

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

IPR2024-00915
U.S. Patent No. 7,480,637

**PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT 7,480,637
CHALLENGING CLAIMS 1-6 AND 21-24**

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.	U.S. PATENT 7,480,637	4
A.	Summary	4
B.	Level of Ordinary Skill in the Art	6
C.	Prosecution History	7
V.	CLAIM CONSTRUCTION.....	8
A.	“resident within” (claims 1, 21)	8
VI.	CLAIMS 1-6 AND 21-24 ARE UNPATENTABLE	11
A.	Ground 1: Claims 1-6 and 21-24 would have been obvious over Mathiassen in view of Ryan.....	11
1.	Overview of Mathiassen	11
2.	Overview of Ryan	16
3.	Motivation to Combine Mathiassen and Ryan	18

4.	Analysis.....	25
a.	Claim 1.....	25
b.	Claim 2.....	55
c.	Claim 3.....	57
d.	Claim 4.....	57
e.	Claim 5.....	60
f.	Claim 6.....	62
g.	Claim 21.....	64
h.	Claim 22.....	79
i.	Claim 23.....	80
j.	Claim 24.....	81
B.	Ground 2: Claims 1-6 and 21-24 would have been obvious over Mathiassen and Ryan in view of Lim.	83
1.	Overview of Lim.....	83
2.	Motivation to Combine Mathiassen and Ryan with Lim.....	85
3.	Analysis.....	87
a.	Claim 1.....	87
b.	Claim 21.....	91
VII.	DISCRETIONARY INSTITUTION	91
A.	Discretionary Denial Under § 325(d) Would be Inappropriate.	91
B.	Discretionary Denial Under § 314(a) Would be Inappropriate.....	91

VIII. CONCLUSION	93
IX. CERTIFICATE OF WORD COUNT	94
X. CLAIMS APPENDIX.....	96

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.
Ex.1006	U.S. Pat. Pub. No. 2005/0109841 to Ryan et al.
Ex.1007	U.S. Pat. Pub. No. 2003/0005336 to Lim et al.
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	U.S. Pat. No. 6,003,115 to Spear et al.
Ex.1011	Reserved
Ex.1012	Reserved
Ex.1013	U.S. Pat. No. 6,760,017 to Banerjee
Ex.1014	U.S. Pat. No. 6,092,117 to Gladwin
Ex.1015	Reserved
Ex.1016	Reserved
Ex.1017	U.S. Pat. Pub. No. 2005/0165700 to Karthik
Ex.1018	U.S. Pat. Pub. No. 2006/0123465 to Ziegler
Ex.1019	U.S. Pat. No. 5,875,464 to Kirk

Ex.1020	U.S. Pat. No. 5,025,366 to Baror
---------	----------------------------------

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 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 1-6 and 21-24 of the '637 patent, Petitioner has filed a Petition challenging claims 7-20 of the '637 patent (IPR2024-00916).

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 (IPR) and that Petitioner is not barred or estopped from requesting IPR of the patent's claims.

III. OVERVIEW OF CHALLENGE AND RELIEF REQUESTED

Petitioner challenges claims 1-6 and 21-24 (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. U.S. 2004/0123113 ("Mathiassen") (Ex.1005); filed December 18, 2002; published June 24, 2004; prior art under 35 U.S.C. §§ 102(a) and 102(b).
2. U.S. 2005/0109841 ("Ryan") (Ex.1006); filed November 16, 2004;

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

published May 26, 2005; prior art under 35 U.S.C. § 102(a).

3. U.S. 2003/0005336 (“Lim”) (Ex.1007); filed July 3, 2001; published January 2, 2003; prior art under 35 U.S.C. §§ 102(a) and 102(b).

Mathiassen, Ryan, and Lim 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 1-6 and 21-24 under the following Grounds:

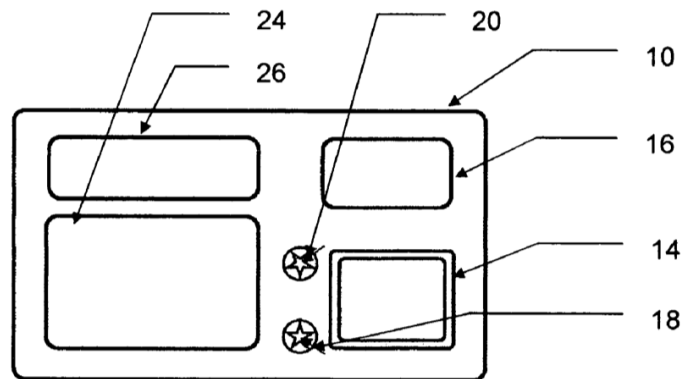
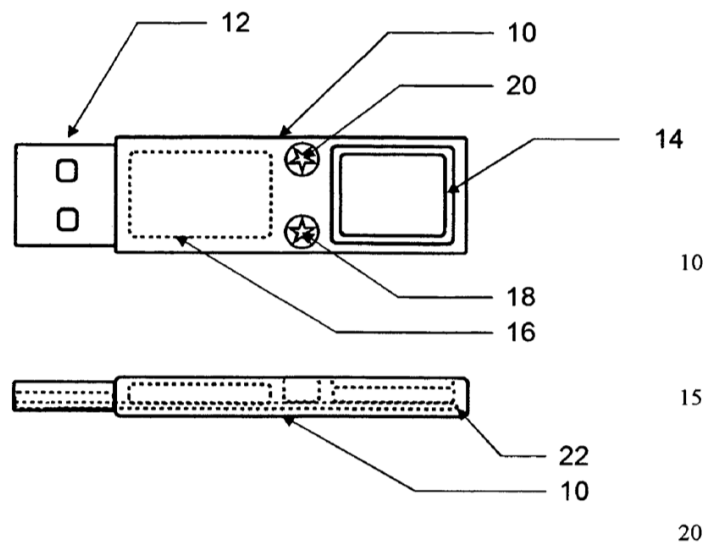
Ground	Claim	Obviousness Basis (§ 103)
#1	1-6, 21-24	Mathiassen in view of Ryan
#2	1-6, 21-24	Mathiassen in view of Ryan and Lim

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

A. Summary

The ’637 patent is directed to a customer authentication apparatus implemented as a USB dongle or wireless card, shown in Figures 1A (USB dongle) and 1B (wireless card), below. 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 merchant by authenticating the user and website. Ex.1001, 3:32-39 (authenticating user), 5:31-35 (authenticating website).



Ex.1001, Figs. 1A and 1B

The ITA apparatus in both configurations (Figs. 1A and 1B) includes a fingerprint sensor array 14 for user authentication, and LED lights 18, 20 for communicating authentication status. Ex.1001, 5:27-31, 5:38-52. 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 LED 18 turns green if the user is authenticated or red in the alternative. Ex.1001, 5:38-46, 5:51-54. If the user is authenticated, the apparatus sends an encrypted packet with the authentication results to the website. Ex.1001, 6:15-26. Once authenticated, the user may complete a transaction on the website. Ex.1001, 6:27-32. The '637 patent explains that the wireless card embodiment in Figure 1B operates the same way, except the wireless card communicates wirelessly. Ex.1001, 6:48-58.

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 likewise, less education may be necessary with additional work experience. Ex.1003, ¶¶40-41.

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. The inventor filed a *pro se* response which was not recognized by the Office, and a notice of abandonment issued. The inventor then assigned the application to Biometric Associates, LP, which filed a response with a petition to revive. Ex.1002, 37-50. In its response, the assignee did not amend claim 1, but added limitations [21.2.3]-[21.2.5] to claim 21 identified below. The assignee argued that “[w]ith the system architecture and methodology of the claimed invention, authentication resides within the apparatus and not in the user’s or web host’s system.” Ex.1002, 47.

The petition to revive was granted, and a Notice of Allowance issued, allowing claims 1-24. The Notice of Allowance identified limitations [1.3.1]-[1.5] as the allowable features. Ex.1002, 25-27; *see infra* §VI.A.4.a.,[1.3.1]-[1.5]. As shown in §VI, limitations [1.3.1]-[1.5] and [21.2.3]-[21.4] are rendered obvious by prior art not considered by the Examiner.

V. CLAIM CONSTRUCTION²

Petitioner submits that all claim terms not addressed below should be construed according to their plain and ordinary meaning.³ Ex.1003, ¶¶42-44.

A. “resident within” (claims 1, 21)

Claim 1 recites “*transaction security software **resident within** and executing on said at least one processor.*” Ex.1001, 8:51-52. Claim 21 contains the same limitation except claim 21 recites “*...on said processor*” instead of “*...on said at least one processor.*” Ex.1001, 11:25-27. The term “*resident within*” should be construed as “temporary storage of the software while the software is being executed.” Ex.1003, ¶45.

The ’637 patent does not define the term “resident within,” but a POSITA would have understood the term “*resident within*” to mean temporary storage of the software while the software is being executed. This construction is based on the disclosure of the ’637 patent and processor architecture at the priority date of the ’637 patent. Ex.1003, ¶46.

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

³ Petitioner does not concede that any term not construed herein meets the statutory requirements of 35 U.S.C. § 112.

The '637 patent specification says that “[r]esident within and executing within the processor 16, is transaction security software.” Ex.1001, 5:12-13. In the next sentence, the '637 patent explains that the “[p]rocessor 16...contains memory **for the execution of programs.**” Ex.1001, 5:13-15. Based on this description, a POSITA would understand that the purpose of the memory within the processor of the '637 patent is temporary storage of software while the software is executed, rather than long-term storage of the software. Ex.1003, ¶¶47-48.

This construction is consistent with the '637 patent's description because the portable apparatus includes non-volatile memory separate from the processor memory. For example, claim 1 of the '637 patent recites “*a memory...coupled to said at least one processor.*” Ex.1001, 8:57-58; *see infra* §VI.A.4.a.,[1.4.1]. This “*memory...coupled to said at least one processor*” is external to the processor and may be non-volatile memory such as “protected memory available to the customer so that the ITA can additionally serve as a virtual disk drive” and for “the secure internal storage of the ITA.” Ex.1001, 5:17-20, 7:63-65. The '637 patent explains that the non-volatile memory of the ITA apparatus is for long-term storage of data, including storage of “the ID [identifier] of the ITA [transaction security software] and its[] cryptographic keys.” Ex.1001, 5:15-20. The '637 patent does not describe long-term storage of software within the processor. Ex.1003, ¶¶49-50.

This construction is also consistent with other prior art. For example, U.S. Patent No. 6,003,115 (“Spear”) (Ex.1010) describes the components of a conventional processor, including cache memory, and how the processor interacts with volatile memory and non-volatile memory. Ex.1010, 1:20-2:47. Spear explains that computer systems at the time included non-volatile memory and a processor. Ex.1010, 1:20-2:47. Non-volatile memory “stor[es] system operating software, application program instructions and data.” Ex.1010, 1:34-38. The processor, or “central processing unit (CPU)...obtains, decodes and executes [the] instructions.” Ex.1010, 1:31-35; Ex.1003, ¶51. During execution of application program instructions, the processor stores the instructions in memory within the processor itself, called a “cache memory.” Ex.1010, 1:60-67 (“To improve the system operating speed small high speed secondary memory is used called cache memory.”). Cache memory is typically “incorporated into the microprocessor chip.” Ex.1010, 2:6-10. During execution, “[a] small subset of the program instructions stored in main memory are also stored in the cache memory to maximize the program operating speed.” Ex.1010, 2:35-37; Ex.1003, ¶51.

Other prior art also supports Petitioner’s construction. For example, U.S. Patent No. 5,875,464 (“Kirk”) (Ex.1019) explains that “[e]ach processor...read[s] the same line of information from main memory into its cache.” Ex.1019, 14:46-49;

see also Ex.1020, 15:65-66 (describing software stored in a processor as “cached instructions or data” within a “Memory array”); Ex.1003, ¶¶52-53.

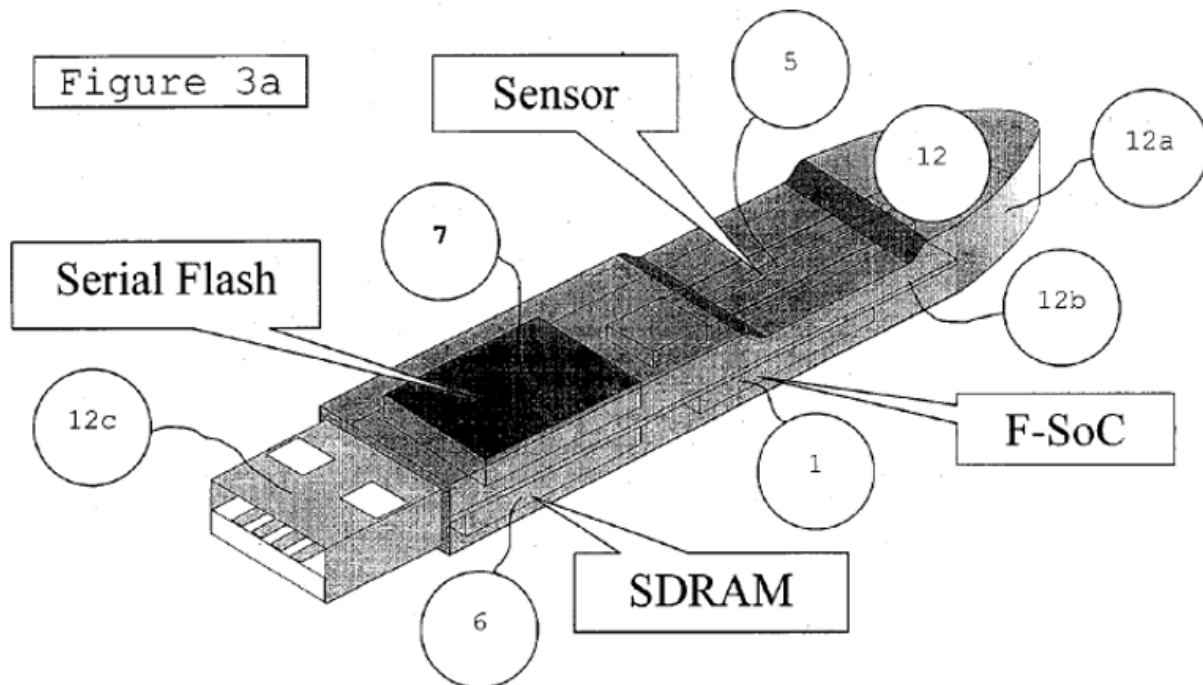
Accordingly, a POSITA would have understood that the term “*resident within*” in claims 1 and 21 means temporary storage of the software while the software is being executed, rather than long-term storage. Ex.1003, ¶54.

VI. CLAIMS 1-6 AND 21-24 ARE UNPATENTABLE

A. Ground 1: Claims 1-6 and 21-24 would have been obvious over Mathiassen in view of Ryan.

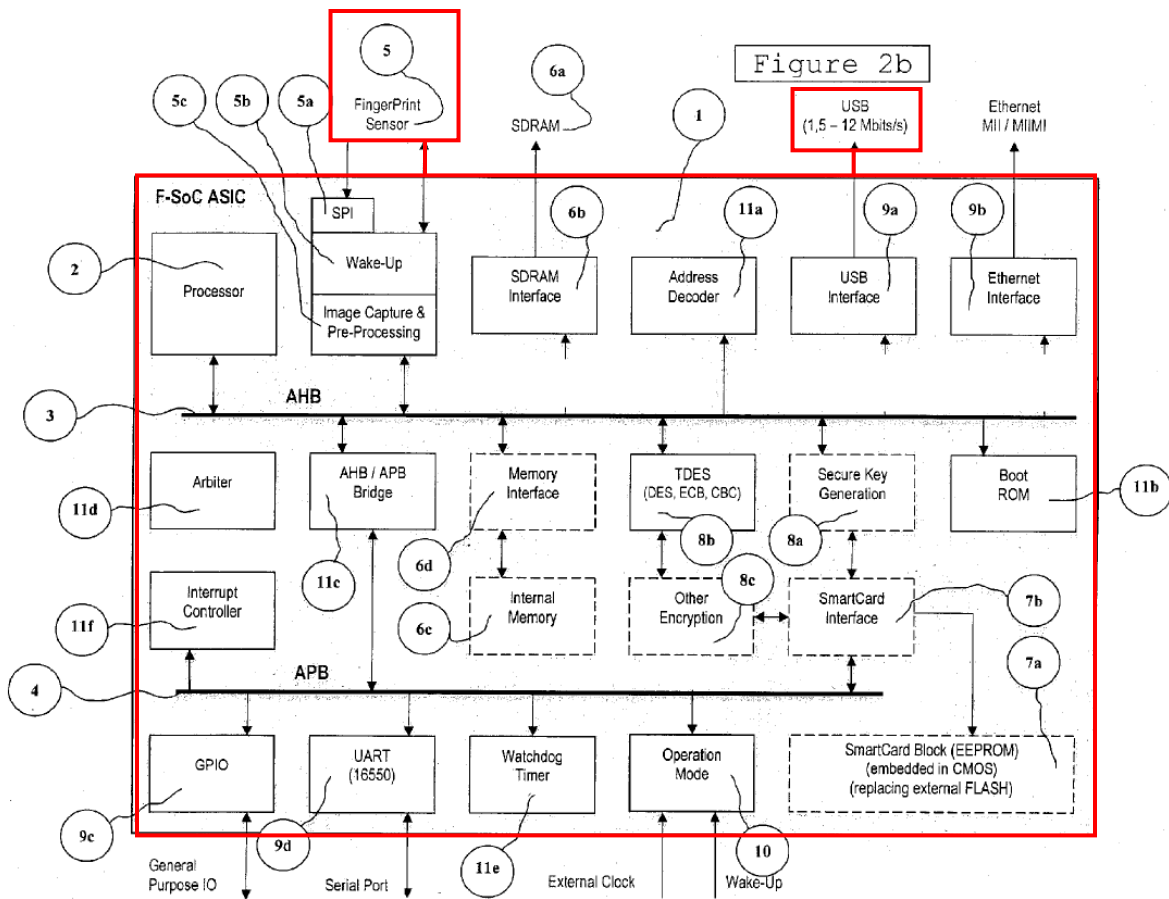
1. Overview of Mathiassen

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 of Mathiassen’s portable device is shown in Figure 3a, below.



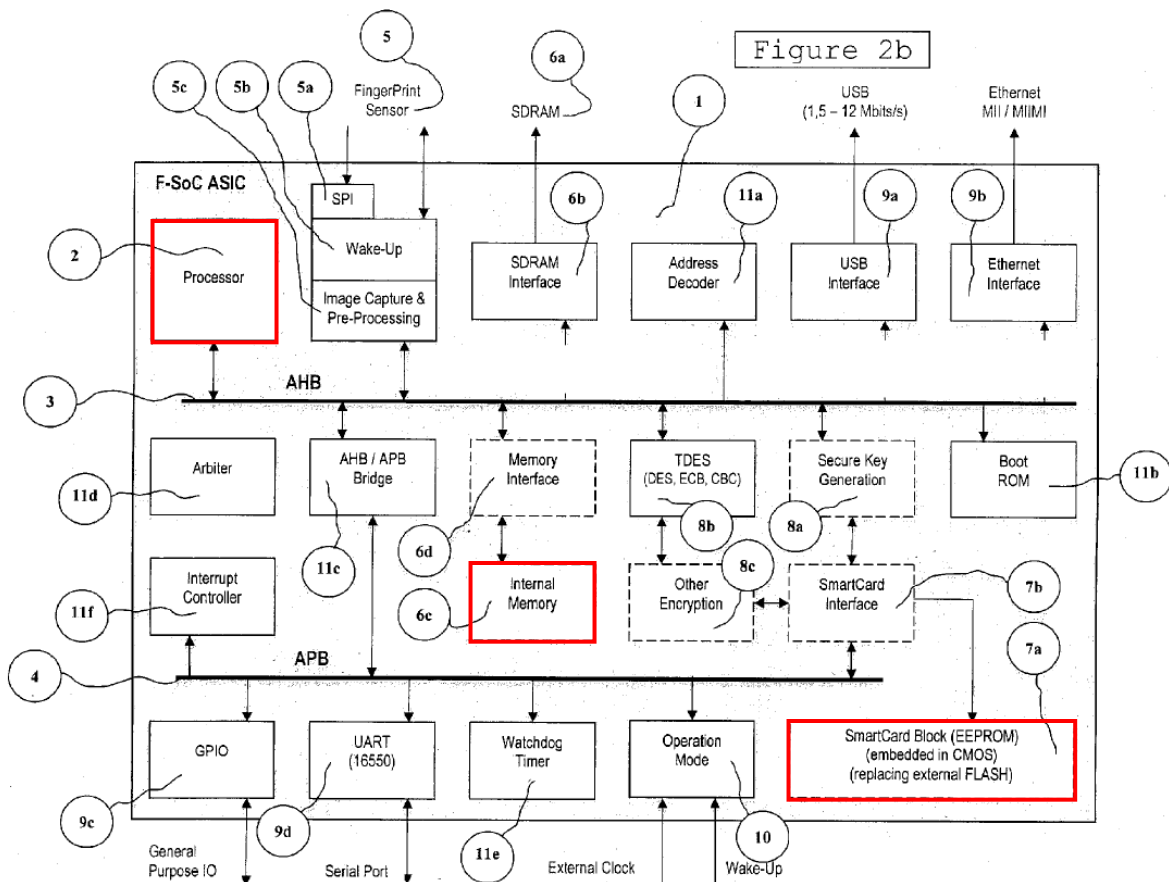
Ex.1005, Fig. 3a

The portable device includes a USB connector referred to as a USB mechanical interface 12C. Ex.1005, [0054]. Mathiassen’s portable device also includes a “biometrics sensor in the form of a fingerprint sensor (5).” Ex.1005, [0048]. The “biometrics sensor in the form of a fingerprint sensor (5) is coupled with a biometrics processor in the form of an integrated circuit—IC (1).” Ex.1005, [0047]-[0048]. The IC 1 of the portable device is illustrated in Figure 2b, shown below. Ex.1005, [0048] (“Two versions of the IC are shown in FIGS. 2A and 2B.”); Ex1003, ¶61.



