

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

**PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT 7,480,637
CHALLENGING CLAIMS 7-20**

TABLE OF CONTENTS

I.	MANDATORY NOTICES UNDER 37 C.F.R. § 42.8.....	1
A.	Real Party-in-Interest	1
B.	Related Matters.....	1
C.	Lead and Back-up Counsel and Service Information	2
II.	CERTIFICATION OF GROUNDS FOR STANDING	3
III.	OVERVIEW OF CHALLENGE AND RELIEF REQUESTED.....	3
A.	Prior Art Patents and Printed Publications.....	3
B.	Statutory Grounds for Challenges	4
IV.	RESCORLA IS A PRINTED PUBLICATION.....	4
V.	U.S. PATENT 7,480,637	6
A.	Summary	6
B.	Level of Ordinary Skill in the Art.....	8
C.	Prosecution History	8
VI.	CLAIM CONSTRUCTION.....	9
VII.	CLAIMS 7-20 ARE UNPATENTABLE	10
A.	Ground 1: Claims 7-9 and 20 would have been obvious over Rescorla in view of Mathiassen.	10
1.	Overview of Rescorla	10
2.	Overview of Mathiassen	11
3.	Motivation to Combine Rescorla with Mathiassen	12

4.	Analysis.....	19
a.	Claim 7.....	19
b.	Claim 8.....	44
c.	Claim 9.....	46
B.	Ground 2: Claims 10-14 would have been obvious over Rescorla in view of Mathiassen and Ryan.	48
1.	Overview of Ryan	48
2.	Motivation to Combine Rescorla and Mathiassen with Ryan	50
3.	Analysis.....	54
a.	Claim 10.....	54
b.	Claim 11	59
c.	Claim 12.....	61
d.	Claim 13.....	62
e.	Claim 14.....	63
C.	Ground 3: Claims 15-20 would have been obvious over Mathiassen in view of Rescorla and Ryan.	63
1.	Motivation to Combine Mathiassen with Rescorla	64
2.	Motivation to Combine Mathiassen and Rescorla with Ryan	65
3.	Analysis.....	66
a.	Claim 15.....	66
b.	Claim 16.....	82

c. Claim 17.....	82
d. Claim 18.....	83
a. Claim 19.....	83
b. Claim 20.....	83
VIII. DISCRETIONARY INSTITUTION	95
A. Discretionary Denial Under § 325(d) Would be Inappropriate.	95
B. Discretionary Denial Under § 314(a) Would be Inappropriate.....	95
IX. CONCLUSION	96
X. CERTIFICATE OF WORD COUNT	97
XI. CLAIMS APPENDIX.....	99

PETITIONER’S EXHIBIT LIST

Ex.1001	U.S. Pat. No. 7,480,637 to Kozlay (“the ’637 patent”)
Ex.1002	Prosecution History of U.S. Pat. No. 7,480,637 (U.S. Application No. 11/317,141)
Ex.1003	Declaration of Dr. Henry Houh under 37 C.F.R. § 1.68
Ex.1004	<i>Curriculum Vitae</i> of Dr. Henry Houh
Ex.1005	U.S. Pat. Pub. No. 2004/0123113 to Mathiassen et al. (“Mathiassen”)
Ex.1006	U.S. Pat. Pub. No. 2005/0109841 to Ryan et al. (“Ryan”)
Ex.1007	U.S. Pat. Pub. No. 2003/0005336 to Lim et al. (“Lim”)
Ex.1008	Declaration of Glenn J. Perry
Ex.1009	Letter Agreement Between Glenn J. Perry and Askeladden L.L.C. dated May 20, 2020
Ex.1010	Reserved
Ex.1011	Reserved
Ex.1012	Reserved
Ex.1013	Reserved
Ex.1014	Reserved
Ex.1015	Eric Rescorla, “SSL and TLS: Designing and Building Secure Systems,” Addison-Wesley, (2001) (“Rescorla”)
Ex.1016	Reserved
Ex.1017	U.S. Pat. Pub. No. 2005/0165700 to Karthik (“Karthik”)
Ex.1018	U.S. Pat. Pub. No. 2006/0123465 to Ziegler (“Ziegler”)

Ex.1019	Reserved
Ex.1020	Reserved
Ex.1021	U.S. Pat. Pub. No. 2005/0193198 to Livowsky (“Livowsky”)
Ex.1022	Reserved
Ex.1023	Reserved
Ex.1024	Declaration of Dr. James L. Mullins
Ex.1025	Declaration of Lee Bernstein
Ex.1026	Public Catalog, U.S. Copyright Office, “SSL and TLS: designing and building secure systems / Eric Rescorla”
Ex.1027	U.S. Pat. Pub. No. 2003/0185391 to Qi et al. (“Qi”)
Ex.1028	U.S. Pat. Pub. No. 2002/0078342 to Matthews (“Matthews”)
Ex.1029	U.S. Pat. Pub. No. 2003/0023845 to VanHeyningen (“VanHeyningen”)
Ex.1030	U.S. Pat. Pub. No. 2003/0231765 to Tardo (“Tardo”)

I. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8**A. Real Party-in-Interest**

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner Askeladden L.L.C. certifies that it is the real party-in-interest in this proceeding. In this regard, Petitioner submits the Declaration of Glenn J. Perry (Ex.1008) and supporting exhibit (Ex.1009). As demonstrated in the Perry Declaration and supporting exhibit, no other party is in privity with Petitioner or exercised control or could exercise control over Petitioner's participation in this proceeding, the filing of this Petition, or the conduct of any ensuing trial. Ex.1008, ¶¶22-28; Ex.1009 (Agreement).

B. Related Matters

According to assignment records, U.S. Patent No. 7,480,637 ("the '637 patent" (Ex.1001)) is currently assigned to Jabaa, L.L.C. ("Jabaa" or "Patent Owner").

As of the filing date of this Petition, and to the best knowledge of Petitioner, the '637 patent is or has been involved in:

Case Caption	Number	Court	Filed	Status
<i>Biometric Associates, LP v. Ulta Beauty, Inc.</i>	2:20-cv-00365	E.D. Tex.	2020-11-18	Terminated
<i>Biometric Associates, LP v. American Eagle Outfitters, Inc.</i>	2:21-cv-00042	E.D. Tex.	2021-02-08	Terminated
<i>Jabaa, L.L.C. v. Foot Locker, Inc.</i>	2:21-cv-00234	E.D. Tex.	2021-06-29	Terminated

<i>Jabaa, L.L.C. v. Caleres, Inc. d/b/a Famous Footwear</i>	2:21-cv-00341	E.D. Tex.	2021-08-30	Terminated
<i>Jabaa, L.L.C. v. Five Below, Inc.</i>	2:21-cv-00461	E.D. Tex.	2021-12-20	Terminated
<i>Jabaa, L.L.C. v. Lululemon Athletica, Inc.</i>	2:22-cv-00248	E.D. Tex.	2022-07-05	Terminated
<i>Jabaa, L.L.C. v. The Kroger Co.</i>	2:22-cv-00479	E.D. Tex.	2022-12-17	Terminated
<i>Jabaa, L.L.C. v. Publix Super Markets, Inc.</i>	1:23-cv-01065	N.D. Ga.	2023-03-13	Terminated

The priority date of the '637 patent is its filing date, December 23, 2005.

Concurrently with the filing of this Petition challenging claims 7-20 of the '637 patent, Petitioner has filed a Petition challenging claims 1-6 and 21-24 of the '637 patent (IPR2024-00915).

C. Lead and Back-up Counsel and Service Information

<u>Lead Counsel</u> Jonathan R. Bowser HAYNES AND BOONE, LLP 2801 N. Harwood Street, Suite 2300 Dallas, TX 75201	Phone: 202-654-4503 Fax: 214-200-0853 jon.bowser.ipr@haynesboone.com USPTO Reg. No. 54,574
<u>Backup Counsel</u> Angela Oliver HAYNES AND BOONE, LLP 2801 N. Harwood Street, Suite 2300 Dallas, TX 75201	Phone: 202-654-4552 Fax: 214-200-0853 angela.oliver.ipr@haynesboone.com USPTO Reg. No. 73,271

Adam Erickson HAYNES AND BOONE, LLP 2801 N. Harwood Street, Suite 2300 Dallas, TX 75201	Phone: 202-654-4531 Fax: 214-200-0853 adam.erickson.ipr@haynesboone.com USPTO Reg. No. 77,434
--	--

Please address all correspondence to lead and back-up counsel. Petitioner consents to electronic service and asks Patent Owner to do the same.

II. CERTIFICATION OF GROUNDS FOR STANDING

Petitioner certifies that the '637 patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting IPR of the claims.

III. OVERVIEW OF CHALLENGE AND RELIEF REQUESTED

Petitioner challenges claims 7-20 (the “challenged claims”) of the '637 patent.¹

A. Prior Art Patents and Printed Publications

The following references are pertinent to the grounds of unpatentability explained below:

1. Eric Rescorla, “SSL and TLS: Designing and Building Secure Systems,” Addison-Wesley, (2001) (“Rescorla”) (Ex.1015); published by Addison-Wesley in 2001. Rescorla qualifies as prior art under 35 U.S.C. §§ 102(a) and 102(b).

¹ The '637 patent is a pre-AIA patent filed on December 23, 2005.

2. U.S. Patent Publication 2004/0123113 (“Mathiassen”) (Ex.1005); filed December 18, 2002; published June 24, 2004. Mathiassen qualifies as prior art under 35 U.S.C. §§ 102(a) and 102(b).
3. U.S. Patent Publication 2005/0109841 (“Ryan”) (Ex.1006); filed November 16, 2004; published May 26, 2005. Ryan qualifies as prior art under 35 U.S.C. § 102(a).

Rescorla, Mathiassen, and Ryan were not considered or cited during prosecution of the ’637 patent.

B. Statutory Grounds for Challenges

This Petition, supported by the declaration of Dr. Henry Houh (Ex.1003) (*see also* Ex.1004), requests cancellation of claims 7-20 under the Grounds listed below:

Ground	Claims	Obviousness Basis (§ 103)
#1	7-9	Rescorla in view of Mathiassen
#2	10-14	Rescorla in view of Mathiassen and Ryan
#3	15-20	Mathiassen in view of Rescorla and Ryan

IV. RESCORLA IS A PRINTED PUBLICATION

“Public accessibility” is “the touchstone in determining whether a reference constitutes a printed publication.” *In re Hall*, 781 F.2d 897, 899 (Fed. Cir. 1986) (cleaned up). A reference is publicly accessible if it was “made available to the extent

that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it.” *Acceleration Bay, LLC v. Activision Blizzard, Inc.*, 908 F.3d 765, 772 (Fed. Cir. 2018) (cleaned up).

Petitioner submits the Declaration of Dr. James L. Mullins (Ex.1024) to show that Rescorla was publicly available more than one year before December 23, 2005. Petitioner submits the Declaration of Lee Bernstein (Ex.1025) to show how the copy of Rescorla submitted as Exhibit 1015 was obtained. Rescorla is a textbook located in the Library of Congress and in the Swem Library at the College of William and Mary. Ex.1024, ¶¶25-34, 43-45, 51-52. The copy at the Library of Congress bears a stamp dated November 7, 2000. Ex.1024, ¶¶27, 45. It was “received by the Library of Congress for creation of Cataloging in Publication (CIP) on 06-27-00 (June 27, 2000)” (Ex.1024, ¶47) and would have been publicly available “by January 8, 2001 or within a few days thereof.” (Ex.1024, ¶¶48, 57). The copy held at the College of William and Mary bears a stamp dated 2001. Ex.1024, ¶30. It was likely received by that library on April 30, 2001, and available to the public “by May 10, 2001, or within a few days thereof.” Ex.1024, ¶¶55, 57. The MARC records for Rescorla at both the Library of Congress and the College of William and Mary show that Rescorla was indexed using topical subject-matter headings, which would have led an interested person of ordinary skill in the art (POSITA) using reasonable diligence to Rescorla. Ex.1024, ¶¶46, 49, 53, 56 (discussing Attachments A-6 and A-8).

Rescorla also could have been located by accessing the *WorldCat* database through an OCLC member library. Ex.1024, ¶¶35-42.

These dates are consistent with the U.S. Copyright Office’s public catalog, which indicates that Rescorla was published in October 2000. Ex.1026. Moreover, Rescorla was cited in a variety of published patents and applications before the priority date of the ’637 patent. Ex.1027, [0038]; Ex.1028, [0006]; Ex.1029, [0014], [0029]; Ex.1030, [0005].

V. U.S. PATENT 7,480,637

A. Summary

The ’637 patent describes a customer authentication apparatus called a USB dongle or wireless card, as shown in Figs. 1A-1B. Ex.1001, Abstract, 4:61-5:35, 6:49-58. The customer authentication apparatus is described 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 and website. Ex.1001, 3:36-39 (authenticating user), 5:35 (authenticating website); Ex.1003, ¶36.

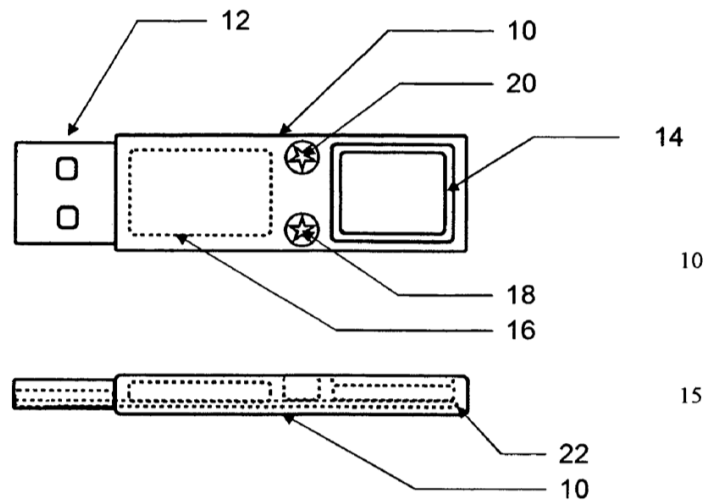


Figure 1A, Internet Transaction Authenticator in USB Dongle Form

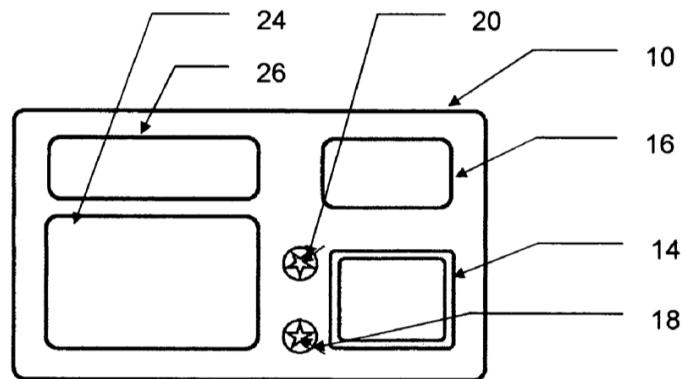


Figure 1B, Internet Transaction Authenticator in Wireless Card Form

Ex.1001, Figs. 1A and 1B

The ITA apparatus includes a fingerprint sensor array 14 and LED lights 18, 20. Ex.1001, 5:27-51. With reference to Figure 1A, after inserting the ITA apparatus into a USB port, the user places a finger on the fingerprint sensor array 14 to authenticate herself, and the color of the LED 18 indicates whether the user is

authenticated. Ex.1001, 5:38-52. If the user is authenticated, the apparatus sends encrypted authentication results to the website. Ex.1001, 6:15-26. The website sends a response. Ex.1001, 6:38-39. The ITA apparatus also authenticates the website. Ex.1001, 5:35, 5:48-50. The user then completes a transaction. Ex.1001, 6:27-32. The wireless card of Figure 1B operates in the same way except the wireless card communicates wirelessly. Ex.1001, 6:48-57; Ex.1003, ¶36.

B. Level of Ordinary Skill in the Art

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 and less education may be necessary with additional work experience. Ex.1003, ¶¶39-40.

C. Prosecution History

The '637 patent was filed as U.S. Patent Application No. 11/317,141 on December 23, 2005. Only one Office Action issued during prosecution. All claims were rejected as obvious over Karthik (U.S. 2005/0165700) (Ex.1017) and Ziegler (U.S. 2006/0123465) (Ex.1018). Ex.1002, 76-90. A *pro se* response was filed but not recognized by the Office, and a notice of abandonment issued. The inventor

assigned the application to Biometric Associates, LP, which filed a response and petition to revive. Ex.1002, 37-50. The assignee did not amend claim 15 but amended claims 7 and 20 to remove the terms “means of.” Ex.1002, 40-46. The assignee argued that the claims were allowable because “authentication resides within the apparatus and not in the user’s or web host’s system.” Ex.1002, 47-49.

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 as the allowable features, despite those limitations not being included in claims 7-20. Ex.1002, 26. As shown in Section VII below, claims 7-20 are rendered obvious by prior art not considered by the Examiner.

VI. CLAIM CONSTRUCTION²

Petitioner submits that for purposes of this proceeding, no claim term requires construction beyond its ordinary and customary meaning. Ex.1003, ¶¶41-43.

² Unless otherwise specified, all **bold** emphasis below has been added. *Italics* is used to signify claim language.

