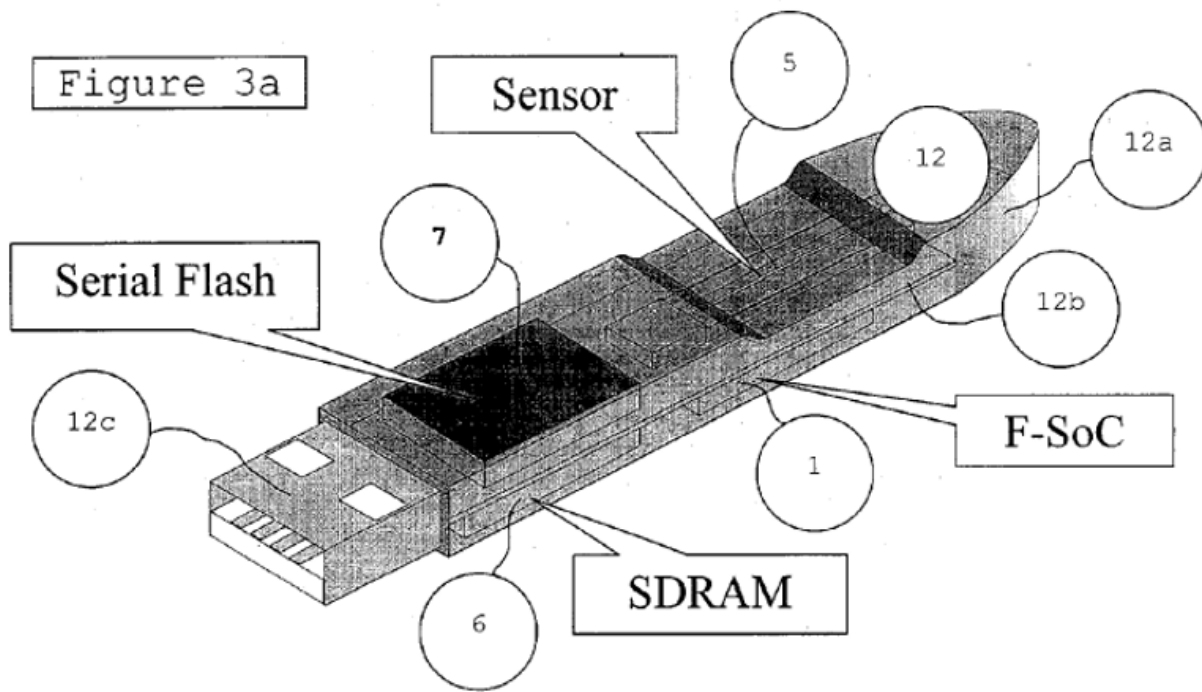
3. Analysis

a) Claim 15

[15.0] A method for generating a customer-initiated transaction request from an authorized customer initiating said request, comprising the steps of:

196. To the extent the preamble is limiting, Mathiassen, Rescorla, and Ryan describe a *method for generating a customer-initiated transaction request from an authorized customer initiating said request*.

197. As explained at [7.2], Mathiassen describes the steps by which its portable device “securely access[es a] server” with an “example involv[ing] a user traveling.” Ex.1005, [0064]-[0065]. In more detail, “[t]o initiate the connection procedure,” the user “will insert the portable device (12 or 13) into the USB port” of the computer and “swipe[] his finger over the fingerprint sensor (5) of the USB Dongle.” Ex.1005, [0065]-[0066]. The portable device used for this procedure is shown in Fig. 3a, below.



Ex.1005, Fig. 3a

198. Mathiassen explains how the user is authenticated biometrically based on the received fingerprint (Ex.1005, [0066]-[0074]), and how a “message/communication” is subsequently compiled (Ex.1005, [0077]-[0083]) and encrypted and sent to the network (Ex.1005, [0084]). Because the user initiates the connection procedure by inserting the device into the port of the computer and swiping her finger over the sensor, this “message/communication” discloses *a customer-initiated...request*.

199. Mathiassen also explains that this connection procedure is used to provide access to a system where a transaction is to be conducted, including “an internet bank.” Ex.1005, Abstract, [0016]-[0017], [0047]. Rescorla similarly

describes how its protocols are used to authenticate a user and a website prior to an online transaction. *See* Ex.1015, 177 (describing using “a new key for every **transaction.**”), 224 (describing “making an online purchase” where “[t]he **transaction is performed over an SSL connection** so you can be certain that you are talking to the correct merchant.”). In addition, Ryan describes multiple types of transactions that may be performed using a similar device. Ex.1006, [0223]-[0227], [0236]. Therefore, the message/communication described in Mathiassen discloses a *customer-initiated transaction request*.

200. This message/communication described in Mathiassen is also from an authorized customer initiating said request because the user of the portable device is first biometrically authenticated. For example, the user is first authenticated by providing a fingerprint via the sensor of Mathiassen’s portable device, where it is compared with master minutiae and the user is authenticated if there is a match. *See* Ex.1005, [0049]-[0050], [0066]-[0073].

201. Thus, Mathiassen describes compiling, encrypting, and sending a message/communication (*generating a customer-initiated transaction request*) from a portable device that biometrically authenticates the user (*from an authorized customer initiating said request*).

[15.1.1] (1) biometrically authenticating said customer using a customer authentication apparatus prior to transmission of said customer-initiated transaction request;

202. Mathiassen describes *biometrically authenticating said customer using a customer authentication apparatus prior to transmission of said customer-initiated transaction request*.

203. Mathiassen explains how the user of the portable device is biometrically authenticated. As explained at [7.2], Mathiassen's portable device includes a subset of administrative software called a "matching algorithm" for fingerprint authentication. Ex.1005, [0072]; *see* Section VIII.A.4.a, [7.2].