Ex.1005, Fig. 2b (annotated)

Figure 2b shows that the IC 1 is coupled to the USB connector (“USB”) and the fingerprint sensor 5. Ex.1005, [0049] (“The sensor (5) is connected to a...pre-processing block (5C) via a first interface block (5A) as well as a wake-up circuit (5B).”), [0050] (“The IC (1) also comprises hardware and/or software required to supply output signals to...second interface blocks” including “USB (9A).”); Ex.1003, ¶61.



Ex.1005, Fig. 2b (annotated)

IC 1 also includes a “central processor (2),” “non-volatile memory (7, 7A, or 7C)” labelled as “SmartCard Block (EEPROM)” shown in Figure 2b (Ex.1005, [0050]), and “volatile memory (6 or 6c)” labelled as “Internal Memory” in Figure 2b (Ex.1005, [0049]). Mathiassen’s portable device includes and executes software (“administrative software” stored in non-volatile memory 7a) for biometrically authenticating the user and cryptographically encapsulating (encrypting) communications sent to external systems. Ex.1005, [0050]. Subsets of the administrative software include a “matching algorithm” for authenticating

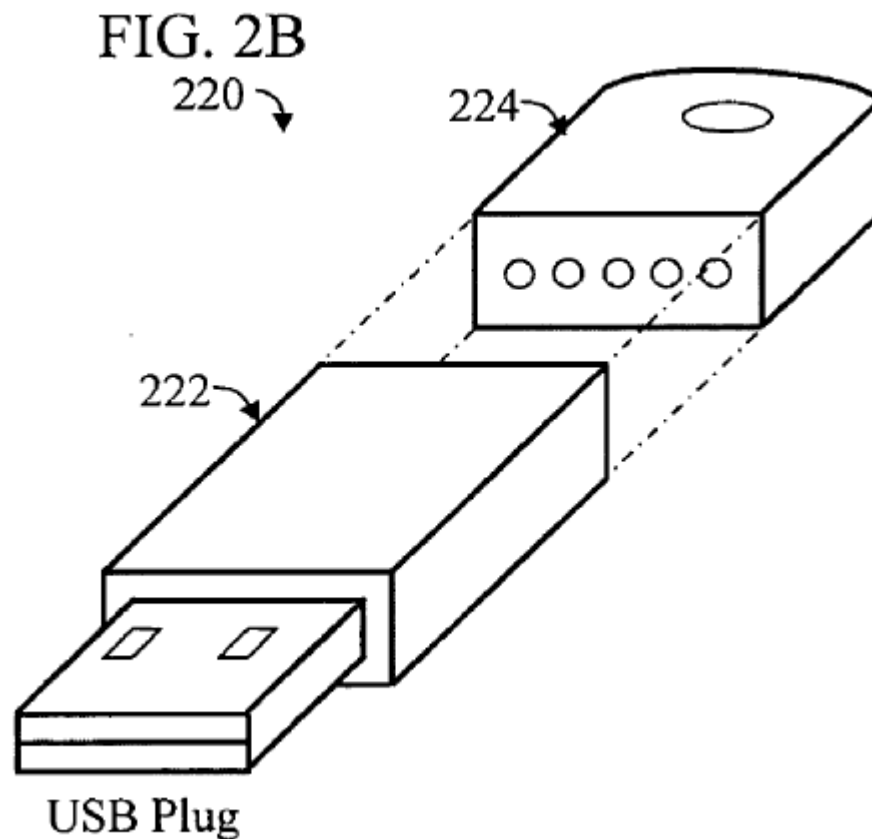
fingerprints (Ex.1005, [0070]-[0072]), and an additional “subset” for encrypting data by “generat[ing] a secure key or password” and “applying...encryption methods” to “produce secured output data.” Ex.1005, [0091]-[0095]; Ex.1003, ¶¶60-63.

In operation, “the network administrator...enroll[s] the user who will be the ‘owner’ of the portable device.” Ex.1005, [0061]. This includes “capturing one or more fingerprints of the new user, and issuing a seed for the SKG [Secure Key Generation] algorithm to such new user.” Ex.1005, [0062]; Ex.1003, ¶64.

After enrollment, the user may use the portable device to biometrically authenticate herself. To do so, the portable device acquires a fingerprint image via the fingerprint sensor 5 (Ex.1005, [0049], [0066]), and compares it to a prestored fingerprint image, called “master minutiae” (Ex.1005, [0050], [0071]). If the acquired fingerprint matches the prestored fingerprint, the user is authenticated. Ex.1005, [0073] (“If the matching is positive, the connection process will automatically continue.”). Mathiassen’s portable device then compiles and encrypts a message conveying that the user is authenticated, which may include a username and password or other identification data, and transmits the message to a network or system. Ex.1005, [0051], [0074], [0076]-[0084] (describing encryption of communications after user authentication); Ex.1003, ¶¶65-67.

2. Overview of Ryan

Ryan describes a “compact personal token apparatus,” also referred to as a “smart fob.” Ex.1006, Abstract, [0149]. Ryan’s smart fob is similar to Mathiassen’s portable device and the ’637 patent’s ITA apparatus. One embodiment of Ryan’s compact personal token apparatus is shown in Figure 2B.

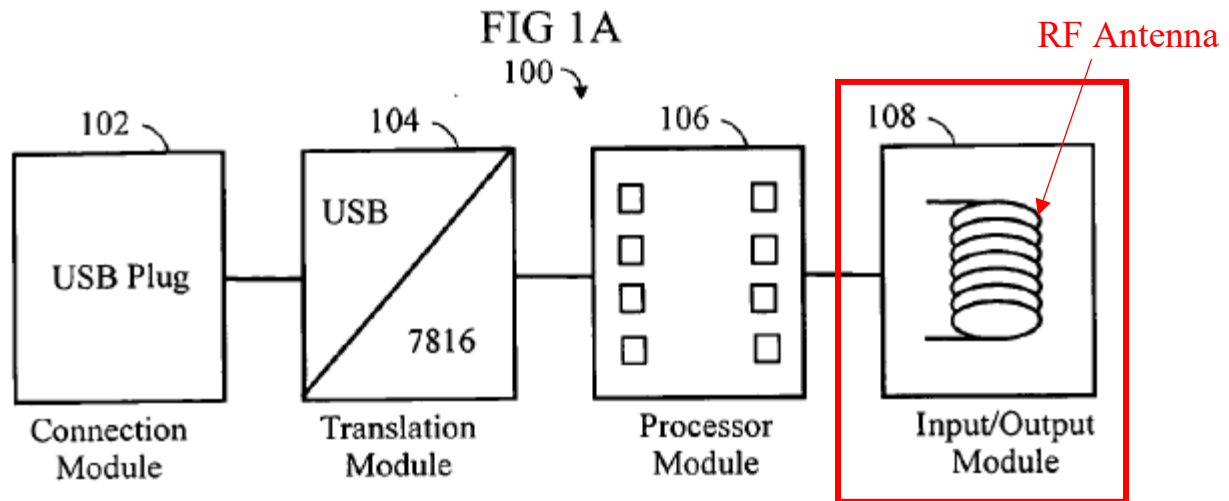


Ex.1006, Fig. 2B

As shown, Ryan’s smart fob includes a “first physical module 222” including a USB plug, also referred to as “the input module.” Ex.1006, [0203]. Ryan’s smart

fob is used to improve communication security for transactions, including, for example, downloading tickets from the internet, storing e-coupons or cash, and making online purchases. Ex.1006, [0223]-[0227], [0236]. Ryan’s smart fob enhances the security of transactions by encrypting transaction data. Ex.1006, [0241] (“packets of data are encrypted”), [0249] (“Personal data, frequency flyer miles as well as credit card details can be encrypted.”), [0367] (“digital content could be encrypted”), [0368] (“all coupons are encrypted as a security feature reducing or eliminating the likelihood that coupon values could be counterfeited or altered in any way.”). In addition, Ryan’s smart fob may authenticate a user with a “biometric—such as fingerprint.” Ex.1006, [0229]; Ex.1003, ¶¶68-70.

Ryan’s smart fob communicates wirelessly with an RF antenna within the second physical module 224 shown in Figure 2B. Ex.1006, [0203] (the “second physical module 224...contains the processor module (e.g., 106, dual interface chip) and output module (e.g., 108, RF antenna and modulator”). The output module 108 within the second physical module 224 is shown in more detail in Figure 1A, below:



Ex.1006, Fig. 1A (annotated)

The RF antenna that facilitates wireless communication is illustrated within the output module 108. Ex.1006, [0182] (“The output module 108 comprises an RF antenna.”); Ex.1003, ¶71.

3. Motivation to Combine Mathiassen and Ryan

A POSITA would have been motivated to modify Mathiassen’s portable device to conduct and authenticate transactions, as taught by Ryan. In addition, a POSITA would have been motivated to modify Mathiassen’s portable device to conduct transactions using a wireless interface, as taught by Ryan, to enable Mathiassen’s portable device to communicate wirelessly with external devices. Ex.1003, ¶72.

First, Mathiassen is analogous art to the ’637 patent. The ’637 patent relates to a portable device for increasing online transaction security through biometric

authentication. Ex.1001, Abstract. Mathiassen is within the same field of endeavor, pertaining 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., a portable device for improving online transaction security by biometrically authenticating a user). Ex.1003, ¶72. In addition, Mathiassen is reasonably pertinent to a particular problem with which the inventor of the ’637 patent was involved (i.e., implementing biometric authentication in a portable device for improving online transaction security). Ex.1005, Abstract; Ex.1003, ¶73.

Ryan is also analogous art to the ’637 patent. Ryan relates to “[a] compact personal token apparatus” (smart fob) for conducting transactions online and biometrically authenticating a user. Ex.1006, Abstract, [0229]. Thus, Ryan is in the same field of endeavor and is reasonably pertinent to the above-identified problem with which the inventor of the ’637 patent was involved. Ex.1003, ¶74.

Second, a POSITA would have been motivated to modify Mathiassen’s portable device to secure online transactions as described by Ryan. Mathiassen describes (1) biometrically authenticating a user (Ex.1005, [0065]-[0074]) and (2) cryptographically encapsulating a message that the user is authenticated, including a user name and password, to ensure that the message is not intercepted or tampered

with (Ex.1005, [0075]-[0098]). This message relates primarily to user authentication that grants the user access to the network. Ex.1005, Abstract; Ex.1003, 75.

Mathiassen does not explicitly describe enhancing the security of transactions, i.e., after the user has already gained access to the network. A POSITA would have been motivated to modify Mathiassen's portable device, which secures the message indicating user authentication, to also enhance security of online transactions, as taught by Ryan. Ex.1006, [0232] ("The smart fob can operate as a security device" for "connect[ing] to a participating merchant's website" and "conduct[ing] a business transaction in a secure fashion."). A POSITA would have been motivated to make this modification because Mathiassen describes using its portable device to "access...an internet bank or a corporate or government intranet" where online transactions would take place. Ex.1005, Abstract. As explained by Ryan, the use of a smart fob for securing online interactions advantageously provides convenience by conducting a wide variety of transactions wirelessly. Ex.1006, [0223], [0235] (wirelessly presenting a ticket at a venue), [0224] (redeeming coupons), [0225] (paying for purchases); Ex.1003, ¶¶74-76.

Modifying Mathiassen's portable device for securing online transactions as taught by Ryan would advantageously ensure that data relating to a transaction is not intercepted or modified, further enhancing security beyond user authentication. Ex.1006, [0368] (encryption of transaction data "reduc[es] or eliminat[es] the

likelihood that coupon values could be...altered”). Modifying Mathiassen’s portable device in this way would advantageously assure the user that a transaction is carried out with the intended network. Ex.1006, [0249] (“inserting the smart fob” ensures that a connection is made “via a secure server”); Ex.1003, ¶77.

For example, by encrypting transaction authentication data itself, only the intended server can decipher the transmitted data and receive money or other sensitive data from the portable device. Ex.1006, [0249] (only the secure server can decrypt “[p]ersonal data, frequent flyer miles, as well as credit card details” and prevents “Internet ‘phishing’ fraud”). The combination would also ensure that exchanged amounts of electronically transferred money are not tampered with. Ex.1006, [0238] (“[T]he savings amount is passed to the cash register to deduct from the total bill.”); [0105] (the “Secure Application Module” of Ryan’s smart fob is “tamper proof”). The combination would increase efficiency of online transactions via biometric authentication and increase trust of users in online entities and vice versa. Ex.1005, [0050], [0072] (describing biometric authentication); Ex.1006, [0249] (describing a secure server that protects against “spam, viruses,” and “Internet ‘phishing’ fraud”). Ex.1003, ¶77.

Third, a POSITA would have been motivated to modify Mathiassen’s portable device to include a wireless interface, as taught by Ryan, to configure

Mathiassen's portable device to communicate wirelessly with external devices, in addition to wired communication. Ex.1003, ¶78.

Ryan's smart fob interacts "via its wireless interface in the real world" (Ex.1006, [0151]) with a wider variety of systems and devices, such as ticket kiosks at venues or similar settings (Ex.1006, [0223] ("the user takes the smart fob to the event where it connects wirelessly with a reader at the venue," [0235] (a user can "wave the device in close proximity to a turnstile equipped with a wireless reader at the entrance.")). Modifying Mathiassen's portable device to communicate transactions wirelessly would, as taught by Ryan, "eliminate[] the need to tender cash" when conducting a wireless transaction. Ex.1006, [0248]; Ex.1003, ¶78.

In view of these advantages, a POSITA would be motivated to modify Mathiassen's portable device to include a wireless interface as taught by Ryan. Doing so would enable Mathiassen's portable device to better perform its stated purpose of facilitating and improving security for online transactions, such as transactions with "an internet bank or a corporate or government intranet," to a wider variety of transactions and settings, such as any of the transactions described in Ryan. Ex.1005, Abstract; Ex.1006, [0223], [0235] (wirelessly presenting a ticket at a venue), [0224] (redeeming coupons), [0225] (paying for purchases); Ex.1003, ¶78.

Accordingly, the Mathiassen-Ryan combination would have been the combination of prior art elements (Mathiassen's portable device with a fingerprint

sensor, configured to authenticate transactions with a wireless interface, as taught by Ryan) according to known methods (Mathiassen's encryption software to encrypt authentication data and Ryan's wireless interface and securing transaction data) to yield the predictable result of biometrically authenticating a user, improving the security of online transactions, and interfacing with other devices, networks, and/or systems through wired and wireless connections. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007); Ex.1003, ¶79.

Further, a POSITA would have had a reasonable expectation of success in modifying Mathiassen's portable device to authenticate online transactions and include a wireless interface because the devices described in Mathiassen and Ryan perform similar functions to achieve similar goals using similar technology. For example, both Mathiassen and Ryan describe biometric authentication. Ex.1005, Fig. 3a, [0048]-[0050]; Ex.1006, [0222]-[0229], [0236]. Both Mathiassen and Ryan encrypt data sent from portable devices (data related to user authentication in Mathiassen and data related to online transactions in Ryan). Ex.1005, [0075]-[0098]; Ex.1006, [0249], [0367]-[0368]. The devices of both Mathiassen and Ryan interact with external devices, networks, and/or systems via communications interfaces. Ex.1005, [0053]; Ex.1006, [0124]. Mathiassen and Ryan each disclose portable devices for authenticating a user. Ex.1005, Abstract; Ex.1006, [0229]. Ryan's smart fob includes a wireless transceiver interface. Ex.1006, Fig. 1A (Input/Output Module

108); Ex.1003, ¶80.

In addition, modifying Mathiassen’s portable device to include a wireless interface as taught by Ryan would be improving a similar device in the same way. *KSR*, 550 U.S. at 417. Mathiassen describes a number of wired communications interfaces by which its portable device communicates with external systems. Ex.1005, [0050], Fig. 2b (interfaces blocks 9A, 9B, 9C, and 9D). Ryan describes a wired communications interface as well as a wireless communications interface that performs the same function of transmitting data to an external device. Ex.1006, [0175] (listing wired interfaces and wireless interfaces equally suitable for communicating “between an external memory/processing apparatus and a personal computer”); Ex.1003, ¶81.

Further, replacing Mathiassen’s wired interface with a wireless one would be a “mere substitution of one element for another known in the field.” *KSR*, 550 U.S. at 416. Ryan explains that both its wired communications interface and wireless communications interface perform the same function of transferring data to and from the smart fob. Ex.1006, [0223], [0235]. Similarly, the ’637 patent admits that a 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 form, and the replacement of the USB interface with a radio circuit such as a Bluetooth or ZigBee

chip with antenna 26”). For all these reasons, a POSITA at the time would have been motivated to modify Mathiassen to include a wireless interface and authenticate transactions, as taught by Ryan. Ex.1003, ¶81.

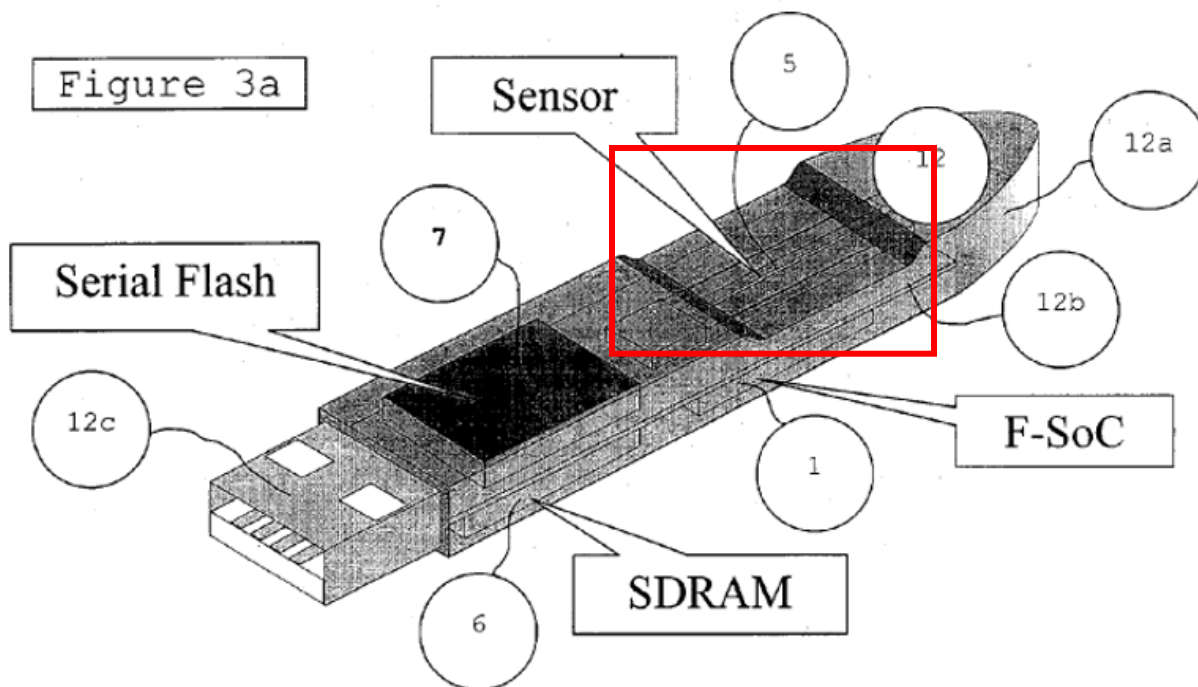
4. Analysis

a. *Claim 1*

[1.0] A biometric customer authentication apparatus for improving online transaction security and for assuring the identity of a customer, comprising:

To the extent the preamble is limiting, Mathiassen and Ryan render it obvious. Ex.1003, ¶¶82-91.

Mathiassen discloses a *biometric customer authentication apparatus*. Specifically, Mathiassen describes “[a] portable or embedded access device,” which is often referred to as a “portable device.” Ex.1005, Abstract. Mathiassen’s portable device is shown in Figure 3a of Mathiassen below.



Ex.1005, Fig. 3a (annotated)

As shown in Figure 3a above, Mathiassen's portable device "comprises an integrated circuit (IC) (1)" (Ex.1005, Abstract), a "biometrics sensor in the form of a fingerprint sensor (5)" (Ex.1005, [0048]), a "non-volatile memory (7, 7A or 7C)" (Ex.1005, [0050]), and "a USB interface (12C)" (Ex.1005, [0054]). Mathiassen's portable device⁴ is a *biometric customer authentication apparatus* because it includes a "biometrics sensor in the form of a fingerprint sensor (5)" (Ex.1005, [0048]), and authenticates a user based on readings from this sensor (Ex.1005, [0048]),

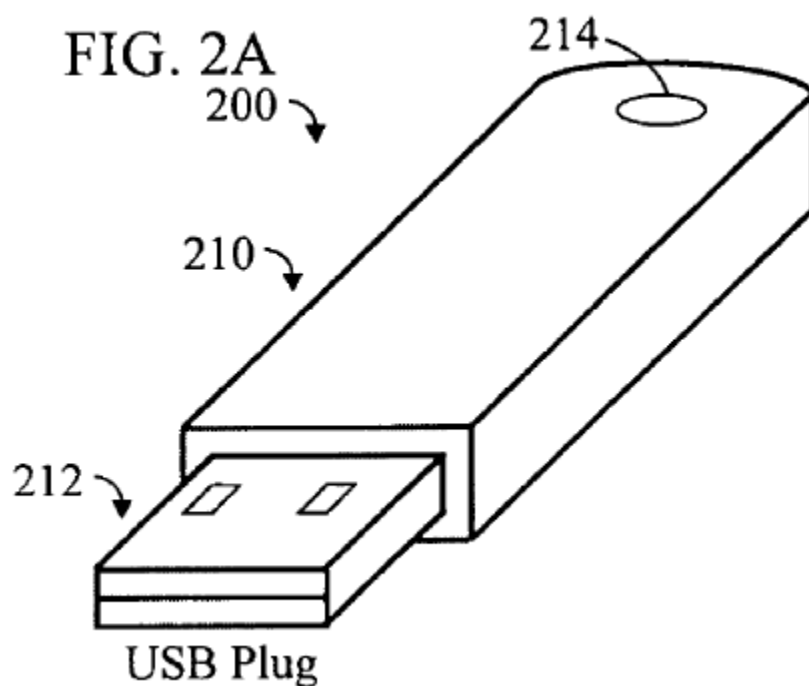
⁴ For brevity, Mathiassen's "portable or embedded access device" is referred to herein as a "portable device."