VII. CLAIMS 7-20 ARE UNPATENTABLE

A. Ground 1: Claims 7-9 and 20 would have been obvious over Rescorla in view of Mathiassen.

1. Overview of Rescorla

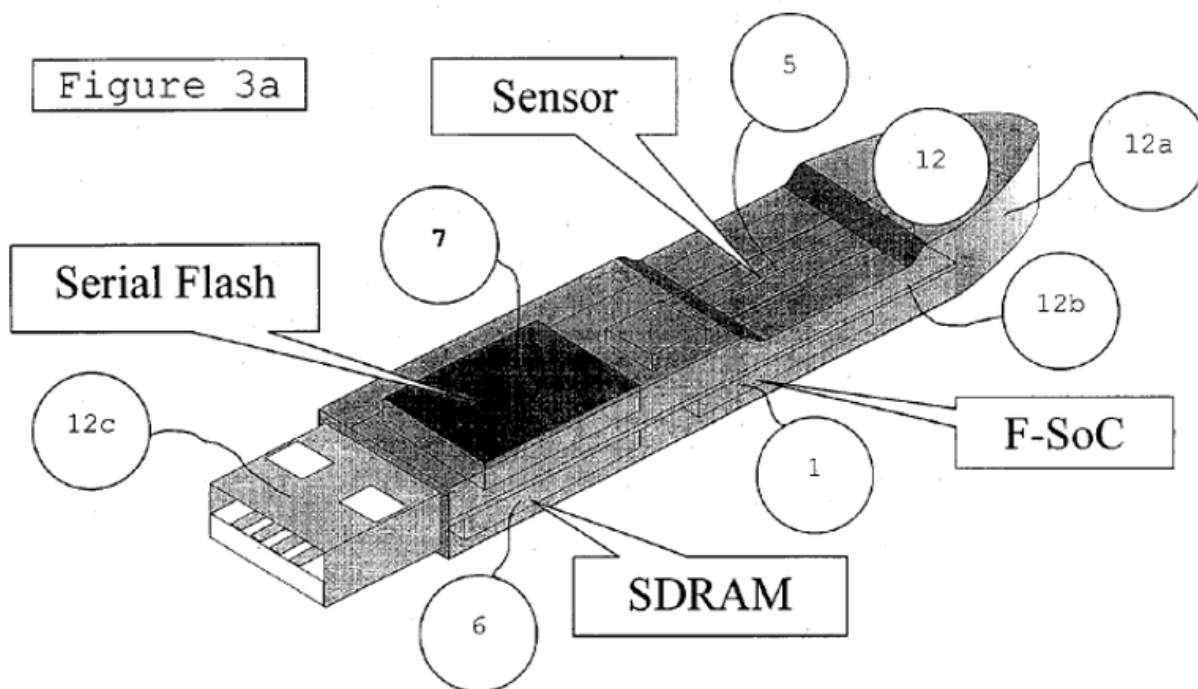
Rescorla describes a SSL/TLS³ “security protocol” that is “by far the most widely deployed security protocol in the world” and that “[e]ssentially every commercial Web browser and server support[s].” Ex.1015, xvii. SSL is used for conducting online transactions. Ex.1015, xvii (“When you buy online using ‘secure’ Web pages..., you’re almost certainly using SSL.”); Ex.1003, ¶50.

Chapters 2-3 of Rescorla provide an overview of SSL/TLS encryption. Rescorla describes how a webpage/server uses SSL/TLS handshake protocols to provide its certificate which “the client verifies.” Ex.1015, 58. SSL/TLS also includes protocols “for cryptographically authenticating the client.” Ex.1015, 96. Rescorla explains “most if not all of what you need to know in order to design secure systems using SSL/TLS...and apply them to new situations.” Ex.1015, xvii. Rescorla explains that its protocols may be implemented with biometric authentication. Ex.1015, 153 (“biometrics add valuable security”). Ex.1003, ¶¶51-54.

³ SSL/TLS is an abbreviation for Secure Sockets Layer/Transport Layer Security.

2. Overview of Mathiassen

Mathiassen describes “[a] portable or embedded access device,” referred to as a “portable device,” that improves communication security by biometrically authenticating a user. Ex.1005, Abstract, [0047]. One implementation is shown in Figure 3a, below. Ex.1003, ¶55.



Ex.1005, Fig. 3a

The portable device includes a USB mechanical interface 12C (Ex.1005, [0054]) and a “fingerprint sensor (5)” (Ex.1005, [0048]). Ex.1003, ¶55.

Mathiassen’s portable device executes software for biometrically authenticating the user and encrypting communications sent to external systems. Ex.1005, [0050], [0091]-[0095]; Ex.1003, ¶¶55-56.

In operation, “the network administrator...enroll[s] the user who will be the ‘owner’ of the portable device.” Ex.1005, [0061]-[0062]. The enrolled user may biometrically authenticate herself via the fingerprint sensor 5. Ex.1005, [0049], [0066]. The portable device compares a received fingerprint to a prestored fingerprint, called a “master minutia.” Ex.1005, [0050], [0072]. If they match, the user is authenticated. Ex.1005, [0073]. Mathiassen’s portable device then compiles and encrypts a message indicating successful authentication and sends it to a network. Ex.1005, [0051], [0074], [0076]-[0084] (describing encryption of communications after user authentication); Ex.1003, ¶¶57-60.

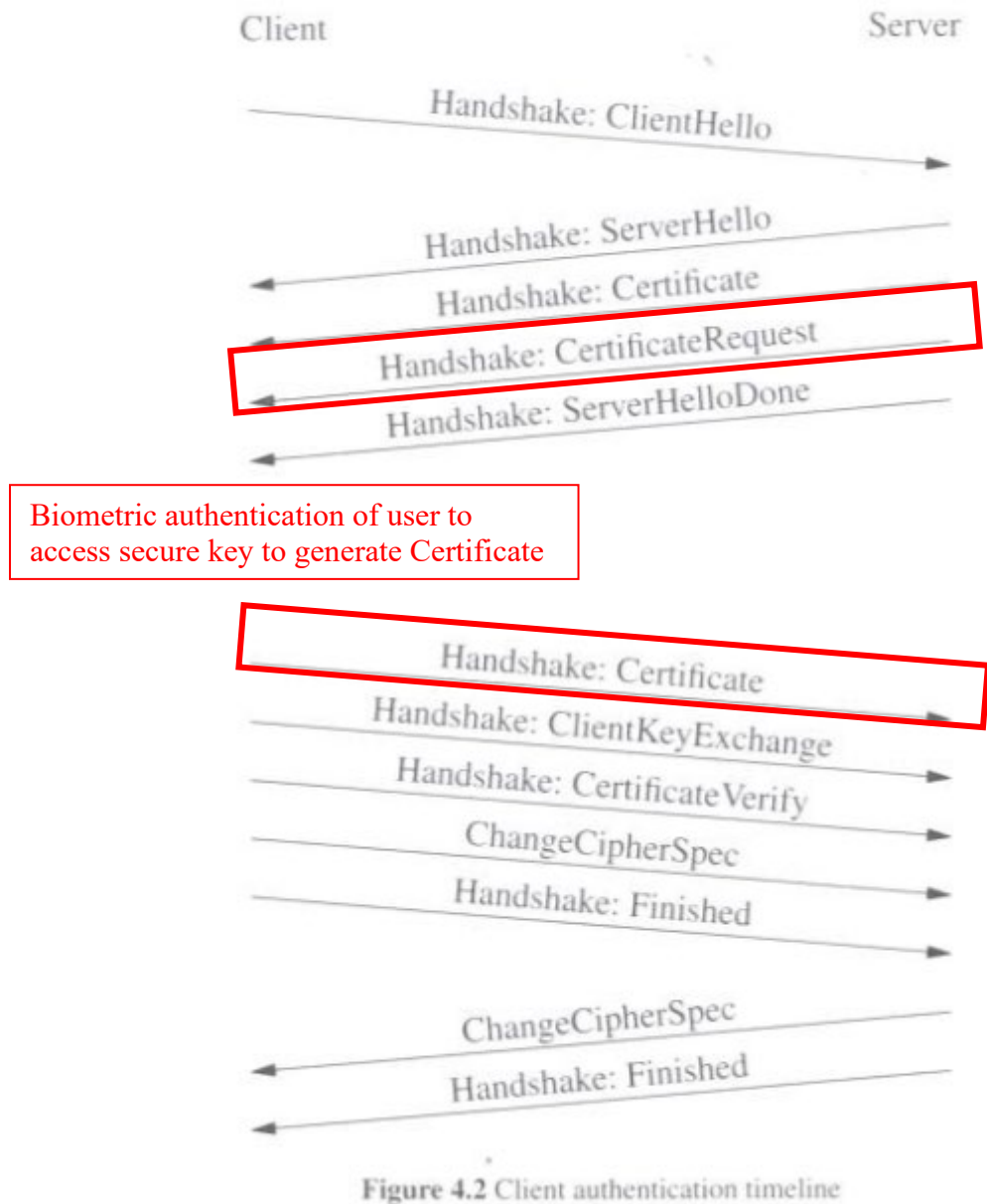
3. Motivation to Combine Rescorla with Mathiassen

A POSITA would have looked to Rescorla for information about how to implement secure two-way communication using SSL protocols, which was “by far the most widely deployed security protocol in the world” at the time. Ex.1015, xvii. Intending to enhance both security and convenience, a POSITA would have been further motivated to execute the client-side protocols of the SSL handshake described by Rescorla using a portable device, as described by Mathiassen, to enhance security through biometric authentication. Ex.1003, ¶¶61-71.

Rescorla shows that SSL protocols for securing communications were well known and widely implemented in the art. Ex.1015, xvii (describing prevalence of SSL). Rescorla explains that SSL protocols may be combined with biometric

authentication. Ex.1015, 153 (“biometrics add valuable security”). Rescorla explains that biometric authentication may be used to gain access to an encryption key “stored in trusted tamper-resistant hardware.” Ex.1015, 153. Mathiassen describes using biometric authentication in the same way. 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.”). Ex.1003, ¶¶62-64.

As explained in more detail below, the combination of Rescorla and Mathiassen would simply implement the steps of biometric authentication described by Mathiassen after the client receives Rescorla’s Handshake: CertificateRequest message and prior to sending its own Handshake: Certificate message, as illustrated in Rescorla, Figure 4.2, annotated below to illustrate the combination. *See* Ex.1015, 98; Ex.1003, ¶65.



Ex.1015, Fig. 4.2 (annotated and modified to illustrate combination)

Neither SSL protocols nor biometric authentication were new at the time of the '637 patent. Mathiassen acknowledges that a variety of handshake protocols had already been developed. Ex.1005, [0084] ("handshake procedures"). Those

handshake protocols included transmitting various requests and acknowledgments between the parties using any number of cryptographic techniques. Ex.1015, 98 (illustrating protocol messages); Ex.1005, [0094] (describing “any of the encryption methods at hand”). Portable devices with processing capabilities for authentication were also well known prior to the ’637 patent. Ex.1005, Fig. 2a (portable device with processor 2); Ex.1006, Fig. 1A (smart fob with processor module 106); Ex.1003, ¶¶66.

First, Rescorla is analogous art to the ’637 patent. The ’637 patent relates to enhancing online transaction security by biometrically authenticating a user and authenticating a website. Ex.1001, Abstract. Rescorla similarly pertains to handshake protocols to authenticate both the client-side and server-side of an online transaction. Ex.1015, 96 (“authenticat[ing]...the server” and “cryptographically authenticating the client”). Rescorla’s techniques can “be applied to a new application protocol with minimal modification” and specifically contemplates biometrics. Ex.1015, xvii, 153 (“Biometric authentication measures...are often used as secure access control measures.”). Thus, Rescorla is in the same field of endeavor (i.e., improving online transaction security by biometrically authenticating a user and authenticating a website). In addition, Rescorla is reasonably pertinent to a particular problem with which the inventor was involved (i.e., performing mutual authentication of a client/user and a server/website). Ex.1015, 96; Ex.1003, ¶¶67-68.

Mathiassen is also analogous art to the '637 patent. The '637 patent describes using a portable device for biometrically authenticating users. Ex.1001, Abstract. Mathiassen is in the same field of endeavor, as it pertains to a portable device for “allowing only authorized users access to” a network through biometric authentication. Ex.1005, Abstract. Thus, Mathiassen is in the same field of endeavor (i.e., improving online transaction security by biometrically authenticating a user). In addition, Mathiassen is reasonably pertinent to a particular problem with which the inventor is involved (i.e., implementing biometric authentication in a portable device for improving online transaction security). Ex.1005, Abstract; Ex.1003, ¶¶69.

Second, a POSITA would have been motivated to implement Rescorla’s handshake protocols using Mathiassen’s portable device. Using biometrics is more secure than passwords because “passwords...may intentionally be passed away to a third person, or unintentionally and illegally acquired.” Ex.1005, [0004]. And “there is a general consensus that biometrics access control is far more secure, and convenient.” Ex.1005, [0015]. However, the adoption of biometric authentication was inhibited by insufficient interoperability with no uniform standard. Ex.1005, [0012]. SSL is both highly adaptable, and widely adopted. Ex.1015, xvii. A POSITA would have implemented Mathiassen’s biometric authentication with a portable device to provide enhanced security and convenience with Rescorla’s SSL protocols for increased interoperability. Ex.1003, ¶70.

In addition, a POSITA would combine Mathiassen's teachings with Rescorla's handshake protocols because, in Mathiassen, biometric authentication is performed entirely within the portable device which does not require "the supplier of the network system architecture" to "make[] any decision on which biometrics standard" to adopt. Ex.1005, [0047]. This results in increased security, convenience, and adoption of biometric authentication. Ex.1005, [0047]-[0048]; Ex.1003, ¶71-72.

In addition, the universal nature of Mathiassen's portable device provides the advantage of adding biometric authentication to any standard device (i.e., one with a standard USB port). No specialized equipment would be required. Mathiassen's device provides biometric authentication even using public terminals. Ex.1005, [0065] ("an Internet Café or a Business Center"). 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, and is, therefore, not limited to any specific protocol. Ex.1005, [0095]; Ex.1003, ¶71.

Accordingly, the Rescorla-Mathiassen combination would have been the combination of prior art elements (SSL handshake protocols from Rescorla, performed by Mathiassen's portable device for biometrically authentication) according to known methods (implementing SSL handshake protocols "to a new application protocol with minimal modification," as taught by Rescorla (Ex.1015,

xvii)) to yield the predictable result of a portable device biometrically authenticating a user and authenticating a website, as taught by Rescorla. Ex.1015, 96; *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007); Ex.1003, ¶73.

Further, a POSITA would have had a reasonable expectation of success in implementing the handshake protocols described by Rescorla using Mathiassen’s portable device. Both Rescorla and Mathiassen disclose handshake protocols. Ex.1005, [0084] (Mathiassen’s portable device generates messages “in a predefined format and sequence (e.g., **handshake procedures**).”); Ex.1015, xvii (SSL/TLS handshake protocols). Mathiassen anticipates modifying its handshake sequences “according to the rules of secure communication of the...network or system (N).” Ex.1005, [0095]. Rescorla’s “*Secure Sockets Layer* (SSL) is by far the most widely deployed security protocol in the world.” Ex.1015, xvii. Meanwhile, one of Mathiassen’s goals is to promote interoperability with a variety of standard systems and protocols. Ex.1005, [0006] (“gain[ing] wide public acceptance”); Ex.1003, ¶74.

Similarly, Rescorla explains that modifying SSL protocols to fit any application would have involved routine skill in the art. Ex.1015, xvii (implementing SSL is simply “recognizing which pattern most closely matches the system” and “using the appropriate technique”); Ex.1003, ¶75.

Accordingly, a POSITA would have been motivated to modify Rescorla to perform client-side functions of an SSL/TLS handshake with Mathiassen's portable device. Ex.1003, ¶76.

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:*

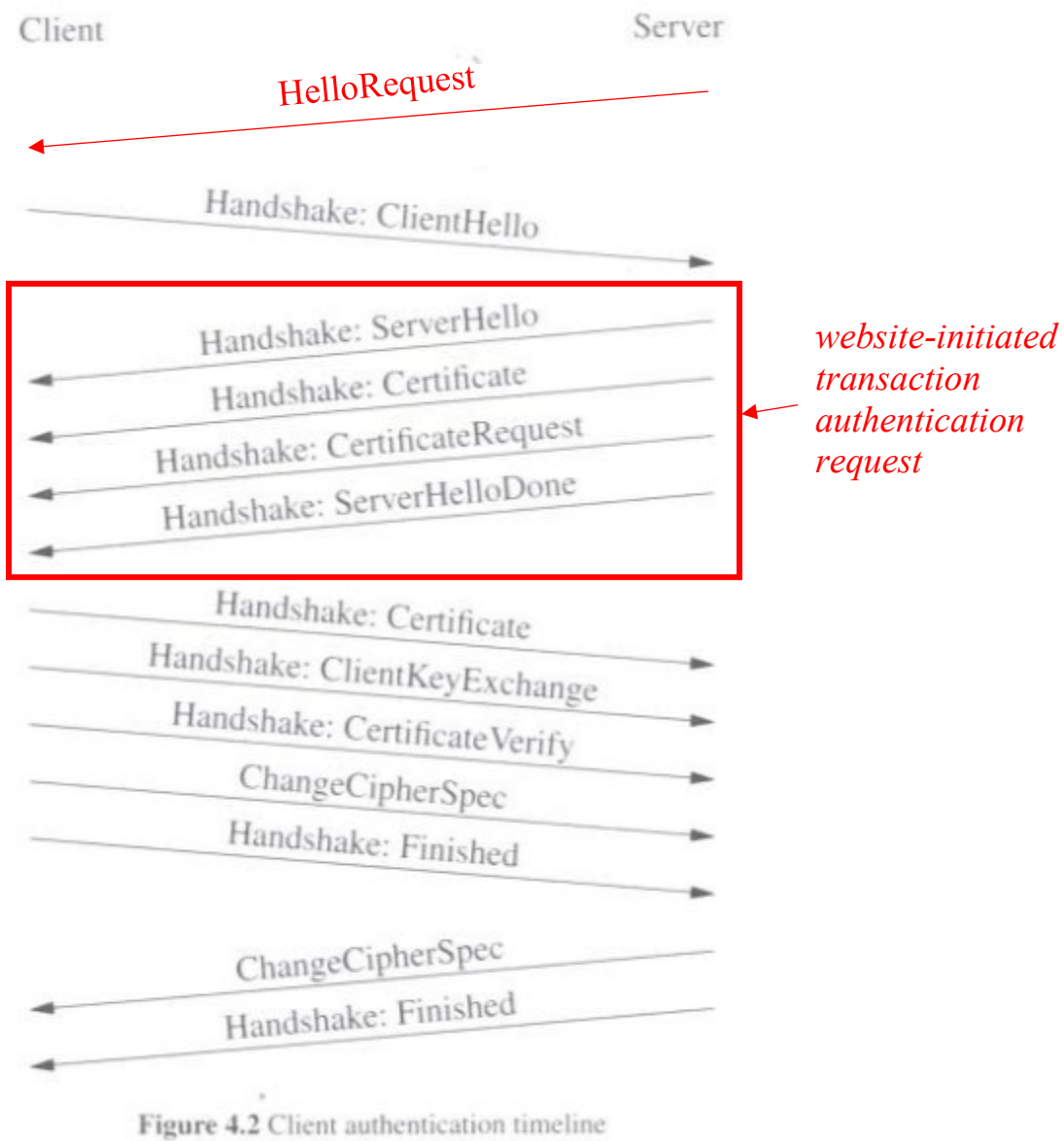
To the extent the preamble is limiting, Rescorla discloses or renders it obvious because Rescorla describes an SSL handshake for authenticating an online transaction between a website and a client initiated by the website server. Ex.1003, ¶77-79.

First, Rescorla describes “SSL for the Web” as a “process,” which discloses a *method*. Ex.1015, 51, 58 (a “handshake **process**”), 256, 413 (“SSL_**METHOD**”); Ex.1003, ¶77.

