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

Declaration of Dr. Henry Houh Under 37 C.F.R. § 1.68
In Support of Petition for *Inter Partes* Review of
U.S. Patent No. 7,480,637
(Claims 1-6 and 21-24)

Ex.1003
Askeladden, L.L.C. / Page 1 of 123

Table of Contents

I. Introduction....4

II. Background and Qualifications....6

III. Understanding of Patent Law....13

IV. The '637 Patent....17

V. Prosecution History of the '637 Patent....19

VI. Level of Ordinary Skill in the Pertinent Art....20

VII. Claim Construction....21

A. "resident within" (claims 1, 21)....22

VIII. Detailed Invalidity Analysis....27

A. Ground 1: Claims 1-6 and 21-24 is rendered obvious over Mathiassen in view of Ryan....28

1. Overview of Mathiassen....29

2. Overview of Ryan....36

3. Motivation to Combine Mathiassen and Ryan....40

4. Analysis....48

a) Claim 1....48

b) Claim 2....82

c) Claim 3....85

d) Claim 4....85

e) Claim 5....88

f) Claim 6....91

g) Claim 21....93

h) Claim 22 109

i) Claim 23 111

j) Claim 24 112

B. Ground 2: Claims 1-6 and 21-24 are rendered obvious over Mathiassen and Ryan in view of Lim 113

1. Overview of Lim 113

2. Motivation to Combine Mathiassen and Ryan with Lim 115

3. Analysis 118

a) Claim 1 118

b) Claim 21 122

IX. Availability for cross-examination 123

X. Conclusion 123

I, Henry Houh, do hereby declare as follows:

I. INTRODUCTION

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

2. I have been asked to provide my opinions regarding whether claims 1-6 and 21-24 (the "Challenged Claims") of the '637 Patent are unpatentable as they would have been obvious to a person having ordinary skill in the art ("POSITA") as of the earliest claimed priority date. It is my opinion that the Challenged Claims would have been obvious to a POSITA after reviewing the prior art discussed below.

3. In preparing this Declaration, I have reviewed:

- Ex.1001, the '637 Patent;
- Ex.1002, the file history of the '637 Patent;
- the prior art references discussed below:
    - Ex.1005, U.S. Patent Publication No. 2004/0123113 to Mathiassen et al. ("Mathiassen");
    - Ex.1006, U.S. Patent Publication No. 2005/0109841 to Ryan et al. ("Ryan");

- Ex.1007, U.S. Patent Publication No. 2003/0005336 to Poo et al. ("Lim");

- the following materials:

  - Ex.1010, U.S. Patent No. 6,003,115 to Spear et al. ("Spear");
  - Ex.1013, U.S. Patent No. 6,760,017 to Banerjee ("Banerjee");
  - Ex.1014, U.S. Patent No. 6,092,117 to Gladwin ("Gladwin");
  - Ex.1017, U.S. Patent Publication No. 2005/0165700 to Karthik ("Karthik");
  - Ex.1018, U.S. Patent Publication No. 2006/0123465 to Ziegler ("Ziegler");
  - Ex.1019, U.S. Patent No. 5,875,464 to Kirk ("Kirk");
  - Ex.1020, U.S. Patent No. 5,025,366 to Baror ("Baror"); and

- any other document cited below.

4. I understand that the '637 Patent issued on January 20, 2009, from U.S. Patent Application No. 11/317,141 ("the '141 Application"), filed December 23,

2005. The face of the '637 Patent lists Douglas Kozlay as inventor. I have been informed by counsel that, according to assignment records, Jabaa, L.L.C. is the current assignee of the '637 Patent.

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

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

a) the documents listed above,

b) any additional documents and references cited in the analysis below,

c) the relevant legal standards, including the standard for obviousness, and

d) my knowledge and experience based upon my work in this area as described below.

II. BACKGROUND AND QUALIFICATIONS

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

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

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

10. I first worked in the field of telecommunications in 1987 as a summer intern at AT&T Bell Laboratories as part of a five-year dual degree program at MIT. I continued to work at AT&T Bell Laboratories as part of this MIT program. While at MIT, I was a teaching assistant ("TA") in the Electrical Engineering and Computer Science Department's core Computer Architectures course. My first TA post, during my senior year, was to a role typically reserved for graduate students. I later became head TA. The course covered various topics in computer architectures. As a TA, I helped write homework assignments, lab assignments, and exams. I also taught in the recitation sections.

11. Later, as part of my doctoral research at MIT from 1991-1998, I was a research assistant in the Telemedia Network Systems ("TNS") group at the

Laboratory for Computer Science. The TNS group built a high-speed gigabit network and created applications that ran over the network. Example applications included ones for remote video capture, processing, and display of video on computer terminals. In addition to working on the design of core network components, I worked on designing and building high-speed links, and designing and writing device drivers for interface cards, and set up the group's web server.

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

13. In January 1998, I defended and submitted my Ph.D. thesis, titled "Designing Networks for Tomorrow's Traffic." As part of my thesis research, I analyzed local area and wide area flows to show a more efficient method for routing packets in a network, based on traffic patterns at the time. The traffic flow data

included Ethernet, IP, TCP or UDP, and RTP header information, which I analyzed to reach the conclusions set forth in my thesis.

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

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

16. The NBX system also featured a computer interface for initiating phone calls, which could also initiate conference calls. The NBX system also supported the Telephony Application Programming Interface ("TAPI") that allowed other computer programs to integrate with our system telephony features. We obtained U.S. Patent No. 6,967,963, entitled "Telecommunication method for ensuring on-time delivery of packets containing time-sensitive data," as part of this work. I also programmed the first prototype of our phone which communicated using IP, and I demonstrated our IP phones working over the Internet when we attended a trade

show in California. The phone connected over the Internet to our headquarters in Andover, MA. I also programmed a data capture and analysis system that provided data on the operation of the system.

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

18. At Empirix, I also redesigned the architecture of the Web Test division's core product, e-Test Suite. E-Test Suite was a software program designed

to perform functional and load testing of web applications. I was technical lead on the project, and also worked on programming a Javascript interpreter for the product. Javascript is the flexible programming layer that allows users to interact with web pages through actions such as clicking and dragging that allows web page programmers to extend the functionality of a web page beyond clicking on links.

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

20. At my educational company, Einstein's Workshop, I created the initial web site and integrated it with online payment solutions. I evaluated, sourced, and configured the point-of-sale system for the company, which involved integration with and setup of mobile shopping terminals. We also teach programming to children of all ages, starting with Scratch programming for young elementary students and advancing through programming in Python and for game development for high school students. I conceived many of the programming classes and have

taught programming to novice and more advanced students. We also created an educational computer-aided design tool, called BlocksCAD. We received a grant, on which I was the principal investigator, to further develop BlocksCAD and successfully met our grant objectives. BlocksCAD was spun-off from Einstein's Workshop and has been part of various incubator/accelerator programs in education as well as at the MIT Media Lab. Today, BlocksCAD is used worldwide in makerspaces as well as in schools throughout the U.S.

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

- U.S. Patent No. 7,975,296, "Automated security threat testing of web pages";
- U.S. Patent No. 7,877,736, "Computer language interpretation and optimization for server testing";
- U.S. Patent No. 7,801,910, "Method and apparatus for timed tagging of media content";
- U.S. Patent 7,590,542, "Method of generating test scripts using a voice-capable markup language";
- U.S. Patent No. 6,967,963, "Telecommunication method for ensuring on-time delivery of packets containing time-sensitive data";

- U.S. Patent Application Publication No. 20070106685, "Method and apparatus for updating speech recognition databases and reindexing audio and video content using the same";
- U.S. Patent Application Publication No. 20070106693, "Methods and apparatus for providing virtual media channels based on media search";
- U.S. Patent Application Publication No. 20070106760, "Methods and apparatus for dynamic presentation of advertising, factual, and informational content using enhanced metadata in search-driven media applications";
- U.S. Patent Application Publication No. 20070112837, "Method and apparatus for timed tagging of media content";
- U.S. Patent Application Publication No. 20070118873, "Methods and apparatus for merging media content"; and
- U.S. Patent Application Publication No. 20090222442, "User-directed navigation of multimedia search results."