[0050] (“fingerprint representations...are compared...with master fingerprint representations” to identify “a positive match.”), [0047] (“a portable access device for allowing only authorized users access...”). Ex.1003, ¶¶83-85.

Mathiassen discloses that its portable device is for *assuring the identity of a customer*. Specifically, Mathiassen teaches providing access to “network[s] or system[s], e.g., a computer terminal, an internet bank or a corporate or government intranet” via its portable device “pending a positive match of [a user’s] fingerprint with an authorized fingerprint representation.” Ex.1005, Abstract, [0050]; Ex.1003, ¶89.

Mathiassen and Ryan render obvious *improving online transaction security*. Mathiassen’s portable device improves “general communication security measures in a network” (Ex.1005, [0047]) and “encrypt[s] general information transactions between the IC (1) [of the portable device] and [a] network server (30)” (Ex.1005, [0050]). Mathiassen explains that online transactions may be carried out with “a computer terminal, an internet bank or a corporate or government intranet.” Ex.1005, Abstract, [0016]; Ex.1003, ¶86.

Ryan describes a similar device, called a “compact personal token apparatus”⁵ (Ex.1006, Abstract) shown in Figure 2A below. Ex.1006, [0201]. Ex.1003, ¶87.



Ex.1006, Fig. 2A

Ryan’s “smart fob can operate as a security device” for “connect[ing] to a participating merchant’s website” and “conduct[ing] a business transaction in a secure fashion.” Ex.1006, [0232]. Examples of online transactions that may be conducted using Ryan’s smart fob include “downloading a ticket” (Ex.1006,

⁵ For brevity, Ryan’s “compact personal token apparatus” is referred to herein as a “smart fob.” Ex.1006, [0149].

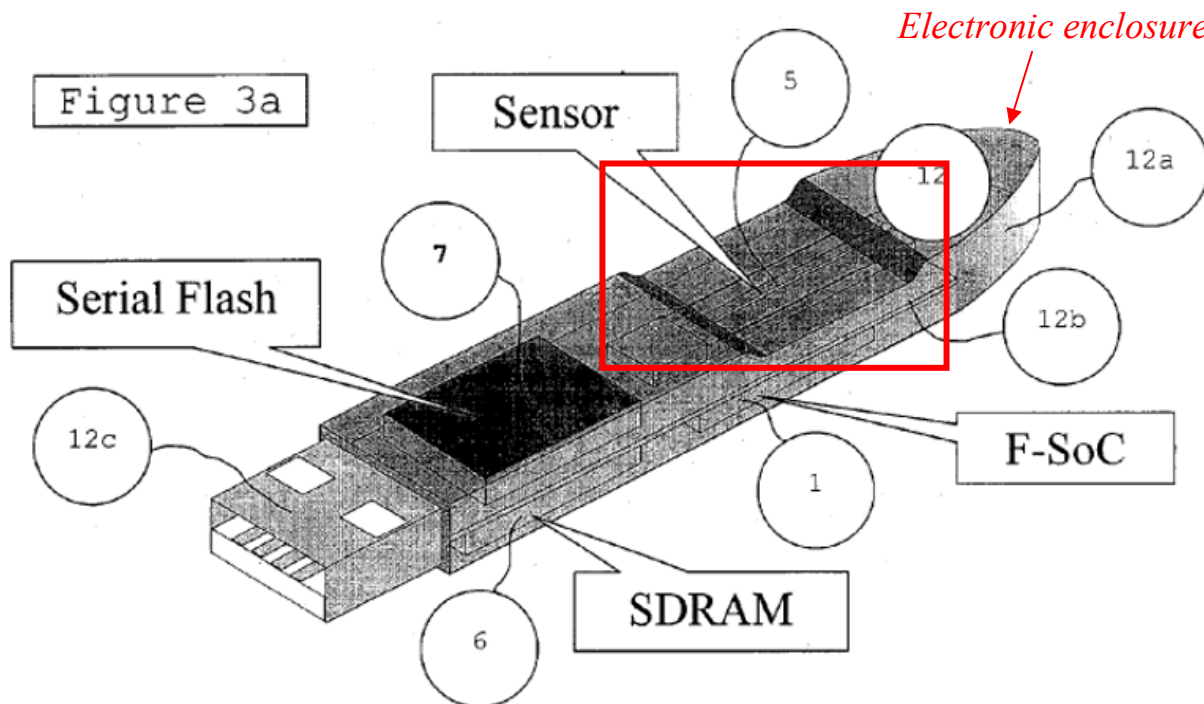
[0223]), “stor[ing] ‘e-coupons’” (Ex.1006, [0224]), and “load[ing] cash” for in-person and/or online payments (Ex.1006, [0225], [0236]). These transactions are completed after successful biometric authentication of the user (Ex.1006, [0229]) and are encrypted (Ex.1006, [0241]). A POSITA would have been motivated to modify Mathiassen’s portable device to be used to improve the security of any of the transactions described in Ryan. *See* §VI.A.3 (Motivation to Combine Mathiassen and Ryan); Ex.1003, ¶¶88, 90.

Thus, the Mathiassen-Ryan combination renders obvious *a biometric customer authentication apparatus* (Mathiassen’s portable device) *for improving online transaction security* (Ryan’s encrypted online transactions) *and for assuring the identity of a customer* (Mathiassen’s user authentication through fingerprint authentication software). Ex.1003, ¶¶90-91.

[1.1.1] an electronic enclosure including a fingerprint sensor disposed thereupon and

Mathiassen discloses or at least renders obvious limitation [1.1.1]. Ex.1003, ¶92.

Specifically, Mathiassen’s “portable device has a housing,” as shown in annotated Figure 3a below. Ex.1005, [0055].



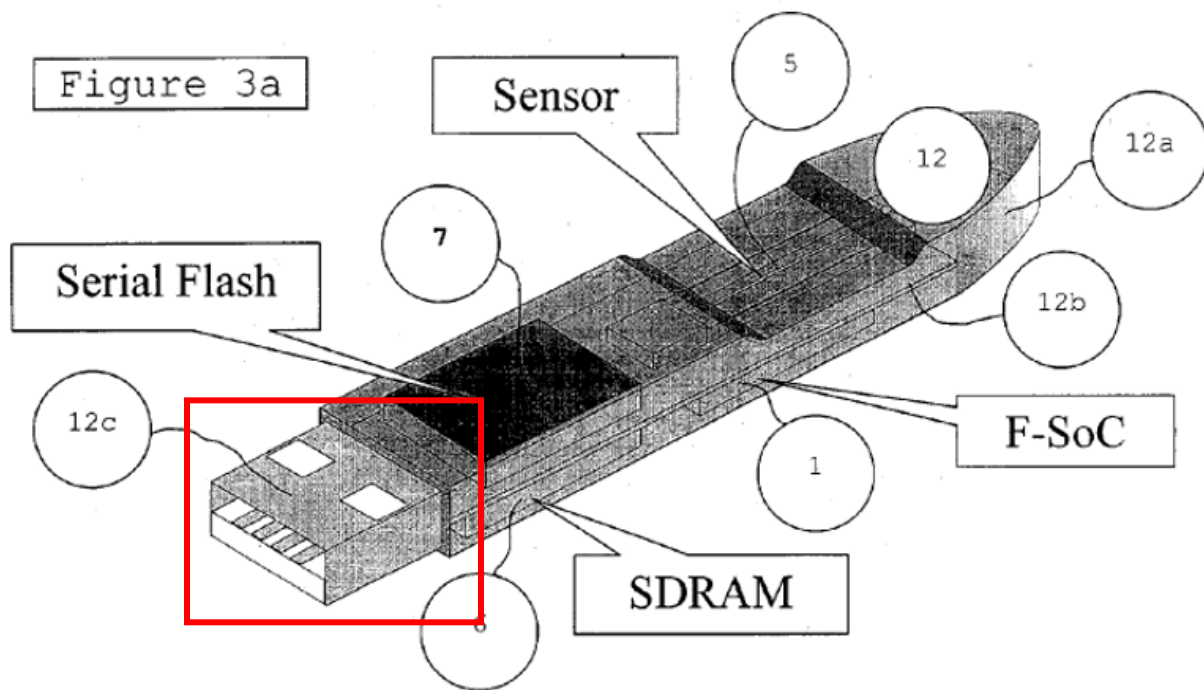
Ex.1005, Fig. 3a (annotated)

This housing discloses the *electronic enclosure* because electronic “components and chips are protected inside [the] housing.” Ex.1005, [0054]. As shown in Figure 3a above, Mathiassen’s housing (*electronic enclosure*) includes a fingerprint sensor 5 on the housing. See §VI.A.4.a.,[1.0]; Ex.1005, [0055] (“the portable device has a housing designed with a recess thus enabling a finger (A) to be placed on, or swiped over the sensor (5)”). Thus, Mathiassen teaches *an electronic enclosure* (a housing) *including a fingerprint sensor* (fingerprint sensor 5) *disposed thereupon*. Ex.1003, ¶92.

[1.1.2] further including an external communications interface;

Mathiassen discloses or at least renders obvious limitation [1.1.2]. Ex.1003, ¶93.

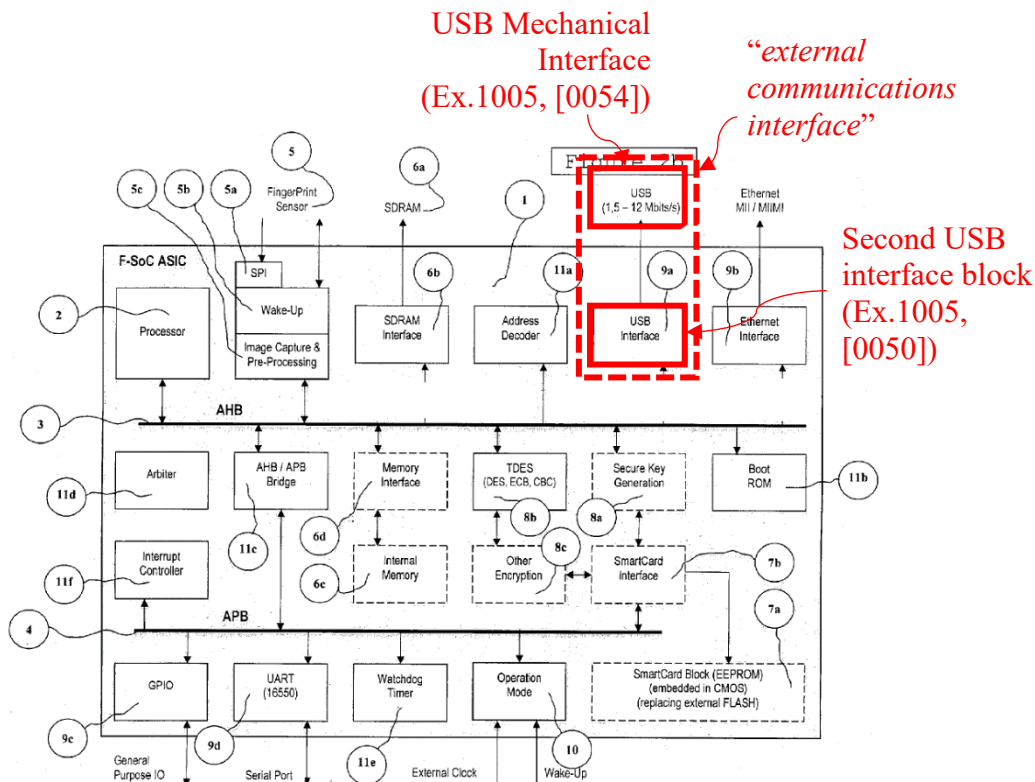
Specifically, Mathiassen discloses that its housing (*electronic enclosure*) includ[es] an external communications interface, which is a physical USB connector or USB plug described as a “USB interface (12C)” shown in Figure 3a below. Ex.1005, [0054].



Ex.1005, Fig. 3a (annotated)

The USB interface 12C works in conjunction with “[e]lectronic surface components [which] support...the USB mechanical interface (12C)...mounted on

the PCB (12B).” Ex.1005, [0054]. These components are illustrated in the IC 1 of the PCB 12B shown in Figure 2b, below. Ex.1005, Fig. 2b, [0054]; Ex.1003, ¶93.



Ex.1005, Fig. 2b (annotated)

Specifically, Mathiassen describes “a number of second interface blocks (9A, 9B, 9C or 9D)” that “comprise hardware and software for supporting a USB (9A)...interface.” Ex.1005, [0050]. As shown, the second USB interface block (9A) is coupled to the physical USB connector, referred to as the “USB mechanical interface (12C).” Ex.1005, [0054]. Together, the USB mechanical interface 12C and the USB interface block 9A disclose an *external communications interface*. Ex.1005, [0050] (“The IC (1) also comprises hardware and/or software required to supply

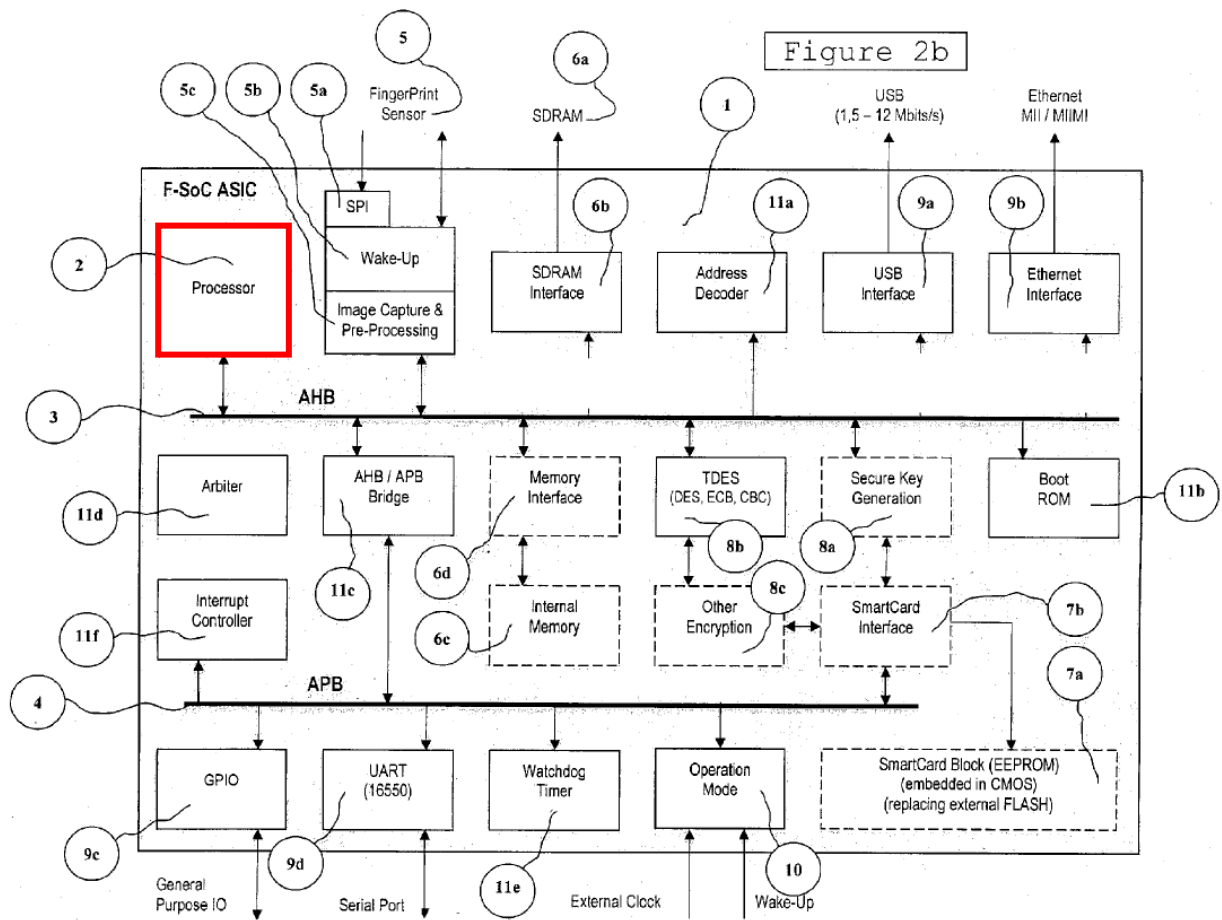
output signals to a number of second interface blocks (9A, 9B, 9C or 9D) for transferring data to other devices and networks (N) external to the IC (1).”). Ex.1003, ¶93.

[1.2.1] at least one processor comprised within said enclosure and

Mathiassen discloses or at least renders obvious limitation [1.2.1]. Ex.1003, ¶94.

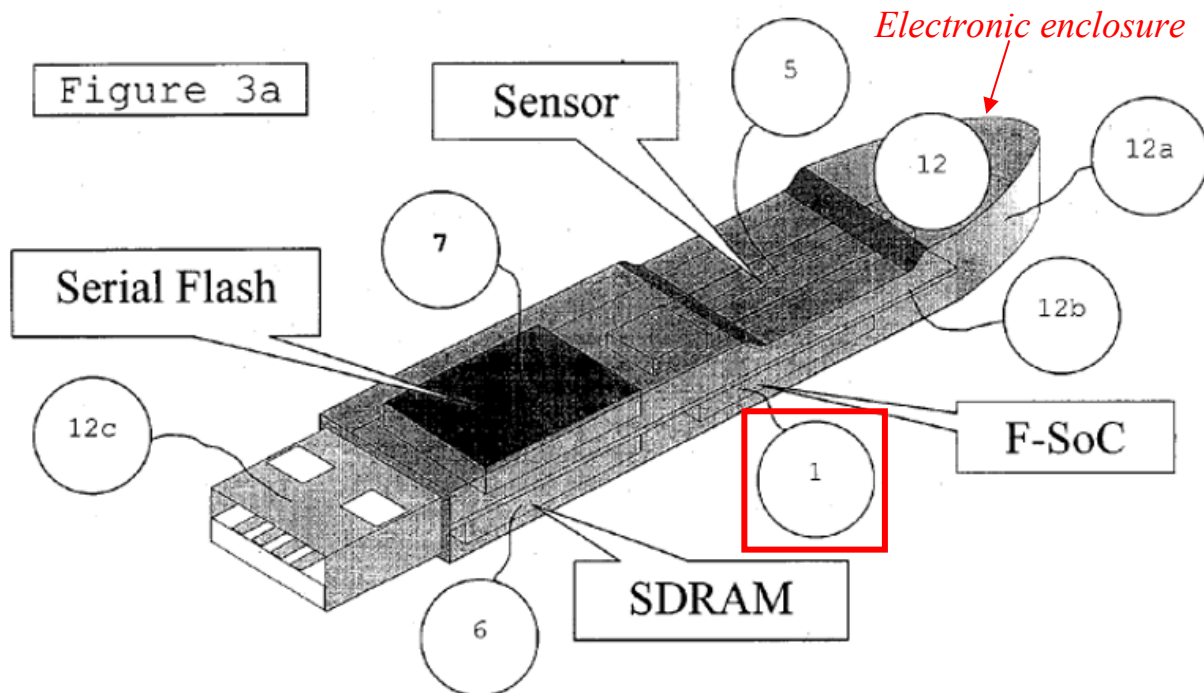
As discussed for limitation [1.1.1], Mathiassen discloses an *enclosure* (housing). Ex.1003, ¶94.

As shown in Figure 2b below, the integrated circuit, which is within Mathiassen’s portable device, includes a processor 2. Ex.1005, [0054] (“the portable device has an IC (1)”), [0050] (“[T]he IC (1)” includes “the central processor (2).”), [0037] (“FIG. 2b [s]hows a second realization of an integrated circuit that is an integral part of the invention.”). Ex.1003, ¶94.



Ex.1005, Fig. 2b (annotated)

As shown in Figure 3a below, the IC 1, which includes the processor 2, is within the housing. Ex.1005, [0048] (“integrated circuit—IC (1)...is the core device of the invention”); Ex.1003, ¶95.