204. The fingerprint sensor 5 captures "raw images" of a fingerprint. Ex.1005, [0049]. The pre-processing block 5C of the integrated circuit (1) converts the received fingerprint to "intermediate results" and passes them on to the processor 2. Ex.1005, [0049]-[0050]. The processor 2 reduces them to "compact fingerprint representations, called minutiae" which are "compared...with master fingerprint representations stored in non-volatile memory (7, 7A or 7C)." Ex.1005, [0050]. In this way, the processor 2 of Mathiassen's portable device *biometrically authenticat[es a] customer*. *See* Section VIII.A.4.a, [7.2].

205. Mathiassen's portable device biometrically authenticates the user/customer before generating, encrypting, or sending the response to the external server (*prior to transmission of said customer-initiated transaction request*).

Mathiassen describes the biometric authentication process again at [0067]-[0073].

In this description, Mathiassen explains that “[o]ne result of the occurrence of a positive match,” (i.e., successful biometric authentication), “could be...the release of an IP address” (Ex.1005, [0074]) and the “calculat[ion] of a secure key” (Ex.1005, [0076]). The secure key calculated as a result of successful biometric authentication is then used “for encryption of a message/communication” (Ex.1005, [0077]), i.e., the *customer-initiated transaction request*, which is “transferred to an external unit, network or system” (Ex.1005, [0084]). The generation and encryption of the message (*see* Ex.1005, [0076]-[0077]) occurs only “[w]hen the central processor (2) has established a positive match between the access attempt minutiae,” (i.e., the received fingerprint), “and the resident master minutiae,” (i.e., the master fingerprint obtained during enrollment and stored in the non-volatile memory).

206. Thus, Mathiassen describes *biometrically authenticating said customer using a customer authentication apparatus prior to transmission of said customer-initiated transaction request*.

[15.1.2] (2) processing, assembling, and cryptographically encapsulating an assertion of a successful biometric authentication of said customer and

207. Mathiassen describes *processing, assembling, and cryptographically encapsulating an assertion of a successful biometric authentication of said customer*.

208. Mathiassen's "message/communication" (Ex.1005, [0077]) corresponds to the *customer-initiated transaction request*. Mathiassen explains how the message/communication is processed, assembled, and encrypted, as well as its contents.

The secure key will be input to the encryption block (8,8B or 8C) for encryption of a message/communication. The message will comprise the following elements,

The device number of the USB Dongle or the PCMCIA card (12 or 13) and the SKG key number (not the key itself) in non-encrypted format.

The IP address of the device (12 or 13) in encrypted format.

The secure key number (in encrypted format).

The user ID, in encrypted format.

Optionally **PKI verification** in encrypted format, in case of authentication of the user holding the electronic certificate.

Other encrypted information required by the particular requirements for secure communication, of the prevailing Intranet.

Ex.1005, [0077]-[0083].

209. The “secure key number” and/or “PKI verification” correspond to *an assertion of a successful biometric authentication*, because they are only generated and included in the message/communication after successful biometric authentication. Ex.1005, [0076] (“When the central processor (2) has established a positive match between the access attempt minutiae and the resident master minutiae, the administrative software...will calculate a secure key.”). In addition, “PKI verification” (Ex.1005, [0082]) specifically refers to “PKI **biometrics** verification” (Ex.1005, [0050]). Therefore, because the message/communication includes “PKI verification,” it is an *assertion of a successful biometric authentication of said customer*.

210. After the message/communication is processed and assembled, as explained above, it is cryptographically encapsulated. Specifically, “[t]**his message/communication is encrypted** to form a secure output in a predefined format and sequence (e.g., handshake procedures).” Ex.1005, [0084].

211. Thus, Mathiassen describes *processing, assembling, and cryptographically encapsulating an assertion of a successful biometric authentication of said customer*.

***[15.2] a provision of a time-varying parameter to prevent replay attacks
encapsulated there within prior to transmission thereof;***

212. Mathiassen and Rescorla describe *provision of a time-varying parameter to prevent replay attacks encapsulated there within prior to transmission thereof*.

213. Mathiassen describes using keys for encryption and authentication that are “valid for a time frame, or alternatively change[] for each transaction.” Ex.1005, [0050]. Mathiassen explains that the key is transmitted to the server. Ex.1005, [0080] (message/communication includes “[t]he secure key number.”). Thus, Mathiassen discloses *provision of a time-varying parameter*, as claimed.

214. A POSITA would have readily understood that time-varying parameters and changing keys would be used to prevent replay attacks. For example, Rescorla defines a “replay attack” as a “security hole” in which “an attacker can take a record off the wire and sent it again to the receiver.” Ex.1015, 22. To prevent replay attacks, Rescorla “ensure[s] that the keys produced by [each] handshake are different from the keys produced by any other handshake.” Ex.1015, 19. This use of a different key for each handshake described in Rescorla is the same technique described by Mathiassen (i.e., “chang[ing]” the key “for each transaction”) that it characterizes as an “alternative[]” to providing a key that is “valid for a time frame.” Ex.1005, [0050]. Therefore, a POSITA would have readily recognized the use of a

time-varying parameter described in Mathiassen would have been *to prevent replay attacks*.

215. Mathiassen also explains that “[t]he secure key will be input...for encryption of a message/communication” (Ex.1005, [0077]) which includes “[t]he secure key number (in encrypted format)” (Ex.1005, [0080]). Therefore, the time-varying secure key is *encapsulated...within* the customer-initiated transaction request *prior to transmission thereof*.

216. Thus, Mathiassen and Rescorla describe this limitation.

[15.3] (3) transmitting by said customer authentication apparatus said cryptographically encapsulated request to at least one external system further comprising at least one of a website and an authentication service provider,

217. Mathiassen describe *transmitting by said customer authentication apparatus said cryptographically encapsulated request to at least one external system further comprising at least one of a website and an authentication service provider*.