III. UNDERSTANDING OF PATENT LAW

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

23. I have been asked to provide my opinions regarding whether claims 1-6 and 21-24 of the ’637 Patent would have been obvious to a POSITA at the time of the alleged invention in light of the prior art.

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

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

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

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

elements according to known methods is likely to be obvious when it does no more than yield predictable results.

28. As mentioned above, I understand that a claim would have been obvious if it unites old elements with no change to their respective functions, or alters prior art by mere substitution of one element for another known in the field and that combination yields predictable results. While it may be helpful to identify a reason for this combination, I understand that there is no rigid requirement of finding an express teaching, suggestion, or motivation to combine within the references. When a product is available, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a POSITA can implement a predictable variation, obviousness likely bars its patentability. For the same reason, if a technique has been used to improve one device and a POSITA would recognize that it would improve similar devices in the same way, using the technique would have been obvious. I understand that a claim would have been obvious if common sense directs one to combine multiple prior art references or add missing features to reproduce the alleged invention recited in the claims.

29. I further understand that certain factors may support or rebut the obviousness of a claim. I understand that such secondary considerations include, among other things, commercial success of the patented invention, skepticism of those having ordinary skill in the art at the time of invention, unexpected results of

the invention, any long-felt but unsolved need in the art that was satisfied by the alleged invention, the failure of others to make the alleged invention, praise of the alleged invention by those having ordinary skill in the art, and copying of the alleged invention by others in the field. I understand that there must be a nexus—a connection—between any such secondary considerations and the alleged invention. I also understand that contemporaneous and independent invention by others is a secondary consideration tending to show obviousness.

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

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

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

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

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

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

IV. THE '637 PATENT

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

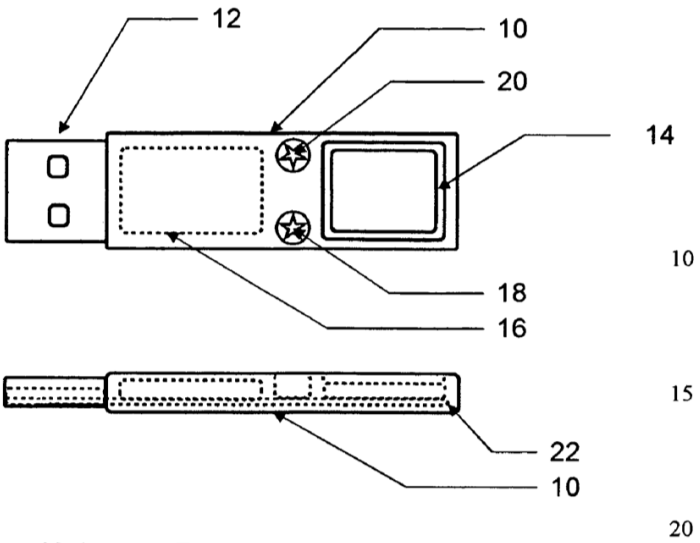


Figure 1A, Internet Transaction Authenticator in USB Dongle Form

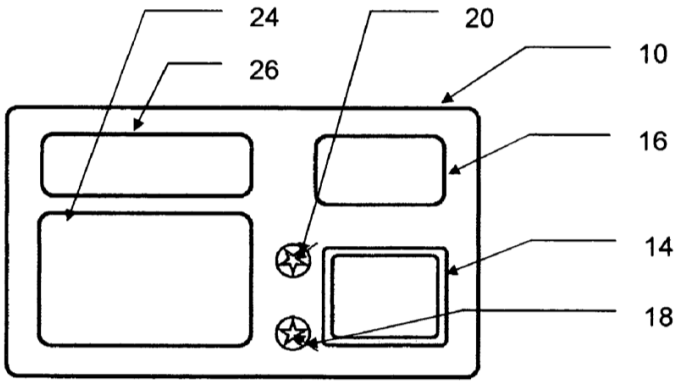


Figure 1B, Internet Transaction Authenticator in Wireless Card Form

'637 Patent, Figs. 1A and 1B

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

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

V. PROSECUTION HISTORY OF THE '637 PATENT

38. The U.S. Patent Application of the '637 Patent (U.S. Patent No. 11/317,141 referred to herein as "the '141 Application") was filed on December 23, 2005. The United States Patent and Trademark Office issued a rejection rejecting all claims as obvious over U.S. Patent Publication No. 2005/0165700 to Karthik,

published on July 28, 2005, and U.S. Patent Publication No. 2006/0123465 to Ziegler, published on June 8, 2006. Ex.1002, 76-90. The inventor filed a response which was not recognized by the Patent Office and a notice of abandonment issued. The inventor assigned the application to Biometric Associates, LP, which filed a response with a petition to revive. In its response, the assignee did not amend claim 1, and added elements [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.

39. The Patent Office issued a Notice of Allowance allowing claims 1-24. Ex.1002, 25. The Notice of Allowance identified elements [1.3.1]-[1.5] as the allowable features of independent claim 1. Ex.1002, 26. As shown in Section VIII below, elements [1.3.1]-[1.5] and [21.2.3]-[21.4] are obvious over prior art not considered by the Examiner.

VI. LEVEL OF ORDINARY SKILL IN THE PERTINENT ART

40. I understand there are multiple factors relevant to determining the level of ordinary skill in the pertinent art, including (1) the levels of education and experience of persons working in the field at the time of the invention; (2) the sophistication of the technology; (3) the types of problems encountered in the field; and (4) the prior art solutions to those problems.

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

VII. CLAIM CONSTRUCTION

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

43. In order to construe the Challenged Claims of the '637 Patent, I have reviewed the entirety of the '637 Patent along with portions of the prosecution history of the '637 Patent. Consistent with the '637 Patent disclosure, I have

interpreted the terms in the Challenged Claims according to their plain and ordinary meaning as understood by a person of ordinary skill in the art, and considered any explicit definitions provided by the specification of the ’637 Patent, where applicable.

44. In my opinion, all claim terms of the ’637 Patent should be construed according to their plain and ordinary meaning. Below, I provide an explanation of the plain and ordinary meaning of the term “resident within” based on the disclosure of the ’637 Patent and other contemporaneous prior art before the priority date of the ’637 Patent.

A. “resident within” (claims 1, 21)

45. Claim 1 contains the terms “transaction security software *resident within* and executing on said at least one processor.” Ex.1001, 8:51-52. Claim 21 contains similar terms. Specifically, claim 21 recites “transaction security software *resident within* and executing on said processor.” Ex.1001, 11:25-27. The term “resident within” in this context means “temporary storage of the software while the software is being executed.”

46. The ’637 Patent does not provide a definition of the term “resident within,” but a POSITA would have understood that the term “*resident within*” in claims 1 and 21 means temporary storage of the transaction security software within a memory of the processor during execution of the software. This definition is based

on the disclosed embodiments of the '637 Patent and basic processor architecture at the time.

47. The '637 Patent specification uses the terms "resident within" one time:

> The processor 16 is multifunctional, providing USB interface processing, fingerprint biometrics processing, transactions processing, and other processing, based on the configuration implemented. **Resident within** and executing within the processor 16, is transaction security software. Processor 16 also contains memory for the execution of programs plus communications buffers for sending and receiving data.

Ex.1001, 5:9-15.

48. As described in the '637 Patent, the security software is "resident within and executing on" the processor 16. A POSITA at the time would have understood that software is executed on a processor, but not stored on the processor long-term. Thus, when the '637 Patent says that the software is resident within and executing within the processor, a POSITA would have understood this terminology to describe executing software that is stored elsewhere, typically within a non-volatile memory, and transferred to the processor during execution, using, for example, volatile memory within the ITA and/or cache memory within the processor. This understanding is supported by the '637 Patent as well. For example, in the next sentence, the '637 Patent explains that the "[p]rocessor 16…contains memory **for**

the execution of programs." Ex.1001, 5:13-14. Based on this description, a POSITA would understand that the memory within the processor of the '637 Patent is for temporary storage of the software and, for example, may correspond to cache memory, while the software is being executed, rather than long-term storage of the software.

49. The portable customer authentication apparatus disclosed in the '637 Patent 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* Section VIII.A.4.a., [1.4.1]. This memory is external to the processor and would 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 "the secure internal storage of the ITA." Ex.1001, 5:17-19, 7:63-64. The '637 Patent explains that the non-volatile memory of the device is for long-term storage of data.