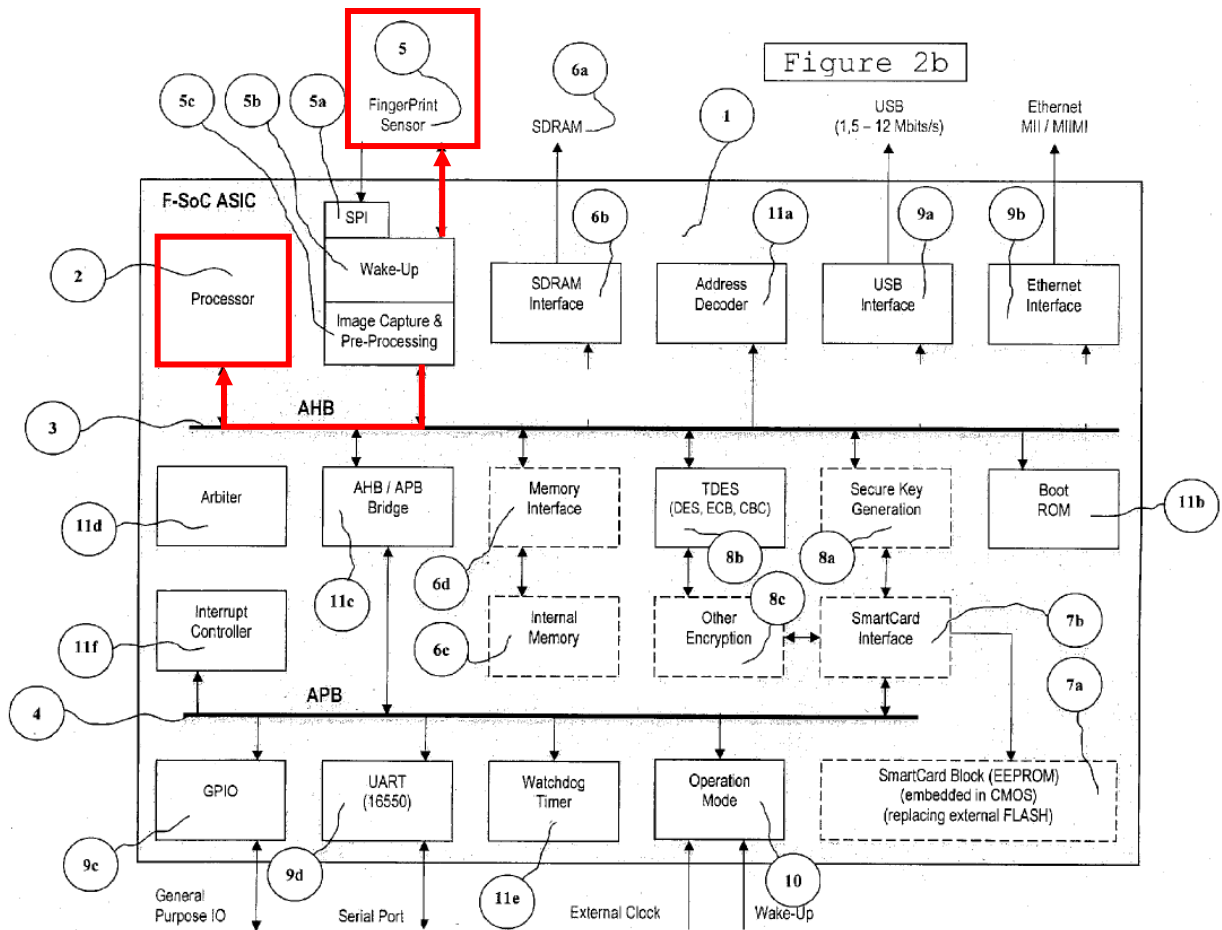
Ex.1005, Fig. 3a (annotated)

Thus, Mathiassen discloses *at least one processor* (processor 2) *comprised within said enclosure* (housing). Ex.1003, ¶96.

[1.2.2] [at least one processor...] coupled to said fingerprint sensor;

Mathiassen discloses or at least renders obvious limitation [1.2.2]. Ex.1003, ¶¶97-98.

As shown in Figure 2b below, the processor 2 of Mathiassen's portable device is coupled to the fingerprint sensor 5 via the high-speed bus 3. Ex.1005, [0066]-[0067]; Ex.1003, ¶97.



Ex.1005, Fig. 2b (annotated)

Mathiassen describes how data is transferred from the fingerprint sensor 5 to the processor 2 via the wake-up block 5B, the pre-processing block 5C, and high-speed bus 3. Ex.1005, [0066]-[0069], [0047] (“the biometrics processor (F) is directly connected to [t]he sensor (B)”). Specifically, when the sensor 5 detects a fingerprint, it “trigger[s] a signal to the wake-up block (5B).” Ex.1005, [0066]. Then, “[t]he pre-processing block ([5]C) will crunch the...captured fingerprint images” (Ex.1005, [0068]) into “reduced data” that is “transferred from the working volatile

memory ([5]C) to the central processor (2) via the high-speed bus (3)” (Ex.1005, [0069]). Ex.1003, ¶97.

Therefore, Matthiassen discloses *at least one processor* (processor 2) *coupled to said fingerprint sensor* (fingerprint sensor 5). Ex.1003, ¶98.

[1.3.1] transaction security software resident within and executing on said at least one processor

Mathiassen discloses or at least renders obvious limitation [1.3.1]. Ex.1003, ¶¶99-103.

First, Mathiassen teaches *transaction security software* described as “administrative software.” Ex.1005, [0050] (memory “used for storing program code, e.g., administrative software”); Ex.1003, ¶99.

Mathiassen’s administrative software discloses *transaction security software* because it contains a subset of software for biometrically authenticating fingerprints (*biometric fingerprint authentication software* (limitation [1.3.2])) and a subset for encrypting output data (corresponding to *cryptographic transaction authentication software* (limitation [1.3.3])). Ex.1005, [0072] (a “subset of the administrative software” includes a “matching algorithm” for authenticating fingerprints), [0091]-[0095] (an additional “subset of administrative software” then “generat[es] a secure key or password” and “appl[ies] encryption methods” to “produce secured output data”); Ex.1003, ¶100.

Second, Mathiassen teaches or at least renders obvious *transaction security software...executing on said at least one processor*. Mathiassen explains that “the administrative software...[is] run on the central processor (2).” Ex.1005, [0050] (“[T]he IC (1)” includes “the central processor (2).”). Thus, Mathiassen’s administrative software, which is run on the processor 2, teaches *transaction security software...executing on said at least one processor*. Ex.1003, ¶101.

Third, Mathiassen teaches or at least renders obvious *transaction security software resident within...said at least one processor*. As discussed in the claim construction analysis above (§V.A), a POSITA would have understood the term *resident within* to mean temporary storage of the software while the software is being executed. Mathiassen’s administrative software is *resident within* the processor 2 when it is executed by the processor 2. Ex.1005, [0050] (“[T]he administrative software...[is] run on the central processor (2).”). Ex.1003, ¶101. As explained in §V.A, when software is executed on a processor, it is resident within a cache memory of the processor. Ex.1003, ¶101. This is consistent with the disclosure of the ’637 patent. The ’637 patent explains that the memory of the processor 16 is for “**the execution of programs,**” not long-term storage. Ex.1001, 5:13-14. Like conventional processor-based architectures, the non-volatile memory of the ’637 patent is used for long-term storage. Ex.1001, 5:15-20; Ex.1003, ¶102.

The architecture of Mathiassen's portable device is the same as the '637 patent, including a non-volatile memory and a central processor. *Compare* Ex.1005, Figure 2b (illustrating memory 7a in communication with processor 2), [0050], *with* '637 Patent, 5:9-20 (describing "processor 16" and "non-volatile memory"). Mathiassen's administrative software, which corresponds to *transaction security software*, is executed by its central processor. Ex.1005, [0050]. Thus, just as the transaction security software of the '637 patent is transferred to its processor 16 for execution, Mathiassen's administrative software is transferred to its central processor 2 for execution. Ex.1005, [0050] ("[T]he administrative software [is] stored in the non-volatile memory (7, 7A or 7C) and run on the central processor (2)."); Ex.1003, ¶103 (citing Ex.1010, 1:20-2:47, Ex.1019, 14:46-49). During the process of transferring software to the processor 2 and executing the software by the processor 2, the administrative security software is resident within the processor 2, thus teaching *transaction security software resident within...said at least one processor*. Ex.1003, ¶103.

[1.3.2] further comprising biometric fingerprint authentication software for authenticating authorized customers

Mathiassen discloses or at least renders obvious limitation [1.3.2]. Ex.1003, ¶¶104-108.

As discussed in limitation [1.3.1], Mathiassen's administrative software corresponds to *transaction security software* (see §VI.A.4.a.,[1.3.1]). A "subset of the administrative software" includes "matching algorithm" software for fingerprint authentication. Ex.1005, [0072]; Ex.1003, ¶104.

In Mathiassen, the fingerprint sensor 5 captures "raw images" of a fingerprint, and the pre-processing block 5C processes the images into "intermediate results." Ex.1005, [0049]. The processor 2 receives the intermediate results and reduces them into "compact fingerprint representations, called minutiae." Ex.1005, [0050]. "These fingerprint representations (master minutiae) are compared by the central processor (2) with master fingerprint representations stored in non-volatile memory (7, 7A or 7C)." Ex.1005, [0050]. In this way, the processor 2 biometrically authenticates a user. 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**...pre-stored in the non-volatile memory (7, 7A or 7C)."). Mathiassen explains this same process of matching a received fingerprint with a pre-stored fingerprint to authenticate a user (Ex.1005, [0065]-[0074]) and clarifies that this "matching algorithm" is "a subset of the administrative software" (Ex.1005, [0072]). Ex.1003, ¶¶105-107.

Thus, Mathiassen teaches *transaction security software* (administrative software) *further comprising biometric fingerprint authentication software for*

authenticating authorized customers (matching algorithm subset of administrative software). Ex.1003, ¶108.

[1.3.3] and also comprising cryptographic transaction authentication software for authenticating transactions;

The combination of Mathiassen and Ryan renders obvious limitation [1.3.3]. Ex.1003, ¶¶109-112.

Mathiassen's administrative software includes an additional subset for generating cryptographic data (*cryptographic transaction authentication software for authenticating transactions*). Ex.1005, [0091]-[0095] (describing "handshake sequences," "generating a secure key," "applying...encryption methods," and "produc[ing] secured output data"). In Mathiassen, if a user wants to securely access a network, a "subset of the administrative software...tailors [an] output secure response to the target network." Ex.1005, [0091]. This secure output is accessed and sent by the portable device after the user is biometrically authenticated. Ex.1005, [0097]. The secure output tailored by the subset of administrative software is cryptographically encapsulated (encrypted) to secure the message from the portable device to the target network that authenticates the user to the network. Ex.1005, [0077]-[0083]. For example, the subset of administrative software contains instructions that enable Mathiassen's portable device to "generat[e] a secure key or password" (Ex.1005, [0093]) "apply[] any of the encryption methods at hand"

(Ex.1005, [0094]), and “tailor[] handshake sequences” (Ex.1005, [0095]). “By these features of the invention a local fingerprint authentication at the device (12 or 13) will be transformed to a password...as per the secure communication procedure of the prevailing network (30).” Ex.1005, [0098]; Ex.1003, ¶¶109-110.

This generated secure output grants the user of Mathiassen’s portable device access to online entities, such as “an internet bank or a corporate or government intranet.” Ex.1005, Abstract. In addition, a POSITA would have understood that Mathiassen’s use of cryptography to secure data sent to a target network for user authentication purposes would also be used to secure data for online transactions because Ryan describes encrypting transaction data. Ex.1006, [0249]. For example, Ryan describes how its smart fob, similar to Mathiassen’s portable device, may be used to secure a variety of online transactions, explaining that “[p]ersonal data, frequent flyer miles as well as credit card details can be encrypted.” Ex.1006, [0249]. In addition, Ryan explains that “merchant...data...could be encrypted.” Ex.1006, [0367]. Ryan also describes how “coupons are encrypted.” Ex.1006, [0368]. In addition, a POSITA would have been motivated to encrypt transaction data as described in Ryan, in addition to user authentication data as described in Mathiassen, to ensure that sensitive transaction data would not be intercepted and tampered with. *See* §VI.A.3; Ex.1006, [0249] (only the secure server can decrypt “[p]ersonal data, frequent flyer miles, as well as credit card details” and prevents “Internet ‘phishing’

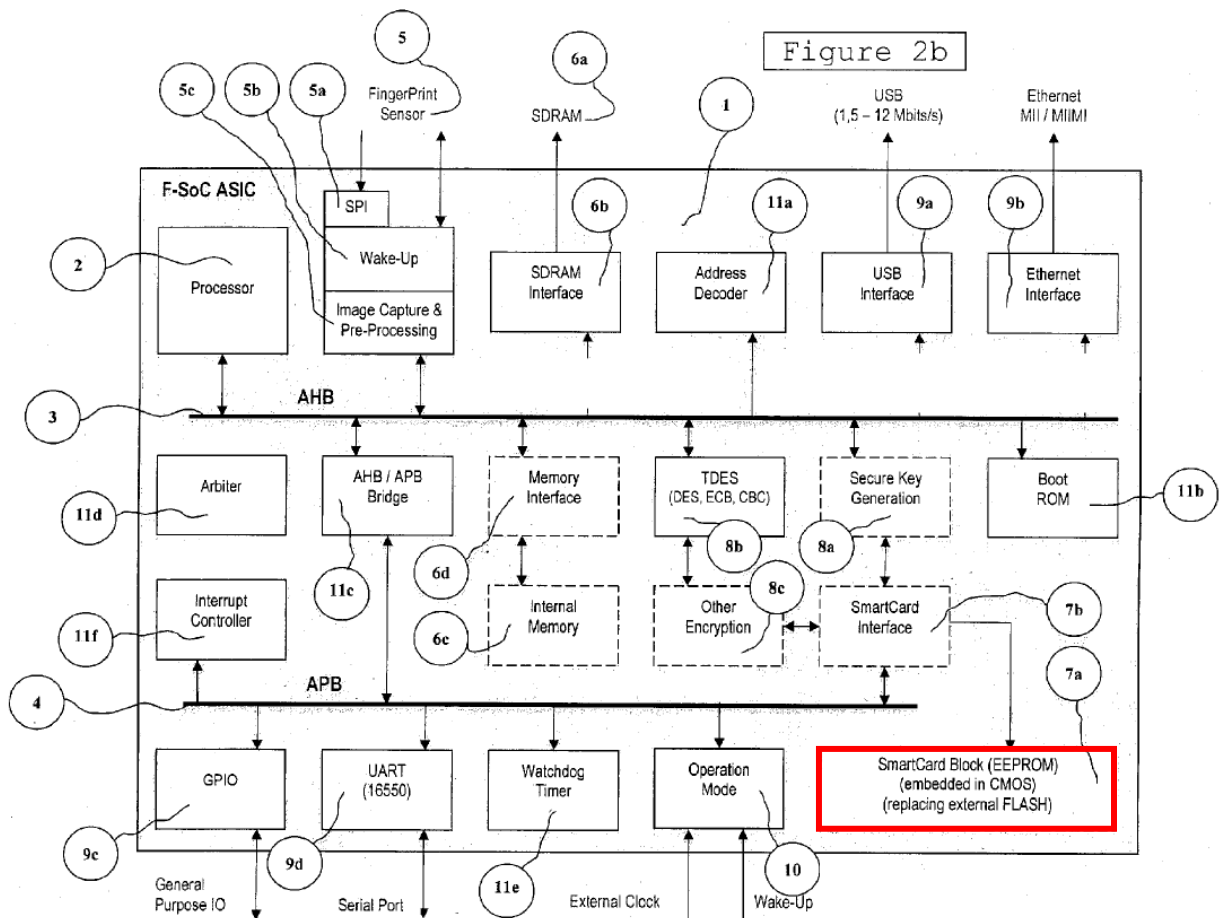
fraud”), [0238], [0105]. Thus, a POSITA would have understood that Mathiassen’s subset of administrative software which encrypts data related to user authentication to access online entities where online transactions occur would also be used to encrypt data relating to online transactions themselves to ensure that these transactions are properly authenticated and not intercepted or modified. Ex.1003, ¶111.

Thus, the Mathiassen-Ryan combination renders obvious *transaction security software* (administrative software) *also comprising cryptographic transaction authentication software for authenticating transactions* (subset of administrative software for generating cryptographic data). Ex.1003, ¶112.

[1.4.1] at least one of a memory and

Mathiassen discloses or at least renders obvious limitation [1.4.1]. Ex.1003, ¶¶113-114.

Mathiassen’s portable device includes “non-volatile memory (7, 7A, or 7C).” Ex.1005, [0050]. Non-volatile memory 7A is highlighted in Mathiassen’s Figure 2b below. Ex.1003, ¶113.



Ex.1005, Fig. 2b (annotated)

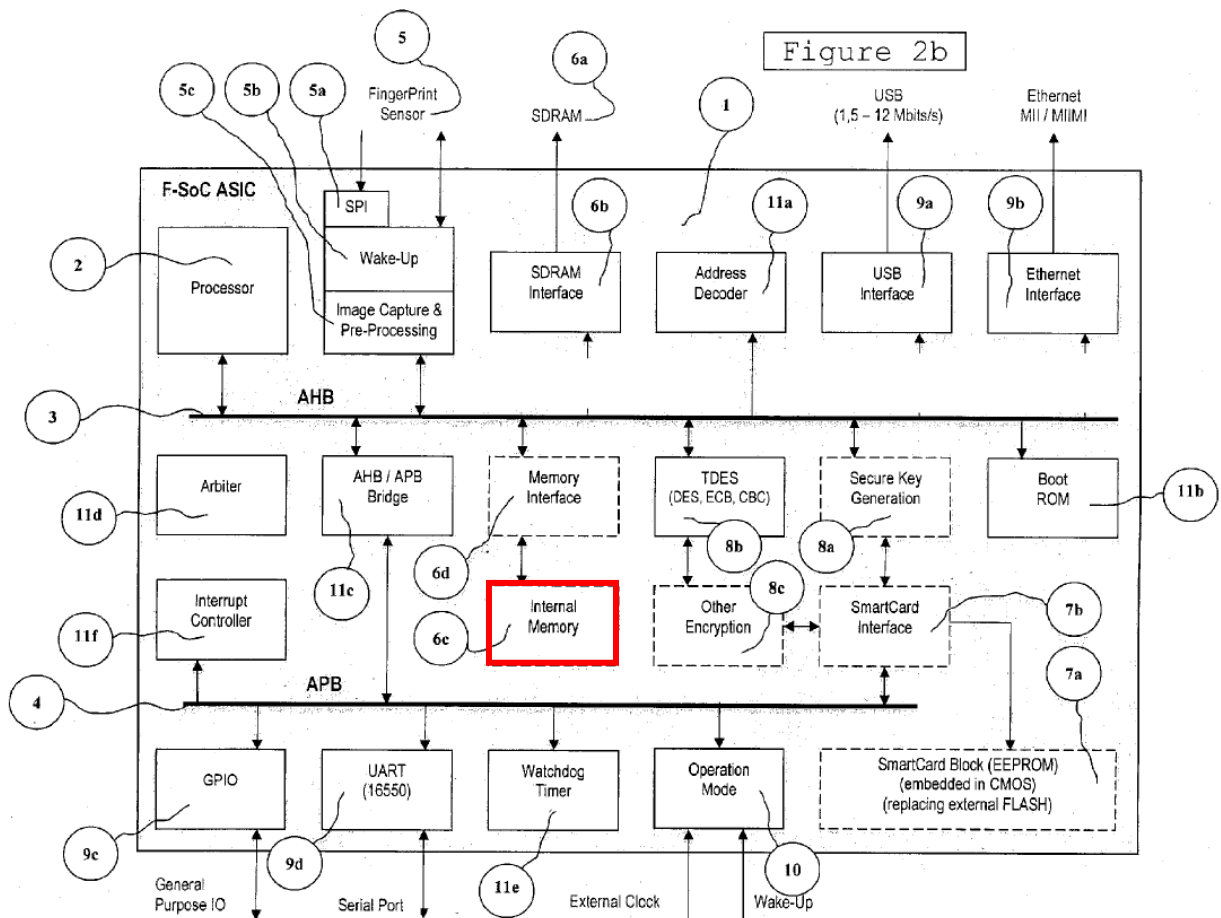
Thus, Mathiassen discloses or at least renders obvious *at least one of a memory* (non-volatile memory 7A). Ex.1003, ¶114.

[1.4.2] a communications buffer

Mathiassen discloses or at least renders obvious limitation [1.4.2]. Ex.1003, ¶¶115-119.

Based on the description in the '637 patent, a POSITA would have understood *a communications buffer* to refer to a memory for sending and receiving data. The

'637 patent uses the term “communications buffer” when describing the processor 16 of the ITA apparatus: “[p]rocessor 16 also contains memory for the execution of programs plus *communications buffers for sending and receiving data.*” Ex.1001, 5:13-15. Mathiassen’s internal memory, highlighted in Figure 2b below, also referred to as “volatile memory (6C),” is a *communications buffer* because it is memory used for sending and receiving data. Ex.1005, [0052] (“volatile memory (6C)” and “data exchange”), [0049]-[0050] (“The volatile memory (6A or 6C) thus provides working memory that is available to other modules on the IC (1)” such as “interface blocks (9A, 9B, 9C or 9D) for transferring data to other devices.”); Ex.1003, ¶¶115-116.



Ex.1005, Fig. 2b (annotated)

Mathiassen discloses that “intermediate” data are stored in the “working volatile memory (6A or 6C)” before being “gradually transferred from the working volatile memory.” Ex.1005, [0068]-[0069]. Thus, the volatile memory 6C is a memory used for sending and receiving data because Mathiassen describes the volatile memory receiving “intermediate” data and transferring that data. Ex.1003, ¶117.