218. Mathiassen explains that the “message/communication” (*said cryptographically encapsulated request*) is sent to the external system:

The calculated communication response is thus a result depending on the above comparison of fingerprints. This **message/communication** is encrypted to form **a secure output** in a predefined format and sequence (e.g. handshake procedures) and **transferred to an external unit, network or system** through one of the communication interfaces.

Ex.1005, [0084].

219. Mathiassen also explains that the external unit, network or system includes a website. For example, Mathiassen explains that its “access-limited apparatus, device, network or system (N)” which receives the message/communication from the portable device may be “an internet bank.” Ex.1005, Abstract, [0047]. A POSITA would have understood that an internet bank includes *a website* as claimed. For example, internet banks are banks whose services are provided primarily, or in some cases, exclusively via a website.

220. In addition, a POSITA would also have understood that the message/communication could alternatively be transmitted to *an authentication service provider* based on additional prior art of the time. For example, an authentication service provider may authenticate a user on behalf of the website with which the user interacts. In that regard, Ryan describes a similar device used for authenticating a user and conducting online transactions whereby “[t]he client user can be authenticated by the ISP or **by a trusted third party.**” Ex.1006, [0245].

221. Thus, Mathiassen describes *transmitting by said customer authentication apparatus said cryptographically encapsulated request to at least one external system further comprising at least one of a website and an authentication service provider.*

[15.4.1] (4) receiving by said at least one external system said request and

222. Mathiassen describes *receiving by said at least one external system said request*.

223. Mathiassen describes “transferr[ing]” (Ex.1005, [0084]) the “message/communication” (*said request*) (Ex.1005, [0077]) “to an external unit, network or system” (Ex.1005, [0084]) (*at least one external system*). In addition, Mathiassen explains that the network 30 receives the request. Ex.1005, [0086] (when the message/communication “is received by e.g. the target server (30) of the network (N)...”). Based on this description, a POSITA would have understood that the “external unit, network or system” *receiv[es] said request*.

224. Thus, Mathiassen discloses or renders obvious this limitation.

[15.4.2] verifying that said request originated from an authenticated customer,

225. Mathiassen and Rescorla describe *verifying that said request originated from an authenticated customer*.

226. Mathiassen explains that when the message/communication “is received by e.g. the target server (30) of the network (N) the receiving server (30) will look up the non-encrypted serial number, or IP address of the device (12 or 13) in the privilege subset of the data repository on the server (30).” Ex.1005, [0086].

227. The server then attempts to decrypt the message/communication after “retriev[ing] the particular seed issued to [the] user.” Ex.1005, [0087]. According to

Mathiassen, “[i]f the decryption fails..., the server (30) will assume that the received communication attempt is false, and the server will abort further steps.” Ex.1005, [0090]. On the other hand, if the encryption succeeds, the server thereby verifies that the message/communication came from a biometrically authenticated user. The server can be assured that the information came from a biometrically authenticated user because the correct information is compiled and encrypted in the message/communication only “if a positive match of the captured fingerprint with the fingerprint representation of an authorized user is obtained.” Ex.1005, [0084]. In this way, “only authorized users [are allowed] access to all types of proprietary networks (LAN, WAN, etc.) typically represented by internet banking applications.” Ex.1005, [0017].

228. Similarly, Rescorla describes verifying that a request originated from an authorized customer. Rescorla illustrates a handshake protocol by which a user (the client) is authenticated by the server in Fig. 4.2.

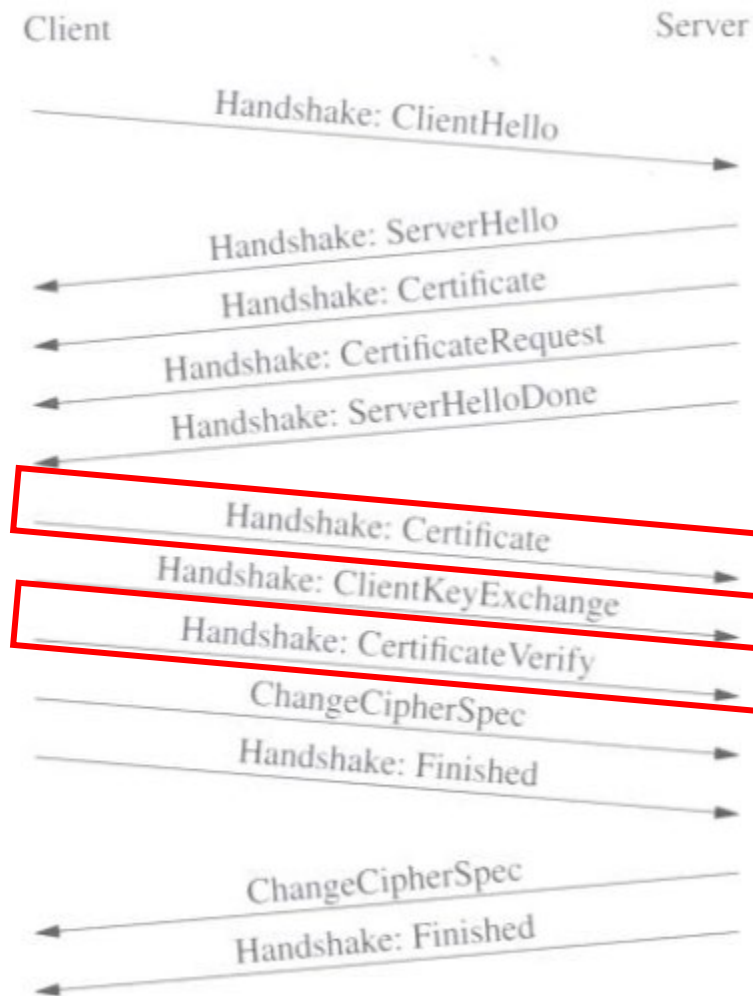


Figure 4.2 Client authentication timeline

Ex.1015, Fig. 4.2 (annotated)

229. As shown in Fig. 4.2, “the client...send[s] the Certificate message...to send its certificate and the CertificateVerify message to authenticate itself.” Ex.1015, 108. “The CertificateVerify does all the actual work of client authentication.” Ex.1015, 111. The server processes the signature of the CertificateVerify message and “[b]ecause only the holder of the private key

corresponding to the certificate could sign this message, the server can conclude that the entity named in the certificate is connecting.” Ex.1015, 111.