> Protected non-volatile memory retains **the ID of the ITA** and **its cryptographic key(s)**. Optionally, there can be protected memory available to the customer so that the ITA can additionally serve as a **virtual disk drive as is commonly done with USB dongles**.

Ex.1001, 5:15-20.

50. The ’637 Patent does not describe long-term storage of software in the processor. *See* Ex.1001.

51. This interpretation of the terms “*resident within*” is also consistent with other prior art at the priority date of the ’637 Patent. For example, U.S. Patent No. 6,003,115 to Spear et al. (“Spear”) describes the basic components of a conventional processor, including cache memory, and how the processor interacts with volatile memory and non-volatile memory.

> A typical computer system consists of a number of modules or components. Computer systems typically include a central processing unit (CPU) such as a microprocessor. The microprocessor is a program-controlled device that **obtains**, **decodes** and **executes** instructions. A computer system also includes storage components for storing system operating software, application program instructions and data. These storage components may be read only memory (ROM), random access memory (RAM), disk or tape storage, or any other suitable storage means.

Ex.1010, 1:30-40.

52. As explained by Spear, a typical processor at the time “obtains” software for execution. Ex.1010, 1:35. 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, 1:34-37. During execution of application program

instructions, the processor stores the instructions in memory within the processor itself, called a cache memory. Ex.1010, 1:60-66 ("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, 2:7-10. 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, 2:34-36.

53. Other references prior to the '637 Patent also support this interpretation of the term "*resident within.*" For example, U.S. Patent No. 5,875,464 to Kirk ("Kirk") describes cache coherency between multiple processors for execution of software and explains how software is transferred from a memory into the processor cache for execution in the context of ensuring that each processor obtains the most recent data.

> A simple scenario which demonstrates a coherence problem is provided by a system with two processors, two caches, and a shared memory. **Each processor has read the same line of information from main memory into its cache**. **One processor then stores new data at this location**.
>
> The cache of this processor (and main memory in the event of a write-through cache) **now contains the latest information**. However, the second processor's cache still contains the old data. If this line remains valid, the ensuing access will return stale data. Different techniques,

such as directory schemes and cache snooping, are used to assure cache coherence in multi-cache systems.

Ex.1019, 14:44-56.

54. Accordingly, a POSITA would have understood that the term "*resident within*" in claims 1 and 21 means temporary storage of the transaction security software within a memory of the processor during execution of the software, as opposed to long term storage.

VIII. DETAILED PATENTABILITY ANALYSIS

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

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

57. I describe in detail below the scope and content of the prior art, as well as any differences between the claimed subject matter and the prior art, on an

element-by-element basis for the Challenged Claims of the ’637 Patent. This analysis supports my finding that the limitations of the Challenged Claims of the ’637 Patent are disclosed in the prior art, or that the differences between the Challenged Claims of the ’637 Patent and the prior art discussed herein are such that the subject matter as a whole would have been obvious at the time of the filing of the ’637 Patent to a person having ordinary skill in the art to which the subject matter pertains.

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

59. I will now describe, in the grounds below, on an element-by-element basis, how the prior art discloses or teaches all elements of the Challenged Claims. Unless otherwise noted, all *italics* refers to claim language, and **bold** or ***bold italics*** is added for emphasis.

A. Ground 1: Claims 1-6 and 21-24 is rendered obvious over Mathiassen in view of Ryan

60. It is my opinion that the combined teachings of Mathiassen and Ryan disclose or render obvious, to a POSITA, the subject matter of each and every element of claims 1-6 and 21-24 of the ’637 Patent.

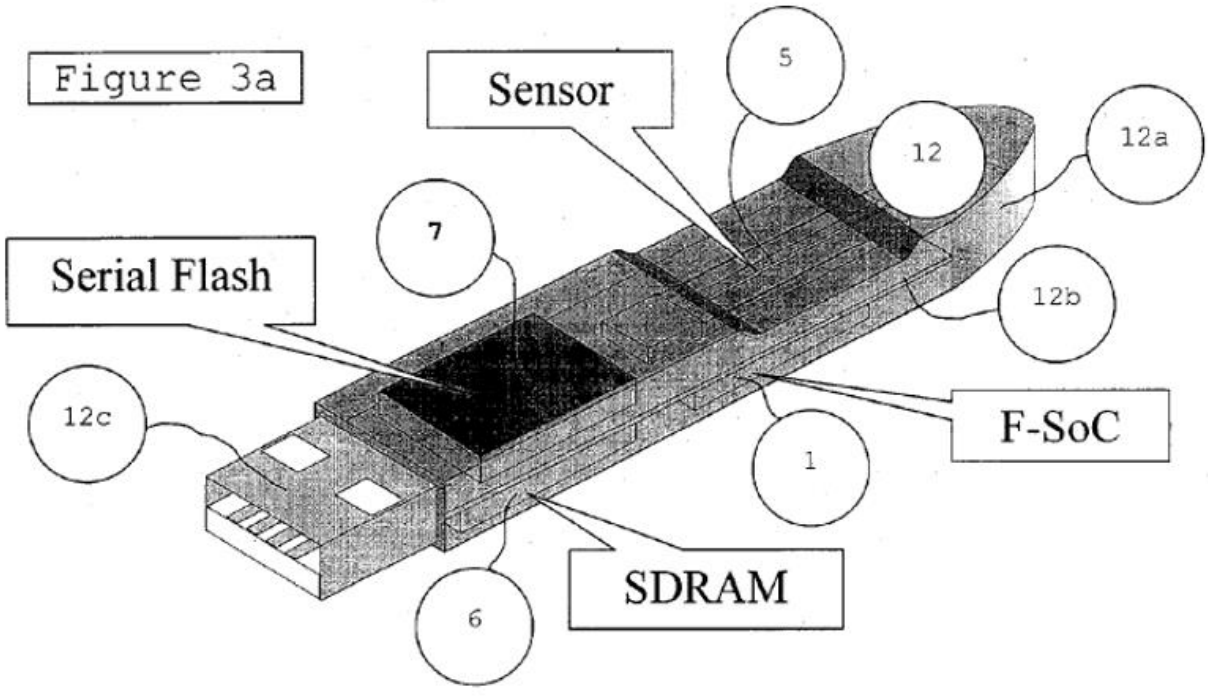
1. Overview of Mathiassen

61. Mathiassen describes "[a] portable or embedded access device." Ex.1005, Abstract.

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

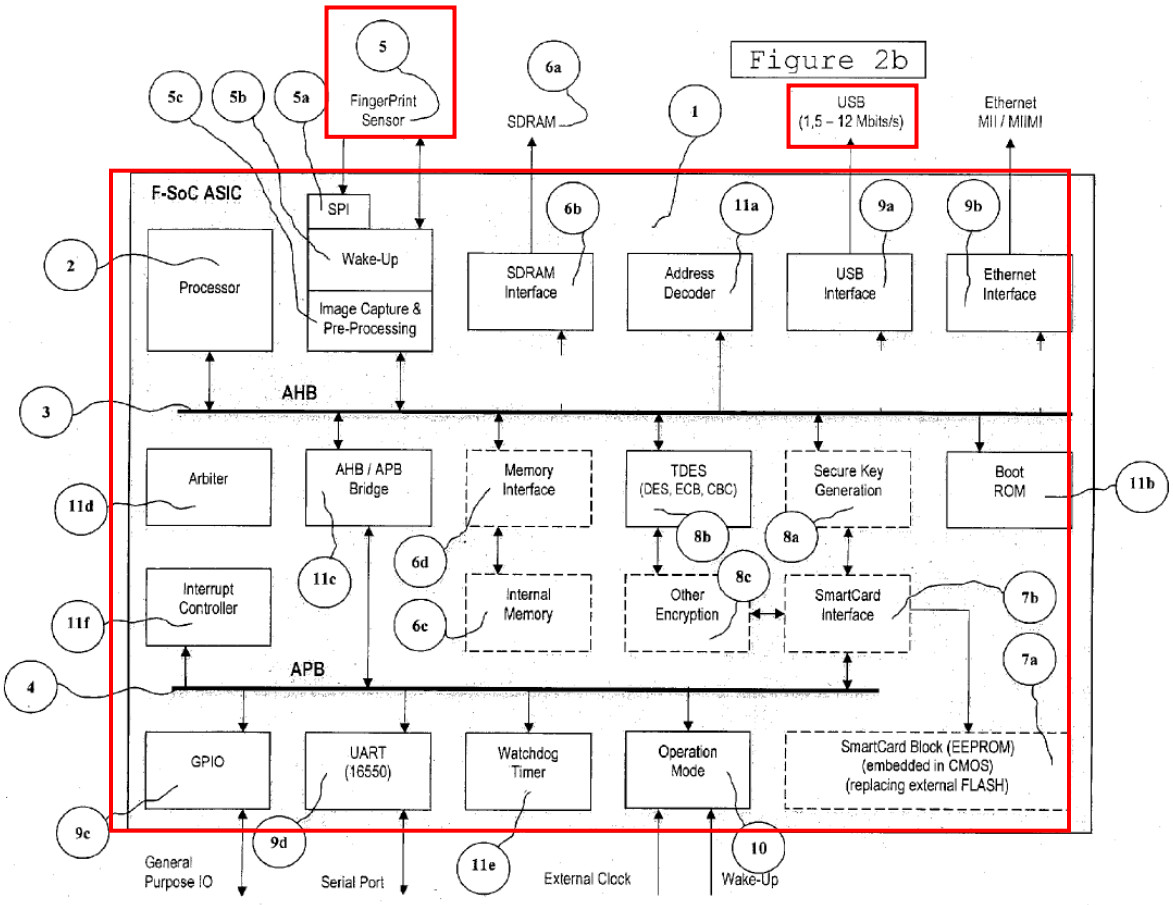
Ex.1005, Abstract.