Second, Rescorla discloses or renders obvious a *website-initiated transaction authentication request*. Specifically, Rescorla describes standard handshake procedures by which a client and server are authenticated. Ex.1015, xvii. A server in Rescorla refers to a website because a client interacts with a server by accessing a website hosted by the server. Ex.1015, 293 (“It’s quite common for a single server...to host Web sites.”), 302 (describing servers hosting merchant websites),

202 (describing a “Server[] under Load” as a “Web site when a large number of people decide to request a page”), 232 (“references to servers must include the fact that it is a secure site”), 291; Ex.1003, ¶¶79.

To initiate transaction authentication, the server hosting a website sends a “HelloRequest” message to the client which causes the client to “send[] the ClientHello” message. Ex.1015, 326; Fig. 4.2 (annotated below to include the HelloRequest message initiating the handshake). After receiving the “ClientHello,” the server sends a “ServerHello” message with the “Certificate,” “CertificateRequest,” and “ServerHelloDone” messages, shown in Figure 4.2, below. Ex.1015, 98; Ex.1003, ¶79.



Ex.1015, Fig. 4.2 (annotated)

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. As shown in more detail hereafter, these messages are *receiv[ed]* by the client. §VII.A.4.a,[7.1.1]. The

Certificate message is *for cryptographically confirming the web site's identity*. §VII.A.4.a,[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*. §VII.A.4.a [7.1.3], [7.1.4]. Because this protocol is initiated by the website first sending the HelloRequest message, this *transaction authentication request* is *website-initiated*. Ex.1003, ¶80.

Thus, the claimed *website-initiated transaction authentication request* includes the following messages in Rescorla:

- Handshake: ServerHello
- Handshake: Certificate,
- Handshake: CertificateRequest, and
- Handshake: ServerHelloDone.

Ex.1003, ¶80.

Third, Rescorla discloses *securely processing and responding to* [the] *website-initiated transaction authentication request*. Rescorla discloses securely processing and responding to the ServerHello, Certificate, CertificateRequest, and ServerHelloDone messages. Regarding the Certificate message, Rescorla explains:

The 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; Ex.1003, ¶¶81-82.

Extracting the public key and generating and encrypting the pre_master_secret discloses *securely processing* the Certificate message because a public key is extracted 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 because it is sent in response to the Certificate message. Ex.1015, 58. The client also *securely process[es] and respond[s]* to the CertificateRequest message by providing its own certificate via the Certificate and CertificateVerify messages. §VII.A.4.a,[7.1.3], Ex.1015, Fig. 4.2; Ex.1003, ¶83.

Thus, Rescorla discloses or renders obvious a process (*method*) for extracting public keys, and generating, encrypting, and sending a pre_master_secret in response to receiving ServerHello, Certificate, CertificateRequest, and ServerHelloDone messages (*securely processing and responding to a website-initiated transaction authentication request*). Ex.1003, ¶84.

[7.1.1] (1) receiving in a customer authentication apparatus said website-initiated transaction authentication message⁴

Rescorla and Mathiassen render obvious limitation [7.1.1] because Rescorla discloses a client receiving ServerHello, Certificate, CertificateRequest, and ServerHelloDone messages (a *transaction authentication message*), and a POSITA would have been motivated to implement Rescorla's SSL protocol such that these messages would be received by Mathiassen's portable device (*receiving in a customer authentication apparatus*). Ex.1003, ¶85.

Rescorla explains that the ServerHello, Certificate, CertificateRequest, and ServerHelloDone messages are received by the client (a portable device such as Mathiassen's in the combination) illustrated in Figure 4.2 below. Ex.1003, ¶¶86-87.

⁴ Petitioner presumes that “*said website-initiated transaction authentication message*” in limitation [7.1.1] refers to the “*website-initiated transaction authentication request*” in limitation [7.0].

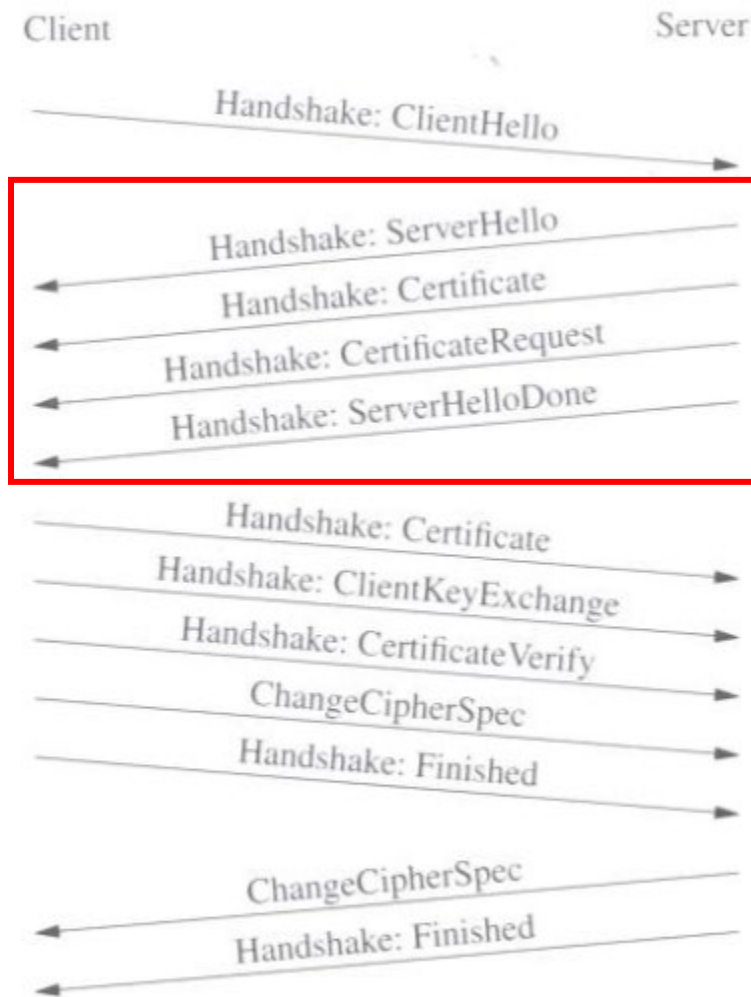


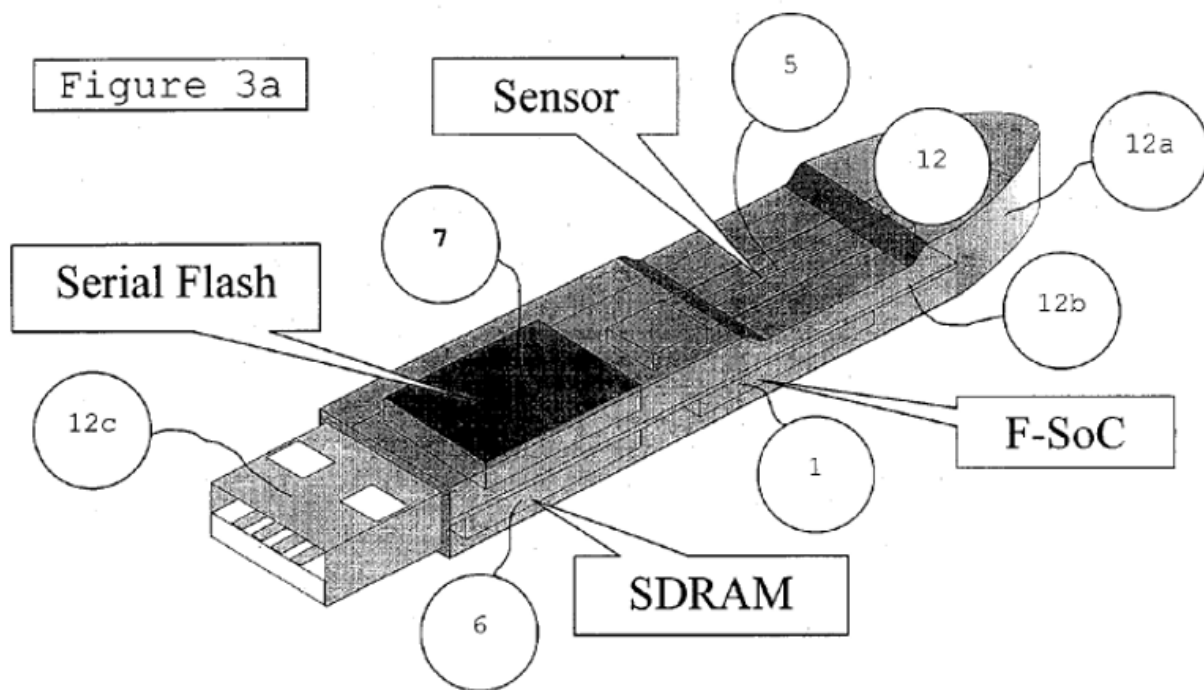
Figure 4.2 Client authentication timeline

Ex.1015, Fig. 4.2 (annotated)

Thus, Rescorla explains that the client receives each of the ServerHello, Certificate, CertificateRequest, and ServerHelloDone messages (*receiving...said website-initiated transaction authentication message*). Ex.1003, ¶88.

In addition, as described in the motivation-to-combine section above (§VII.A.3), a POSITA would have been motivated, based on the teachings of

Mathiassen, to implement the handshake protocols described in Rescorla with Mathiassen's portable device. Mathiassen's portable device is a *customer authentication apparatus*. Ex.1003, ¶84. Mathiassen describes a "portable device." Ex.1005, Abstract. Mathiassen's portable device is depicted in Figure 3a, below. Ex.1003, ¶89.



Ex.1005, Fig. 3a

Mathiassen's portable device⁵ is a *customer authentication apparatus* because it authenticates a user with a "fingerprint sensor (5)." Ex.1005, [0048], [0050]

⁵ For brevity, Petitioner refers to Mathiassen's "portable or embedded access device" as a "portable device."

(“fingerprint representations...are compared...with master fingerprint representations” to identify “a positive match”). As described above in §VII.A.3, a POSITA would have been motivated to implement SSL/TLS handshake protocols described by Rescorla in Mathiassen’s portable device. Ex.1003, ¶90.

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 and is not limited to any specific protocol. Ex.1005, [0095]. Meanwhile, SSL handshake sequences are “the most widely deployed security protocol in the world.” Ex.1015, xvii. Therefore, a POSITA would have used Mathiassen’s portable device to perform Rescorla’s SSL handshake sequences. §VI.A.3; Ex.1003, ¶¶91-92.

Thus, Rescorla and Mathiassen render obvious receiving by Mathiassen’s portable device (*receiving in a customer authentication apparatus*) the ServerHello, Certificate, CertificateRequest, and ServerHelloDone messages described by Rescorla (*said website-initiated transaction authentication message*). Ex.1003, ¶93.

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

Rescorla and Mathiassen render obvious limitation [7.1.2] because Rescorla explains how the client (a portable device like Mathiassen’s in the combination) uses the Certificate message (part of the *website-initiated transaction authentication message*) to authenticate the website server. Ex.1003, ¶94.

Rescorla's SSL procedures are used for cryptographically verifying a website (for cryptographically confirming the web site's identity) via the Certificate message in Figure 4.2, below. Ex.1003, ¶95.

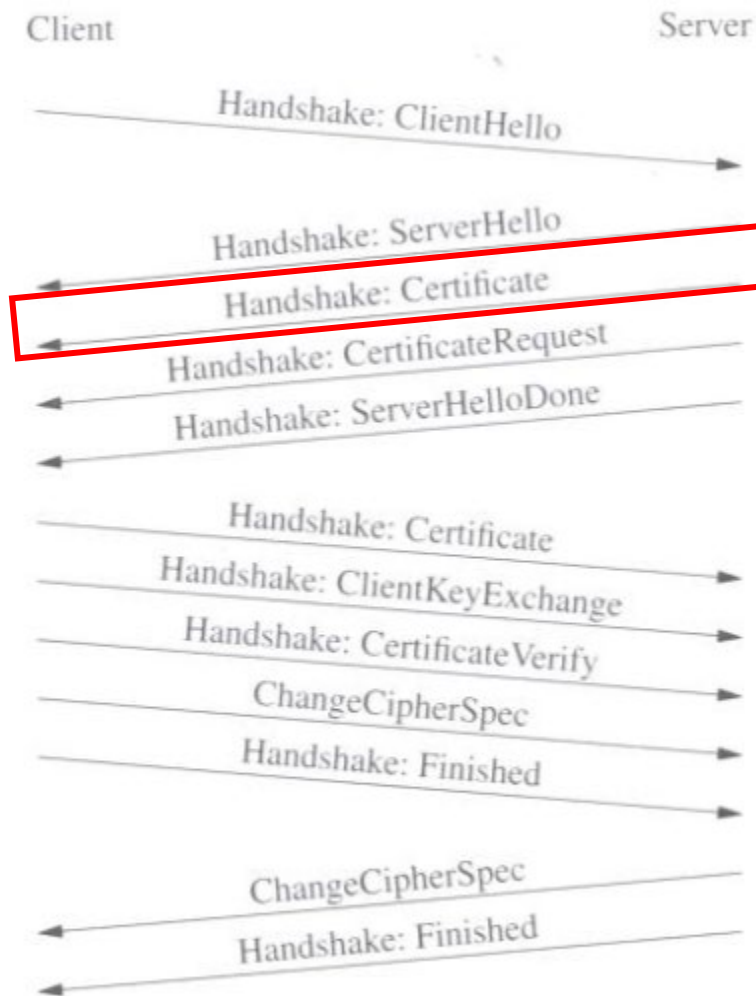


Figure 4.2 Client authentication timeline

Ex.1015, Fig. 4.2 (annotated)

The server “sends its certificate in the Certificate message.” Ex.1015, 60. The server’s “certificate contain[s] the server’s public key [and] provides the server’s identity for authentication purposes.” Ex.1015, 58. To verify the certificate, the client compares the identity of the server in the certificate to an “expected identity” that is “already...known to the client.” Ex.1015, 156. “[T]he expected identity” must “match the identity in the certificate.” Ex.1015, 156. This exchange of certificates between the website and client is part of establishing a cryptographic connection. *See* Ex.1015, 9-12. Thus, Rescorla’s Certificate message (part of the *website-initiated transaction authentication message*) sends the server’s certificate for cryptographic verification and is for *cryptographically confirming the web site’s identity*. Ex.1003, ¶¶96-97.

A POSITA would have been motivated to use Mathiassen’s portable device to perform website authentication. Mathiassen describes how its portable device may be used for “PKI [public key infrastructure] verification.” Ex.1005, [0082], [0012] (“PKI system with electronic certificates”), [0050] (“PKI biometrics verification and hand-shake sequences”). A portable device capable of performing PKI verification via electronic certificates would readily perform the steps of website authentication described by Rescorla. Ex.1003, ¶98; *see* §VII.A.3.

In addition, a POSITA would have had a reasonable expectation of success in authenticating a website’s identity with a portable device. Ex.1003, ¶99 (discussing

Ex.1006, [0249] (describing using a portable device to prevent “viruses, worm, spam and Internet ‘phishing’ fraud”), Ex.1021, Abstract, [0033] (describing “a personal authentication token” for “mutually authenticat[ing] senders and/or recipients of electronic transactions”)).

Thus, Rescorla and Mathiassen render obvious a portable device that receives a Handshake: Certificate message (part of the *website-initiated transaction authentication message*) including a website’s certificate for verifying website authentication (*for cryptographically confirming the web site’s identity*). Ex.1003, ¶100.

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

Rescorla and Mathiassen render obvious limitation [7.1.3] because Rescorla describes how the client (Mathiassen’s portable device in the combination) sends a Certificate message to the website server in response to a CertificateRequest (part of the *website-initiated transaction authentication message*). Further, Rescorla and Mathiassen describe accessing encryption keys using biometric authentication, such that the Certificate message sent by the portable device would indicate *biometric authentication*. Ex.1003, ¶101.

As shown in Figure 4.2 below, Rescorla's CertificateRequest message *requests...a corroborating response* (the Certificate and CertificateVerify messages) from the client to authenticate the client. Ex.1003, ¶¶102-103.

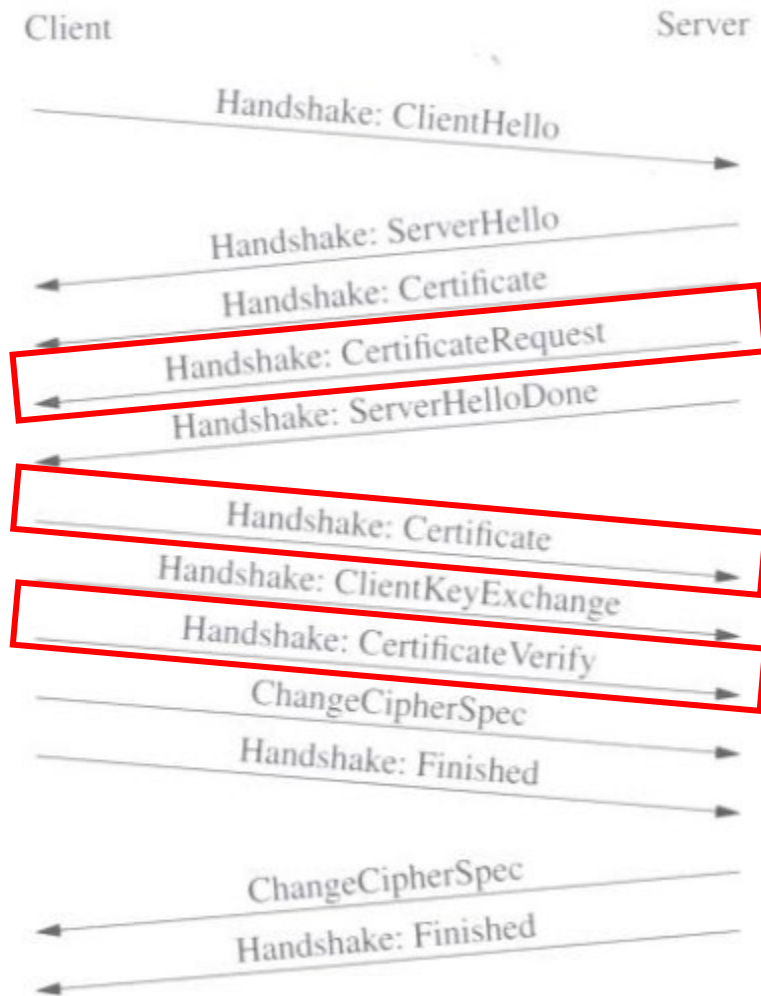


Figure 4.2 Client authentication timeline

Ex.1015, Fig. 4.2 (annotated)

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; Ex.1003, ¶¶104-105.