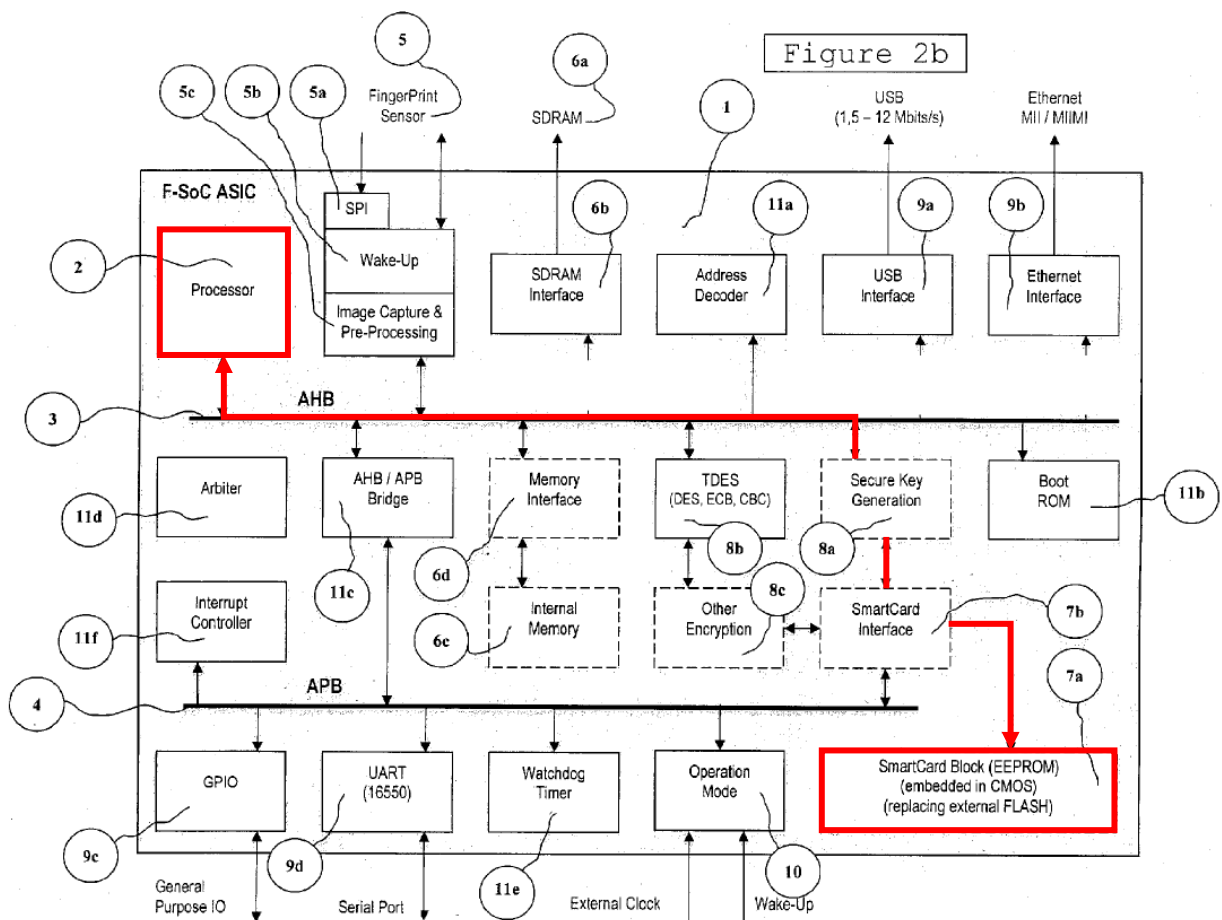
In addition, “[t]he volatile memory (6A or 6C)...provides working memory that is available to other modules on the IC (1).” Ex.1005, [0049]. These modules include interfaces 9A, 9B, 9C, and 9D used for “transferring data to other devices.” Ex.1005, [0050]. Accordingly, the volatile memory is also memory for sending and receiving external data. Ex.1003, ¶118.

Thus, Mathiassen’s volatile memory 6C is a memory used for sending and receiving data and discloses or render obvious *a communications buffer* as claimed. Ex.1003, ¶119.

[1.4.3] coupled to said at least one processor and

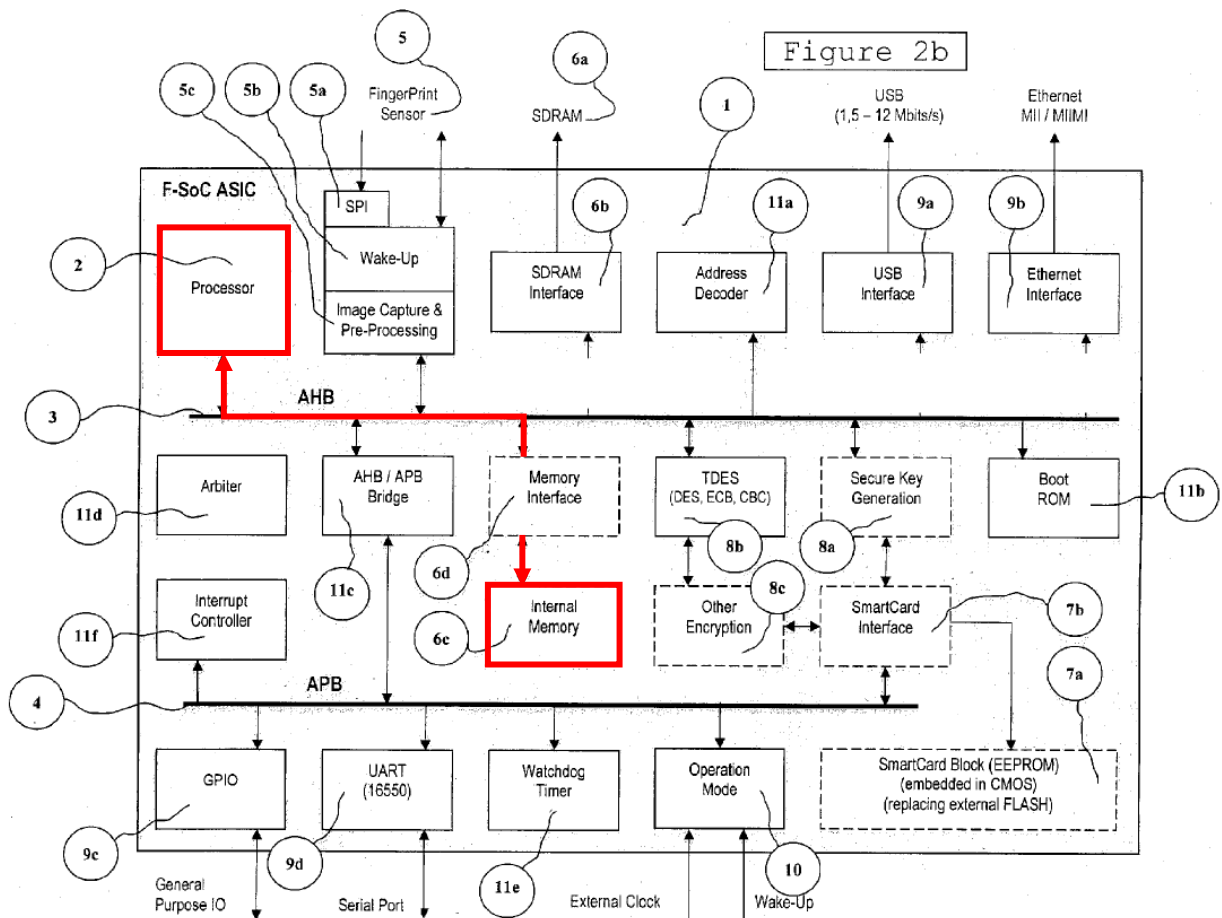
Mathiassen discloses or at least renders obvious limitation [1.4.3]. Ex.1003, ¶¶120-122. As explained at limitation [1.4.1], Mathiassen’s non-volatile memory 7A is *at least one of a memory*. As explained at limitation [1.4.2], Mathiassen’s volatile memory 6C is *a communications buffer*. As shown below, both the non-volatile memory 7A and the volatile memory 6C are coupled to the processor 2 in Mathiassen.

Mathiassen teaches that “[t]he non-volatile memory (7, 7A or 7E) [is] coupled to the high-speed bus (3) via a second memory interface block,” and “[t]he processor unit (2) is also connected to the high-speed bus (3).” Ex.1005, [0050]. This coupling of the non-volatile memory 7A to the processor 2 is illustrated in Figure 2b below. Ex.1003, ¶120.



Ex.1005, Fig. 2b (annotated)

Mathiassen's volatile memory 6C, which corresponds to a *communications buffer* (see §VI.A.4.a.,[1.4.2]), "[is] connected to the high-speed bus (3)" (Ex.1005, [0049]), and "[t]he processor unit (2) is also connected to the high-speed bus (3)" (Ex.1005, [0050]). This is also shown in Figure 2b below. Ex.1003, ¶121.



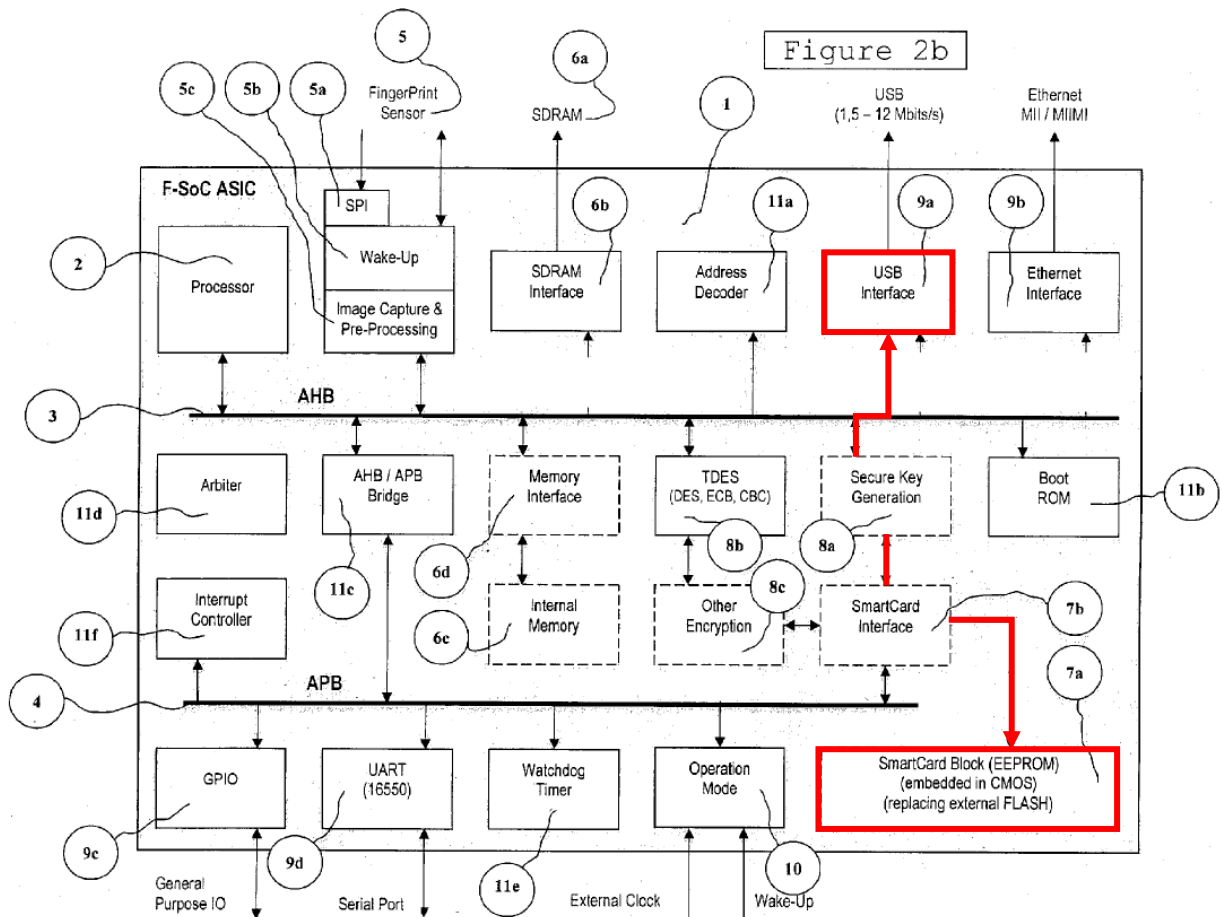
Ex.1005, Fig. 2b (annotated)

Thus, Matthiassen teaches *at least one of a memory* (non-volatile memory 7A) *and a communications buffer* (volatile memory 6C) *coupled to said at least one processor*. Ex.1003, ¶122.

[1.4.4] [at least one of a memory and a communications buffer] further coupled to said external communications interface; and

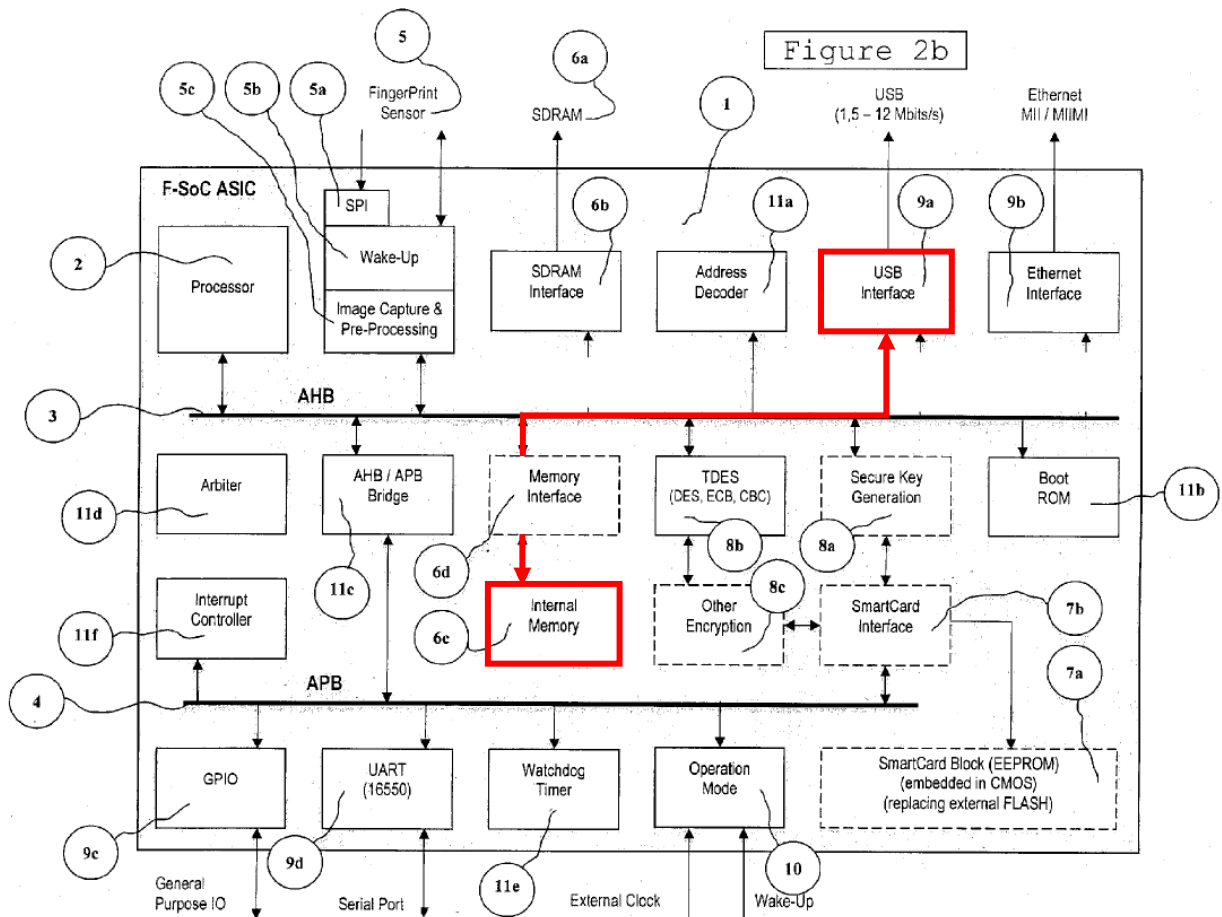
Matthiassen discloses or at least renders obvious limitation [1.4.4]. Ex.1003, ¶¶123-125.

As discussed above, Mathiassen's external communications interface includes the USB mechanical interface 12C and the USB interface block 9A in Figure 2b. *See* §VI.A.4.a.,[1.1.2]. As shown below, the non-volatile memory 7A is coupled to the USB communications interface 9A. Ex.1005, [0075] (describing transferring "a Java applet from its non-volatile memory (7, 7A or 7E)...via the USB port (9A)"). Ex.1003, ¶123.



Ex.1005, Fig. 2b (annotated)

Mathiassen also shows its volatile memory 6C, which corresponds to a “communications buffer” (see §VI.A.4.a.,[1.4.2]), coupled to the USB communications interface 9A, as shown in Figure 2b below. Ex.1005, [0049]-[0050] (“The volatile memory (6A or 6C) thus provides working memory that is available to other modules on the IC (1)” such as “interface blocks (9A, 9B, 9C or 9D).”); Ex.1003, ¶¶123-124.



Ex.1005, Fig. 2b (annotated)

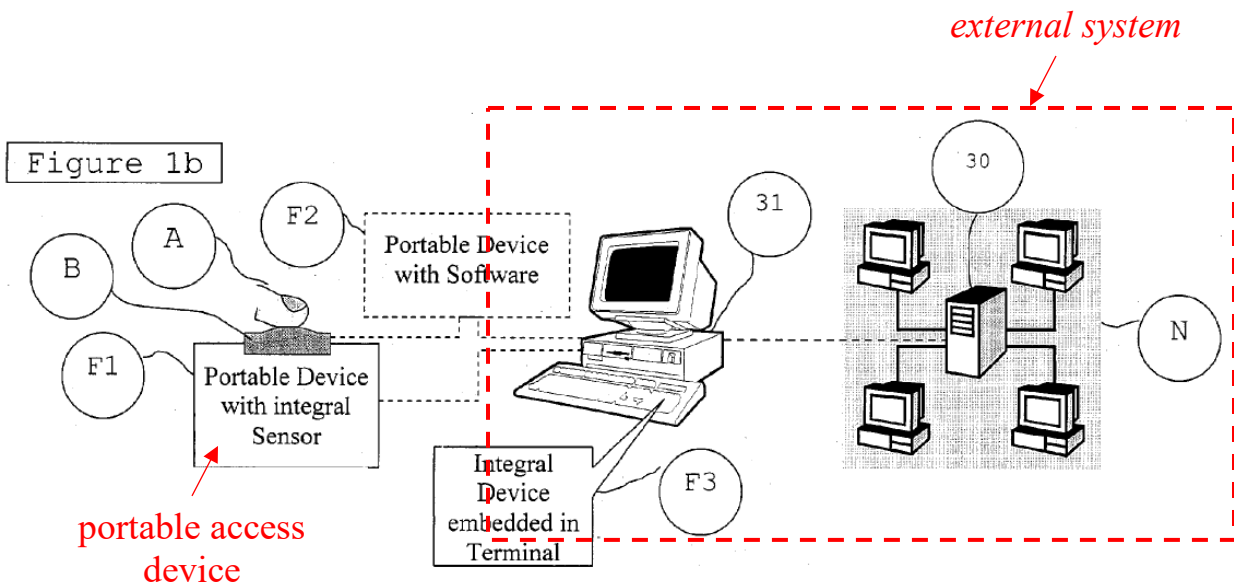
Thus, Mathiassen teaches *at least one of a memory* (non-volatile memory 7A) *and a communications buffer* (volatile memory 6C) *further coupled to said external communications interface* (USB interface 9A and USB mechanical interface 12C). Ex.1003, ¶125.

[1.5] a communications subsystem coupled into said external communications interface for relaying data messages between at least one external system and said apparatus.

Mathiassen discloses or at least renders obvious limitation [1.5]. Ex.1003, ¶¶126-131.

As explained in limitation [1.1.2] (§VI.A.4.a), Mathiassen's external communications interface includes the USB mechanical interface 12C and USB interface block 9A. The USB interface block 9A is a *subsystem coupled into said external communications interface* because it is a component of the external communications interface. Ex.1003, ¶¶126-127.

In addition, Mathiassen explains that the “second interface block[] (9A...)” is “for transferring data to other devices and networks (N) external to the IC (1)” such as an “external access-limited apparatus, device or system.” Ex.1005, [0050]. Mathiassen illustrates such an external system as the network N, which includes the server 30 and computer terminal 31 in Figure 1b below. Ex.1005, [0053] (“a server (30) in a network” and “a terminal (31) of the network”). Ex.1003, 127.



Ex.1005, Fig. 1b (annotated)

Figure 1b, above, shows Mathiassen’s “portable access device” (Ex.1005, [0047]), which corresponds to the claimed *apparatus*, in communication with an *external system* including a “server (30) in a network (N)” and “a terminal (31) of the network” (Ex.1005, [0053]); Ex.1003, ¶128.

Thus, Mathiassen teaches a *communications subsystem* (USB interface 9A) coupled into said *external communications interface* (USB interface 9A and USB mechanical interface 12C) for relaying data messages between at least one external system (network N) and said *apparatus* (portable device). Ex.1003, ¶129.