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



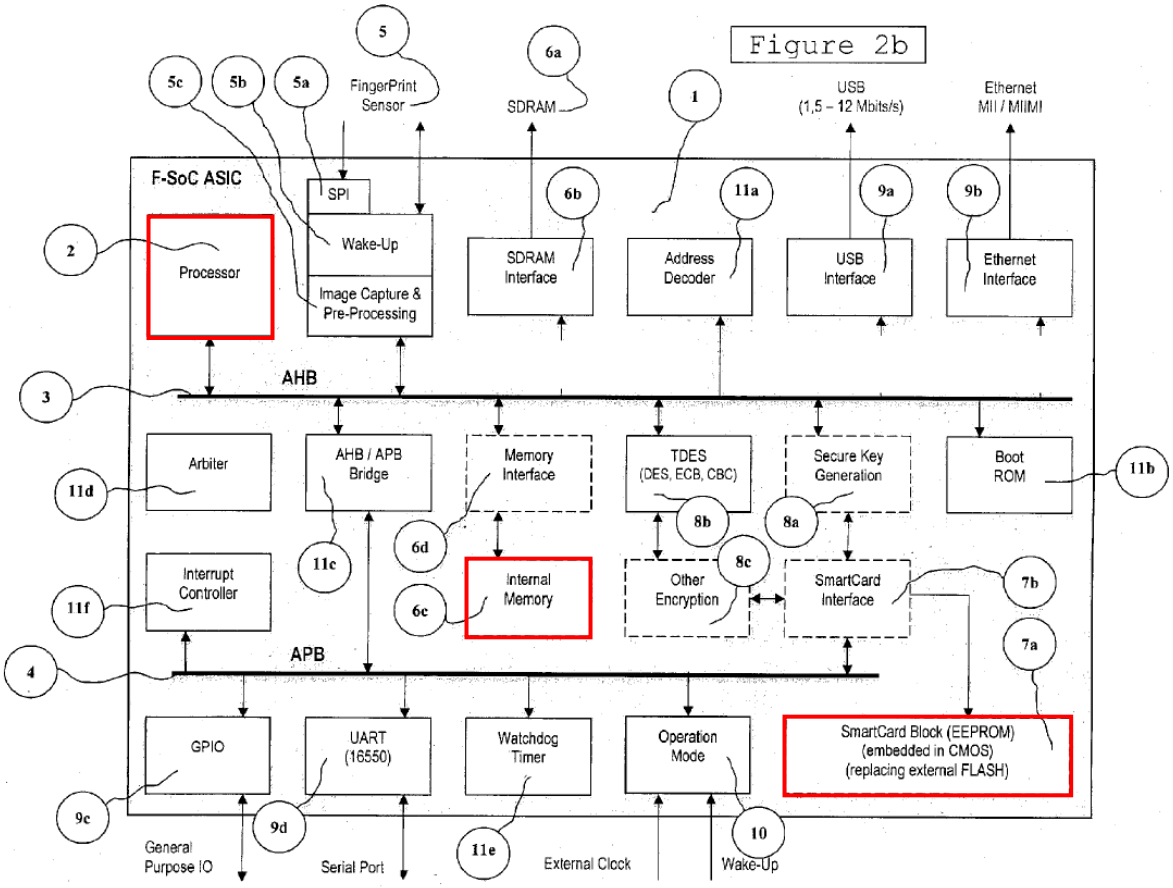
Ex.1005, Fig. 3a

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



Ex.1005, Fig. 2b (annotated)

62. The IC 1 is coupled to the USB connector ("USB") and the fingerprint sensor 5, as shown in Fig. 2b. Mathiassen explicitly explains that the IC 1 is coupled to the fingerprint sensor 5 because "[t]he sensor (5) is connected to a…pre-processing block (5C) via a first interface block (5A) as well as a wake-up circuit (5B)." Ex.1005, [0049]. In addition, Mathiassen explains that the IC 1 is coupled to the USB connector because "[t]he IC (1) also comprises hardware and/or software required to supply output signals to…second interface blocks" including "USB (9A)." Ex.1005, [0050].



Ex.1005, Fig. 2b (annotated)

63. Fig. 2b also illustrates that the IC 1 includes a "central processor (2)." Ex.1005, [0050]. The IC 1 also includes a "non-volatile memory (7, 7A, or 7C)." Ex.1005, [0050]. In Fig. 2b, the non-volatile memory is labeled as "SmartCard Block (EEPROM)." The IC 1 also includes "volatile memory (6 or 6c)." Ex.1005, [0049]. The volatile memory is labelled as "Internal Memory" in Fig. 2b. Mathiassen's portable device includes and executes software that it refers to as "administrative software." Ex.1005, [0050]. Like most conventional processing systems, and similar to the architecture described in Spear (*see* § VIII.A.), the administrative software is stored in non-volatile memory. In Mathiassen, the administrative software is stored in the non-volatile memory 7a specifically and is configured for biometrically authenticating the user and cryptographically encapsulating[1] communications sent to external systems. Ex.1005, [0050]. Subsets of the administrative software perform different functions. Specifically, a "matching algorithm" of the administrative software authenticates fingerprints (Ex.1005, [0070]-[0072]), and an additional "subset" of the administrative software encrypts data by "generat[ing] a secure key or password" and "appl[ying] encryption methods" to "produce secured output data." Ex.1005, [0091]-[0095].

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

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

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

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

65. After the user is enrolled, she may use the portable device to biometrically authenticate herself. To do so, "[t]he user will insert the portable device (12 or 13) into the USB port." Ex.1005, [0065]. After the user places her finger on the sensor 5, the portable device acquires a fingerprint image. Ex.1005,

[0049], [0066]. The device then compares the acquired fingerprint image to a prestored fingerprint image, called a "master minutia." Ex.1005, [0050], [0071]. If the acquired fingerprint matches the prestored fingerprint, the user is authenticated. Ex.1005, [0073]. ("If the matching is positive, the connection process will automatically continue."). Mathiassen's portable device then compiles and encrypts a message conveying that the user is authenticated, which may include a username and password of the user or other identification data, and transmits the message to a network or system in communication with the portable device. This process is explained by Mathiassen in detail.

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

Ex.1005, [0051].

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

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

Ex.1005, [0074].