230. As previously explained in Section VIII.C.1, Mathiassen explains that its portable device would be readily designed to participate in “handshake sequences according to the rules of secure communication of the” external system with which it communicates. Ex.1005, [0095], [0084], [0091]. Given that Mathiassen does not limit its device to one particular handshake protocol, and Rescorla describes SSL as “the most widely deployed security protocol in the world” (Ex.1015, xvii), a POSITA would easily incorporate features of SSL handshake sequences into Mathiassen’s portable device.

231. Thus, Mathiassen and Rescorla describe *verifying that said request originated from an authenticated customer.*

[15.5] (5) responding to said request using a secure data message comprising a cryptographic transaction authentication response and transmitting said response to said customer authentication apparatus;

232. Mathiassen and Rescorla describe *responding to said request using a secure data message comprising a cryptographic transaction authentication response and transmitting said response to said customer authentication apparatus.*

233. As explained at [15.4.2], Rescorla describes verifying that a request from a client originates from an authenticated client based on the Certificate and

CertificateVerify messages it receives. Ex.1015, Fig. 4.2, 108, 111; *see* Section VIII.C.2.a, [15.4].

234. Rescorla also discloses a response in the form of the Handshake: Finished message highlighted in Fig. 4.2 below.



Figure 4.2 Client authentication timeline

Ex.1015, Fig. 4.2 (annotated)

235. The “Handshake: Finished” message is sent in response to receiving the client’s Certificate and CertificateVerify messages and indicates that both parties to

a transaction have been authenticated. Ex.1015, 81. As a result, the Handshake: Finished message corresponds to a *cryptographic transaction authentication response* that is *transmit*[ed] to the client.

236. Thus, Mathiassen and Rescorla describe *responding to said request using a secure data message comprising a cryptographic transaction authentication response and transmitting said response to said customer authentication apparatus.*

[15.6] (6) receiving and verifying by said customer authentication apparatus that said response to said request represents a response from a legitimate website; and

237. Mathiassen and Rescorla describe *receiving and verifying by said customer authentication apparatus that said response to said request represents a response from a legitimate website.*

238. As explained above at [7.1.2], Rescorla describes protocol steps by which the client verifies that communications from a website come from a legitimate website. See Section VIII.A.4.a, [7.1.2].

239. After the server has sent its Certificate message to the client, as illustrated in Fig. 3.5 and, optionally, the client has sent its own Certificate message (see Ex.1015, Fig. 4.2), the server sends the “Handshake: Finished” message to the client, which, as explained at [15.5] corresponds to the claimed *response*.



Figure 4.2 Client authentication timeline

Ex.1015, Fig. 4.2 (annotated)

240. Rescorla explains that it is only after the Finished message is sent from the server to the client that application data may be securely exchanged.

The SSLv3 specification allows a party to start sending application data as soon as that party's Finished message is sent. However, this creates a security risk for client data if the connection has been attacked. If the attacker has changed the handshake to negotiate a weaker cipher suite, the client can't detect this until it receives the server's Finished

message. To fix this, in TLS **the client must wait until it has received the server's Finished message before it can send its first byte of data**. Note that this isn't a security problem if the server chose the most secure of the client's ciphers, but rather than trying to detect this case, **it's safest to simply wait for the other server's Finished message**.

Ex.1015, 65.

241. Rescorla further explains that the Finished message is what “allows an implementation to verify that none of the handshake messages have been tampered with by an attacker.” Ex.1015, 81. Thus, the Handshake: Finished message sent from the server to the client in response to the client's Certificate message allows the client to verify that it comes *from a legitimate website*.

242. In addition, after the handshake is completed, when any application data is sent by the server to the client, it is encrypted. Ex.1015, 455 (“After the handshake is completed, the keys and algorithms are used to encrypt the application data traffic”). Therefore, if the client can successfully decrypt any received application data, it *verif[ies]...that* the received message is *a response from a legitimate website*. In that regard, any application data message sent from the server to the client, as illustrated in Fig. 3.5, similarly corresponds to a *response* received by the client for *verifying...that said response...represents a response from a legitimate website*.