Thus, Rescorla’s CertificateRequest message, which is part of a *website-initiated transaction authentication message*, requests a *corroborating response* in the form of the Certificate and/or CertificateVerify messages. Ex.1003, ¶106.

The Certificate and CertificateVerify messages are used for *authentication of an enrolled customer*. Rescorla explains that “[t]he CertificateVerify does all the actual work of client authentication.... 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, 108, (the client “sends its certificate and the CertificateVerify message to authenticate itself”); Ex.1003, ¶107.

In the combination, a POSITA would have been used Rescorla’s teaching of requesting the Certificate and CertificateVerify messages from Mathiassen’s portable device (*requesting said apparatus provide a corroborating response including a biometric authentication*). For example, Rescorla discloses the use of biometrics with its system: “biometrics add valuable security.” Ex.1015, 153. While Rescorla advises against using biometrics to create the encryption key due to the variation of data obtained by a biometric input device, Rescorla expressly states that

a biometric is well-suited “to control access” while “the key is stored in trusted tamper-resistant hardware.” Ex.1015, 153; Ex.1003, ¶¶63, 108.

Mathiassen teaches using biometrics to access encryption keys, or seeds⁶ used to generate encryption keys, just as Rescorla advises. Ex.1005, [0050] (“Access to such extended encryption will be given to the user **pending a positive match** of his fingerprint with an authorized fingerprint.”), [0076] (“When the central processor (2) has established a positive match..., [t]he general algorithm will generate the secure key”). In addition, the request for authentication described in Rescorla-Mathiassen is of an *enrolled customer*. See Ex.1005, [0060]-[0062] (describing initial enrollment of user). Thus, Rescorla and Mathiassen render obvious *a biometric authentication of an enrolled customer*. Ex.1003, ¶109.

Finally, in the combination, the corroborating response to the CertificateRequest would include a biometric authentication of the user. Ex.1003, ¶110. For example, Mathiassen describes the contents of the message sent from its portable device to the external server to indicate user authentication. Ex.1005, [0078]-[0083]. This response includes, in part, “[t]he secure key number,” and “PKI verification in encrypted format.” Ex.1005, [0080], [0082]. This message is generated only “if a positive match of the captured fingerprint with the fingerprint

⁶ A seed is used to create an encryption key. See Ex.1005, [0050], [0076].

representation...is obtained.” Ex.1005, [0085]. The receiving server then “retrieve[s] the particular seed issued to the user, during enrolment” and inputs the seed into the “secure key generation algorithm SKG on the server” to verify the user. Ex.1005, [0087]; Ex.1015, 84-85 (describing using seeds for key generation); Ex.1003, ¶110.

A POSITA would have been motivated to biometrically control access to the secure key using Mathiassen’s portable device and then use the key to authenticate the user to the server. §VII.A.3. Rescorla expressly contemplates just such an arrangement. Ex.1015, 153; Ex.1003, ¶111.

Thus, Rescorla and Mathiassen describe sending a CertificateRequest message, part of the *website-initiated transaction authentication message*, to the portable device requesting Certificate and CertificateVerify messages for user authentication (*requesting said apparatus provide a corroborating response*) and the portable device providing an encrypted response after biometric authentication of the user of the device (*including a biometric authentication of an enrolled customer*). Ex.1003, ¶112.

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

Rescorla and Mathiassen render obvious limitation [7.1.4] because Mathiassen describes cryptographically encapsulating a message to a server

confirming user authentication in response to the CertificateRequest message, and a POSITA would have been motivated to cryptographically encapsulate the Certificate and CertificateVerify messages. Ex.1003, ¶113.

Mathiassen describes cryptographically encapsulating a response referred to as a “message/communication.” Ex.1005, [0077] (“encryption of a message/communication”). As explained at [7.1.3], it would have been obvious for the Certificate and/or CertificateVerify messages of Rescorla to be generated as a corroborating response after authentication of the user. Ex.1003, ¶114.

Rescorla further explains that the Certificate and/or CertificateVerify messages are used to verify the identity of the client. §VII.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. §VII.A.4.a,[7.1.3]; Ex.1003, ¶115.

Therefore, in the combination, it would have been obvious to cryptographically encapsulate Rescorla’s Certificate/CertificateVerify messages using the encryption described in Mathiassen. Ex.1005, [0077]-[0083] (describing “encryption of a message/communication” indicating successful biometric authentication); Ex.1003, ¶116.

In addition, because Rescorla’s Certificate/CertificateVerify messages are used to verify the client (Ex.1015, 111, 108) and Mathiassen’s “message/communication” is generated only after the user is biometrically

authenticated (Ex.1005, [0074]-[0077]), these messages *originate[] from a legitimate customer*, and the encapsulation of the message is done *in order to prove that said response originates from a legitimate customer*. Ex.1003, ¶116.

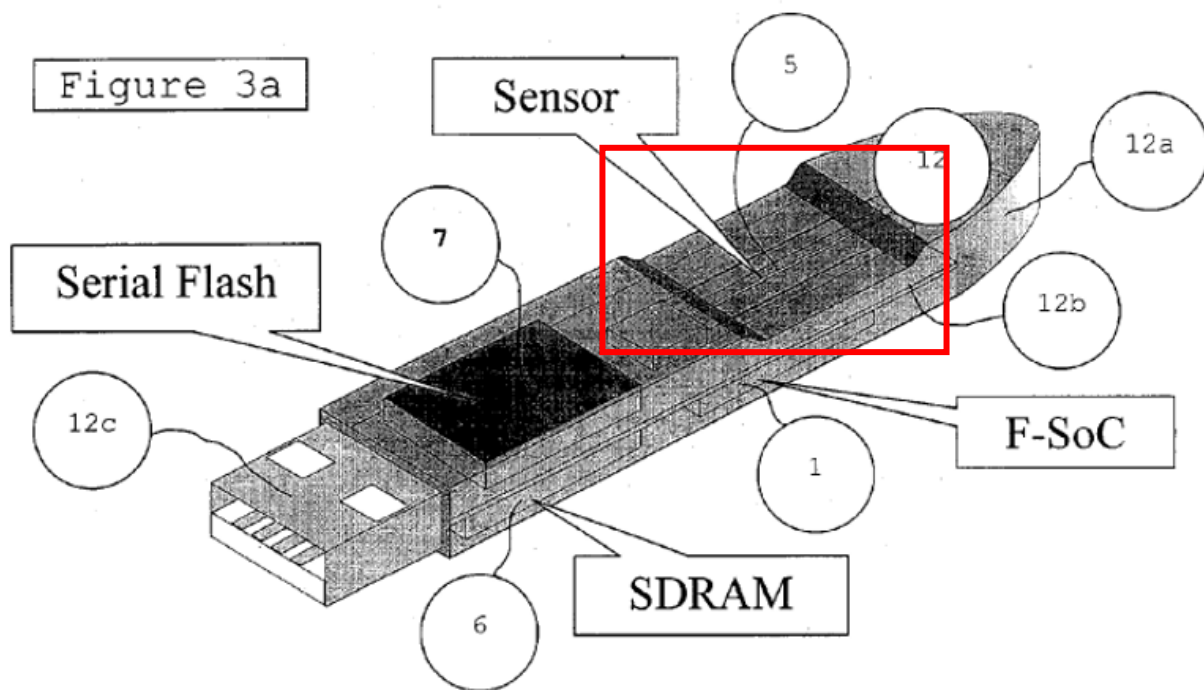
Thus, Rescorla and Mathiassen describe encrypting the Certificate and/or CertificateVerify messages (*including a cryptographic encapsulation of said response*) which verify the identity of the user (*in order to prove that said response originates from a legitimate customer*). Ex.1003, ¶117.

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

Rescorla and Mathiassen render obvious limitation [7.2] because Mathiassen describes biometrically authenticating the user before transmitting a confirmation of user authentication to the server, and, in the Rescorla-Mathiassen combination, a POSITA would have been motivated to implement biometric authentication before Rescorla's Certificate and CertificateVerify messages are transmitted. Ex.1003, ¶118.

As explained in limitation [7.1.3], Rescorla discloses the use of biometric verification to “control access” to keys for encryption of a message indicating user authentication. Ex.1015, 153. Mathiassen provides details regarding biometric authentication. Ex.1003, ¶119.

Specifically, Mathiassen's portable device includes a subset of administrative software referred to as a "matching algorithm" for fingerprint authentication. Ex.1005, [0072]. The fingerprint sensor 5 of the portable device, shown in Figure 3a below, captures "raw images" of a fingerprint. Ex.1005, [0049]-[0050]; Ex.1003, ¶120.

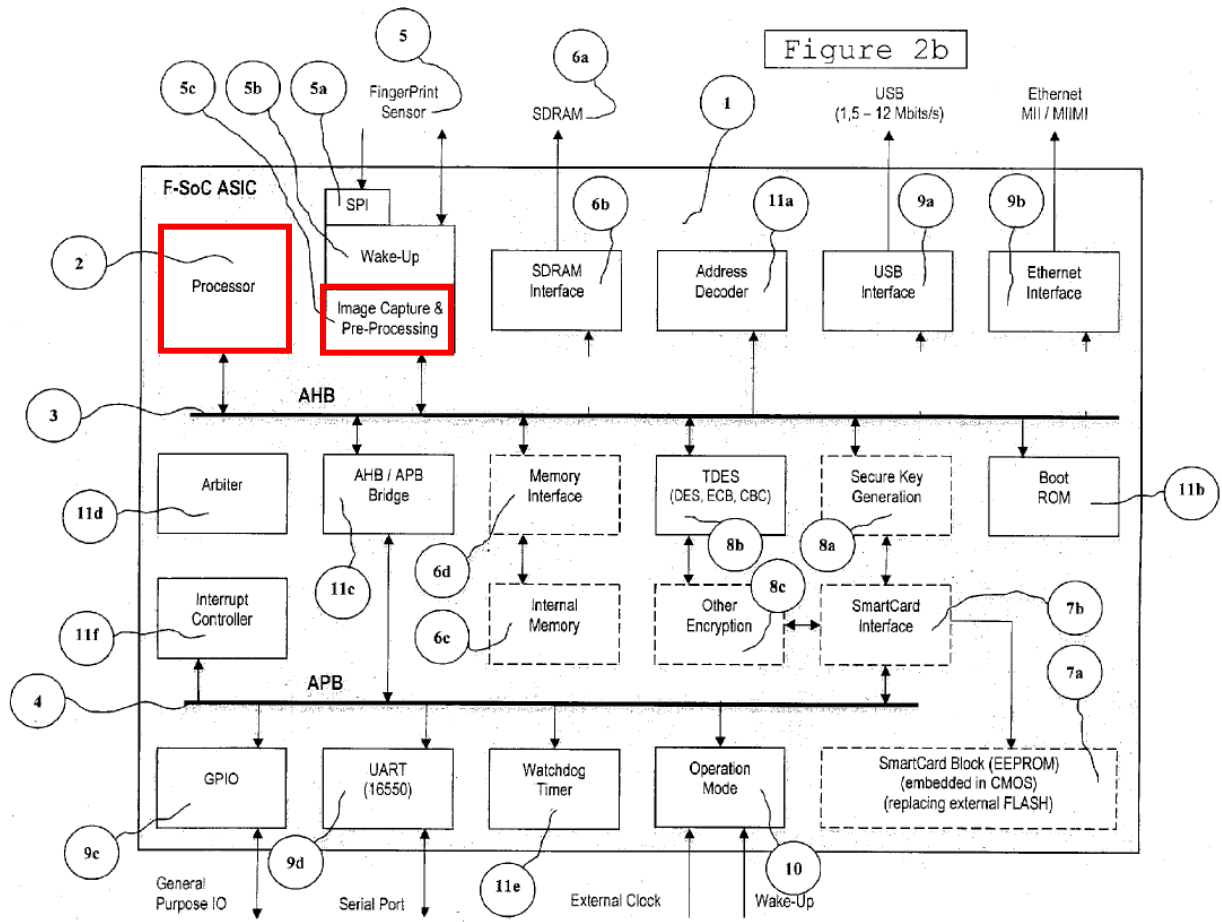


Ex.1005, Fig. 3a (annotated)

The portable device includes an integrated circuit 1 illustrated in Figure 2b, shown below. The fingerprint sensor 5 receives a fingerprint. Ex.1005, [0049]. The pre-processing block 5C processes the fingerprint and converts it into "intermediate results." Ex.1005, [0049]. The processor 2 then executes the matching algorithm which compares the intermediate results "with master fingerprint representations."

Ex.1005, [0049]-[0050]. If there is a match, the user is biometrically authenticated.

Ex.1005, [0050]; Ex.1003, ¶¶121-122.



Ex.1005, Fig. 2b (annotated)

Thus, Mathiassen discloses or renders obvious *biometrically authenticating said customer by said customer authentication apparatus*. Ex.1003, ¶¶121-122.

This biometric authentication occurs before sending the response to the external server. Ex.1005, [0050] (“Access to such extended encryption will be given to the user **pending a positive match** of his fingerprint.”); Ex.1003, ¶¶123-124.

Thus, the Rescorla-Mathiassen combination renders obvious *biometrically authenticating said customer by said customer authentication apparatus prior to transmitting said response to said request*. Ex.1003, ¶125.

[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;

Rescorla and Mathiassen render obvious limitation [7.3] because Mathiassen describes biometrically authenticating the user before transmitting a cryptographically encapsulated confirmation of user authentication to the server, and a POSITA would have been motivated to implement biometric authentication in the Rescorla-Mathiassen combination before Rescorla's Certificate and CertificateVerify messages are transmitted. Ex.1003, ¶126.

In Mathiassen, an output indicating successful biometric authentication is only generated after the user is authenticated:

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]; Ex.1003, ¶127.

Mathiassen also 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]. The portable device first biometrically authenticates the user via the fingerprint scanner (Ex.1005, [0065]-[0073]) and then encrypts the “message/communication” as “[o]ne result of” successful biometric authentication (Ex.1005, [0074]-[0077]). Ex.1003, ¶128.

Thus, Rescorla and Mathiassen disclose or render obvious generating and encrypting a message/communication (*performing said cryptographic encapsulation of said response by said customer authentication apparatus*) after successful biometric authentication (*only after successful completion of said biometric authentication of said customer using fingerprint biometrics*). Ex.1003, ¶129.

[7.4] (4) transmitting said response to said request; and

Rescorla and Mathiassen render obvious limitation [7.4] because Rescorla describes transmitting the Certificate and CertificateVerify messages. Ex.1003, ¶130.

In Rescorla, the Certificate and CertificateVerify messages are transmitted from the client to the server, as shown in Figure 4.2 below. Ex.1015, 97 (“The client responds by sending a Certificate message...and a CertificateVerify message.”); Ex.1003, ¶131.

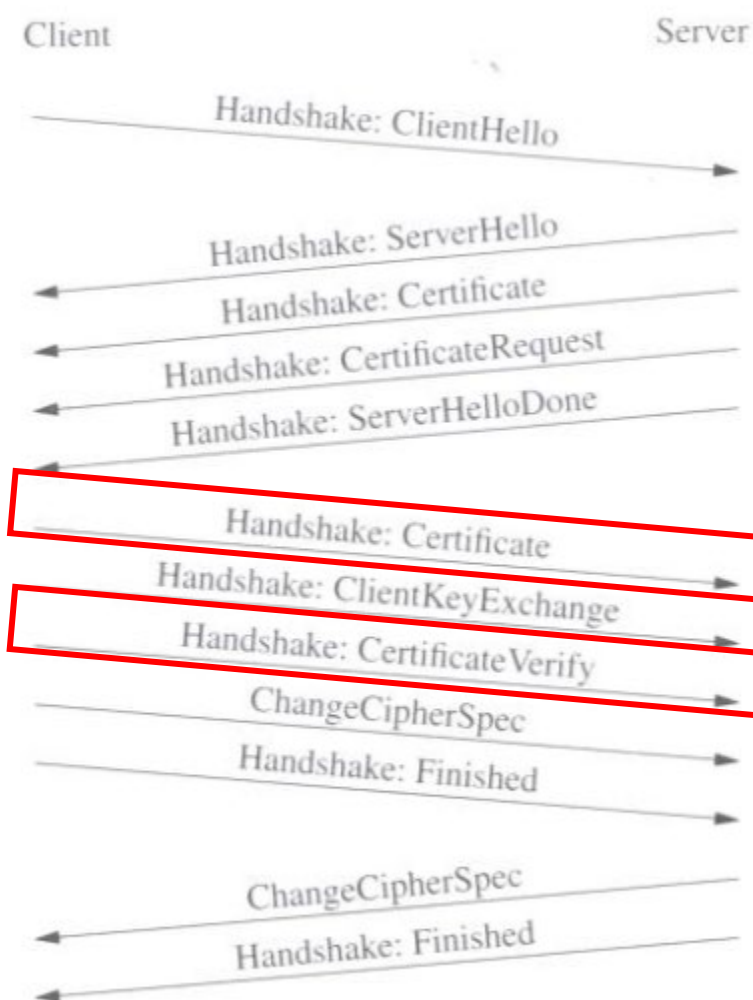


Figure 4.2 Client authentication timeline

Ex.1015, Fig. 4.2 (annotated)

Similarly, Mathiassen discloses “transferr[ing]” its “message/communication.” Ex.1005, [0084]; Ex.1003, ¶132.

Thus, the Rescorla-Mathiassen combination renders obvious the client transmitting Rescorla’s Certificate and CertificateVerify messages to the server, which would indicate successful biometric authentication of the user as described by

Mathiassen's message/communication to the server, which teaches *transmitting said response to said request*. Ex.1003, ¶133.