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

> When the central processor (2) has established a positive match between the access attempt minutiae and the resident master minutiae, the administrative software stored in the non-volatile memory (7, 7A or 7E) will calculate a secure key. The secure key will either be calculated by an algorithm executed on the central processor (2) (in case of FIG. 2A), or alternatively by a dedicated hardware block (8A) in case of FIG. 2B). The general algorithm will generate the secure key, and the particular key or password will be generated as a result of the seed being inputted to the algorithm. This seed will either be scrambled and stored in scrambled format in non-volatile memory (7) in the alternative of FIG. 2a, or be securely stored in a SmartCard environment (7A) in case of the alternative IC architecture outlined in FIG. 2b.
>
> The secure key will be input to the encryption block (8,8B or 8C) for encryption of a message/communication. The message will comprise the following elements,
>
> The device number of the USB Dongle or the PCMCIA card (12 or 13) and the SKG key number (not the key itself) in non-encrypted format.
>
> The IP address of the device (12 or 13) in encrypted format.

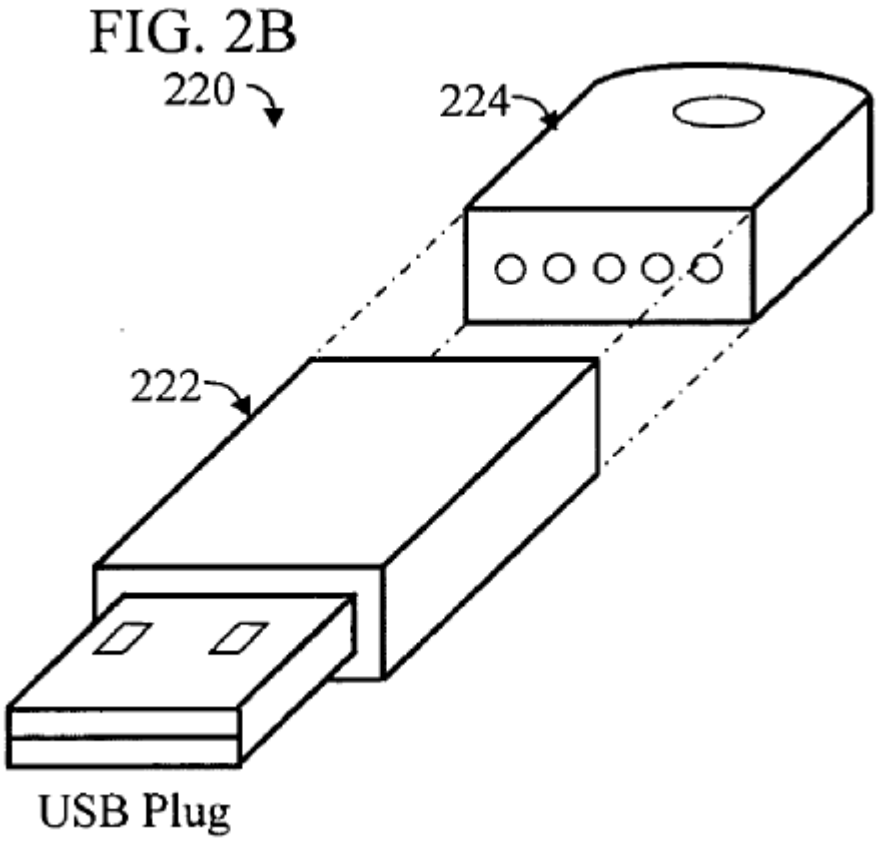
> The secure key number (in encrypted format).
>
> The user ID, in encrypted format.
>
> Optionally PKI verification in encrypted format, in case of authentication of the user holding the electronic certificate.
>
> Other encrypted information required by the particular requirements for secure communication, of the prevailing Intranet.
>
> The calculated communication response is thus a result depending on the above comparison of fingerprints. This message/communication is encrypted to form a secure output in a predefined format and sequence (e.g. handshake procedures) and transferred to an external unit, network or system through one of the communication interfaces.

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

2. **Overview of Ryan**

68. Ryan describes "[a] compact personal token apparatus, suitably resembling a conventional USB memory fob in size, shape, and form which can be plugged into a PC and interfaced with the virtual world of the Internet." Ex.1006, Abstract. For purposes of simplicity, I will refer to Ryan's compact personal token apparatus as a "smart fob" because Ryan uses this term. Ex.1006, [0149]. Ryan's smart fob both resembles and performs similar functions as Mathiassen's portable

device and the '637 Patent's ITA apparatus. Ryan describes multiple embodiments of its smart fob, one of which is shown in Fig. 2B below.



Ex.1006, Fig. 2B

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

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

Ex.1006, [0203].

69. Ryan's smart fob is used to improve communication security for a wide variety of transactions. Ryan lists several exemplary transactions.

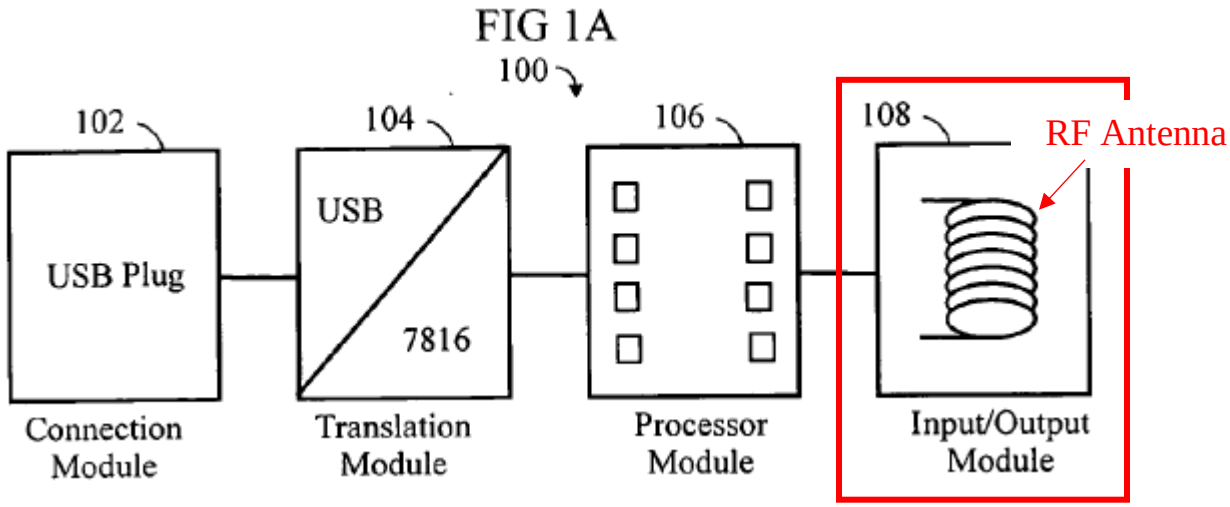
> In use, for example, the user plugs the smart fob into his PC, or other Internet capable device (appliance), connects to the Internet, and interacts with a service or content provider to upload and/or download information. For example, downloading a ticket. Then, the user takes the smart fob to the event where it connects wirelessly with a reader at the venue to allow entrance and stamp the ticket (e.g., set a flag indicating that the ticket was used).
>
> In another example, a consumer can use the smart fob to store "e-coupons" on the smart fob—loaded via the Internet. Then taking the Smart fob to a participating merchant, use the coupons to receive a savings or price reduction on the product.
>
> In another example, a consumer could load cash value to the smart fob via the Internet and use the cash in the real world—at participating merchants—to buy a meal, newspaper, etc.
>
> In another example, which can be called "kids fob" (also, without prejudice to potential trademark rights)—parents can provide their young children with a smart fob loaded with a preset amount of cash

> and send them off to the mall or participating theatre and know that the money will be used as intended.
>
> In another example, a consumer could use the smart fob to load cash via the internet—and while still connected to the PC use the stored value to pay cash for products or services on the internet. This addresses the concern that consumers still have some reservations about giving out their credit card information over the Internet.
>
> …
>
> In another example, a consumer can load cash to the electronic purse of the smart fob device via Internet banking, and while still connected to the PC use the stored value to pay for online products or services.

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

70. Ryan's smart fob enhances the security of transactions by encrypting "packets of data" sent and received as part of these transactions. Ex.1006, [0241]. As a specific example, Ryan explains that "[p]ersonal data, frequency flyer miles as well as credit card details can be encrypted and stored in the smart fob." Ex.1006, [0249]. Similarly, "digital content could be encrypted for limited time use or conditional access." Ex.1006, [0367]. In addition, "all coupons are encrypted as a security feature reducing or eliminating the likelihood that coupon values could be counterfeited or altered in any way." Ex.1006, [0368]. Ryan's smart fob may authenticate a user with a "biometric—such as fingerprint, iris scan etc." Ex.1006, [0229].