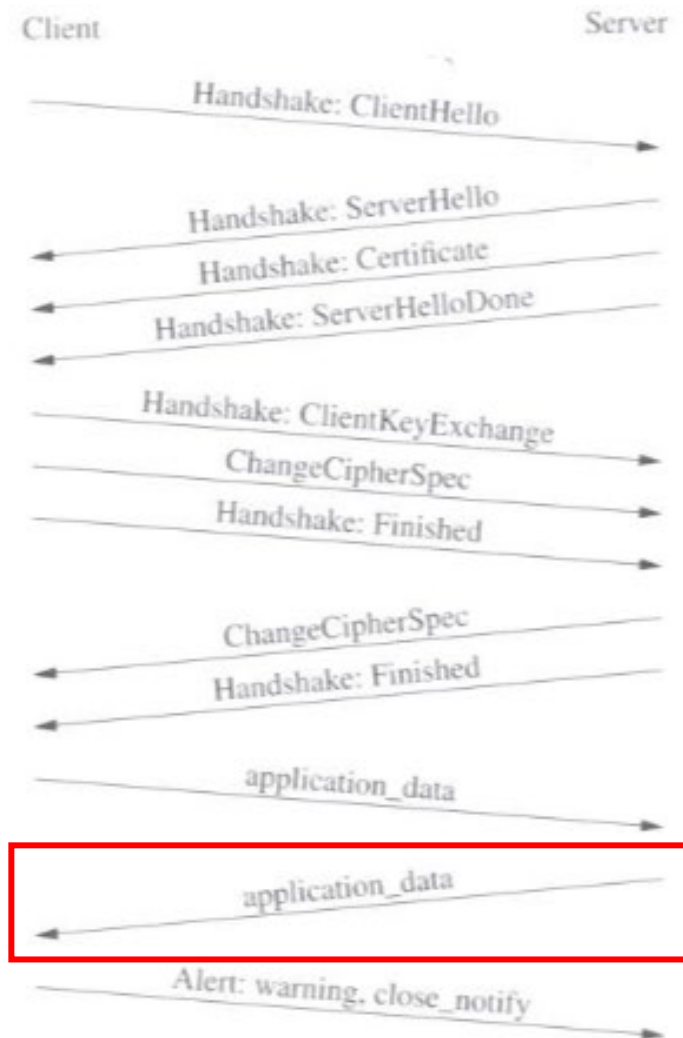


Figure 3.5 Time sequence of SSL messages

Ex.1015, Fig. 3.5 (annotated)

243. Thus, Mathiassen and Rescorla describe *receiving and verifying by said customer authentication apparatus that said response to said request represents a response from a legitimate website.*

[15.7] (7) actuating at least one of a visual indicator cue and an audible indicator cue and a displayed indicator cue on said transaction authentication apparatus indicating that said response has been received from a legitimate website.

244. Mathiassen describes *actuating at least one of a visual indicator cue and an audible indicator cue and a displayed indicator cue on said transaction authentication apparatus indicating that said response has been received from a legitimate website.*

245. As explained previously at [11.0], Mathiassen explains that its device may include “3 LEDs (Light Emitting Diodes; green, yellow and red).” Ex.1005, [0124]. While Mathiassen explains that these LEDs are used to indicate whether a user has been authenticated (Ex.1005, [0138]), a POSITA, based on the prior art at the time, would have understood that the LEDs could be used to convey the status of any functionality of the device. *See, e.g.,* Ex.1006, [0312] (“LEDs can be incorporated into the device...to alert a user that certain functions are occurring.”). Specifically, when Mathiassen’s device is modified to incorporate handshake protocols for authenticating a website (*see* Sections VIII.A.4.a, [7.1.2], VIII.C.2.a, [15.6]), a POSITA would have recognized that the LEDs, or alternatively any other indicators of the device, could also convey to a user *that said response has been received from a legitimate website.*

246. Thus, Mathiassen describes this limitation.

b) Claim 16

[16.0] The method of claim 15, wherein said step 1 of cryptographically authenticating that said request originates from a legitimate customer and step 2 of biometrically authenticating said customer is indicated by means of at least one of a visual indicator cue and an audible indicator cue and a displayed indicator cue.

247. Limitation [16.0] is the same as limitation [11.0]. The Mathiassen-Rescorla combination describe limitation [16.0] for the same reasons as in limitation [11.0]. See Section VIII.A.4.d, [11.0].

c) Claim 17

[17.0] The method of claim 16, wherein said visual indicator cue comprises at least one of lighting a light emitting diode and lighting a general purpose indicator light and displaying a visual indicator cue on a display.

248. Limitation [17.0] is the same as limitation [12.0]. The Mathiassen-Rescorla combination describe limitation [17.0] for the same reasons as in limitation [12.0]. See Section VIII.A.4.e, [12.0].

d) Claim 18

[18.0] The method of claim 16, wherein said audible indicator cue comprises the sounding of at least one of a beep tone and a chime tone.

249. Limitation [18.0] is the same as limitation [13.0]. The Mathiassen-Rescorla combination describe limitation [18.0] for the same reasons as in limitation [13.0]. See Section VIII.A.4.f, [13.0].

a) Claim 19

[19.0] The method of claim 16, wherein said displayed indicator cue further comprises at least one of a predetermined indicator legend cue and a predetermined symbol cue and a predetermined image cue.

250. Mathiassen and Ryan describe *wherein said displayed indicator cue further comprises at least one of a predetermined indicator legend cue and a predetermined symbol cue and a predetermined image cue.*

251. As explained with reference to limitation [14.0], Mathiassen describes using “3 LEDs (Light Emitting Diodes; green, yellow and red)” to indicate the status of the portable device (Ex.1005, [0124]) and Ryan describes the use of “an LCD screen” to display a variety of information (Ex.1006, [0132]). *See* Section VIII.B.2.b, [14.0].

252. As explained at [14.0], any of the display elements described in Ryan (e.g., messages regarding status (Ex.1006, [0214]), “one or two line[s]” of text (Ex.1006, [0250]), or a “barcode” (Ex.1006, [0264])) correspond to *a predetermined symbol cue or a predetermined image cue*, as claimed.

253. For at least the same reasons, Mathiassen and Ryan disclose or render obvious wherein said displayed indicator cue further comprises at least one of a predetermined indicator legend cue and a predetermined symbol cue and a predetermined image cue.

b) Claim 20

[20.0] A method for improving online transaction security, the steps comprising:

254. To the extent the preamble is limiting, Mathiassen and Rescorla describe a *method for improving online transaction security*.

255. Mathiassen discloses a “portable device” that implements “handshake procedures” that improve “general communication security measures in a network.” Ex.1005, [0047], Fig. 3a.