To the extent Patent Owner argues the terms *external communications interface* or *communications subsystem* map to different components of the ’637 patent than the mappings presented herein, Petitioner submits that the combination of Mathiassen and Ryan nonetheless render claim limitation [1.5] obvious because

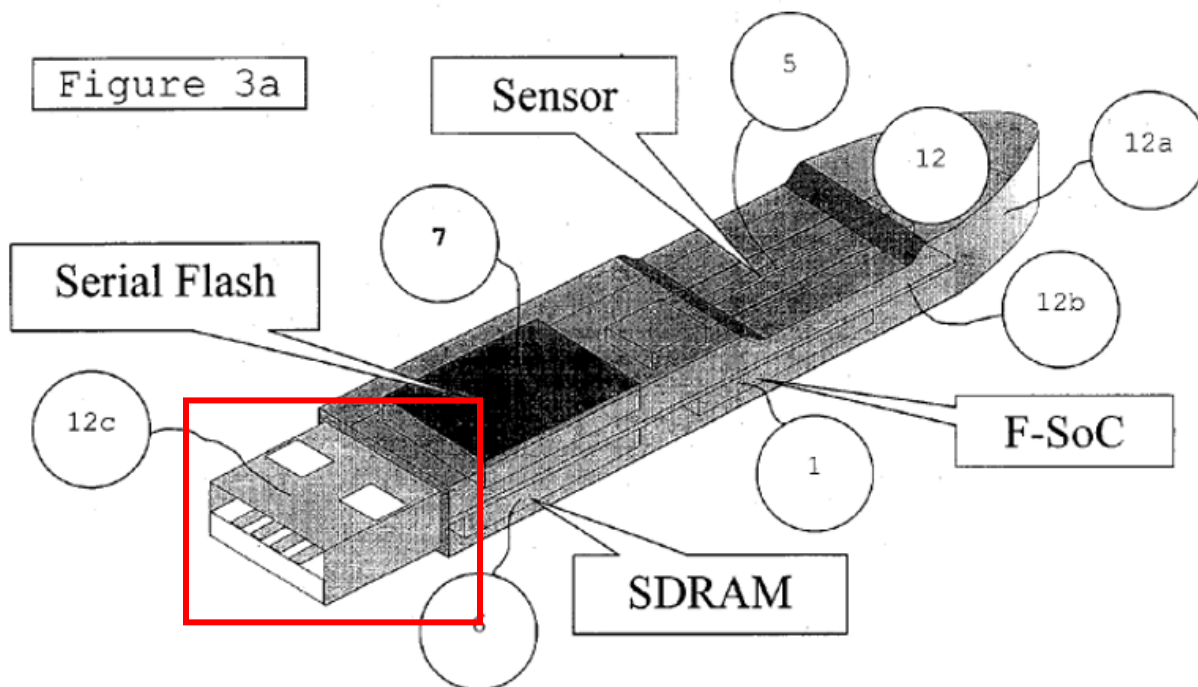
Mathiassen and Ryan describe the same components used for external communication. Specifically, the '637 patent provides only two embodiments of an *external communications interface* including a *communications subsystem*: (1) a standard USB plug (Ex.1001, Fig. 1A) and (2) a standard wireless antenna (Ex.1001, Fig. 1B). The combination of Mathiassen and Ryan teach both of these embodiments. Specifically, Mathiassen's portable device includes a "USB interface (12C)" illustrated as a physical USB plug. Ex.1005, [0054], Fig. 3a; §§VI.A.4.b-c. Ryan's "compact personal token apparatus comprises a wireless interface." Ex.1006, [0124], Fig. 1A, Fig. 2B; §VI.A.2 (Overview of Ryan), §VI.A.4.d (limitation [4.0]). The '637 patent does not describe either of these interfaces (the USB plug or wireless antenna) as anything more than the same conventional USB connectors and antennas described in Mathiassen and Ryan. Ex.1003, ¶129. Thus, to the extent Patent Owner characterizes different components as mapping to the claim terms *external communications interface* or *communications subsystem*, Mathiassen and Ryan disclose the same components and these mappings would also be disclosed or rendered obvious. Ex.1003, ¶¶130-131.

b. Claim 2

[2.0] The apparatus of claim 1, wherein said external communications interface further comprises a physical interface connector for physical insertion into an external interface port disposed upon one of a host system and said at least one external system.

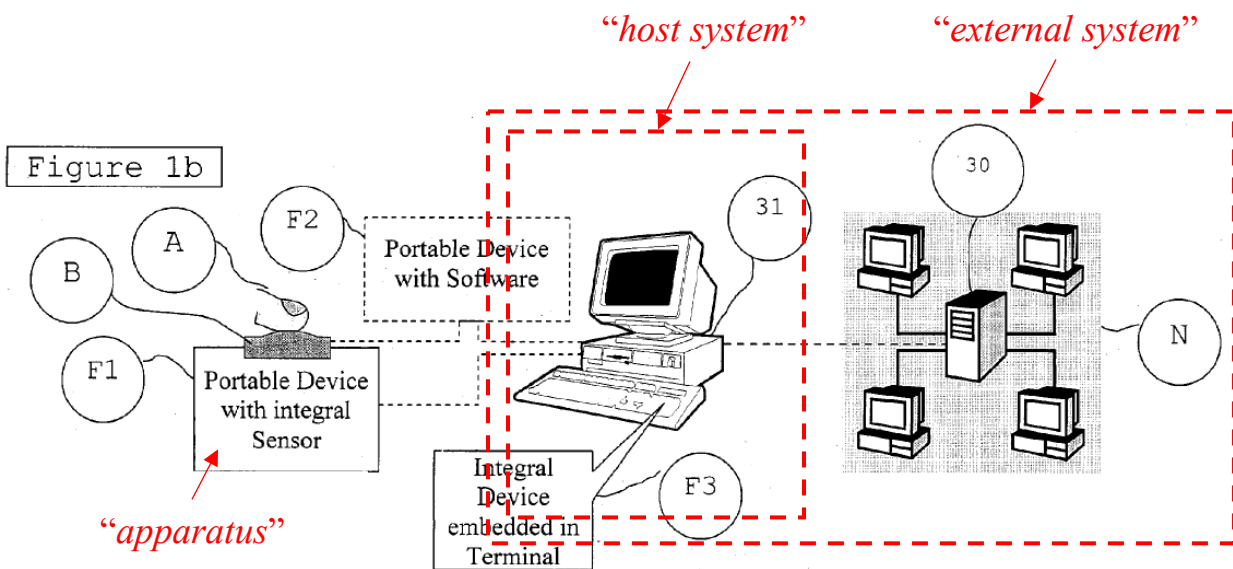
Mathiassen renders obvious limitation [2.0]. Ex.1003, ¶¶132-135.

As previously described at [1.1.2] (§VI.A.4.a), Mathiassen's USB mechanical interface 12C and USB interface block 9A correspond to an *external communications interface*. Mathiassen's USB mechanical interface 12C, illustrated in Figure 3a, is a *physical interface connector*. Ex.1005, [0065] (“[t]he user will insert the portable device (12 or 13) into [a] USB port”); Ex.1003, ¶132.



Ex.1005, Fig. 3a (annotated)

Thus, Mathiassen's USB mechanical interface 12C is *for physical insertion into an external interface port* because it is "insert[ed]...into [a] USB port." Ex.1005, [0065]. This USB port is on the computer terminal 31, a *host system* of the *external system* shown in Figure 1b. Ex.1003, ¶133.



Ex.1005, Fig. 1b (annotated)

The computer terminal 31 includes the USB connector port. Ex.1005, [0053] (“the IC (1) is a portable device to be plugged into a terminal (31).”). The USB port of the computer terminal 31 is an external interface port of *one of a host system and said at least one external system*. Ex.1003, ¶134. Mathiassen's network N corresponds to *said external system*. See §VI.A.4.a,[1.5]. The computer terminal 31 is part “of the network” N. Ex.1005, [0053]. The computer terminal 31 is a *host system* and described as a “host device.” Ex.1005, claim 9; Ex.1003, ¶134.

Thus, Mathiassen teaches *a physical interface connector* (USB mechanical interface 12C) *for physical insertion into an external interface port* (USB port of computer terminal 31) *disposed upon one of a host system* (computer terminal 31) *and said at least one external system* (network N). Ex.1003, ¶135.

c. Claim 3

[3.0] The apparatus of claim 2, wherein said external communications interface further comprising said physical interface connector, further comprises a USB connector for insertion into an external interface port disposed upon one of said host system and said at least one external system.

Mathiassen renders obvious limitation [3.0]. Ex.1003, ¶136.

Claim 3 further defines the *physical interface connector* of claim 2 as a *USB connector*. The physical interface connector of Mathiassen described at claim 2 is a USB connector that inserted into the terminal 31 of network N. Ex.1005, [0054] (“USB interface (12C)”), [0065] (“[t]he user will insert the portable device (12 or 13) into [a] USB port”), [0053]; Ex.1003, ¶136.

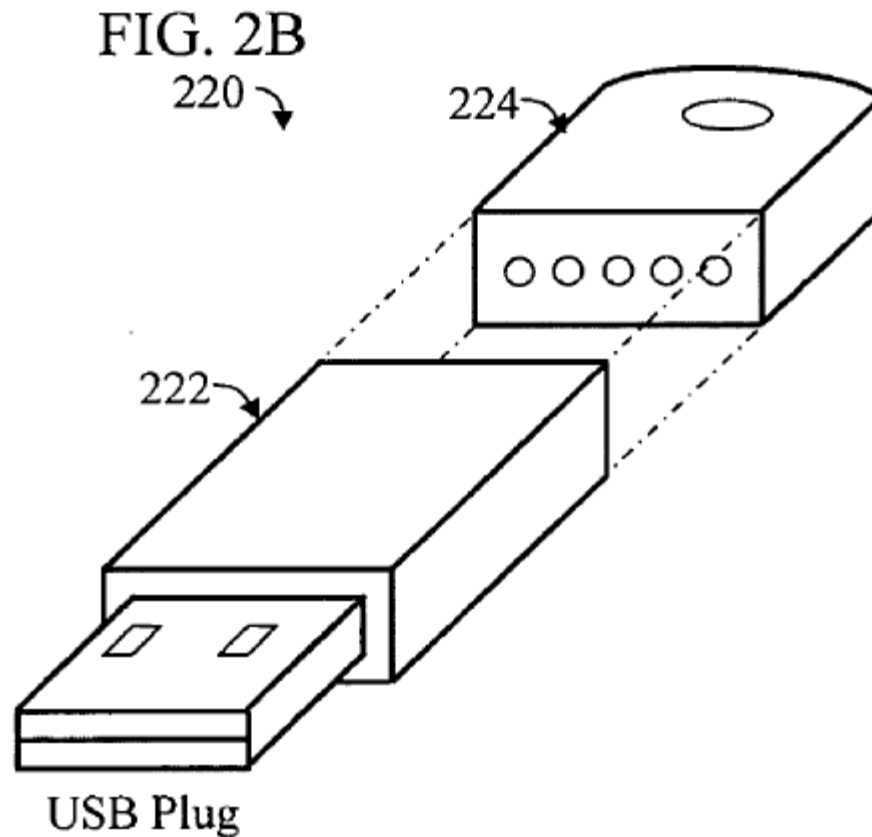
d. Claim 4

[4.0] The apparatus of claim 1, wherein said external communications interface further comprises a first wireless transceiver for wirelessly communicating with a second wireless transceiver communications interface aboard one of a host system and said at least one external system.

The combination of Mathiassen and Ryan renders obvious limitation [4.0]. Ex.1003, ¶¶137-140.

Mathiassen's portable device includes an external communications interface. *See* §VI.A.4.a,[1.1.2]. While Matthiassen's USB mechanical interface 12C and USB interface block 9A correspond to the '637 patent's *external communications interface*, Mathiassen also contemplates multiple other types of communications interfaces, including “a number of second interface blocks (9A, 9B, 9C or 9D).” Ex.1005, [0050]. These interface blocks facilitate data communication via “USB (9A), Ethernet (9B), GPIO (9C), PCMCIA/UART (9D) and/or SmartCard (7C).” Ex.1005, [0050]. While Mathiassen does not explicitly disclose a wireless interface, given the multiple types of interfaces contemplated, a POSITA at the time would have understood that Mathiassen's portable device would be readily modified to include a wireless interface, as taught by Ryan. *See* §VI.A.3; Ex.1003, ¶137.

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



Ex.1006, Fig. 2B

As shown in Figure 2B, Ryan's smart fob includes a "first physical module 222" that contains the USB plug, also referred to as "the input module," and a "second physical module 224" referred to as an "output module." Ex.1006, [0203]. The output module within the second physical module 224 includes an "RF antenna and modulator." Ex.1006, [0203], Fig. 1A. Ryan explains how its smart fob communicates wirelessly with other external devices that also have wireless transceivers. *See, e.g.*, Ex.1006, [0235] ("wav[ing] the device in close proximity to a turnstile **equipped with a wireless reader**") [0229] ("wav[ing] the smart fob in front of a reader"); Ex.1003,

¶¶138-139; *see also* §VI.A.3 (motivation to combine wireless functionality of Ryan with Mathiassen’s portable device).

Thus, the Mathiassen-Ryan combination renders obvious *a first wireless transceiver* (RF antenna 108 within second physical module 224) *for wirelessly communicating with a second wireless transceiver communications interface* (wireless reader of external device) *aboard one of a host system* (computer terminal 31) *and said at least one external system* (network N). Ex.1003, ¶140.

e. Claim 5

[5.0] The apparatus of claim 1, wherein said at least one of a memory and a communications buffer is further adapted for storing and retrieving data and for communicating data messages between said apparatus and said at least one external system via said external communications interface.

Mathiassen renders obvious limitation [5.0]. Ex.1003, ¶¶141-145.

Mathiassen’s “non-volatile memory (7, 7A, or 7C)” (Ex.1005, [0050]) corresponds to the *memory* claimed. *See* §VI.A.4.a,[1.4.1]. Mathiassen’s non-volatile memory 7A *is...adapted for storing and retrieving data*. Ex.1005, [0050] (“The non-volatile memory (7, 7A or 7E)...is typically used for storing program code, e.g. administrative software, tailored security output responses, secret information like seed and key number(s) for the encryption, electronic certificates and fingerprint representations in the form of so-called minutiae.”). Similarly, the non-volatile memory 7A is for “data exchange.” Ex.1005, [0052]; Ex.1003, ¶141.

Mathiassen's non-volatile memory 7A is also *adapted for...communicating data messages between said apparatus and said at least one external system via said external communications interface*. Specifically, the non-volatile memory 7A stores communication data to be sent to the network N, including, for example, a “tailored security output response[.]” Ex.1005, [0050]. This response includes a “message communication” which may comprise “an IP address” (Ex.1005, [0074], [0077]) and a “seed” corresponding to a “secure key” (Ex.1005, [0076], [0080]), both of which are stored within the non-volatile memory 7A (Ex.1005, [0050] (“seed, key numbers, IP address, etc. may by...stored on a regular Flash memory (7), or...in SmartCard environments (7A or 7C)”). This data is sent from Mathiassen's portable device to the network 30, which corresponds to an *external system*. Ex.1005, [0086]. Thus, by storing data to be communicated, the non-volatile memory 7C is *adapted for...communicating data messages between said apparatus and said at least one external system via said external communications interface*. Ex.1003, ¶142.

Mathiassen's “volatile memory (6C)” (Ex.1005, [0052]) teaches the claimed *communications buffer*. See §VI.A.4.a,[1.4.2]. Mathiassen's volatile memory 6C is also *adapted for storing and retrieving data*. For example, the volatile memory 6C temporarily stores “fingerprint data” in “intermediate form.” Ex.1005, [0068]. The volatile memory 6C also temporarily stores an “access minutiae table.” Ex.1005, [0070]; Ex.1003, ¶143.

Mathiassen's volatile memory 6C is also *adapted for...communicating data messages between said apparatus and said at least one external system via said external communications interface*. Mathiassen's volatile memory 6C is used for temporary storage of communication data because the USB interface block (9A) is used “for transferring data to other devices and networks (N) external to the IC (1)” and is supported by the volatile memory 6C. Ex.1005, [0050], [0049] (“The volatile memory (6A or 6C) thus provides working memory that is available to other modules on the IC (1).”). The volatile memory 6C thus facilitates the storage, transmission, and reception of communication data. Ex.1003, ¶144.

Thus, Mathiassen discloses *said at least one of a memory (non-volatile memory 7A) and a communications buffer (volatile memory 6C) is further adapted for storing and retrieving data and for communicating data messages between said apparatus (portable device) and said at least one external system (network N) via said external communications interface (USB interface 9A and USB mechanical interface 12C)*. Ex.1003, ¶145.

f. Claim 6

[6.0] The apparatus of claim 1, further adapted for cryptographically encapsulating said data messages into secure data messages to effectuate secure data transmission including sending said secure data messages to said at least one external system only after completion of biometric fingerprint authentication by said customer initiating said transaction.

Mathiassen renders obvious limitation [6.0]. Ex.1003, ¶¶146-149.

Mathiassen's portable device compiles and encrypts a message that includes "[t]he device number of the USB Dongle" (Ex.1005, [0078]), "[t]he IP address of the device" (Ex.1005, [0079]), "[t]he secure key number" (Ex.1005, [0080]), "[t]he user ID" (Ex.1005, [0081]), "PKI verification" (Ex.1005, [0082]), as well as any "[o]ther encrypted information" (Ex.1005, [0083]). "This message/communication is encrypted to form a secure output in a predefined format and sequence" showing that this data message is *cryptographically encapsulat[ed]...to effectuate secure data transmission* as claimed. Ex.1005, [0084]; Ex.1003, ¶146.

This secure data message/communication is sent to the network N, which corresponds to *said...external system*. Ex.1005, [0084] ("This message/communication is...transferred to an external unit, network or system."), [0086] ("[T]his information is received by e.g. the target server (30) of the network (N)."). Mathiassen also explains that this transmission of the "message/communication" is done after the user is biometrically authenticated using their fingerprint. Ex.1005, [0084]-[0085] (the "response is thus a result depending on the above comparison of fingerprints"); Ex.1003, ¶¶147-148. This biometric authentication is initiated by the user placing his or her finger on the fingerprint scanner of Mathiassen's portable device. *See* Ex.1005, [0066] ("To initiate the connection procedure, the user swipes his finger over the fingerprint sensor (5).").

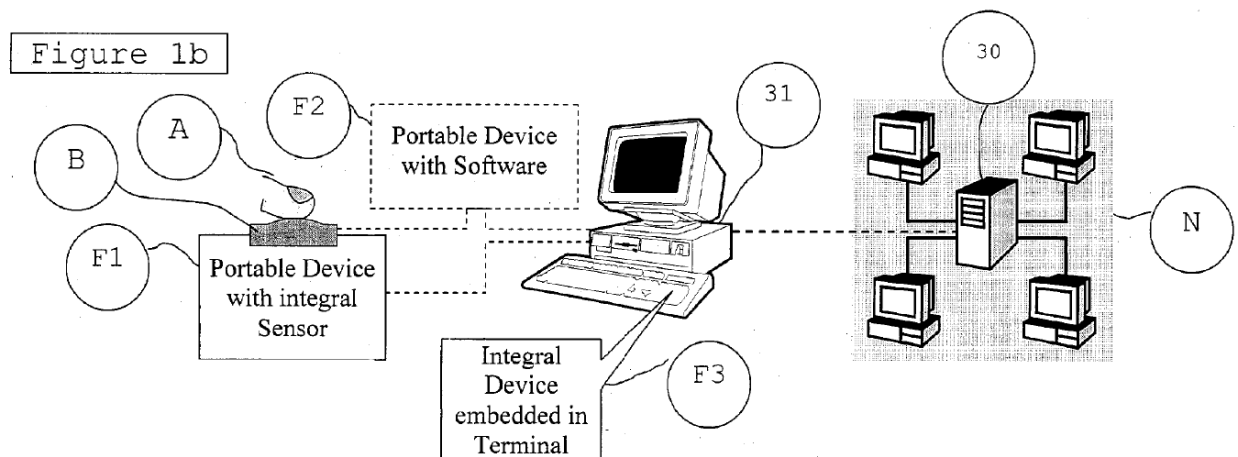
Thus, Mathiassen discloses *cryptographically encapsulating said data messages into secure data messages* (message/communication encrypted to form a secure output) *to effectuate secure data transmission including sending said secure data messages to said at least one external system* (transferring to an external unit, network, or system) *only after completion of biometric fingerprint authentication by said customer* (biometric user authentication using their fingerprint) *initiating said transaction* (initiated by user swiping finger over sensor), as claimed. Ex.1003, ¶149.

g. Claim 21

[21.0] A system for initiating, authenticating and completing transactions by at least one customer using a biometric customer authentication apparatus, comprising:

To the extent the preamble is limiting, Mathiassen and Ryan render it obvious. Ex.1003, ¶¶150-154.

Mathiassen illustrates *[a] system* in Figure 1b below. Ex.1005, [0047]-[0053] (describing a system including “a portable access device” including “an integrated circuit...exemplified in FIGS. 2A and 2B,” “a terminal (31),” a “network server (30),” within “network (N)”). Ex.1003, ¶150.

**Ex.1005, Fig. 1b**

Mathiassen explains that the system shown in Figure 1b is for *initiating...and completing transactions* such as providing user access to “a computer terminal, an internet bank or a corporate or government intranet.” Ex.1005, Abstract, [0047] (this system is “e.g. a computer terminal, an internet or corporate or government intranet...as shown schematically in FIG. 1B”). Multiple operations of a process are described by which a “user may...access the server (30) of the network (N) from a terminal (31) in the network (N).” Ex.1005, [0064]. Mathiassen describes a user securely accessing the server to initiate a “transaction” (Ex.1005, [0050]) by “insert[ing] the portable device (12 or 13) into the USB port” (Ex.1005, [0065]). “To initiate the connection procedure, the user swipes his finger over the fingerprint sensor (5) of the USB Dongle.” Ex.1005, [0066]. The process is completed when the server (30) receives and attempts to decrypt the compiled secure message from

Mathiassen portable device, either allowing or denying access to the user. *See* Ex.1005, [0086]-[0090]; Ex.1003, ¶151

Mathiassen also explains that the system shown in Figure 1b is for *authenticating...transactions*. In particular, after the sensor 5 senses a finger of the user, “[t]he pre-processing block (SC) will immediately start capturing the fingerprint image from the sensor (5).” Ex.1005, [0067]. The pre-processing block and central processor 2 then convert the data to a reduced format (called “compact minutia”) (Ex.1005, [0068]-[0070]), after which the central processor 2 compares the compact minutia with a “master minutia table” to determine if there is a match (Ex.1005, [0071]-[0073]). If there is a match, a secure message is generated (Ex.1005, [0078]-[0083]), and “[t]his message/communication is encrypted to form a secure output in a predefined format and sequence” (Ex.1005, [0084]). As described in limitations [1.0] and [1.3.3] (§§VI.A.3 and VI.A.4.a), a POSITA would have been motivated to implement this process to encrypt data transferred as part of an online transaction, as taught by Ryan to ensure that sensitive data, such as money amounts or recipients, are not tampered with. *See* §VI.A.3; Ex.1003, ¶152.