71. In addition, Ryan's smart fob communicates wirelessly via an RF antenna within the second physical module 224 in Fig. 2B. Ryan explains that the "second physical module 224…contains the processor module (e.g., 106, dual interface chip) and output module (e.g., 108, RF antenna and modulator." Ex.1006, [0203]. The output module 108 within the second physical module 224 is shown in more detail in Fig. 1A, shown below.



Ex.1006, Fig. 1A (annotated)

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

3. Motivation to Combine Mathiassen and Ryan

72. 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 include a wireless interface, as taught by Ryan, to enable Mathiassen's portable device to communicate wirelessly with external devices.

73. Mathiassen's portable device is analogous to the ITA apparatus of the '637 Patent. The '637 Patent describes a portable apparatus used for increasing online transaction security by biometrically authenticating a user. Ex.1001, Abstract. Mathiassen discloses a device with substantially the same functionality, as it pertains to a portable device for "allowing only authorized users access to" a network through biometric authentication. Ex.1005, Abstract. Thus, Mathiassen is engaged in a similar field (i.e., a portable device for improving online transaction security by biometrically authenticating a user). In addition, Mathiassen is relevant to the problem the '637 purports to solve (i.e., implementing biometric authentication in a portable device for improving online transaction security). Ex.1005, Abstract.

74. Ryan's smart fob is also analogous to the '637 Patent's ITA apparatus. Ryan's smart fob is for conducting transactions online. Ex.1006, Abstract, [0223]-[0227], [0236]; *see* § VIII.A.2. Like the '637 Patent's ITA apparatus, Ryan's smart fob also biometrically authenticates the user.

> In another example, the Smart fob could store a biometric—such as fingerprint [*sic*], iris scan etc., in a memory cell that is locked and when using the smart fob to gain access to a controlled area, the user touches his finger to a reader, waves the smart fob in front of a reader, the fingerprint is compared to the stored info, the user's identity is verified, and he is granted access.

Ex.1006, [0229].

Thus, Ryan is in the same field of endeavor and is reasonably relevant to the above-identified problem with which the inventor of the ’637 Patent was involved.

75. A POSITA would also have been motivated to modify Mathiassen’s portable device to be used to conduct online transactions as described by Ryan, and enhance the security of those transactions. In particular, Mathiassen describes (1) biometrically authenticating a user (Ex.1005, [0065]-[0074]) and, after a user is authenticated, (2) cryptographically encapsulating a message that the user is authenticated, including a user name and password, to ensure that the message itself is not intercepted or tampered with as it is sent to the target network (Ex.1005, [0075]-[0098]). While this message relates primarily to user authentication that grants the user access to the network (Ex.1005, Abstract), a POSITA would have understood that Mathiassen’s portable device could have been easily modified to use the same principles of authentication and communication security to conduct and secure online transactions as taught by Ryan. A POSITA would also have been motivated to make this modification, as explained in more detail below.

76. In particular, Ryan explains that its “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]. A POSITA would have been motivated to make this modification to Mathiassen’s portable device because Mathiassen describes using its portable device for a very similar function: to

"access…an internet bank or a corporate or government intranet," all of which are settings where online transactions take place. Ex.1005, Abstract. Ryan itself provides that would cause the POSITA to make the modification. Specifically, Ryan provides that the use of a smart fob for securing online interactions advantageously provides convenience to the user by conducting a wide variety of transactions wirelessly while enhancing security. Ex.1006, [0223], [0235] (wirelessly presenting a ticket at a venue), [0224] (redeeming coupons), [0225] (paying for purchases).

77. Modifying Mathiassen's portable device for securing online transactions as taught by Ryan would provide the benefit of ensuring that data relating to a transaction is not intercepted or modified, further enhancing security beyond just user authentication.

> Optionally, all coupons are encrypted as a security feature reducing or eliminating the likelihood that coupon values could be counterfeited or altered in any way.

Ex.1006, [0368].

Modifying Mathiassen's portable device in this way would also assure the user of the portable device that a transaction is being carried out with the intended network.

> For example, by simply inserting the smart fob into the USB port of a telephone linked PC, an automatic Internet connection to the website of the user's favourite airline is established, **via a secure server** to authenticate the user and **block spam, viruses, and SMTP (simple**

> **mail transfer protocol) based attacks**. Personal data, frequent flyer miles as well as credit card details can be encrypted and stored in the smart fob. Tickets can also be downloaded onto the smart fob and used in contactless mode at the airline check-in desk. This "client user to secure server to host server" concept **blocks pop-up windows, viruses, worms, spam and Internet "phishing" fraud**. The airline can use the platform to attract other merchants that compliment the airline's product portfolio.

Ex.1006, [0249]

As described above, because transaction authentication data is secured via encryption, only the intended server would be able to 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."). Ryan also explains that the principles it teaches ensure exchanged amounts of electronically transferred money are correct and not tampered with. For example, "the savings amount is passed to the cash register to deduct from the total bill" (Ex.1006, [0238]) and the "Secure Application Module" of Ryan's smart fob is "tamper proof" (Ex.1006, [0105]) such that the savings amount transferred is not tampered with. As a result, the trust of users in online entities and vice versa is increased. Ex.1006, [0050], [0072] (describing biometric authentication); Ex.1006, [0249] (describing a secure

server that protects against "spam, viruses,…SMTP," and "Internet 'phishing' fraud.").

78. A POSITA would also have been motivated to modify Mathiassen's portable device to include a wireless interface, as taught by Ryan. This modification would allow Mathiassen's portable device to communicate wirelessly with external devices, in addition to the wired communication techniques that Mathiassen's portable device utilizes to communicate with external devices. Ryan's wireless interface allows the smart fob to interact "via its wireless interface in the real world." Ex.1006, [0151]. This increased flexibility for external communication allows Ryan's smart fob to interface with a wider variety of systems and devices, such as ticket kiosks at venues or similar settings. For example, Ryan explains how its device may be used at an "event where it connects wirelessly with a reader at the venue." Ex.1006, [0223]. Similarly, a user can "wave the device in close proximity to a turnstile equipped with a wireless reader at the entrance." Ex.1006, [0235]. A POSITA would have recognized these advantages and been motivated to incorporate a wireless interface into Mathiassen's portable device to provide the same increased functionality. Modifying Mathiassen's portable device to conduct transactions wirelessly would, as taught by Ryan, "eliminate[] the need to tender cash" when conducting a wireless transaction. Ex.1006, [0248]. 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 accomplish 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).

79. The combination of Mathiassen and Ryan would have been the combination of commonly known elements. Mathiassen's disclosure shows that a portable device with a fingerprint sensor that authenticates was well known. Ryan's disclosure shows that using a compact personal apparatus to conduct transactions with a wireless interface was also well known. In addition, Mathiassen shows that it was well known to include and execute encryption software to encrypt authentication data within a portable device. As a result, the combination of Mathiassen and Ryan merely yields the predictable result of biometrically authenticating a user, improving the security of online transactions, and a wireless interface. It is my opinion, supported by the prior art disclosures themselves, that all the claimed elements of the '637 Patent constituted basic and well-known technology at the time and would have been easily combinable.

80. In particular, a POSITA would have had a clear expectation of success in modifying Mathiassen's portable device to include the features taught by Ryan. The devices described by both Mathiassen and Ryan authenticate a user biometrically. Ex.1005, Fig. 3a, [0048]-[0050]; Ex.1006, [0229]. The devices described by both Mathiassen and Ryan encrypt data. Mathiassen's portable device encrypts data related to user authentication. Ex.1005, [0075]-[0098]. Ryan's smart fob encrypts data related to online transactions in Ryan. 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].