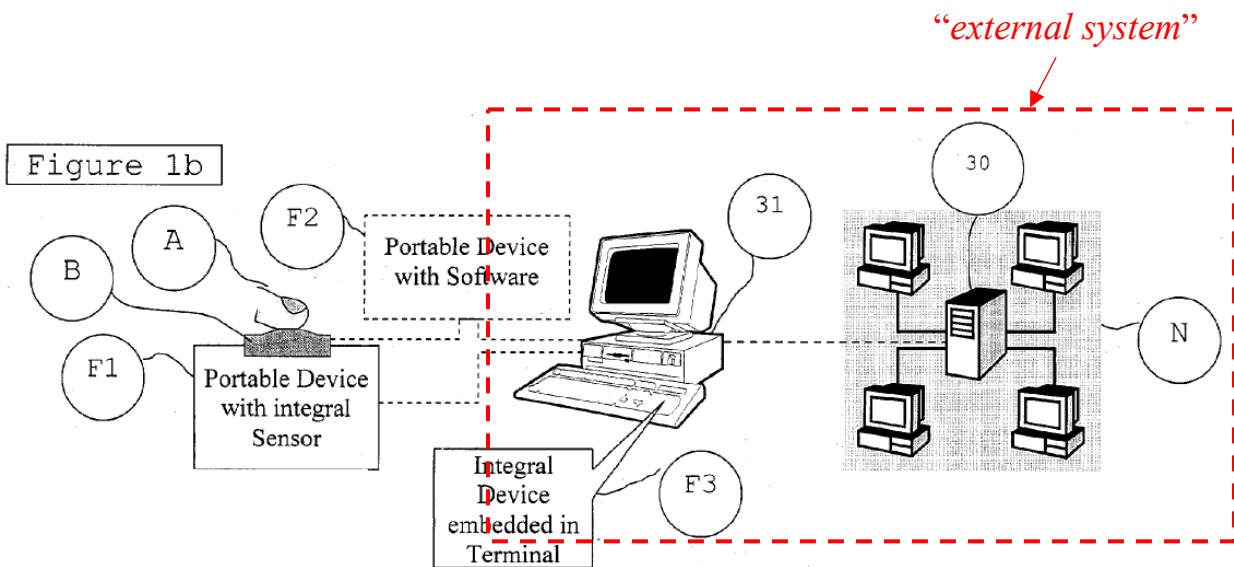
[7.5] (5) verifying by at least one of said website and at least one external system that said response satisfactorily authenticates said customer.

Rescorla and Mathiassen render obvious limitation [7.5] because Rescorla explains how the website server uses the Certificate and CertificateVerify messages to ensure that the client was authenticated. Ex.1003, ¶134.

As explained at [7.1.4], the Certificate and CertificateVerify messages are used for *authentication of an enrolled customer*. §VII.A.4.a,[7.1.3]. Rescorla explains that “sending the Certificate message...and the CertificateVerify message” is how the client “authenticate[s] itself.” Ex.1015, 108; Ex.1015, 111 (“The CertificateVerify does all the actual work of client authentication.”). Thus, Rescorla explains *verifying...that said response satisfactorily authenticates said customer*. Ex.1003, ¶135.

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. As explained at [7.0], the server described in Rescorla includes a *website*. Ex.1015, 202 (describing “Servers under Load” as a “Web site”), 232 (describing the server as a “secure site”); §VII.A.4.a,[7.0]; Ex.1003, ¶136.

Mathiassen also confirms that a website is part of *at least one external system*. For example, Mathiassen's Figure 1b illustrates how a portable device communicates with a "network (N)" that includes multiple "server(s) (30)." Ex.1005, [0051]; Ex.1003, ¶137.



Ex.1005, Fig. 1b (annotated)

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*. Ex.1003, ¶138.

To the extent the *external system* is a system separate from the *website* or the server that hosts the website, a POSITA would have understood that Rescorla teaches this scenario as well. Rescorla describes the use of "Key Distribution

Centers,” a known way for a “trusted third party” to “authenticate other parties.” Ex.1015, 8. Rescorla explains that a key distribution center is “a secure machine somewhere on the network” that retains keys on behalf of senders and receivers of a transaction. Ex.1015, 8. Thus, the key distribution center described by Rescorla is an external system, separate from the website, for *verifying...that said response satisfactorily authenticates said customer*. See also Ex.1006, [0245] (explaining that “[t]he client user can be authenticated by the ISP or **by a trusted third party**”); Ex.1003, ¶¶137-138.

Thus, Rescorla and Mathiassen render obvious *verifying by at least one of said website and at least one external system that said response satisfactorily authenticates said customer*. Ex.1003, ¶139.

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.

Rescorla and Mathiassen render obvious claim 8 because Mathiassen describes including a device number, IP address, and user ID in the cryptographically encapsulated message. In the proposed combination, that message corresponds to Rescorla’s Certificate and/or CertificateVerify messages. Ex.1003, ¶140.

As explained at [7.3], Mathiassen discloses *performing cryptographic encapsulation of said transaction authentication response*⁷ by said customer authentication apparatus. §VII.A.4.a,[7.3]. Mathiassen further explains that the transaction authentication response includes an identification of the portable device. Ex.1003, ¶141.

Mathiassen describes several “elements” included in the “message/communication” sent to the server that *explicitly identify*[] the portable device, 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]). A POSITA would have included such elements with the Certificate and/or CertificateVerify messages to ensure that the correctly assigned portable device was used for authentication. Ex.1003, ¶142.

Thus, Rescorla and Mathiassen render obvious *explicitly identifying said customer authentication apparatus*. Ex.1003, ¶143.

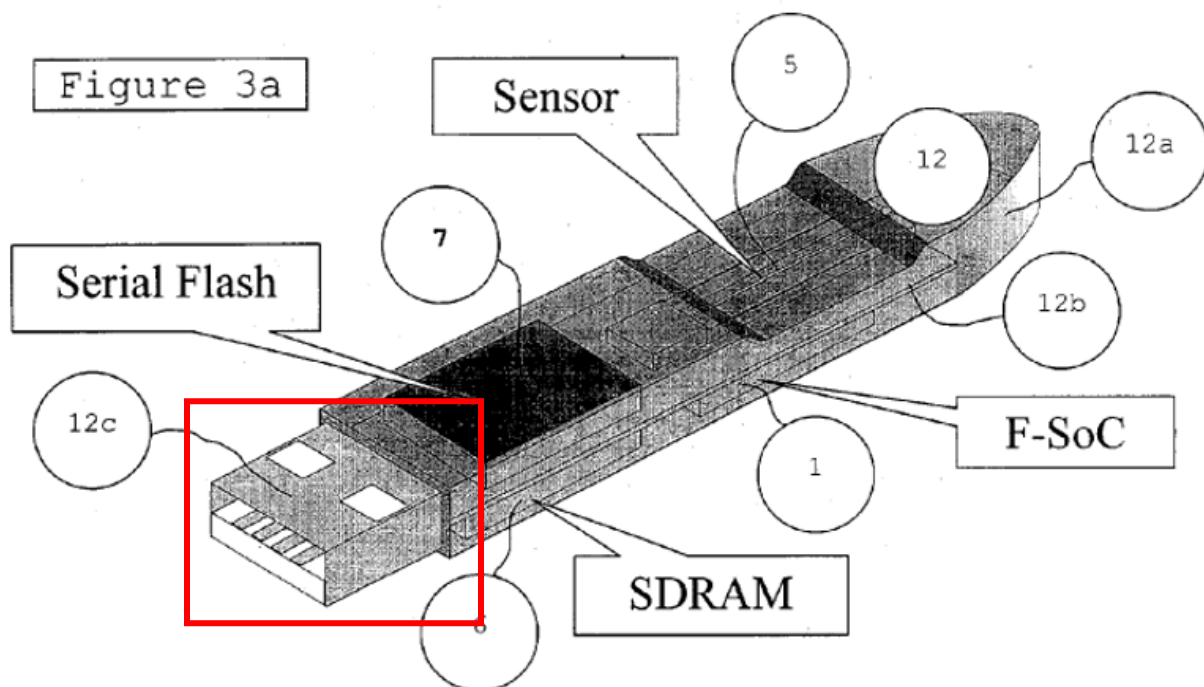
⁷ [T]ransaction authentication response lacks antecedent basis. For purposes of this petition, petitioner assumes it refers to “said response” from [7.3].

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.

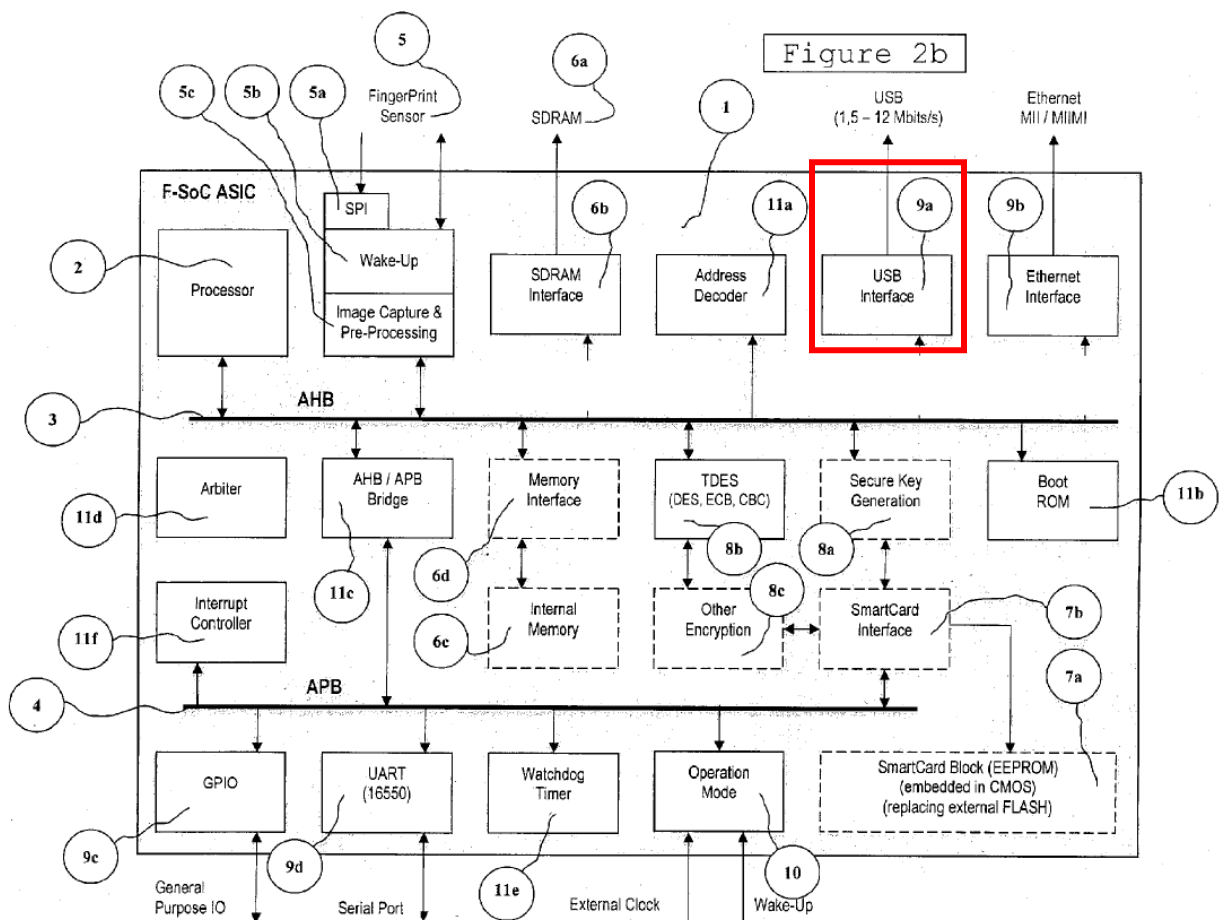
Rescorla and Mathiassen render obvious limitation [9.0] because, in the combination, the Certificate and CertificateVerify messages described in Rescorla (*said transaction authentication response*) would be transmitted to the website server via the USB interface described in Mathiassen. Ex.1003, ¶144.

Mathiassen discloses a “USB interface (12C)” which is *an external interface connector*. Ex.1005, [0054]; Ex.1003, ¶145.



Ex.1005, Fig. 3a (annotated)

Mathiassen's device also includes "second interface blocks (9A, 9B, 9C, or 9D)" that "support...the USB mechanical interface (12C)." Ex.1005, [0054], [0050], Fig. 2b; Ex.1003, ¶146.



Ex.1005, Fig. 2b (annotated)

Interface block 9A facilitates "transferring data to other devices and networks (N)." 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 (Mathiassen's portable device). Ex.1003, ¶147.

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*). Mathiassen describes a “user...insert[ing] the portable device (12 or 13) into the USB port” of a computer. Ex.1005, [0065]. After the user is authenticated, an encrypted response is “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]; Ex.1003, ¶148.

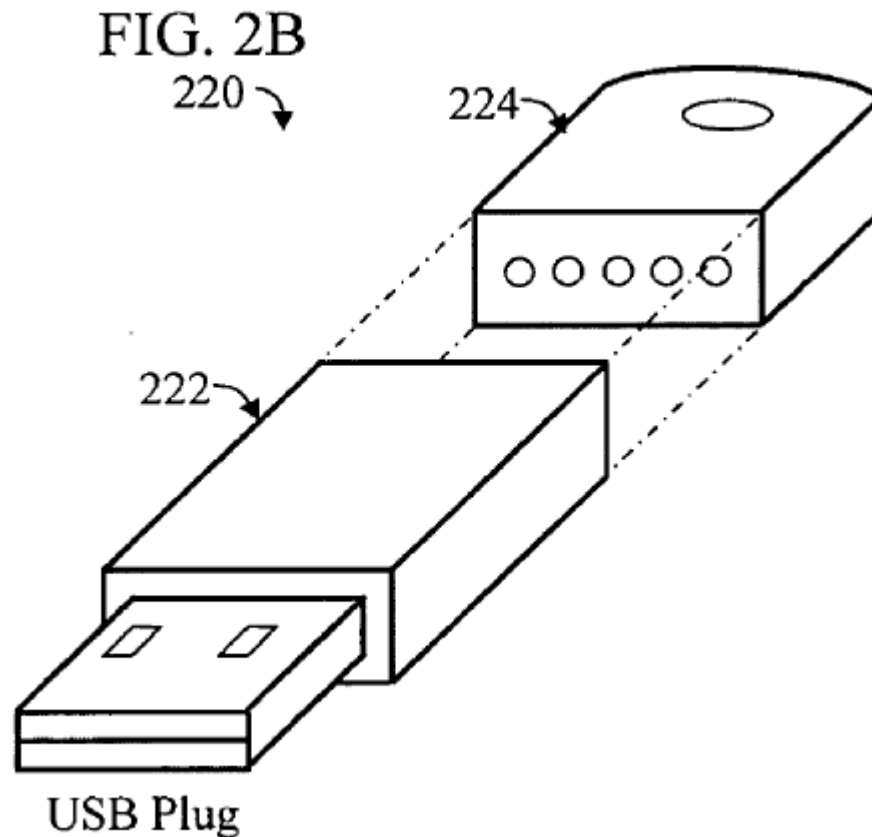
Thus, Rescorla and Mathiassen render this limitation obvious. Ex.1003, ¶149.

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

1. Overview of Ryan

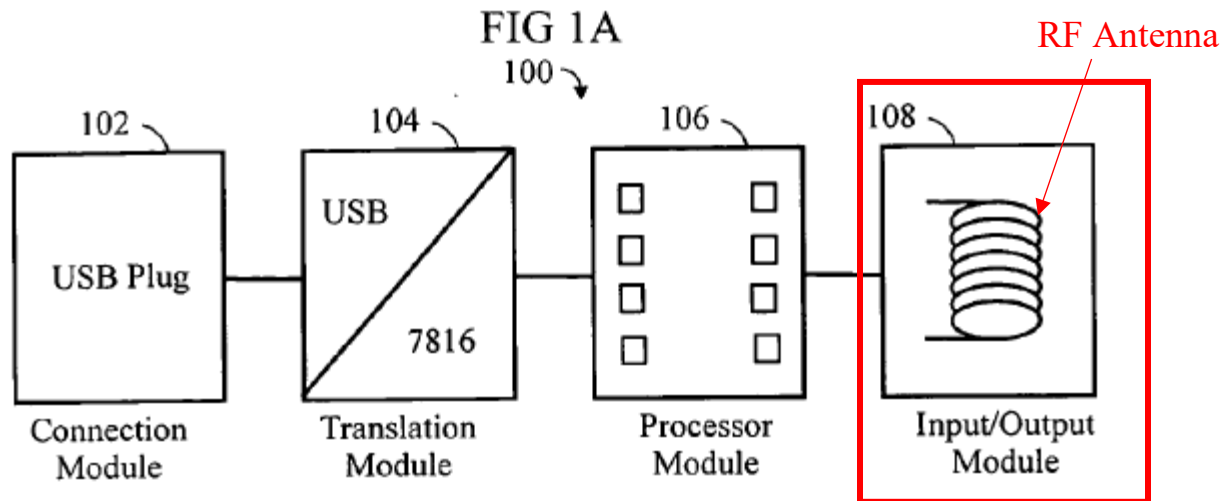
Ryan describes a “compact personal token apparatus” similar to Mathiassen's portable device and the '637 patent's ITA apparatus. Ex.1006, Abstract. Ryan refers to its apparatus with a number of terms, but for purposes of this petition, it will be

referred to as a “smart fob.” Ex.1006, [0149]. One embodiment is shown in Figure 2B. Ex.1003, ¶150.



Ex.1006, Fig. 2B

Ryan’s smart fob includes a “first physical module 222” including a USB plug. Ex.1006, [0203]. Ryan’s “second physical module 224...[and] output module (e.g., 108, RF antenna...)” is for wireless communication. Ex.1006, [0203]. The RF antenna is shown in Figure 1A, below. Ex.1006, [0182]; Ex.1003, ¶¶150, 153.



Ex.1006, Fig. 1A (annotated)

Like the '637 patent and Mathiassen, Ryan's smart fob may authenticate a user with a "biometric—such as fingerprint." Ex.1006, [0229]. Ryan's smart fob also "may comprise an LCD screen" to display indicators, images, or symbols. Ex.1006, [0132], [0219], [0250], [0264]; Ex.1003, ¶¶151. Ryan's smart fob improves communication security for a wide variety of transactions. Ex.1006, [0223]-[0227], [0236]; Ex.1003, ¶152. Ryan's smart fob also encrypts data packets. Ex.1006, [0241], [0249], [0367]-[0368], [0229]; Ex.1003, ¶153.

2. Motivation to Combine Rescorla and Mathiassen with Ryan

In the proposed Rescorla-Mathiassen-Ryan combination, a POSITA would have been motivated to modify Mathiassen's portable device to include a wireless interface, as taught by Ryan, enabling Mathiassen's portable device to transact wirelessly. A POSITA would have modified Mathiassen's portable device to

implement an LCD screen. Ex.1003, ¶155. This combination would be easily implemented with Rescorla’s SSL protocols because SSL anticipates wireless implementation. Ex.1015, 47 (describing “the Wireless Application Forum’s WTLS” as an “SSL variant[]”).

First, Ryan is analogous art to the ’637 patent. Ryan relates to “[a] compact personal token apparatus” for conducting transactions online and biometrically authenticating a user. Ex.1006, Abstract, [0229]. Thus, Ryan is in the same field of endeavor (i.e., improving security through biometric authentication) and is reasonably pertinent to the above-identified problem with which the inventor is involved (i.e., biometrically authenticating a user of a compact device). Ex.1003, ¶156.