Mathiassen and Ryan disclose or at least render obvious *initiating, authenticating and completing transactions by at least one customer using a biometric customer authentication apparatus*. Specifically, Figure 1b of Mathiassen illustrates a customer interacting with the biometric authentication apparatus and

initiating a transaction by her finger A shown in Figure 1b placed on the sensor B and described throughout Mathiassen. *See, e.g.*, Ex.1005, [0046] (“The User places, or swipes his finger (A) over the access/input device with a fingerprint sensor (B).”), [0066] (“To initiate the connection procedure, the user swipes his finger over the fingerprint sensor (5).”); Ex.1003, ¶153.

Thus, the Mathiassen-Ryan combination teach a *system* (portable device, computer terminal 31, and network N) *for initiating, authenticating and completing transactions* (transactions taught by Ryan) *by at least one customer* (the user) *using a biometric customer authentication apparatus* (Mathiassen’s biometric authentication apparatus). Ex.1003, ¶154.

[21.1] said at least one customer enrolled into said customer authentication apparatus;

Mathiassen discloses or at least renders obvious limitation [21.1]. Ex.1003, ¶¶155-157.

Mathiassen explains how “[t]he network administrator...will then enroll the user who will be the ‘owner’ of the portable device (12 or 13).” Ex.1005, [0061]. This 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]; Ex.1003, ¶¶155-156.

Thus, Mathiassen discloses *said at least one customer* (the user) *enrolled into said customer authentication apparatus* (portable device). Ex.1003, ¶157.

[21.2.1] said customer authentication apparatus including (i) a fingerprint sensor coupled to a processor,

Limitation [21.2.1] is similar to limitations [1.1.1], [1.2.1], and [1.2.2]. In particular, limitation [1.1.1] recites *an electronic enclosure including a fingerprint sensor disposed thereupon*. The Mathiassen-Ryan combination discloses or at least renders obvious limitation [21.2.1] for the same reasons as in limitation [1.1.1]. For example, Mathiassen’s portable device includes a fingerprint sensor. Ex.1005, [0055]; §VI.A.4.a,[1.1.1]; Ex.1003, ¶158.

Limitation [1.2.1] recites *at least one processor comprised within said enclosure*. The Mathiassen-Ryan combination discloses or renders obvious *said customer authentication apparatus including...a processor* for the same reasons as in limitation [1.2.1]. For example, Figure 2b of Mathiassen illustrates the processor 2 within the IC 1 of the portable device. Ex.1005, [0054] (“the portable device has an IC (1)”), [0050] (“[T]he IC (1)” includes “the central processor (2)”); *see* §VI.A.4.a,[1.2.1]; Ex.1003, ¶159.

Limitation [1.2.2] recites *coupled to said fingerprint sensor*. The Mathiassen-Ryan combination discloses or renders obvious *a fingerprint sensor coupled to a processor* for the same reasons as in limitation [1.2.2]. This coupling of the

fingerprint sensor 5 to the processor 2 is illustrated in Figure 2b of Mathiassen. Ex.1005, Fig. 2b; *see* §VI.A.4.a,[1.2.2]; Ex.1003, ¶160.

[21.2.2] (ii) an external communications interface adapted for communicating with at least one external system, and

Limitation [21.2.2] is similar to limitation [1.1.2]. In particular, limitation [1.1.2] recites *an electronic enclosure...further including an external communications interface*. Mathiassen discloses or renders obvious *an external communications interface* of limitation [21.2.2] for the same reasons as in limitation [1.1.2]. *See* §VI.A.4.a, [1.1.2]; Ex.1003, ¶161.

Limitation [21.2.2] adds that the external communications interface is *adapted for communicating with at least one external system*. As explained previously, Mathiassen’s USB mechanical interface 12C and USB interface block 9A correspond to the *external communications interface* claimed. *See* §VI.A.4.a,[1.1.2]. Mathiassen explains that “interface blocks (9A, 9B, 9C or 9D) [are] for transferring data to other devices and networks (N) external to the IC (1).” Ex.1005, [0050]. Thus, Mathiassen’s external communications interface, including the USB mechanical interface 12C and USB interface block 9A, is *adapted for communicating with at least one external system*. Ex.1003, ¶162.

[21.2.3] (iii) transaction security software resident within and executing on said processor and further comprising

[21.2.4] biometric fingerprint authentication software for authenticating authorized customers

[21.2.5] and also comprising cryptographic transaction authentication software for authenticating transactions;

Limitations [21.2.3]-[21.2.5] are the same as limitations [1.3.1]-[1.3.3], respectively. The Mathiassen-Ryan combination discloses or renders obvious limitations [21.2.3]-[21.2.5] for the same reasons as in limitations [1.3.1]-[1.3.3], respectively. *See* §VI.A.4.a,[1.3.1]-[1.3.3]; Ex.1003, ¶¶163-165.

[21.3.1] said at least one external system adapted for communicating with said customer authentication apparatus and

Limitation [21.3.1] is similar to limitation [2.0]. In particular, limitation [2.0] recites an *external system*. As explained with regard to limitation [2.0], Mathiassen's network N corresponds to the *external system* and includes the server 30 and computer terminal 31. Ex.1005, [0053], Fig. 1b; *see* §VI.A.4.b,[2.0]; Ex.1003, ¶166.

Mathiassen teaches that its network N is *adapted for communicating with said customer authentication apparatus*, as claimed. For example, Mathiassen describes how its portable device communicates with the network N when it is inserted into a port, such as a USB port of the terminal 31. Ex.1005, [0053]. Communications sent between the portable device and the network N include “automatically loading a Java applet” (Ex.1005, [0075]) and/or creating and “transferr[ing] to an external unit,

network or system” a “message/communication” (Ex.1005, [0077], [0084]). Ex.1003, ¶167.

Thus, Mathiassen’s network N is adapted for communication with Mathiassen’s portable device and corresponds to *said at least one external system adapted for communicating with said customer authentication apparatus*. Ex.1003, ¶168.

[21.3.2] having at least one of a physical external communications interface port and

Limitation [21.3.2] is also similar to limitation [2.0]. In particular, limitation [2.0] recites *an external interface port disposed upon...said at least one external system*. As explained with regard to limitations [2.0] and [3.0], the terminal 31 of the network N includes a USB port. Ex.1005, [0065] (to access “the network (N),” “[t]he user will insert the portable device (12 or 13) into [a] USB port”). Thus, the network N, which includes a USB port corresponds to an *external system...having at least one of a physical external communications interface port*, as claimed. Ex.1003, ¶169.

[21.3.3] a wireless communications interface for receiving secure data messages; and

Limitation [21.3.3] is similar to limitation [4.0]. In particular, limitation [4.0] recites *communicating with a second wireless transceiver communications interface aboard...said at least one external system*. As explained regarding limitation [4.0],

a POSITA at the time would have been motivated to modify Mathiassen’s portable device to include a wireless communications interface, as taught by Ryan. *See* §VI.A.4.d,[4.0]. According to the Mathiassen-Ryan combination, Mathiassen’s portable device is adapted to communicate wirelessly with the Network N. A POSITA would have been further motivated to modify Mathiassen’s Network N to include a similar wireless communications interface, as taught by Ryan and explained below. Ex.1003, ¶170.

In particular, Ryan teaches an external system that includes a wireless communications interface. For example, Ryan’s smart fob includes “means for wireless communication.” Ex.1006, [0038]. This may include “an RF antenna” (Ex.1006, [0182]), a “Bluetooth compatible interface” (Ex.1006, [0277]), or other wireless communications interfaces. Ryan explains that its smart fob communicates wirelessly with external systems. Ex.1006, [0223] (“[T]he user takes the smart fob to the event where it connects wirelessly with a reader at the venue.”). A POSITA at the time would have understood that if an external device, such as the “reader” described by Ryan, connected wirelessly with Ryan’s smart fob, that external device would include a wireless communications interface. Thus, a POSITA would have understood that any of the devices of the network N would include a similar wireless communications interface because Ryan’s smart fob would not be able to

communicate wirelessly if other devices did not include wireless communications interfaces. *See* Ex.1006, [0235]; §VI.A.4.d,[4.0]; Ex.1003, ¶171.

In addition, a POSITA's understanding that the network N would include a wireless communications interface, such as those described by Ryan, is supported by the prior art at the time. For example, the terminal 31 in Mathiassen is depicted and described as a standard computer device. Ex.1005, Fig. 1b, [0100]. Standard computers at the time, like the terminal 31 included wireless interfaces. Ex.1013, 1:54-60 (“[w]ireless LAN systems are known in the art...[to] enable various desktop and/or portable personal computers to be connected” wirelessly); Ex.1014, 4:13-22 (“the remote host computer 101 is provided with a transceiver 115 for radio communication with a transceiver 116 in the wireless interface device 100”). Thus, a POSITA would have understood that Mathiassen's network N would include a wireless communications interface like the external systems that interact with the wireless communications interface of Ryan's smart fob. *See, e.g.*, Ex.1006, [0235] (“a turnstile equipped with a wireless reader”), [0223] (describing Ryan's smart fob “connect[ing] wirelessly with a reader at the venue”). A POSITA would have been motivated to include a wireless transceiver within Mathiassen's terminal 31 and/or network N for the same reasons a wireless interface would be included in Mathiassen's portable device explained above. For example, wireless communication increases convenience, allowing interaction “in the real world”

(Ex.1006, [0151]) with a wider variety of systems and devices (*see* Ex.1006, [0223], [0235]). *See* §VI.A.3. Thus, the combination of Mathiassen and Ryan teach the *wireless communications interface* of limitation [21.3.3]. Ex.1003, ¶¶172-173.

In addition, Mathiassen teaches that its network N is *for receiving secure data messages*. For example, Mathiassen explains that the network N enforces secure communication. Ex.1005, [0050] (“The rules of secure communication [are] enforced on the prevailing network (N).”). In addition, Mathiassen explains that the message sent from its portable device and received by the network N is “encrypted” and is a “secure communication between the IC (1) and the network server (30)” of the network N. Ex.1005, [0050]; Ex.1003, ¶174.

Thus, Mathiassen’s network N, which receives secure messages from the portable device, in combination with Ryan’s external systems capable of wireless communication, renders obvious *a wireless communications interface for receiving secure data messages*. Ex.1003, ¶175.

[21.4] at least one transaction processing application residing within said at least one external system including at least one part of a web application accessed by said at least one external system adapted for transmitting and receiving requests and responses to and from said customer authentication apparatus.

Mathiassen and Ryan render obvious limitation [21.4]. Ex.1003, ¶¶176-183.

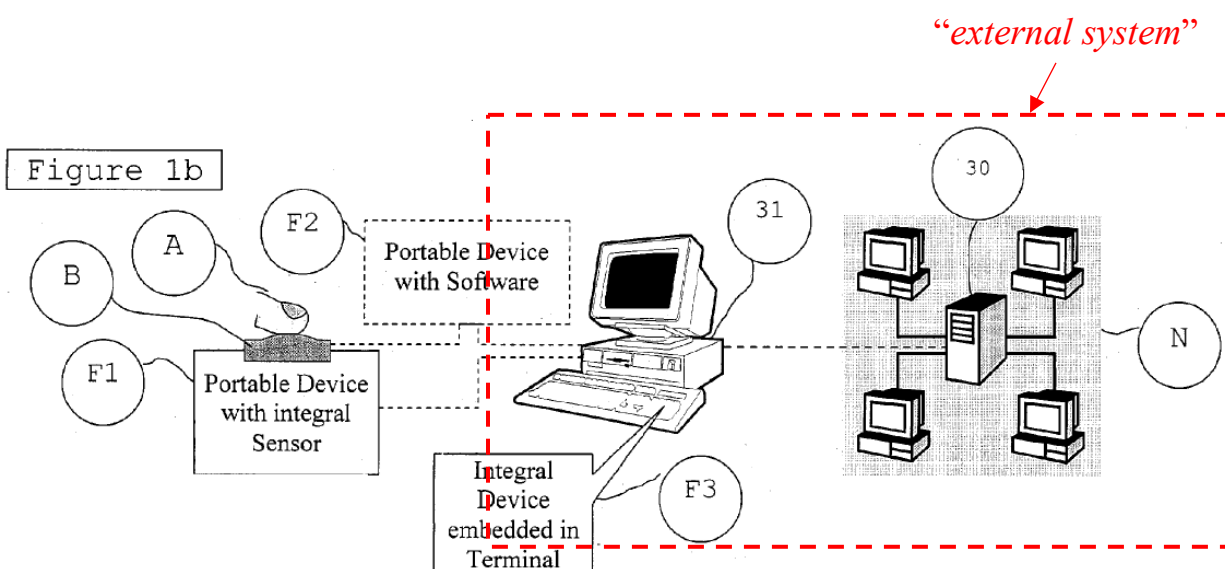
Mathiassen describes an “internet banking application” which is *at least one transaction processing application*. Ex.1005, [0017]. Transactions that would be

processed by an internet banking application would include transferring or otherwise managing money or accessing various other services provided by the website of the internet banking application. *See* Ex.1006, [0236] (“load[ing] cash...via Internet banking”), [0251] (“load[ing] funds from their bank account via the Internet”); Ex.1003, ¶176.

However, to the extent Mathiassen does not explicitly describe the internet banking application *processing transaction[s]*, as claimed, this conventional feature would be obvious in view of Ryan. Ryan discloses numerous examples of online transactions, including “e-commerce” applications (Ex.1006, [0024]) in which its smart fob “connects to the Internet, and interacts with a service or content provider to upload and/or download information” (Ex.1006, [0235]). Ryan explains several types of transaction applications carried out on the network in conjunction with the smart fob, including “download[ing] ‘e-coupons’ to the smart fob device” from a merchant’s online website (Ex.1006, [0238]), “load[ing] cash to the electronic purse of the smart fob device via Internet banking,” and “us[ing] the stored value to pay for online products or services.” (Ex.1006, [0236]). A POSITA would have recognized that Mathiassen’s internet banking application would be capable of processing transactions as described by Ryan (*see* Ex.1006, [0236] (“load[ing] cash...via Internet banking”), [0251] (“load[ing] funds from their bank account”)) because it would greatly increase convenience for customers by allowing banking

transactions to be completed (depositing checks, transferring money, withdrawing money) without going to a physical bank location. Ex.1003, ¶177.

Mathiassen also explains that its internet banking application is part of Mathiassen's network N, which renders obvious that it *resid[es] within said at least one external system*, as claimed. As explained at limitation [2.0] (§VI.A.4.b), Mathiassen's network N, which includes the servers 30 and a terminal 31 that receives the portable device, corresponds to the *external system* claimed. This is illustrated in annotated Figure 1b, below.



Ex.1005, Fig. 1b (annotated)

Mathiassen explains that the internet banking application is part of the network N, and is therefore part of the *external system*. See Ex.1005, [0016] (explaining that the portable device is used to access a “network or system, e.g.,...**an internet bank**”),

[0047] (network N may be “**an internet bank** or a corporate or government intranet”); Ex.1003, ¶176.

In addition, it would have been obvious that Mathiassen’s internet banking application *include[es] at least one part of a web application*. As shown by Ryan, a web application is an application on the internet. *See, e.g.*, Ex.1006, [0024] (“e-commerce” application), [0232] (“merchant’s website”), [0249] (airline’s website), [0329] (“a web site offering e-coupons”), [0332] (“manufacturer’s website”), [0034] (“a website, running a demo application”); Ex.1003, ¶178. Based on Ryan’s disclosure of several different types of website and web applications, Mathiassen’s internet banking application would include a web application, such as a website or particular web page of the internet banking application. Ex.1003, ¶178.

Mathiassen’s internet banking application is accessed by the network N, which renders obvious *a web application accessed by said at least one external system*. For example, Mathiassen explains that the portable device is inserted in a port of the terminal 31. Ex.1005, [0053], [0065]. The terminal 31 then accesses the internet banking application after authenticating the user. Ex.1005, [0065] (“connect[ing] to the Intranet server (30) of the network (N) from an Internet Café or a Business Center”). As shown in annotated Figure 1b above, the terminal 31 is part of the network N, which corresponds to the *external system*. Ex.1005, [0053]

(“terminal (31) of the network”). Therefore, the terminal 31, as part of the *external system*, accesses the internet banking application in Mathiassen. Ex.1003, ¶179.

Mathiassen’s network N is *adapted for transmitting and receiving requests and responses to and from said customer authentication apparatus*. For example, “the IC (1) is designed as a multi-purpose tool that can...communicate with external devices and networks (N) by bridging the biometrics from the sensor (5) to a non-biometrics representation into the network (N) and onto its server(s) (30).” Ex.1005, [0051]. Similarly, Mathiassen describes how a secure message is “transferred to an external unit, network or system,” such as the network N, “through one of the communication interfaces.” Ex.1005, [0084]. Thus, the network N receives requests and responses from the portable device. Ex.1003, ¶¶180-182.

Thus, the Mathiassen-Ryan combination renders obvious *at least one transaction processing application* (Mathiassen’s internet banking application) *residing within said at least one external system* (Mathiassen’s network N) *including at least one part of a web application* (web page of Mathiassen’s internet banking application) *accessed by said at least one external system* (computer terminal 31) *adapted for transmitting and receiving requests and responses to and from said customer authentication apparatus* (Mathiassen’s portable device). Ex.1003, ¶183.

h. Claim 22

[22.0] The system of claim 21, wherein a trusted third party Authentication Service Provider performs authentication services on behalf of at least one customer authentication apparatus and said at least one external system.

Mathiassen and Ryan render obvious limitation [22.0]. Ex.1003, ¶¶184-186.

As explained previously, Mathiassen describes authentication services. *See* §§VI.A.4.a,[1.3.2]-[1.3.3]. Mathiassen describes comparing an acquired fingerprint with a master fingerprint. Ex.1005, [0049]-[0050]. If the acquired fingerprint matches, the user is authenticated and allowed to access the network N. Ex.1005, [0049]-[0050]. Mathiassen describes this authentication being performed either by the IC 1, by the computer terminal 31, or another machine of the network 30. Ex.1005, Fig. 1A, [0046] (“The entire image from the sensor (B) is transmitted from the access/input device to the processor (C) (e.g. a PC) where implemented Software Module(s) (D)...perform[s] a matching locally at the PC (C) or transmits the interpreted fingerprint essentials to a server in a network (E).”). Mathiassen, however, does not explain whether the PC (C) is a third party, i.e., separate from the network N. Ex.1003, ¶184.

Ryan explains that “[t]he client user can be authenticated by the ISP or **by a trusted third party.**” Ex.1006, [0245]. As taught by Ryan, a POSITA would have been motivated to configure Mathiassen’s system to allow for authentication by a third party. Ex.1006, [0245]. This would allow merchants to outsource user

authentication and/or transaction authentication so these services would not have to be created or managed in house leading to cost savings and increased flexibility in implementation. Ex.1003, ¶¶184-185.

Thus, the Mathiassen-Ryan combination renders obvious *a trusted third party Authentication Service Provider* (trusted third party of Ryan) *performs authentication services on behalf of at least one customer authentication apparatus* (Mathiassen's portable device) *and said at least one external system* (Mathiassen's network N). Ex.1003, ¶186.

i. Claim 23

[23.0] The system of claim 21, wherein said customer authentication apparatus communicates with an external system by means of a USB interface connector.

Claim 23 is similar to claims 2 and 3. In particular, claim 3 recites the *external communications interface* of the biometric customer authentication apparatus *further comprises a USB connector for insertion into an external interface port disposed upon one of said host system and said at least one external system.* Mathiassen discloses or renders obvious *said customer authentication apparatus communicates with an external system by means of a USB interface connector* for the same reasons as in claims 2 and 3. Ex.1003, ¶187.

As explained regarding claim 2, Mathiassen illustrates the USB mechanical interface 12C in Figure 3a which corresponds to a *USB interface connector*. The

USB mechanical interface 12C is physically inserted into the computer terminal 31 which is a part of the network N corresponding to the *external system*. Ex.1005, [0053], (“the IC (1) is a portable device to be plugged into a terminal (31) of the network”). When the USB mechanical interface 12C is inserted into the USB port of the terminal 31, Mathiassen’s portable device communicates with the external system. Ex.1005, [0050] (“secure communication between the IC (1) and the network server (30)”); Ex.1003, ¶188.

Thus, Mathiassen teaches *said customer authentication apparatus* (portable device) *communicates with an external system* (network N) *by means of a USB interface connector* (USB mechanical interface 12C). Ex.1003, ¶189.

j. Claim 24

[24.0] The system of claim 21, wherein said transaction authentication apparatus⁶ communicates with an external system by means of a wireless communications link.

Claim 24 is similar to claim 4. In particular, claim 4 recites that the customer authentication apparatus includes *a first wireless transceiver for wirelessly communicating with a second wireless transceiver communications interface*

⁶ Petitioner notes that “*said transaction authentication apparatus*” lacks antecedent basis in claims 21 and 24. It appears that “*said transaction authentication apparatus*” refers to the *customer authentication apparatus* of claim 21.

aboard one of a host system and said at least one external system. The Mathiassen-Ryan combination teaches or at least renders obvious limitation [24.0] for the same reasons as claim 4. Ex.1003, ¶190.