256. Mathiassen’s portable device “encrypt[s] general information transactions between [the] IC (1) [of the portable device] and [a] network server (30).” Ex.1005, [0050]. Such transactions may include transactions with “an internet bank.” Ex.1005, Abstract. To enhance the security of online transactions, as explained above at [7.2], [15.1.1], and [15.4.2], Mathiassen’s portable device biometrically authenticates the user of the device. Ex.1005, [0049]-[0050], [0065]-[0073]. Based on the biometric authentication, the portable device assembles and encrypts a “message/communication” to be sent to the network 30. Ex.1005, [0077]. The message/communication sent to the network 30 indicates that the user has been biometrically authenticated.

257. In addition, Rescorla describes SSL/TLS handshake procedures, which, as explained above at Sections VIII.A.3, VIII.C.1, would have been readily implemented by Mathiassen’s portable device. The handshake procedures described

in Rescorla also *improv[e] transaction security*. In particular, Rescorla explains that SSL is a “security protocol” used for virtually every online transaction. Ex.1015, xvii (“When you buy online using ‘secure’ Web pages..., you’re almost certainly using SSL.”).

258. Rescorla also describes authenticating the website or server with which the user is communicating during an online transaction. More specifically, and as explained at [7.1.2] and [15.6], the server sends the Certificate message that “contain[s] the server’s public key [and] provides the server’s identity for authentication purposes.” Ex.1015, 58.

259. Thus, Mathiassen and Rescorla describe this limitation.

[20.1] (1) enrolling a person into a customer authentication apparatus;

260. Mathiassen describes *enrolling a person into a customer authentication apparatus*.

261. Mathiassen explains a process by which a user is enrolled to use the portable device. Ex.1005, [0060]-[0064].

262. Mathiassen explains the enrollment process in detail.

The network administrator will organize issue of the portable devices (12 or 13) to the authorized users in a personalization process for the chip/IC (1) wherein data is pre-stored into the chip/IC (1). This involves loading the IP address of a targeted Intranet server, the selected encryption algorithm, and other data characterizing the Intranet, onto

the portable device (12 or 13). This information is either scrambled by block (8) for storage on external non volatile Flash memory (7), or alternatively stored securely in embedded non-volatile SmartCard memory (7A) or on an external non-volatile Smart Card memory (7E).

The network administrator, or persons he has delegated authority to, will then enroll the user who will be the “owner” of the portable device (12 or 13)....

Enrolment of a new user, by the administrator or a sub-administrator, will be performed on a terminal connected to the server (30). The administrator (or a sub-administrator) will perform the enrolment procedure of a new user, including capturing one or more fingerprints of the new user, and issuing a seed for the SKG algorithm to such new user. Eventually the administrator, or sub-administrator, will complete this procedure by counter-signing with his fingerprint. If the counter-signature fingerprint matches that of an authorized administrator, or sub-administrator, the enrolment procedure is deemed valid, and the personalized data downloaded to the portable device (12 or 13) connected to the terminal. If the counter-signature is not authenticated, the enrolment is deemed to be non-valid, and will be aborted.

The user has, by the above enrolment and issuance of a portable device (12 or 13), become authorized to access the Intranet network (N), or parts thereof.

Ex.1005, [0060]-[0063].

263. Therefore, Mathiassen describes enrolling a person to use the portable device, which discloses *enrolling a person into a customer authentication apparatus*.

[20.2] (2) deploying said person and said customer authentication apparatus together at an external system where at least one transaction can be generated;

264. Mathiassen and Rescorla describe *deploying said person and said customer authentication apparatus together at an external system where at least one transaction can be generated*.

265. Mathiassen describes the “network (N)” (Ex.1005, [0086]), as “an external unit, network or system” (Ex.1005, [0084]). Mathiassen’s network N is *an external system*.

266. Mathiassen also explains that, after a user is enrolled to use the portable device, she may access the network (N) (*external system*) via a terminal of the network (N). In particular, the user may “access the server (30) of the network (N) from a terminal (31) in the network (N).” Ex.1005, [0064]. Because the user is physically present at the “terminal (31) in the network (N)” which corresponds to the *external system*, Mathiassen describes *deploying said person...at an external system*.

267. In addition, Mathiassen explains that the user uses the portable device at the terminal (31). To describe the connection process, Mathiassen provides an

“example involv[ing] a user traveling.” Ex.1005, [0065]. The user “will insert the portable device (12 or 13) into the USB port...of the terminal (31).” Ex.1005, [0065]. Thus, Mathiassen discloses or renders obvious *deploying said customer authentication apparatus...at an external system.*

268. Mathiassen also explains that the external system is where *at least one transaction can be generated.* For example, Mathiassen describes the network that the user accesses via the portable device as an “access-limited apparatus, device, network or system, e.g.,...an internet bank.” Ex.1005, Abstract. Similarly, Mathiassen explains that the portable device is used to allow access to “all types of proprietary networks (LAN, WAN, etc.) typically represented by internet banking applications.” Ex.1005, [0017]. An internet bank is where at least one transaction can be generated.

269. In addition, Rescorla’s SSL/TLS protocols are used for conducting online transactions. *See* Ex.1015, xvii (describing how almost all online transactions are secured via SSL).

270. Therefore, Mathiassen and Rescorla describe *deploying said person and said customer authentication apparatus together at an external system where at least one transaction can be generated.*

[20.3] (3) communicating between said customer authentication apparatus and said external system;

271. Mathiassen describes *communicating between said customer authentication apparatus and said external system*.

272. Mathiassen's portable device includes "an integrated circuit (IC) (1)...to provide secure communication with the said access-limited apparatus, device, network or system." Ex.1005, Abstract. Similarly, Mathiassen describes "a secure communication between the IC (1) and the network server (30)" and "transferring data to other devices and network (N) external to the IC (1)." Ex.1005, [0050]; *see also* Ex.1005, [0051] ("Thereby the IC (1) is designed [to] communicate with external devices and networks (N)."). In describing generating and transmitting the message/communication as a secure output, Mathiassen provides detailed explanations of communicating between the portable device and network (N). *See* Ex.1005, [0084]-[0086] ("This message/communication is encrypted to form a secure output...and transferred to an external unit, network or system through one of the communication interfaces" and is specifically "received by e.g. the target server (30) of the network (N).").