Second, a POSITA would have been motivated to include a wireless interface, as taught by Ryan, to configure Mathiassen’s portable device to communicate wirelessly. Mathiassen anticipates wireless communication in other embodiments of its device. Ex.1005, [0147]-[0151]. Ryan’s wireless interface allows the smart fob to interact “via its wireless interface in the real world” (Ex.1006, [0151]) with a variety of systems, devices and 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”)). Modifying Mathiassen’s portable device to communicate

transactions wirelessly would “eliminate[] the need to tender cash.” Ex.1006, [0248]. In view of these advantages, a POSITA would be motivated to include a wireless interface in Mathiassen’s portable device. Doing so would improve Mathiassen’s portable device’s ability to facilitate and improve security of online transactions, such as transactions with “an internet bank or a corporate or government intranet,” as well as the transactions described in Ryan. Ex.1005, Abstract; Ex.1006, [0223], [0235] (presenting a ticket at a venue), [0224] (redeeming coupons), [0225] (paying for purchases). Ex.1003, ¶157.

In addition, a POSITA would have implemented an LCD screen, as described by Ryan, in Mathiassen’s portable device. Ryan’s LCD screen displays “messages regarding status or other relevant information to the user.” Ex.1006, [0219], [0250] (“seat reservation number”), [0264] (“[i]nformation, news or special offers,” and “discounts...in barcode format”). While Mathiassen’s portable device includes LEDs (Ex.1005, [0124], [0135], [0138]) and a “beeper” (Ex.1005, [0120]), Mathiassen’s user must remember the predetermined meaning for each notification type (e.g., a flashing “red LED” signifies that “the user ID does not match” (Ex.1005, [0138])). A POSITA would have been motivated to include Ryan’s LCD screen in Mathiassen’s portable device to increase the flexibility and specificity of messages provided. For example, error messages may be displayed explaining specifically why the user was not authenticated (e.g., insufficient fingerprint quality). An LCD

screen (Ex.1006, [0132]) would also enable Mathiassen's portable device to perform the additional functions described by Ryan, listed above, such as displaying a "seat reservation number." Ex.1006, [0219], [0250], [0264]; Ex.1003, ¶158.

Accordingly, the Rescorla-Mathiassen-Ryan combination would have been the combination of prior art elements (Mathiassen's portable device implementing Rescorla's handshake protocols with a wireless interface and LCD screen) according to known methods (Mathiassen's encryption software to encrypt authentication data, Rescorla's protocols, and Ryan's wireless interface for securing transaction data and LCD screen) to yield the predictable result of authenticating users and servers through wired and wireless connections and reporting the status of transactions or functions via an LCD display. *KSR*, 550 U.S. at 416; Ex.1003, ¶159.

Further, a POSITA would have had a reasonable expectation of success in modifying Mathiassen's portable device to include a wireless interface and LCD display because Ryan discloses a highly similar device. 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 encrypt data. Ex.1005, [0075]-[0098]; Ex.1006, [0249], [0367]-[0368]. Both interact with external systems via communications interfaces. Ex.1005, [0053]; Ex.1006, [0124]; Ex.1003, ¶160.

In addition, modifying Mathiassen's portable device to include a wireless interface would be improving a similar device in the same way. *KSR*, 550 U.S. at

417. Mathiassen describes multiple communications interfaces. 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 perform the same function. Ex.1006, [0175], [0223], [0235]. Similarly, the '637 patent itself acknowledges that its wired interface and wireless interface are interchangeable equivalents. Ex.1001, 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.”). Thus, a POSITA at the time would have been motivated to modify Mathiassen to include a wireless interface to authenticate transactions. Ex.1003, ¶¶161-162.

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.

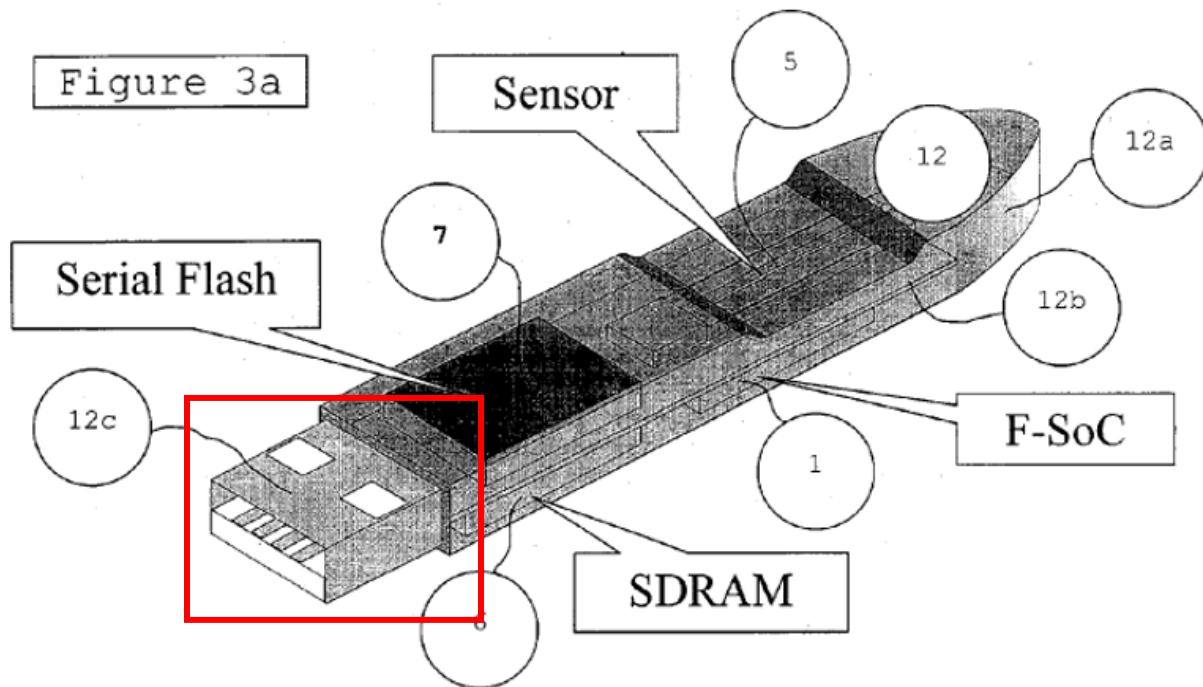
Rescorla, Mathiassen, and Ryan render obvious limitation [10.0] because the Certificate and CertificateVerify messages described by Rescorla would be

transmitted from the portable device described by Mathiassen to the website server via a wireless transceiver as described by Ryan. Ex.1003, ¶163.

As explained at [7.4], Rescorla and Mathiassen render obvious *transmitting said [transaction authentication] response to said request*.

In addition, Mathiassen renders obvious *transmitting said cryptographically encapsulated secure data message* because its “message/communication is encrypted to form a secure output” and “transferred...through one of the communication interfaces.” Ex.1005, [0084]; Ex.1003, ¶164.

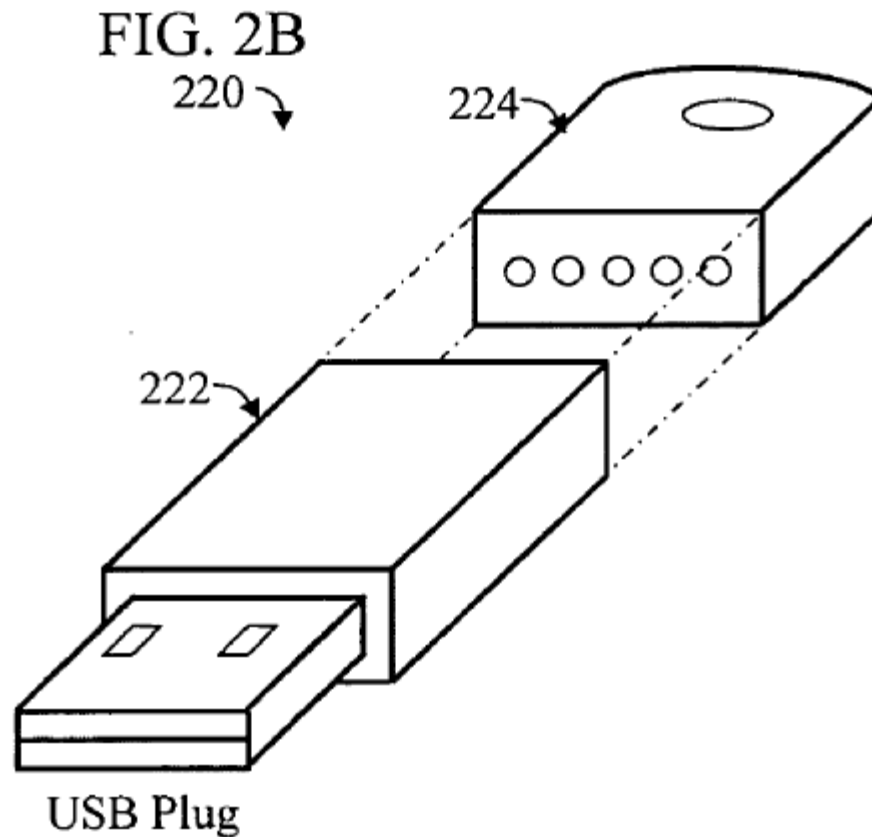
Specifically, Mathiassen’s portable device includes *an external communications interface*, which includes a physical USB connector, “USB interface (12C).” Ex.1005, [0054], [0084]; Ex.1003, ¶¶164-166.



Ex.1005, Fig. 3a (annotated)

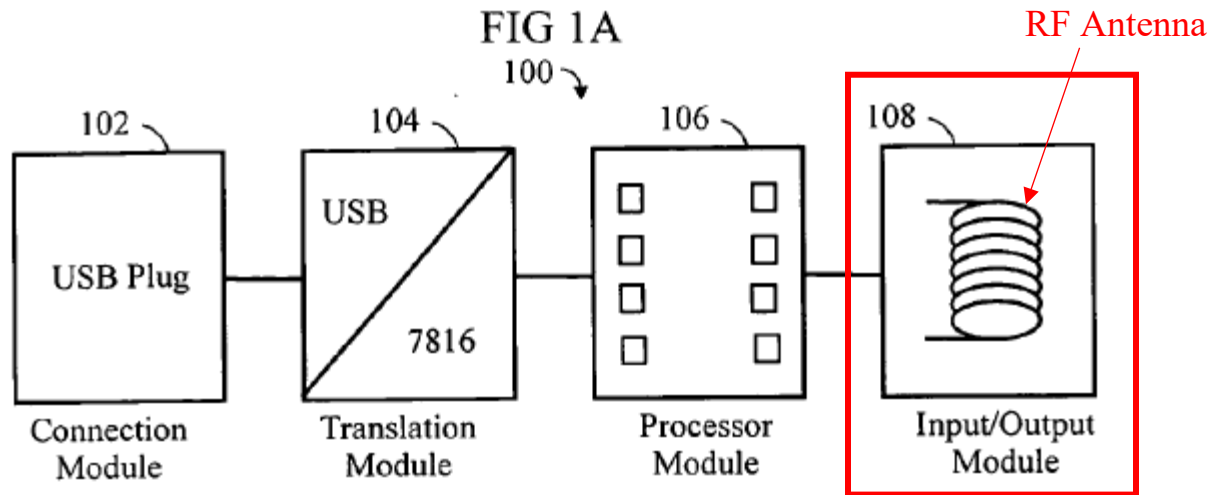
A POSITA would have modified Mathiassen's portable device to include a wireless interface. §VII.B.2; Ex.1003, ¶155-162.

Ryan's smart fob, shown in Figure 2B, "comprises a wireless interface." Ex.1006, [0124]; Ex.1003, ¶168.



Ex.1006, Fig. 2B

Ryan's smart fob includes a "first physical module 222" or "input module," and a "second physical module 224" or "output module." Ex.1006, [0203]. The second physical module 224 includes an "RF antenna and modulator" shown in Figure 1A, below. Ex.1006, [0203]; Ex.1003, ¶169.



Ryan’s wireless interface “enabl[es] communication with a personal device” external to the smart fob. Ex.1006, [0038]. Thus, Mathiassen and Ryan render obvious *a wireless transceiver (RF antenna) comprised within said customer authentication apparatus* (Mathiassen’s portable device). Ex.1003, ¶170. And in the Rescorla-Mathiassen-Ryan combination, this message corresponds to Rescorla’s CertificateVerify message. §VII.A.4.a,[7.1.3].

In addition, Ryan describes wireless communication when the smart fob is *within a range of an external system having a wireless transceiver*. Ryan describes specific ranges of wireless communication. Ex.1006, [0045] (“a 30-foot range” for “Bluetooth”), [0080] (“up to 50 inches distance” for “RF-ID tags”), [0089] (“short-range communication” for “NFC”), [0121] (“range of a Wi-Fi access point”). Ryan’s smart fob is “present[ed] to the point of sale (POS) contactless reader terminal”

(Ex.1006, [0335]) and “communicate[s] with contactless readers” (Ex.1006, [0370]). Based on the provided ranges, a POSITA would have understood that the message/communication described in Mathiassen would be transmitted wirelessly after the portable device was *within range of an external system having a wireless transceiver communications interface*. Ex.1003, ¶170.

Thus, Rescorla, Mathiassen, and Ryan render obvious transferring an encrypted message/communication from Mathiassen, and/or sending Certificate and CertificateVerify messages from Rescorla (*transmitting said cryptographically encapsulated secure data message*) through a wireless communications interface, as taught by Ryan (*by an external communications interface comprising a wireless transceiver comprised within said customer authentication apparatus*) when the portable device is within a range of an external system, as taught by Ryan (*after said apparatus is within range of an external system having a wireless transceiver communications interface*). Ex.1003, ¶171.

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.

Rescorla, Mathiassen, and Ryan render obvious claim 11 because Mathiassen and Ryan describe using various indicators. Ex.1003, ¶172.

Mathiassen describes “3 LEDs (Light Emitting Diodes; green, yellow and red)” that indicate whether the user has been authenticated, which correspond to *a visual indicator cue*. Ex.1005, [0124]. “If the user ID does not match...the red LED will flash.” Ex.1005, [0138]. If the user was authenticated, the green LED will flash. Other prior art confirms similar use of LEDs. *See, e.g.*, Ex.1006, [0312] (“LEDs can be incorporated into the device...to alert a user that certain functions are occurring.”), Ex.1007, [0035] (“LED 73 lights up to indicate that an authentication process is underway.”); Ex.1003, ¶173.

Mathiassen also discloses a “beeper” that “beep[s] for a pre-set period of say 10,0 seconds” when registering a fingerprint (*an audible indicator cue*). Ex.1005, [0119]-[0120]. Using the beeper to similarly indicate various functions, including that the request originated from a legitimate customer verified through cryptographic authentication and/or biometric authentication, would have been obvious. A POSITA would have been motivated to also include an audible indicator to communicate information where the visual cue would be insufficient, e.g. if a user is looking away or visually impaired. Ex.1003, ¶174.

Ryan’s smart fob includes “an LCD screen” that displays messages (*a displayed indicator cue*). Ex.1006, [0132]. Using an LCD screen as described by Ryan to indicate successful cryptographic authentication of the request or biometric authentication of the user would have similarly been obvious, and a POSITA would

have been motivated to include an LCD screen to specify clear messages. §VII.B.2 Ex.1003, ¶175.

In addition, based on Ryan’s disclosures, a POSITA would have understood that any of these indicators would readily “be incorporated into the device...to alert a user that certain functions are occurring,” Ex.1006, [0312], [0219], [0250], [0264] (displaying seat reservations and barcodes), and a POSITA would have expected success in doing so. Ex.1003, ¶176.

Thus, Rescorla, Mathiassen, and Ryan render obvious indicating that a request originates from a legitimate customer and that the customer is biometrically authenticated (*step 1...and step 2*) via an LED (*indicated by means of at least one of a visual indicator cue*), a beeper (*and an audible indicator cue*), and an LCD screen (*and a displayed indicator cue*). Ex.1003, ¶177.

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.

Rescorla, Mathiassen, and Ryan render obvious claim 12 because Mathiassen and Ryan describe using various indicators on a portable device to confirm that functions have occurred. Ex.1003, ¶178.

As explained with reference to claim 11, Mathiassen discloses “3 LEDs” (*a light emitting diode*). Ex.1005, [0124]. An LED is *a general purpose indicator light*

because LEDs were commonly used light sources in small electronic devices. Ex.1003, ¶179. Ryan’s “LCD screen” would readily display an indicator that showed a user was successfully authenticated because Ryan describes using an LCD screen for various indicators, *see* Ex.1006, [0219], [0250], [0264], which renders obvious *displaying a visual indicator cue on a display*. Ex.1003, ¶179.

Thus, Rescorla, Mathiassen, and Ryan render obvious *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*. Ex.1003, ¶180.

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.

Rescorla, Mathiassen, and Ryan render obvious claim 13 because Mathiassen describes using audible indicators on a portable device. Ex.1003, ¶181.

As described at claim 11, Mathiassen describes “a beeper.” Ex.1005, [0120]; §VII.B.3.b,[11.0]. It would be obvious that the same components used to generate a beep tone would be used to generate a chime tone to indicate the same status. Ex.1003, ¶¶182-183.

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.

Rescorla, Mathiassen, and Ryan render obvious claim 14 because Ryan describes using various indicators on a portable device to confirm that functions have occurred. Ex.1003, ¶184.

Ryan’s LCD screen “display[s] messages regarding status or other relevant information.” Ex.1006, [0214]. Ryan’s LCD screen displays a 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 elements correspond to *a predetermined legend cue, a predetermined symbol cue or a predetermined image cue*. Ex.1003, ¶185-187.

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

Ground 3 shows why claims 15-20 would be obvious over Mathiassen in view of Rescorla and Ryan. Mathiassen discloses a majority of claim 15’s limitations, including biometrically authenticating the customer, generating a request and a time-varying parameter, sending the request, and actuating a visual indicator cue. §VII.C.3.a,[15.0]-[15.4.1], [15.7]. Therefore, Mathiassen is presented first in

Ground 3.⁸ While a POSITA would likely have found claim limitations [15.4.2]-[15.7] obvious based on Mathiassen’s disclosure alone, the combination in Ground 3 reinforces that these limitations would also have been obvious in view of Mathiassen as modified by Rescorla and Ryan.

1. Motivation to Combine Mathiassen with Rescorla

As explained previously, a POSITA would have been motivated to implement SSL/TLS handshake protocols described by Rescorla with Mathiassen’s portable device. §VII.A.3. A POSITA would similarly have been motivated to combine Mathiassen with Rescorla. Ex.1003, ¶188.