81. Ryan's smart fob includes a wireless transceiver interface. Ex.1006, Fig. 1A (Input/Output Module 108)). Mathiassen's portable device describes several different types of interfaces and would be easily modified to include a wireless one. Ex.1005, [0050]. In that regard, modifying Mathiassen's portable device to include a wireless interface as taught by Ryan would be improving a similar device in the same way. Mathiassen describes a number of wired communications interfaces by which its portable device communicates with external systems. Ex.1005, [0050], Fig. 2b (interfaces blocks 9A, 9B, 9C, and 9D). Ryan describes a wired communications interface as well as a wireless communications interface that performs the same function of transmitting data to an external device. Ex.1006,

[0175] (listing wired interfaces and wireless interfaces equally suitable for communicating "between an external memory/processing apparatus and a personal computer."). Ryan explains that both its wired communications interface and wireless communications interface perform the same function of transferring data to and from the smart fob. Ex.1006, [0223], [0235]. Similarly, the '637 Patent itself, like Ryan, explains that its wired interface and wireless interface are interchangeable equivalents. Specifically, Fig. 1B is "the same as the USB model in FIG. 1A except for a change in physical form from that of a stick-type enclosure to a card or similar, and the replacement of the USB interface with a radio circuit such as a Bluetooth or ZigBee chip with antenna 26." Ex.1001, 6:50-54. Using a wireless interface instead of a wired interface in a portable device would have been well within the skillset of a POSITA at the time because these interfaces would have been seen as easily interchangeable. A POSITA at the time would have recognized that the features of Mathiassen and Ryan would be easily combined and would have been motivated to modify Mathiassen to include a wireless interface and authenticate transactions, as taught by Ryan.

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:

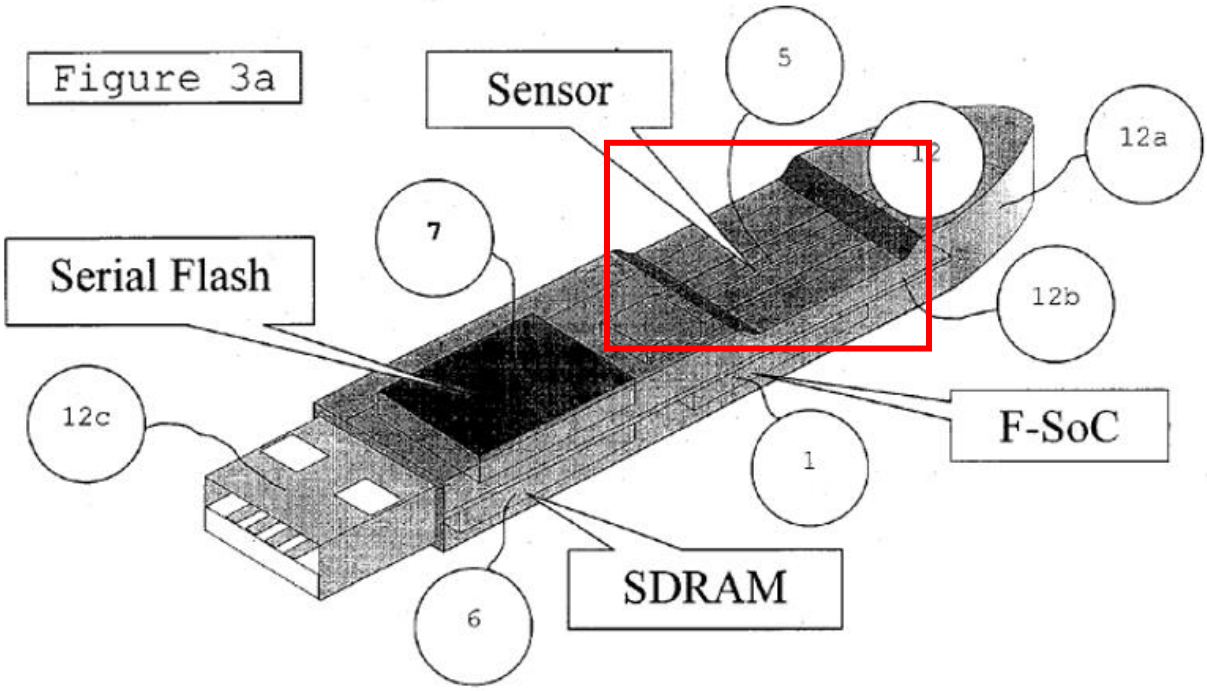
82. I have been informed that the preamble of claim 1 is not limiting. To the extent that the preamble is limiting, Mathiassen and Ryan discloses or at least renders obvious *a biometric customer authentication apparatus for improving online transaction security and for assuring the identity of a customer*.

83. Specifically, Mathiassen discloses a *biometric customer authentication apparatus*.

> A portable or embedded access device is provided for being coupled to, and for allowing only authorized users access to, an access-limited apparatus, device, network or system, e.g. a computer terminal, an internet bank or a corporate or government intranet. The access device comprises an integrated circuit (IC) (1) providing increased security by bridging the functionality of biometrics input from a user and, upon positive authentication of the user's fingerprint locally to provide secure communication with the said access limited apparatus, device, network or system, whether local or remote.

Ex.1005, Abstract.

84. Mathiassen often refers to the "portable or embedded access device" as a "portable device." Ex.1005, Abstract. The portable device is shown in Fig. 3a of Mathiassen below.



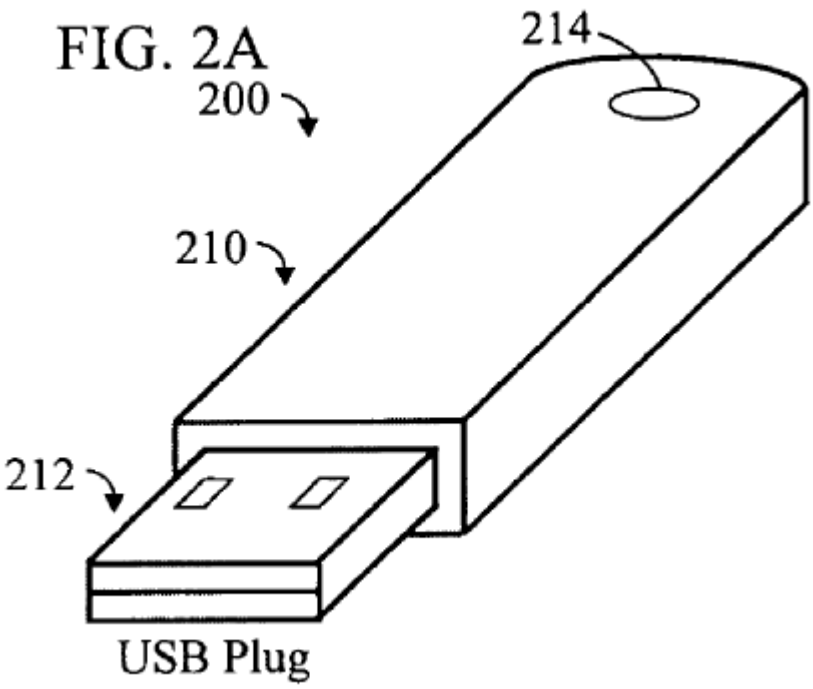
Mathiassen , Fig. 3a (annotated)

85. As shown in Fig. 3a above, Mathiassen's portable device "comprises an integrated circuit (IC) 1." Ex.1005, Abstract. Mathiassen's portable device also includes a "biometrics sensor in the form of a fingerprint sensor (5)…coupled with [the] IC (1)." Ex.1005, [0048]. Mathiassen's portable device includes a non-volatile memory 7 (Ex.1005, [0050]) and a USB interface 12C (Ex.1005, [0054]). Mathiassen's portable device includes a "biometrics sensor in the form of a fingerprint sensor (5)." Ex.1005, [0050]. Mathiassen's device authenticates a user based on readings from this sensor by comparing "fingerprint representations… with master fingerprint representations" to identify "a positive match." Ex.1005, [0050]. Mathiassen also describes its portable device as "a portable access device for

allowing only authorized users access…." Ex.1005, [0047]. Based on these disclosures, Mathiassen's portable device is a *biometric customer authentication apparatus*.

86. Mathiassen and Ryan also show *improving online transaction security*. Matthiassen'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].

87. Ryan describes a similar device, called a "compact personal token apparatus," "apparatus," and "smart fob." Ex.1006, Abstract. Ryan's smart fob is shown in Fig. 2A below. Ryan's "compact personal token apparatus" is also referred to as a "smart fob" and will be referred to as a smart fob throughout. Ex.1006, [0149].