273. Thus, Mathiassen describes *communicating between said customer authentication apparatus and said external system*.

[20.4] (4) authenticating said person by said customer authentication apparatus while said apparatus is communicating with said external system;

274. Mathiassen describes *authenticating said person by said customer authentication apparatus while said apparatus is communicating with said external system*.

275. As explained with reference to limitations [7.2] and [15.1.1] above, Mathiassen discloses or renders obvious *biometrically authenticating said customer using a customer authentication apparatus*. In particular, Mathiassen's portable device includes a subset of administrative software called a "matching algorithm" for fingerprint authentication. Ex.1005, [0072]. The device captures a fingerprint, converts it to "intermediate results" for comparing "with master fingerprint representations stored in non-volatile memory (7, 7A or 7C)." Ex.1005, [0049]-[0050]. In this way, Mathiassen's portable device biometrically authenticates a user.

276. Mathiassen also explains that this biometric authentication occurs while the portable device (*said apparatus*) is communicating with the network (N) (*said external system*). In particular, Mathiassen explains that biometric authentication occurs after the occurs after the portable device is inserted into the terminal 31 of the network N. Ex.1005, [0065]-[0066] ("The user will insert the portable device (12 or 13) into the USB port" and "[t]o initiate the connection procedure, the user swipes

his finger over the fingerprint sensor (5)”), [0067]-[0074] (describing biometric authentication after inserting the portable device).

277. In addition, Rescorla describes customer authentication as part of a SSL/TLS handshake procedure. In particular, Fig. 4.2 below shows customer authentication occurring with the server sending a CertificateRequest message from the server to the client and the client responding with the Certificate and CertificateVerify messages.

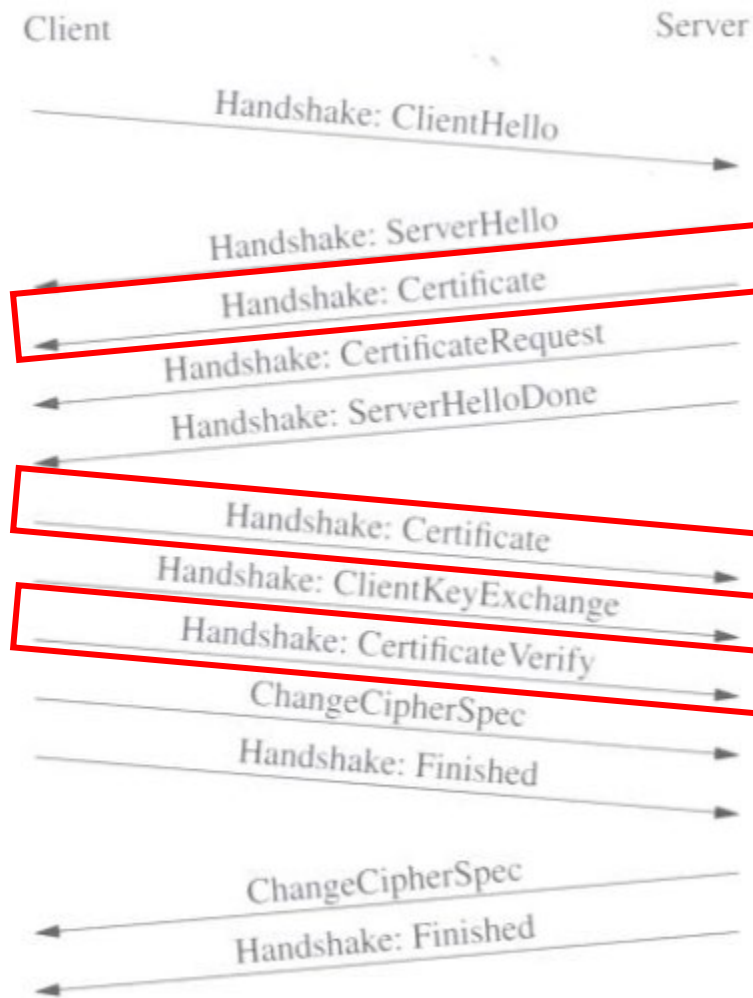


Figure 4.2 Client authentication timeline

Ex.1015, Fig. 4.2 (annotated)

278. As illustrated, these messages are sent and received in the context of an SSL/TLS handshake, which corresponds to communication between the client and the server.

279. Thus, Mathiassen and Rescorla describe *authenticating said person by said customer authentication apparatus while said apparatus is communicating with said external system.*

***[20.5] (5) initiating and generating of said at least one request by said person
after said apparatus has authenticated said person;***

280. Mathiassen describes *initiating and generating of said at least one request by said person after said apparatus has authenticated said person.*

281. As explained at limitation [7.2] previously, Mathiassen discloses *biometrically authenticating...prior to transmitting said response to said request.* For the same reasons, Mathiassen describes initiating and generating of said at least one request by said person after said apparatus has authenticated said person.

282. Mathiassen's "message/communication" (Ex.1005, [0077]) corresponds to the *request* claimed. Mathiassen explains that "[a]ccess to such extended encryption" of the message/communication "will be given to the user **pending a positive match** of his fingerprint **with an authorized fingerprint**...pre-stored in the non-volatile memory (7, 7A or 7C)." Ex.1005, [0050]. Similarly, Mathiassen explains that "[w]hen the central processor (2) has established a positive match between the access attempt minutiae and the resident master minutiae," thus biometrically authenticating the user, "the administrative software...will calculate a secure key...for encryption of [the] message/communication." Ex.1005, [0076]-[0077].