First, as explained at Ground 1, Mathiassen and Rescorla are analogous art to the ’637 patent. §VII.A.3; Ex.1003, ¶188.

Second, because Mathiassen’s portable device is not limited to specific handshake protocols, a POSITA would readily implement Rescorla’s SSL/TLS handshake protocols. Allowing Mathiassen’s portable device to authenticate websites increases communication security, which is one of Mathiassen’s stated objectives. Ex.1005, Abstract, [0002]; Ex.1003, ¶189.

⁸ “[C]haracterizing references as primary and secondary is merely a matter of presentation with no legal significance.” *Schwendimann v. Neenah, Inc.*, 82 F.4th 1371, 1384 (Fed. Cir. 2023).

Authenticating websites prevents phishing attacks, keeping the user's confidential information from unintended recipients. Ex.1015, 291 (avoiding giving credit card information to “a fake server”). This increases the user's trust in online surfing. Authenticating websites also allows using public terminals safely. Ex.1005, [0065]. Further, a POSITA would have had an expectation of success in using Mathiassen's portable device to authenticate a website as described by Rescorla. §VII.A.3; Ex.1003, ¶¶190-193.

Accordingly, a POSITA would have been motivated to modify Mathiassen's portable device to perform the handshake sequences described by Rescorla. §VII.A.3; Ex.1003, ¶194.

2. Motivation to Combine Mathiassen and Rescorla with Ryan

As explained previously, a POSITA would have been motivated to modify Mathiassen's portable device to implement an LCD screen, as described by Ryan. §VII.B.2. This same reasoning applies to the combination of Mathiassen and Rescorla with Ryan regarding claims 15-20. Ex.1003, ¶195.

3. Analysis

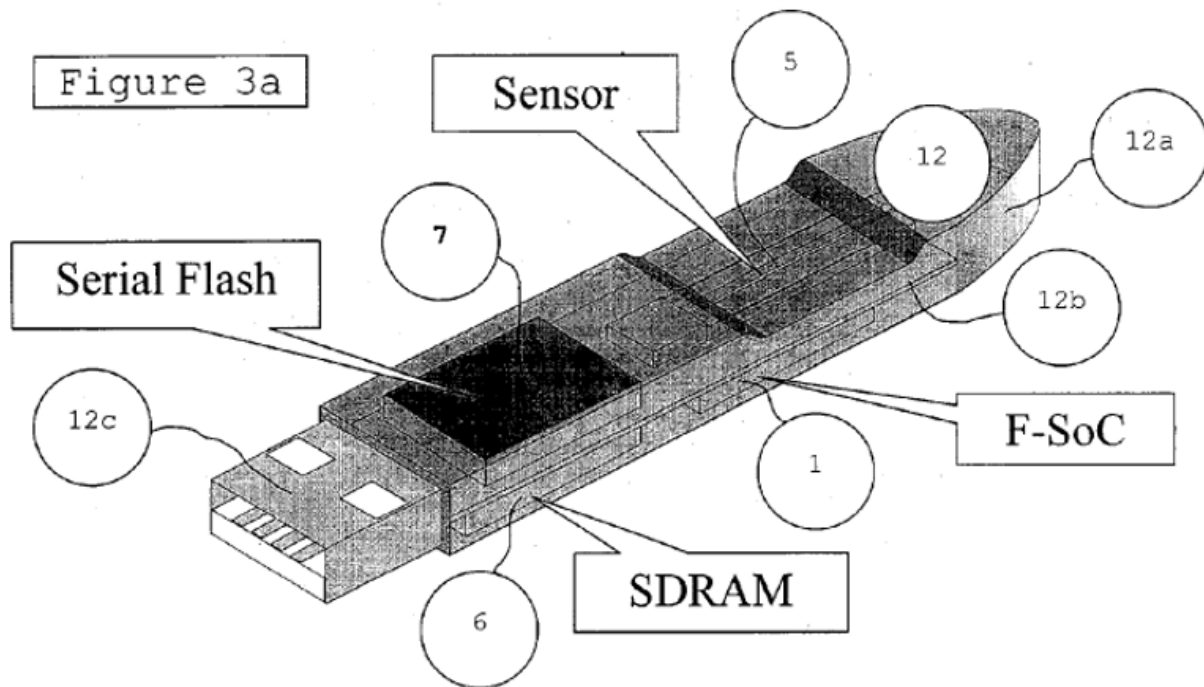
a. *Claim 15*

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

To the extent the preamble is limiting, the combination of Mathiassen and Ryan render it obvious. Ex.1003, ¶196.

First, Mathiassen discloses *[a] method*. Ex.1005, [0002] (“**methods...**to obtain a high level of security”). Ex.1003, ¶197.

Second, Mathiassen renders obvious *generating a customer-initiated transaction request from an authorized customer initiating said request*. “To initiate the connection procedure,” the user “insert[s] the portable device (12 or 13) into the USB port” of the computer and “swipes his finger over the fingerprint sensor (5).” Ex.1005, [0065]-[0066]. The portable device is shown below. Ex.1003, ¶197.



Ex.1005, Fig. 3a

The user is biometrically authenticated based on the scanned fingerprint. Ex.1005, [0066]-[0074]. Mathiassen's portable device then compiles and encrypts a "message/communication" (Ex.1005, [0077]-[0083]) and sends it to "an external unit, network or system" (Ex.1005, [0084]). This "message/communication" discloses *a customer-initiated...request*. Ex.1003, ¶198.

Mathiassen's connection procedure provides access to a system where a transaction is conducted, including "an internet bank." Ex.1005, Abstract, [0016]-[0017], [0047]. In addition, Ryan describes multiple types of transactions with a similar device. Ex.1006, [0223]-[0227], [0236]. Therefore, Mathiassen's

message/communication discloses a *customer-initiated transaction request*.

Ex.1003, ¶199.

Mathiassen's message/communication is from *an authorized customer* because the user is previously enrolled as the authorized user. Ex.1005, [0049]-[0050], [0066]-[0073] (comparing a fingerprint to a previously obtained master fingerprint), [0061] (enrolling the user with the portable device); Ex.1003, ¶200.

Thus, Mathiassen and Ryan render obvious compiling, encrypting, and sending a message/communication (*[a] method for generating a customer-initiated transaction request*) from a portable device that biometrically authenticates the user (*from an authorized customer initiating said request*). Ex.1003, ¶201.

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

Mathiassen renders obvious limitation [15.1.1] because Mathiassen describes biometrically authenticating the user prior to generating and sending the message/communication. Ex.1003, ¶202.

As explained at [7.2], Mathiassen's portable device is a *customer authentication apparatus* that *biometrically authenticat[es]* a user by executing a subset of administrative software called a "matching algorithm" by the processor 2. Ex.1005, [0072]; §VI.A.4.a,[7.2], Ex.1003, ¶203.

The fingerprint sensor 5 captures “raw images” of a fingerprint. Ex.1005, [0049]. The pre-processing block 5C converts the received fingerprint to “intermediate results” and passes them 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, which corresponds to a *customer authentication apparatus* ([7.2]), *biometrically authenticat[es a] customer*. §VII.A.4.a,[7.2]; Ex.1003, ¶204.

Mathiassen’s biometric authentication occurs before sending the message/communication to the external server (*prior to transmission of said customer-initiated transaction request*). “One result of” successful biometric authentication (Ex.1005, [0074]) is the “calculat[ion] of a secure key” (Ex.1005, [0076]). The secure key is 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]). Ex.1003, ¶205.

Thus, Mathiassen renders obvious a portable device that biometrically authenticates the authorized user (*biometrically authenticating said customer using a customer authentication apparatus*) before sending the message/communication

to an external system (*prior to transmission of said customer-initiated transaction request*). Ex.1003, ¶206.

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

Mathiassen renders obvious limitation [15.1.2] because Mathiassen's message includes "[t]he secure key number" and "PKI verification in encrypted format" (Ex.1005, [0077]-[0083]). Ex.1003, ¶207.

As explained at [15.1.1], Mathiassen's "message/communication" (Ex.1005, [0077]) discloses the claimed *customer-initiated transaction request*. The message/communication is *processed, assembled, and encrypted*. Ex.1005, [0076]-[0084]. The "message/communication" includes "[t]he secure key number" and "PKI verification in encrypted format" (Ex.1005, [0077]-[0083]), which disclose *an assertion of a successful biometric authentication* because they are generated 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]) refers to "PKI **biometrics** verification" (Ex.1005, [0050]) and is an *assertion of a successful biometric authentication of said customer*. Ex.1003, ¶¶208-209.

After the message/communication is processed and assembled, it “**is encrypted** to form a secure output...(e.g., handshake procedures).” Ex.1005, [0084], Ex.1003, ¶210.

Thus, Mathiassen renders obvious *processing, assembling, and cryptographically encapsulating an assertion of a successful biometric authentication of said customer*. Ex.1003, ¶211.

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

Mathiassen and Rescorla render obvious limitation [15.2.2] because they describe a key that is valid for a time frame. Ex.1005, [0050]; Ex.1003, ¶212.

Mathiassen describes a key that is “valid for a time frame, or alternatively changes for each transaction.” Ex.1005, [0050]. This key is transmitted to the server as part of the message. Ex.1005, [0080] (message/communication includes “[t]he secure key number”). Thus, Mathiassen discloses *provision of a time-varying parameter...there within*. Ex.1003, ¶213.

While the claim language *to prevent replay attacks* merely states an intended use of the alleged invention and is, therefore, non-limiting, *In re Anderson*, 662 F. App’x 958, 963 (Fed. Cir. 2016), the combination renders this language obvious regardless.

A “replay attack” is 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. Mathiassen describes this same technique (i.e., “chang[ing]” the key “for each transaction”) as an “alternative[]” to providing a key that is “valid for a time frame.” Ex.1005, [0050]. Thus, both techniques are used to prevent replay attacks. Ex.1005, [0050]; Ex.1015, 19. Thus, Mathiassen and Rescorla describe providing a key that is valid for a time frame to *prevent replay attacks*. Ex.1003, ¶214.

Mathiassen’s “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*. Ex.1003, ¶215.

Thus, Mathiassen and Rescorla render this limitation obvious. Ex.1003, ¶216.

[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,

Mathiassen, Rescorla, and Ryan render obvious limitation [15.3] because Mathiassen describes transmitting the cryptographically encapsulated message/communication to an external unit, network, or system, and Ryan explains

that such a message may be received and processed by a trusted third party. Ex.1003, ¶217.

Mathiassen explains that the “message/communication” (*said cryptographically encapsulated request*) is “transferred to an external unit, network or system through one of the communication interfaces.” Ex.1005, [0084]. Mathiassen’s external unit, network, or system includes *a website*, described as “an internet bank.” Ex.1005, Abstract, [0047]. Rescorla similarly describes a website. Ex.1015, 202 (“a given site”), 234 (a “company’s Web site”); Ex.1003, ¶¶218-219.

Mathiassen’s description of providing the message/communication to a server hosting a website, such as “an internet bank” renders this limitation obvious. Ex.1005, Abstract, [0047]. However, Ryan and Rescorla also disclose transmitting the message/communication to *an authentication service provider*. Ex.1006, [0245] (“[t]he client user can be authenticated by the ISP or **by a trusted third party**”); Ex.1015, 8; (“trusted third party” to “authenticate other parties”); Ex.1003, ¶¶219-220. A POSITA would have transmitted the message/communication to a trusted third party as described by Ryan and Rescorla because doing so would allow organizations to outsource security enforcement increasing convenience and reducing costs.

Thus, Mathiassen, Rescorla, and Ryan render obvious sending an encrypted message/communication from the portable device (*transmitting by said customer*

authentication apparatus said cryptographically encapsulated request) to a website or trusted third party (*to at least one external system further comprising at least one of a website and an authentication service provider*). Ex.1003, ¶221.

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

Mathiassen renders obvious limitation [15.4.1]. Ex.1003, ¶222.

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*). The message/communication “is received by e.g. the target server (30) of the network (N)....” Ex.1005, [0086]; Ex.1003, ¶223-224.

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

Mathiassen and Rescorla render obvious limitation [15.4.2] because Mathiassen explains how the server processes the message/communication to authenticate the client. Ex.1003, ¶225.

When Mathiassen’s 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).” Ex.1005, [0086]; Ex.1003, ¶226.

Mathiassen’s server then decrypts the message/communication after “retriev[ing] the particular seed issued to [the] user.” Ex.1005, [0087]; Ex.1015, 84-

85 (describing using seeds for key generation). “If this decryption fails..., the server (30) will assume that the received communication attempt is false, and the server will abort further steps.” Ex.1005, [0090]. If the encryption succeeds, the server verifies that the message/communication came from a biometrically authenticated user because the correct information is 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.” Ex.1005, [0047]. Thus, Mathiassen renders obvious *said request originated from an authenticated customer*. Ex.1003, ¶227.

Rescorla describes *verifying that [said] request originated from an authorized customer* by a handshake protocol as shown in Figure 4.2. Ex.1003, ¶228.



Figure 4.2 Client authentication timeline

Ex.1015, Fig. 4.2 (annotated)

As shown, “the client...send[s] the Certificate message...to send its certificate and the CertificateVerify message to authenticate itself,” which the server uses to confirm the identity of the client. 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. As explained at §VII.C.1, a POSITA would have been motivated to implement Rescorla’s handshake protocols in Mathiassen’s portable device. Ex.1003, ¶¶229-230.

Thus, Mathiassen and Rescorla render obvious *verifying that said request originated from an authenticated customer*. Ex.1003, ¶231.

[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;

Mathiassen and Rescorla render obvious limitation [15.5] because Rescorla describes providing a Handshake: Finished message after both parties are authenticated, and a POSITA would have been motivated to send such a message to the portable device described by Mathiassen after authentication is complete. Ex.1003, ¶232.

As explained at [15.4.2], Rescorla’s server verifies that a request from a client originates from an authenticated client using the Certificate and CertificateVerify messages. Ex.1015, Fig. 4.2, 108, 111; §VII.C.3.a,[15.4]; Ex.1003, ¶233.

Rescorla also discloses a Handshake: Finished message sent from the server to the client (*a cryptographic transaction response*). Ex.1003, ¶234.



Figure 4.2 Client authentication timeline

Ex.1015, Fig. 4.2 (annotated)

The “Handshake: Finished” message is “encrypted with the new cryptographic parameters” and is a response to the client’s Certificate and CertificateVerify messages (*responding to said request using a secure data message*) indicating that both parties were authenticated. Ex.1015, 81. Ex.1003, ¶235; §VII.C.1.

Thus, Mathiassen and Rescorla render obvious sending a Handshake: Finished message (*responding to said request using a secure data message*) which is encrypted (*comprising a cryptographic transaction authentication response and transmitting said response to said customer authentication apparatus*). Ex.1003, ¶236.

[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

Mathiassen and Rescorla render obvious limitation [15.6] because Rescorla explains that its Handshake: Finished message, received by Mathiassen's portable device, denotes that both parties, including the website server, were authenticated. Ex.1003, ¶237.

As explained above at [7.1.2], Rescorla describes steps by which the client verifies that a website is legitimate. §VII.A.4.a,[7.1.2]; Ex.1003, ¶238.

Referring to Rescorla's Figure 4.2, after the server sends its Certificate message to the client and the client sends its own Certificate message, the server sends the "Handshake: Finished" message to the client, which, as explained in limitation [15.5], corresponds to the claimed *receiving...by said customer authentication apparatus...said response*. Ex.1003, ¶239.

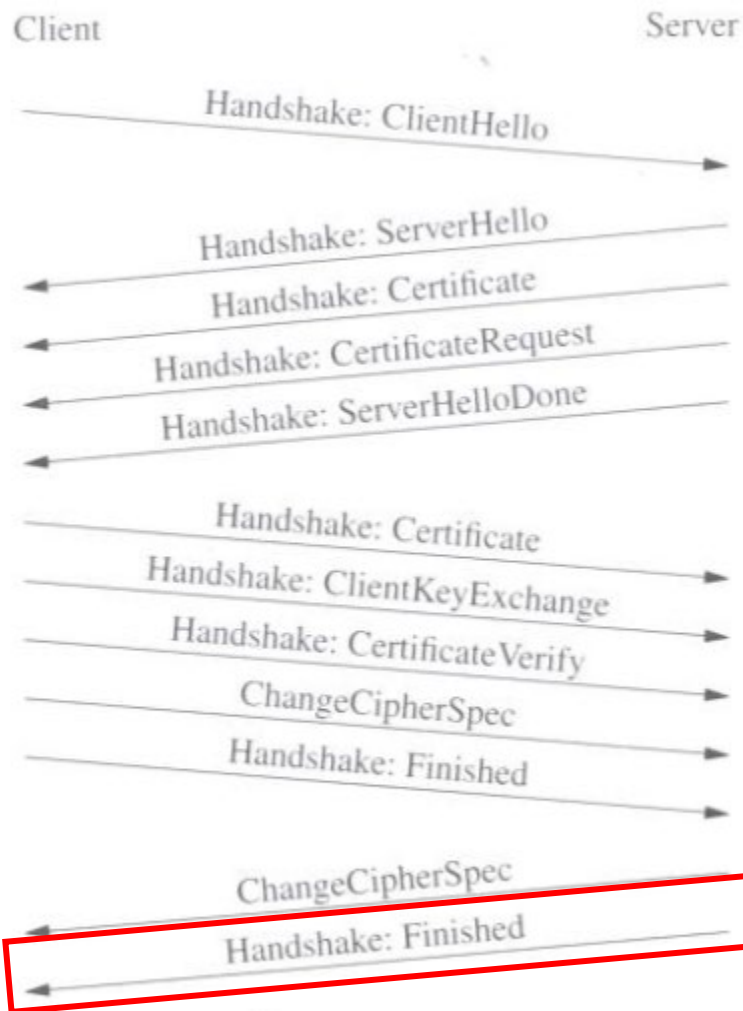


Figure 4.2 Client authentication timeline

Ex.1015, Fig. 4.2 (annotated)

It is only after the Handshake: Finished message is sent that application data may be securely exchanged. Ex.1015, 65 (“the client must wait until it has received the server’s Finished message before it can send its first byte of data”). That message “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 also verifies that it comes *from a legitimate website*.

Ex.1003, ¶¶240-242.

Thus, Mathiassen and Rescorla render obvious receiving a Handshake: Finished message (*receiving and verifying by said customer authentication apparatus that said response to said request represents a response from a legitimate website*). Ex.1003, ¶243.

[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.