As explained in limitation [4.0] (§§VI.A.2 and VI.A.4.d), Ryan’s smart fob includes a wireless transceiver. Ex.1006, [0124] (Ryan’s “compact personal token apparatus comprises a wireless interface.”). Similarly, Ryan describes devices external to the smart fob, corresponding to the external system claimed, which “also comprise[] means for wireless communication.” Ex.1006, [0038]. These wireless transceivers form a *wireless communications link* because they facilitate wireless communication. Ex.1006, [0038] (wireless interface “enabl[es] communication with a personal device” external to the smart fob). A POSITA would have been motivated to combine wireless communication described by Ryan with Mathiassen’s system to be used “in the real world” (Ex.1006, [0151]) with a wider variety of systems and devices (Ex.1006, [0223], [0235], [0248]). *See* §VI.A.3; Ex.1003, ¶191.

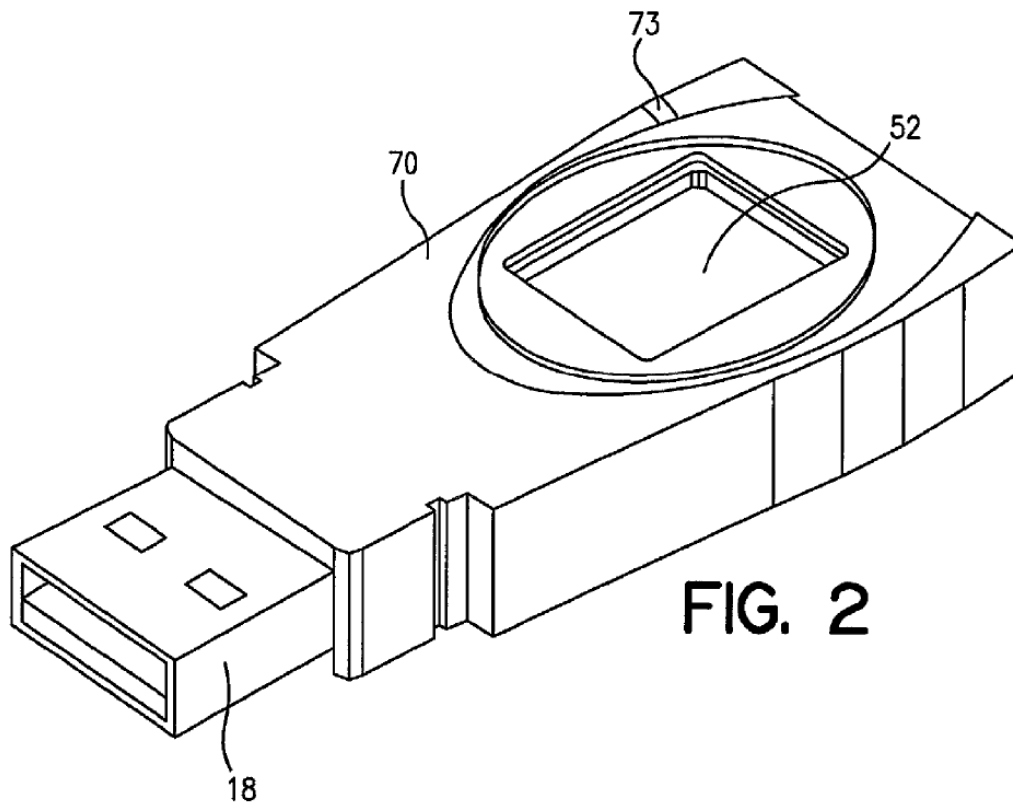
Thus, Ryan’s smart fob which communicates wirelessly with an external device teaches *said transaction authentication apparatus communicates with an external system by means of a wireless communications link.* Ex.1003, ¶192.

B. Ground 2: Claims 1-6 and 21-24 would have been obvious over Mathiassen and Ryan in view of Lim.

Ground 2 is included to show that limitation [1.3.1] of Claim 1 and limitation [21.2.3] of claim 21 also would have been obvious over the Mathiassen-Ryan combination in view of Lim (“the Mathiassen-Ryan-Lim combination”). Ex.1003, ¶200.

1. Overview of Lim

Lim describes an “[a]pparatus and method” for “implementing biometrics-based access control to a restricted resource.” Ex.1007, Abstract. Lim’s device is shown in Figs. 2-9. Figure 2 is shown below:

**FIG. 2****Ex.1007, Fig. 2**

Lim's device includes a fingerprint sensor 52 "disposed on the top side of portable device 70." Ex.1007, [0035]. Lim's device also includes "a microprocessor, a non-volatile memory coupled thereto, and a biometrics-based authentication module controlled by the microprocessor." Ex.1007, [0007]. Lim's device includes a "USB connector 18." Ex.1007, Fig. 2, [0035]; Ex.1003, ¶193.

Lim's authentication module is software described as an authentication engine 12. Ex.1007, [0024]. "Authentication engine 12...comprises a template generator 12a and a verification module 12b." Ex.1007, [0024]. The template

generator 12a “is used to generate an encoded version of an image of a fingerprint” and the verification module 12b “is used to compare a newly generated template against a stored template to validate the authenticity of a fingerprint provided by someone purporting to be an authorized user.” Ex.1007, [0024]. In this way, authentication engine 12 authenticates a user. Lim’s authentication software may be located in any location within the device, including the microprocessor 11. Ex.1007, [0025]; Ex.1003, ¶194.

2. Motivation to Combine Mathiassen and Ryan with Lim

First, Lim is analogous art to the ’637 patent. Lim is within the same field of endeavor as the ’637 patent, as it pertains to increasing online transaction security by biometrically authenticating a user with an “access control device.” Ex.1007, Abstract, [0001]; Ex.1003, ¶¶192-195. In addition, Lim is reasonably pertinent to a particular problem with which the inventor of the ’637 patent was involved (i.e., a biometrics-based device for accessing a system and improving online transaction security). Ex.1007, Abstract (“Apparatus and method for implementing biometrics-based access control to a restricted resource” using “a portable device”), [0002] (“utilized in business, educational and home computing”). Ex.1003, ¶195.

Second, as described at §VI.A.3, a POSITA would have been motivated to modify Mathiassen according to the teachings of Ryan regarding conducting wireless transactions. A POSITA would have been similarly motivated to modify

the Mathiassen-Ryan combination to incorporate the conventional details of where software is stored, as taught by Lim. For example, Lim explains that its software, “authentication engine 12,” may be stored long-term in the processor, “microprocessor 11.” Ex.1007, [0025] (“authentication engine 12 is implemented as part of microprocessor 11”). As described by Mathiassen, consolidating functions or structures within the same component, such as “integrat[ing]” “volatile memory (6C) and non-volatile memory (7A)” within “the IC (1),” advantageously “enhanc[es] the security and speed of operation of the device.” Ex.1005, [0052]. A POSITA would have recognized that similarly storing software within the processor itself would enhance security and speed of the device. Ex.1003, ¶196.

Accordingly, the Mathiassen-Ryan-Lim combination would have been the combination of prior art elements (Mathiassen’s portable device configured to conduct wireless transactions as taught by Ryan combined with Lim’s teaching regarding software stored within the processor) according to known methods (Lim’s explanation of the location of software in circuit architecture) to yield predictable results (increased security and speed as expected by Mathiassen). *KSR*, 550 U.S. at 416 (2007); Ex.1005, [0052]; Ex.1003, ¶196. A POSITA would also understand that storing software within the processor of the portable device would free up non-volatile memory of Mathiassen’s portable device for storage of other data, a feature described as a specific embodiment in Mathiassen. Ex.1005, [0058] (explaining that

non-volatile memory could be expanded such that the portable device could also be used for “general portable data storage”); Ex.1003, ¶197.

A POSITA would have had reasonable expectation of success in incorporating Lim’s details regarding the location of software within a portable device taught by the Mathiassen-Ryan combination because Lim demonstrates that a similar device of similar processing capability and storage capacity includes software resident within the processor. Ex.1003, ¶¶198-199. In particular, Mathiassen discloses a device with an “ARM 9” processor (which is a reduced instruction set computer (RISC) processor) “or equivalent” (Ex.1005, [0050]), “[a]n SDRAM chip (6), typically at least with 4 MB capacity,” and “a non-volatile serial Flash chip (7), typically at least 256 Kbytes capacity” (Ex.1005, [0054]), as well as “extra capacity beyond the 256 Kbytes minimum” (Ex.1005, [0058]). Lim similarly describes a device with a “RISC processor” (Ex.1007, [0024]) and “a storage capacity between 8 MB and 512 MB” (Ex.1007, [0023]); Ex.1003, ¶¶198-199.

3. Analysis

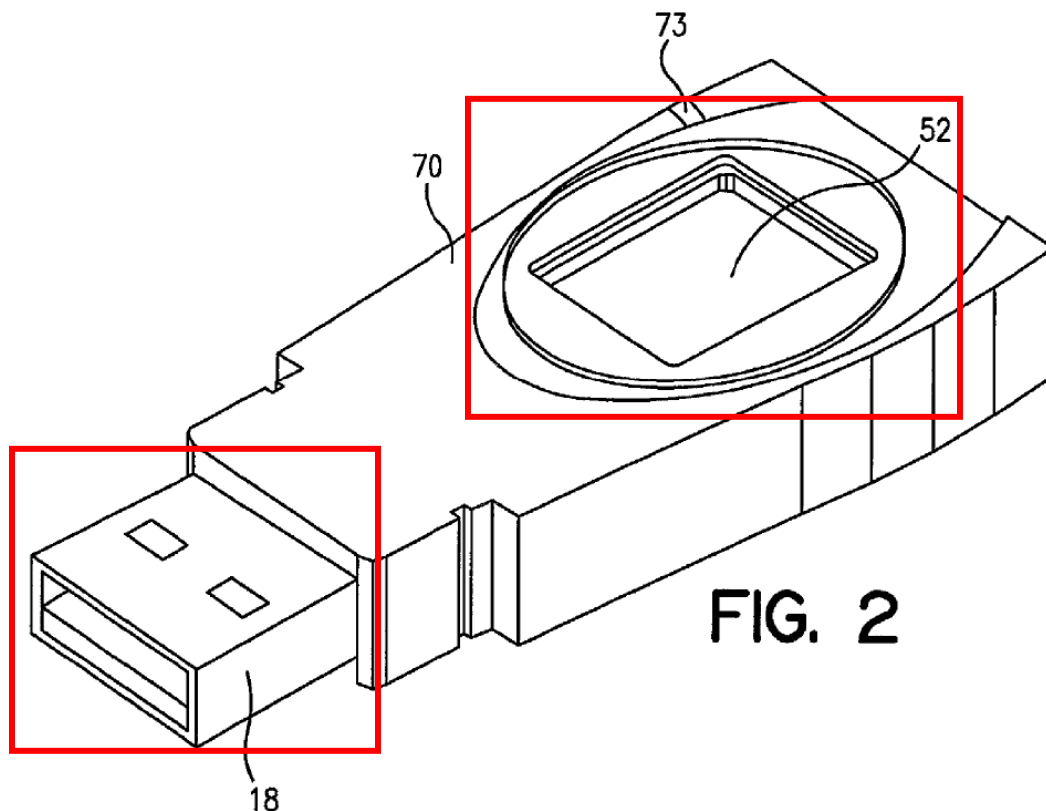
a. Claim 1

The Mathiassen-Ryan combination renders obvious limitations [1.0]-[1.2] and [1.3.2]-[1.5] for the reasons in Ground 1. Ground 2 shows that limitation [1.3.1] also would have been obvious over the Mathiassen-Ryan combination in view of Lim (“the Mathiassen-Ryan-Lim combination”). Ex.1003, ¶200.

[1.3.1] transaction security software resident within and executing on said at least one processor further comprising

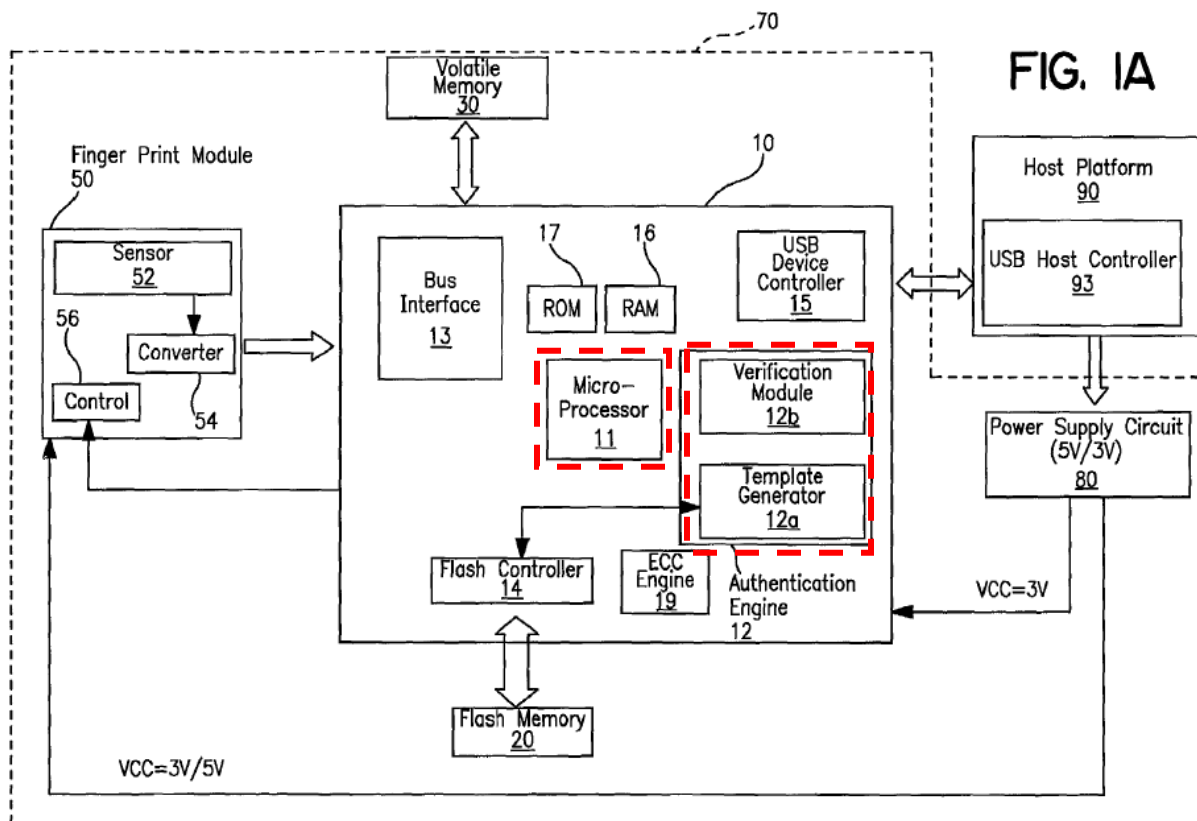
Mathiassen, Ryan, and Lim render obvious limitation [1.3.1]. Ex.1003, ¶¶201-204.

Lim describes a “portable device 70” that includes a “USB connector 18” and a “[f]ingerprint module 50...with sensor 52 disposed on the top side of the portable device 70” for biometrically authenticating users. Ex.1007, [0035], Fig. 2 (reproduced below); Ex.1003, ¶201.



Ex.1007, Fig. 2 (annotated)

The portable device includes a “microprocessor 11” and an “authentication engine 12.” Ex.1007, [0024], Fig. 1A (reproduced below). Lim’s authentication engine 12 is software similar to Mathiasen’s administrative software. Mathiasen’s administrative software corresponds to the claimed *transaction security software* (see §§VI.A.4.a,[1.3.1]-[1.3.3]) and its similarity to Lim’s authentication engine shows that a POSITA would have reasonably expected to successfully store Mathiasen’s administrative software within a processor. Ex.1007, [0024] (“Authentication engine 12 in turns comprises a template generator 12a and a verification module 12b.”); Ex.1003, ¶202.



Ex.1007, Fig. 1A (annotated)

Lim explains that the authentication engine 12 is *resident within and executing on said at least one processor* as claimed. As previously explained in the claim construction section above (§V.A), the '637 patent provides that when software is executed on a processor, it is resident within a memory of the processor and is thus resident within the processor. However, even if the terms *resident within...at least one processor* are interpreted to require software to be permanently stored within the processor, Lim discloses this interpretation as well. Specifically, while the authentication engine 12 is illustrated as a separate entity from the microprocessor 11, Lim explains that “where authentication engine 12 is to be placed is a design choice.” Ex.1007, [0025]. Lim also provides several embodiments in which the authentication engine 12 is part of the microprocessor or another processor.

In another embodiment, authentication engine 12 is implemented **as part of microprocessor 11**. In still another embodiment, authentication engine 12 is **implemented as a processor** separate from microprocessor 11.

Ex.1007, [0025] (emphasis added); Ex.1003, ¶203.

Thus, the Mathiassen-Ryan-Lim combination renders obvious *transaction security software* (Lim’s authentication engine 12) *resident within and executing on said at least one processor* (Lim’s microprocessor 11 or standalone processor). Ex.1003, ¶204.

b. Claim 21

The Mathiassen-Ryan combination renders obvious limitations [21.0]-[21.2.2] and [21.2.4]-[21.4] for the reasons in Ground 1. Ground 2 shows that Limitation [21.2.3] also would have been obvious over the Mathiassen-Ryan combination in view of Lim (“the Mathiassen-Ryan-Lim combination”). Ex.1003, ¶205.

[21.2.3] (iii) transaction security software resident within and executing on said processor and further comprising

Limitations [21.2.3] is the same as limitation [1.3.1]. The Mathiassen-Ryan-Lim combination renders obvious limitation [21.2.3] for the same reasons as in limitation [1.3.1]. *See* §VI.B.3.a,[1.3.1]; Ex.1003, ¶206.

VII. 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 1-2 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.

VIII. CONCLUSION

The Board should institute an IPR trial for claims 1-6 and 21–24 and then cancel these claims as unpatentable.

Respectfully submitted,

Dated: May 24, 2024

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

IX. 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 (§§II-VIII) has 13,964 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 1001-1010, 1013-1014, and 1017-1020; 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

X. CLAIMS APPENDIX

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

Claim 1

[1.0] A biometric customer authentication apparatus for improving online transaction security and for assuring the identity of a customer, comprising:

[1.1.1] an electronic enclosure including a fingerprint sensor disposed thereupon and

[1.1.2] further including an external communications interface;

[1.2.1] at least one processor comprised within said enclosure and

[1.2.2] coupled to said fingerprint sensor;

[1.3.1] transaction security software resident within and executing on said at least one processor

[1.3.2] further comprising biometric fingerprint authentication software for authenticating authorized customers

[1.3.3] and also comprising cryptographic transaction authentication software for authenticating transactions;

[1.4.1] at least one of a memory and

[1.4.2] a communications buffer

[1.4.3] coupled to said at least one processor and

[1.4.4] further coupled to said external communications interface; and

[1.5] a communications subsystem coupled into said external communications interface for relaying data messages between at least one external system and said apparatus.

Claim 2

[2.0] The apparatus of claim 1, wherein said external communications interface further comprises a physical interface connector for physical insertion into an external interface port disposed upon one of a host system and said at least one external system.

Claim 3

[3.0] The apparatus of claim 2, wherein said external communications interface further comprising said physical interface connector, further comprises a USB connector for insertion into an external interface port disposed upon one of said host system and said at least one external system.

Claim 4

[4.0] The apparatus of claim 1, wherein said external communications interface further comprises a first wireless transceiver for wirelessly communicating with a second wireless transceiver communications interface aboard one of a host system and said at least one external system.

Claim 5

[5.0] The apparatus of claim 1, wherein said at least one of a memory and a communications buffer is further adapted for storing and retrieving data and for communicating data messages between said apparatus and said at least one external system via said external communications interface.

Claim 6

[6.0] The apparatus of claim 1, further adapted for cryptographically encapsulating said data messages into secure data messages to effectuate secure data transmission including sending said secure data messages to said at least one

external system only after completion of biometric fingerprint authentication by said customer initiating said transaction.

Claim 21

[21.0] A system for initiating, authenticating and completing transactions by at least one customer using a biometric customer authentication apparatus, comprising:

[21.1] said at least one customer enrolled into said customer authentication apparatus;

[21.2.1] said customer authentication apparatus including (i) a fingerprint sensor coupled to a processor,

[21.2.2] (ii) an external communications interface adapted for communicating with at least one external system, and

[21.2.3] (iii) transaction security software resident within and executing on said processor and further comprising

[21.2.4] biometric fingerprint authentication software for authenticating authorized customers

[21.2.5] and also comprising cryptographic transaction authentication software for authenticating transactions;

[21.3.1] said at least one external system adapted for communicating with said customer authentication apparatus and

[21.3.2] having at least one of a physical external communications interface port and

[21.3.3] a wireless communications interface for receiving secure data messages; and

[21.4] at least one transaction processing application residing within said at least one external system including at least one part of a web application accessed by said at least one external system adapted for transmitting and receiving requests and responses to and from said customer authentication apparatus.

Claim 22

[22.0] The system of claim 21, wherein a trusted third party Authentication Service Provider performs authentication services on behalf of at least one customer authentication apparatus and said at least one external system.

Claim 23

[23.0] The system of claim 21, wherein said customer authentication apparatus communicates with an external system by means of a USB interface connector.

Claim 24

[24.0] The system of claim 21, wherein said transaction authentication apparatus communicates with an external system by means of a wireless communications link.