283. Thus, Mathiassen describes *initiating and generating of said at least one request by said person after said apparatus has authenticated said person.*

[20.6] (6) transmitting a request message indicating that said person was authenticated by said apparatus and that said transaction was initiated by an authenticated person; an

284. Mathiassen describes *transmitting a request message indicating that said person was authenticated by said apparatus and that said transaction was initiated by an authenticated person.*

285. As explained with reference to limitation [15.3], Mathiassen describes “transferr[ing]” the “message/communication...to an external unit, network or system through one of the communication interfaces.” Ex.1005, [0084]. Mathiassen further explains that this message/communication indicates that the user was authenticated by the apparatus and that the transaction was initiated by an authenticated person. As explained at [15.1.2], the message/communication transmitted from Mathiassen’s portable device to the network N is an *assertion of a successful biometric authentication of said customer*. Mathiassen explains that the secure key number, which is part of the message/communication, is only accessed if the user is biometrically authenticated. Ex.1005, [0076] (“When the central processor (2) has established a positive match between the access attempt minutiae and the resident master minutiae, the administrative software...will calculate a secure key.”). In addition, Mathiassen explains that “PKI verification” (Ex.1005, [0082]) includes “PKI **biometrics** verification” (Ex.1005, [0050]). For these same reasons, Mathiassen’s message/communication *indicat[es] that said person was*

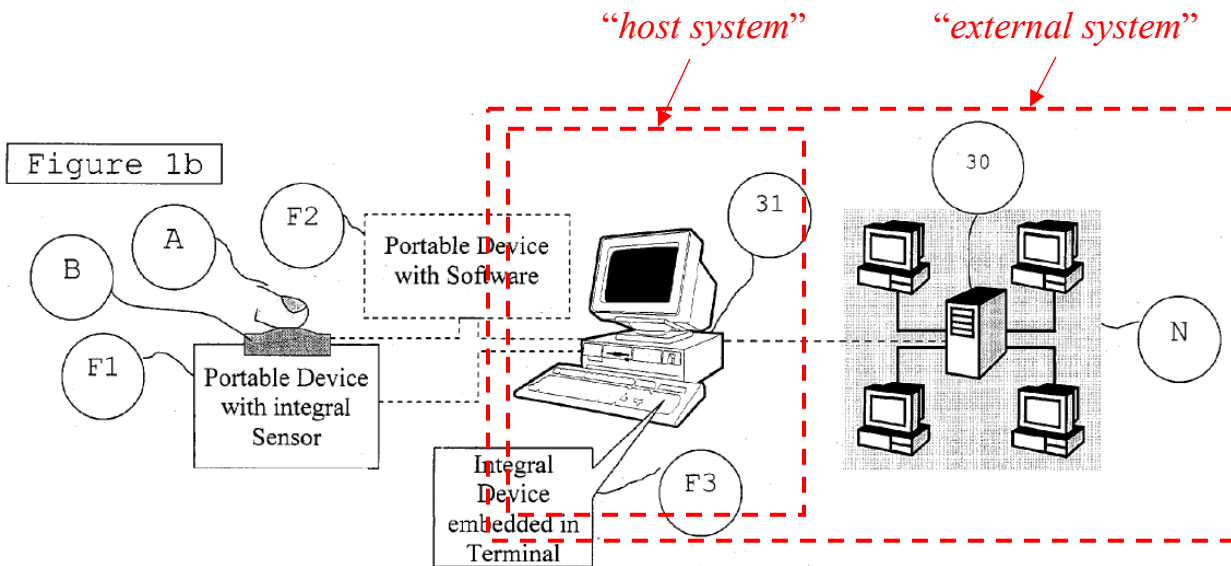
authenticated by said apparatus and that said transaction was initiated by an authenticated person, as claimed.

286. Thus, Mathiassen describes *transmitting a request message indicating that said person was authenticated by said apparatus and that said transaction was initiated by an authenticated person.*

[20.7] (7) receiving in said host system said authenticated-person-initiated-transaction message.

287. Mathiassen describes *receiving in said host system said authenticated-person-initiated-transaction message.*

288. Mathiassen's terminal 31 corresponds to a *host system* because it includes a USB port into which the portable device is inserted. Ex.1005, [0053] ("the IC (1) is a portable device to be plugged into a terminal (31)."). The terminal 31 is also part of the network N (*external system*). Ex.1005, [0053] ("a terminal (31) of the network.").



Ex.1005, Fig. 1b (annotated)

289. Mathiassen explains that the message/communication is sent from the portable device to the network N. *See* Ex.1005, [0084] (“The calculated communication response...is encrypted to form a secure output in a predefined format and sequence (e.g. handshake procedures) and **transferred to an external unit, network or system** through one of the communication interfaces.”). This message/communication is first received by the terminal 31, which is part of the network N, via the USB interface 12C, and passed on to the ultimate destination server or terminal within the network N. Ex.1005, [0084] (describing “transferr[ing]” the message/communication “through one of the communication interfaces.”). Thus, the terminal 31 (host system) *receives...said authenticated-person-initiated-transaction message*.

290. Thus, Mathiassen describes *receiving in said host system said authenticated-person-initiated-transaction message*.

IX. AVAILABILITY FOR CROSS-EXAMINATION

291. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross examination in the case and that cross examination will take place within the United States. If cross examination is required of me, I will appear for cross examination within the United States during the time allotted for cross examination.

X. CONCLUSION

292. I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct, and that all statements made of my own knowledge are true and that all statements made on information and belief are believed to be true. I understand that willful false statements are punishable by fine or imprisonment or both. *See* 18 U.S.C. § 1001.

Date: May 20, 2024

Respectfully submitted,

A handwritten signature in black ink that reads "Henry H. Houh". The signature is written in a cursive, slightly slanted style.

Henry Houh