Mathiassen and Ryan render obvious limitation [15.7] because Mathiassen and Ryan describe using indicators to confirm that steps were performed. Ex.1003, ¶244.

As explained at claim 11, Mathiassen discloses an LED indicator (*a visual indicator cue*) and a “beeper” (*an audible indicator cue*). Ex.1005, [0124], [0120]. Ryan’s smart fob includes “an LCD screen” (*displayed indicator cue*). Ex.1006, [0132]; §VII.B.3.b,[11.0]; Ex.1003, ¶245.

These indicators would be used to convey “that certain functions are occurring.” Ex.1006, [0312]; §§VI.A.4.a,[7.1.2], VI.C.2.a,[15.6]; Ex.1003, ¶245. Doing so would be a predictable combination of known elements.

Thus, a POSITA would have recognized that any indicators of the device, would readily be used to convey to a user *that said response has been received from a legitimate website*. Ex.1003, ¶246.

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.

Limitation [16.0] is the same as limitation [11.0]. The Mathiassen-Rescorla-Ryan combination renders it obvious for the same reasons. §VI.B.3.b,[11.0]; Ex.1003, ¶237.

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.

Limitation [17.0] is the same as limitation [12.0]. The Mathiassen-Rescorla-Ryan combination renders it obvious for the same reasons. §VII.B.3.c,[12.0]; Ex.1003, ¶248.

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.

Limitation [18.0] is the same as limitation [13.0]. The Mathiassen-Rescorla-Ryan combination renders it obvious for the same reasons. §VII.B.3.d,[13.0]; Ex.1003, ¶249.

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.

Limitation [19.0] is the same as limitation [14.0]. The Mathiassen-Rescorla-Ryan combination renders it obvious for the same reasons. §VII.B.3.d,[13.0]; Ex.1003, ¶¶250-253.

b. Claim 20

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

To the extent the preamble is limiting, Mathiassen and Rescorla render it obvious. Ex.1003, ¶254.

Mathiassen discloses *[a] method*. Ex.1005, [0002] (“**methods**...to obtain a high level of security.”). Ex.1003, ¶254.

Mathiassen’s “portable device” implements “handshake procedures,” Ex.1005, [0084], that improve “general communication security measures in a network,” Ex.1005, [0047]. Ex.1003, ¶255.

Mathiassen's portable device biometrically authenticates users and "encrypt[s] general information transactions," thus, *improving online transaction security*. Ex.1005, [0050]; §VII.A.4.a,[7.0]; Ex.1003, ¶256.

In addition, Rescorla describes SSL/TLS handshake procedures, which, as explained above at §§VII.A.3 and VII.C.1 (describing using handshake protocols to establish secure two-way communication), *improv[e] transaction security*. Thus, Mathiassen and Rescorla render obvious [a] *method for improving online transaction security*. Ex.1003, ¶¶257-259.

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

Mathiassen renders obvious limitation [20.1]. Ex.1003, ¶260.

Mathiassen describes enrolling a user with the portable device. Ex.1005, [0060]-[0064]; Ex.1003, ¶261. The "network administrator...will then enroll the user who will be the 'owner' of the portable device (12 or 13)." Ex.1005, [0060]-[0061]. The process includes "capturing one or more fingerprints of the new user and issuing a seed for the SKG algorithm to such new user." Ex.1005, [0062]. Then, "the administrator...will complete this procedure by counter-signing with his fingerprint." Ex.1005, [0062]-[0064]; Ex.1003, ¶262.

Thus, Mathiassen discloses enrolling a person to use the portable device, which renders obvious *enrolling a person into a customer authentication apparatus*. Ex.1003, ¶263.

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

Mathiassen and Rescorla render obvious limitation [20.2] because Mathiassen describes a user inserting the portable device into a computer connected to an external network to complete an online transaction, as described by Rescorla. Ex.1003, ¶264.

First, Mathiassen describes the “network (N)” (Ex.1005, [0086]), as “an external unit, network or system” (Ex.1005, [0084]) (*an external system*). Ex.1003, ¶265.

After a user is enrolled, she may “access the server (30) of the network (N)” (*external system*) “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),” (*external system*), Mathiassen renders obvious *deploying said person...at an external system*. Ex.1003, ¶266.

In addition, Mathiassen explains that 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*. Ex.1003, ¶267.

Mathiassen also explains that the external system is where *at least one transaction can be generated*. The network the user accesses via the portable device

is an “access-limited apparatus, device, network or system, e.g.,...**an internet bank.**” Ex.1005, Abstract. The portable device can also be used to access “all types of proprietary networks (LAN, WAN, etc.) typically represented by **internet banking applications.**” Ex.1005, [0017]. An internet bank is where transactions occur. Ex.1003, ¶268.

In addition, Rescorla explains that every online transaction “almost certainly us[es] SSL.” Ex.1015, xvii; Ex.1003, ¶269.

Thus, Mathiassen and Rescorla render obvious *deploying said person and said customer authentication apparatus together at an external system where at least one transaction can be generated.* Ex.1003, ¶270.

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

Mathiassen renders obvious limitation [20.3]. Ex.1003, ¶271.

Mathiassen’s portable device includes “an integrated circuit (IC) (1)...to provide secure communication.” Ex.1005, Abstract. This “secure communication” is “between the IC (1) and the network server (30).” Ex.1005, [0050], [0051] (“the IC (1) is designed” to “communicate with external devices and networks (N)”), [0084]-[0086] (“a secure output...received by e.g. the target server (30) of the network (N).”); Ex.1003, ¶272.

Thus, Mathiassen renders obvious *communicating between said customer authentication apparatus and said external system*. Ex.1003, ¶273.

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

Mathiassen and Rescorla render obvious limitation [20.4] because Mathiassen describes biometrically authenticating a user after the portable device is connected to the external network and while exchanging handshake messages as described by Rescorla. Ex.1003, ¶274.

As explained at [7.2] and [15.1.1] above, Mathiassen renders obvious *biometrically authenticating said customer using a customer authentication apparatus*. Mathiassen's portable device includes a "matching algorithm" that captures a fingerprint and compares it "with master fingerprint representations." Ex.1005, [0072], [0049]-[0050]. Thus, Mathiassen's portable device biometrically authenticates a user (*authenticating said person by said customer authentication apparatus*). Ex.1003, ¶275.

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 portable device is inserted into terminal 31 of network N. Ex.1005, [0065]-[0066] ("The user will insert the portable device (12 or 13) into the USB port" and "swipes

his finger over the fingerprint sensor (5)”), [0067]-[0074] (describing biometric authentication after inserting device); Ex.1003, ¶276.

In addition, Rescorla describes customer authentication as part of a SSL/TLS handshake procedure. Figure 4.2, below, shows customer authentication occurring with the server sending a CertificateRequest message to the client and the client responding with the Certificate and CertificateVerify messages. Ex.1015, 97; Ex.1003, ¶277.

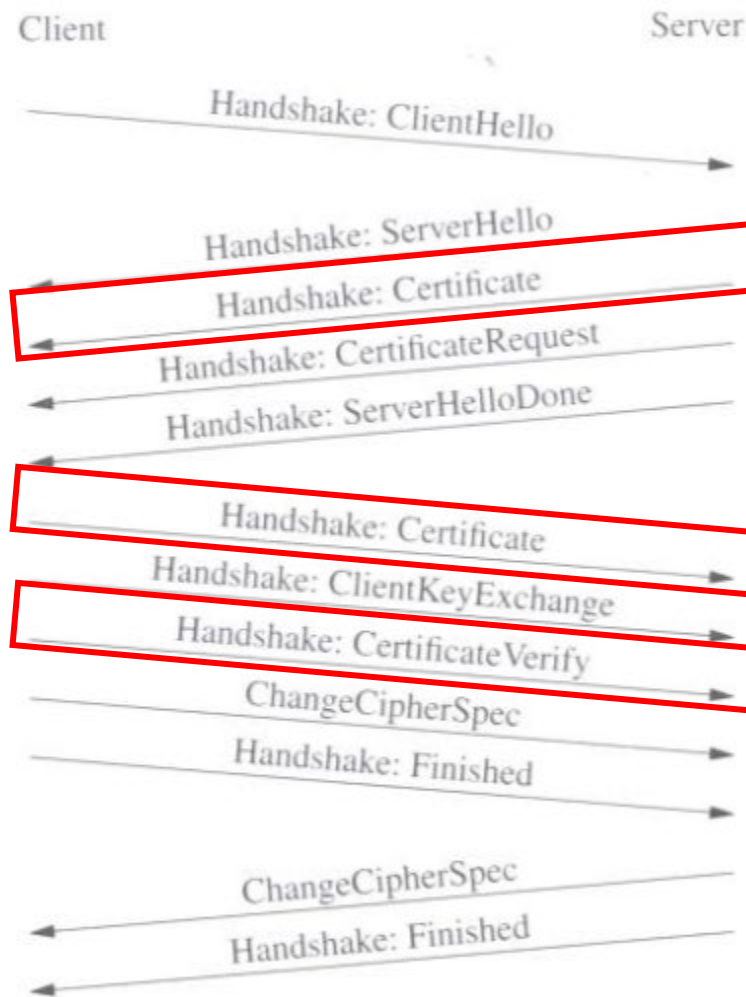


Figure 4.2 Client authentication timeline

Ex.1015, Fig. 4.2 (annotated)

These messages are transmitted during an SSL/TLS handshake, which corresponds to communication between the client and server (*authenticating...while said apparatus is communicating with said external system*). Ex.1003, ¶278; §VI.C.1.

Thus, Mathiassen and Rescorla render obvious *authenticating said person by said customer authentication apparatus while said apparatus is communicating with said external system*. Ex.1003, ¶279.

[20.5] (5) initiating and generating of said at least one request⁹ by said person after said apparatus has authenticated said person;

Mathiassen renders obvious limitation [20.5]. Ex.1003, ¶280.

As explained at [7.2], 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...after said apparatus has authenticated said person*. Ex.1003, ¶281.

Mathiassen explains that the request is *by said person*. Ex.1005, [0060]-[0065] (describing initial enrollment of user and initiation of transaction authentication by enrolled user); Ex.1003, ¶281.

⁹ *[S]aid at least one request* lacks antecedent basis in claim 20. However, *said at least one request* appears to correspond to *a request message* that is transmitted at [20.6]. This term also appears to correspond to *said authenticated-person-initiated-transaction message* of [20.7] and bears similarities to the *customer-initiated transaction request from an authorized customer* of [15.0].

Mathiassen's "message/communication" (Ex.1005, [0077]) corresponds to *said at least one request*. This message/communication is generated "**pending a positive match** of his fingerprint **with an authorized fingerprint**." Ex.1005, [0050], [0076]-[0077] ("[w]hen the central processor (2) has" biometrically authenticated the user, "the administrative software...will calculate a secure key...for encryption of [the] message/communication."); Ex.1003, ¶282.

Thus, Mathiassen discloses or renders obvious *initiating and generating of said at least one request by said person after said apparatus has authenticated said person*. Ex.1003, ¶283.

[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; and

Mathiassen renders obvious limitation [20.6]. Ex.1003, ¶284.

As explained at [15.3], Mathiassen describes "transferr[ing]" the "message/communication" (*request message*) "to an external unit, network or system through one of the communication interfaces." Ex.1005, [0084]. This message/communication indicates that the user was authenticated by the portable device 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*. The secure key number, 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.* Ex.1003, ¶285.

Thus, Mathiassen discloses or renders obvious *transmitting a request message indicating that said person was authenticated by said apparatus and that said transaction was initiated by an authenticated person.* Ex.1003, ¶286.

[20.7] (7) receiving in said host system said authenticated-person-initiated-transaction message.¹⁰

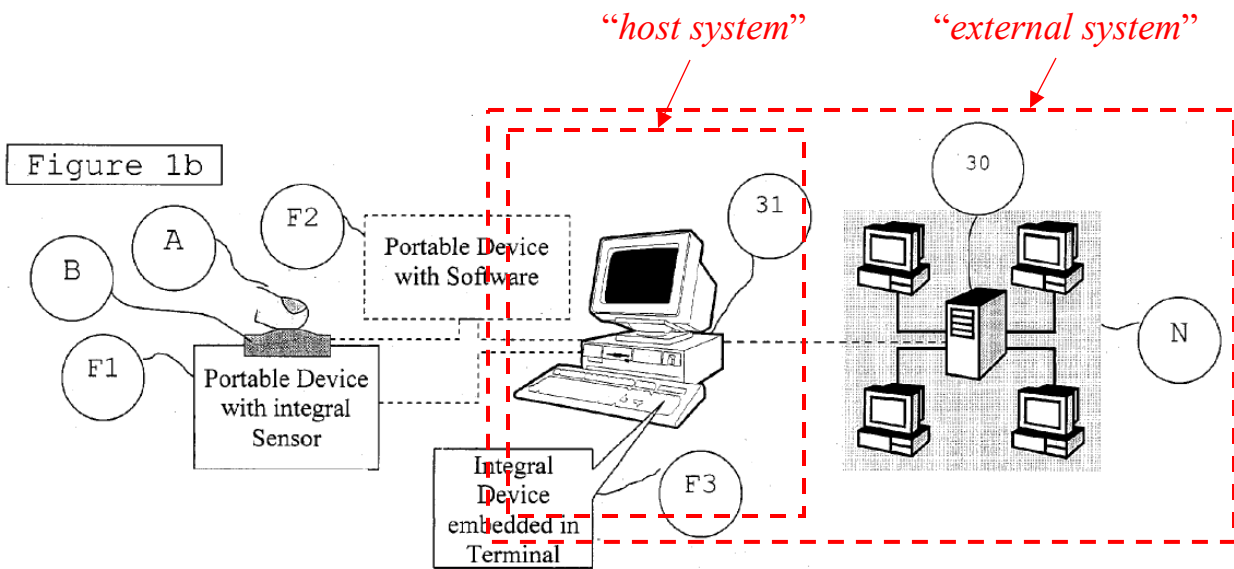
Mathiassen renders obvious limitation [20.7]. Ex.1003, ¶287.

The claim term *host system* lacks antecedent basis. The term *host system* is also not included in the specification of the ’637 patent. The only description of the

¹⁰ As described in limitation [20.5], *said authenticated-person-initiated-transaction message* is believed to correspond to *said at least one request*.

host system is found in claims 2-4 of the '637 patent, which are not addressed in this Petition. Claims 2-4 of the '637 patent claim different ways in which the portable device communicates with a host system, including via a *physical interface port* (claim 2) that receives *a USB connector* of the apparatus (claim 3) or via a *second wireless transceiver* (claim 4). Based on this description, a host system is the device with which the customer authentication apparatus interacts and through which it communicates with the external system, i.e., the specific machine into which the portable device is inserted. Ex.1003, ¶288.

Mathiassen describes this arrangement, illustrated in Figure 1b, below. Mathiassen's terminal 31 is 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)"). Terminal 31 is also part of network N (*external system*). Ex.1005, [0053] ("a terminal (31) of the network"); Ex.1003, ¶288.



Ex.1005, Fig. 1b (annotated)

Mathiassen explains that the message/communication is sent from the portable device to network N. 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 terminal 31, which is part of network N, via USB interface 12C, and forwarded to the ultimate destination within network N. Ex.1005, [0084] (describing “transferr[ing]” the message/communication); §VI.C.3.a,[15.4.1], Ex.1005, [0077], [0086]. Thus, the terminal 31 (host system) *receives...said authenticated-person-initiated-transaction message*. Ex.1003, ¶289.

Thus, Mathiassen discloses or renders obvious *receiving in said host system said authenticated-person-initiated-transaction message*. Ex.1003, ¶290.

VIII. DISCRETIONARY INSTITUTION

A. Discretionary Denial Under § 325(d) Would be Inappropriate.

The Board should not exercise its discretion under 35 U.S.C. §325(d) to deny this Petition. None of the prior art in Grounds 1-3 above was of record or cited during examination of the '637 patent. Thus, the first part of the *Advanced Bionics* framework is not met. *Advanced Bionics*, IPR2019-01469, Paper 6 at 8 (Feb. 13, 2020) (precedential).

B. Discretionary Denial Under § 314(a) Would be Inappropriate.

The Board should not exercise its discretion to deny institution under the *General Plastic* framework. The '637 patent has not been challenged in any IPR petition. Further, the '637 patent is no longer being actively litigated in any district court litigation.

IX. CONCLUSION

The Board should institute an IPR trial for claims 7-20 and cancel these claims as unpatentable.

Respectfully submitted,

Dated: May 24, 2024

/Jonathan R. Bowser/
Jonathan R. Bowser
Counsel for Petitioner
Reg. No. 54,574

X. CERTIFICATE OF WORD COUNT

Under 37 C.F.R. § 42.24, the undersigned attorney for the Petitioner, Askeladden, L.L.C., declares that the argument section of this Petition (Sections II-IX) has 13,787 words, according to the word count tool in Microsoft Word™.

/Jonathan R. Bowser/
Jonathan R. Bowser
Counsel for Petitioner
Reg. No. 54,574

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Askeladden, L.L.C.
Petitioner

§ Petition for *Inter Partes* Review
§
§ U.S. Patent No. 7,480,637
§
§

CERTIFICATE OF SERVICE

The undersigned certifies, under 37 C.F.R. §§ 42.105 and 42.6, that service was made on the Patent Owner as detailed below.

Date of service May 24, 2024

Manner of service Federal Express

Documents served Petition for *Inter Partes* Review, including Exhibit List; Exhibits 1001-1009, 1015, 1017, 1018, 1021, and 1024-1030; and Petitioner's Power of Attorney

Persons served Douglas Kozlay (Agent/Attorney of Record)
1101 E33rd Street, Suite E303
Baltimore, MD 21218

Jabaa, LLC (Courtesy Copy – Assignee)
12 Dexter Road
Garland, ME 04939

Cortney S. Alexander (Courtesy Copy – Litigation counsel)
Kent & Risley LLC
5755 North Point Parkway Suite 57
Alpharetta, GA 30022

/Jonathan R. Bowser/
Jonathan R. Bowser
Counsel for Petitioner
Reg. No. 54,574

XI. CLAIMS APPENDIX

U.S. Patent 7,480,637
(Claim Numbering in Petition Added)

Claim 7

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

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

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

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

[7.1.4] further including a cryptographic encapsulation of said response 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;

[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;

[7.4] transmitting said response to said request; and

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

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.

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.

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.

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.

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.

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.

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.

Claim 15

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

[15.1.1] (1) 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

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

[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,

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

[15.4.2] 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;

[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

[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.

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.

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.

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.

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.

Claim 20

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

[20.1] (1) 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;

[20.3] (3) 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;

[20.5] (5) 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; and

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