Ex.1006, Fig. 2A

88. Ryan explains how its smart fob can be used to securely complete online transactions.

> **The smart fob can operate as a security device**. For example, the smart fob starts an auto-run application, after insertion in an Internet-connected PC. In simple terms, the PC user is automatically connected to a participating merchant's website and **can conduct a business transaction in a secure fashion, without the fear of anyone spying or manipulating the data**.

Ex.1006, [0232].

Ryan provides an extensive list of examples of online transactions that may be conducted using Ryan's smart fob.

> In use, for example, the user plugs the smart fob into his PC, [and] download[s] a ticket. Then, the user takes the smart fob to the event where it connects wirelessly with a reader at the venue to allow entrance ….
>
> In another example, a consumer can use the smart fob to store "e-coupons" on the smart fob—loaded via the Internet. Then taking the smart fob to a participating merchant, use the coupons to receive a savings or price reduction on the product.
>
> In another example, a consumer could load cash value to the smart fob via the Internet and use the cash in the real world….
>
> In another example,…parents can provide their young children with a smart fob loaded with a preset amount of cash….
>
> In another example, a consumer could use the smart fob to load cash via the internet—and while still connected to the PC use the stored value to pay cash for products or services on the internet….

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

Prior to completing these transactions, Ryan anticipates biometrically authenticating the user. Ex.1006, [0229]. The transaction data are also encrypted. Ex.1006, [0241]. A POSITA would have been motivated to modify Mathiassen's portable device to improve the security of any of the transactions described in Ryan. *See* § VIII.A.3.

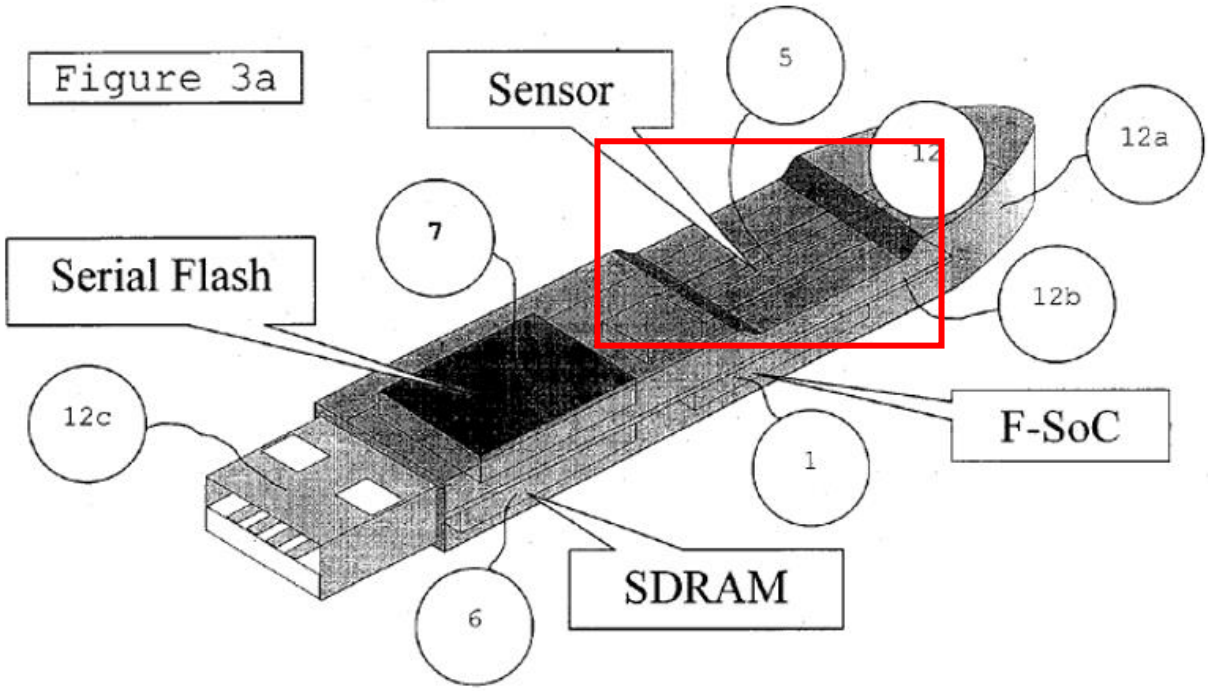
89. Mathiassen also discloses *assuring the identity of a customer*. Specifically, Mathiassen teaches providing access to "network[s] or system[s], e.g., a computer terminal, an internet bank or a corporate or government intranet" via its portable device "pending a positive match of [a user's] fingerprint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

90. A POSITA would have been motivated to modify Mathiassen's portable device to conduct and authenticate transactions, as taught by Ryan, for the reasons presented in Section VIII.A.3.

91. 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).

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

92. Mathiassen's "portable device has a housing," as shown in annotated Fig. 3a below, corresponds to *an electronic enclosure including a fingerprint sensor disposed thereupon*. Ex.1005, [0055].

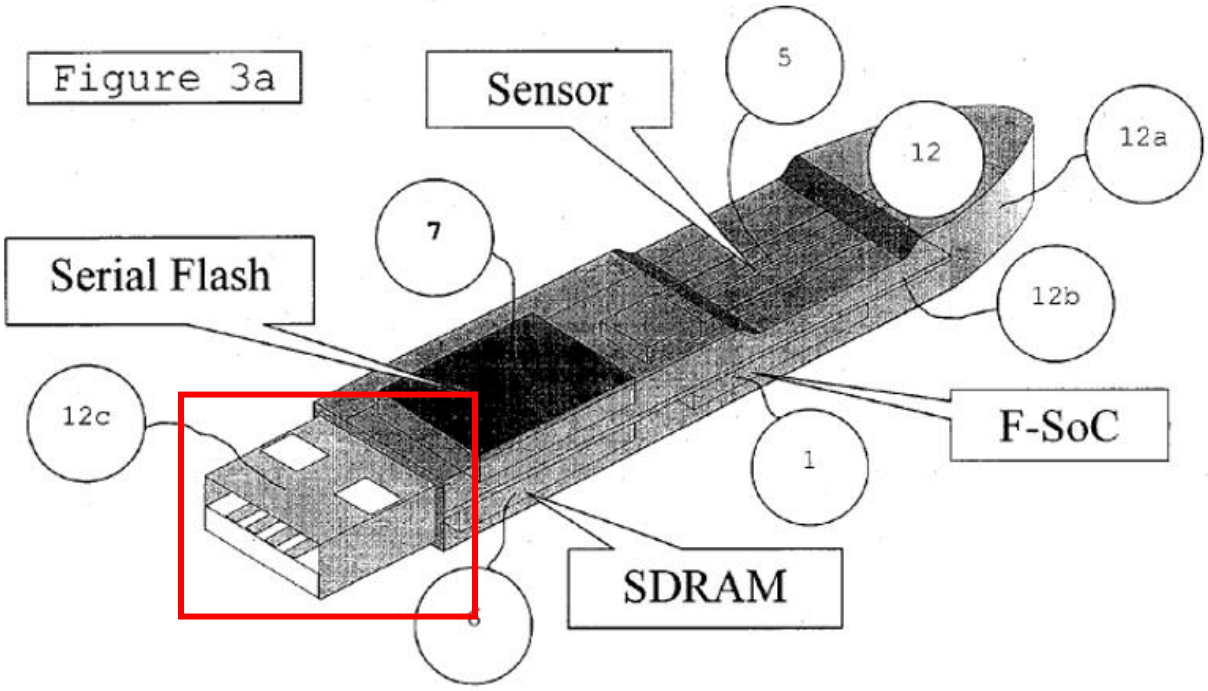


Mathiassen , Fig. 3a (annotated)

Mathiassen's housing is an *electronic enclosure* because it houses electronic components. For example, Mathiassen explains that its "components and chips are protected inside [the] housing." Ex.1005, [0054]. As shown in Fig. 3a above, Mathiassen's housing (*electronic enclosure*) includes a fingerprint sensor 5. *See* § VIII.A.4.a., [1.0]. Mathiassen further explains that "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)." Ex.1005, [0055]. Thus, Mathiassen teaches *an electronic enclosure* (a housing) *including a fingerprint sensor* (fingerprint sensor 5) *disposed thereupon*.

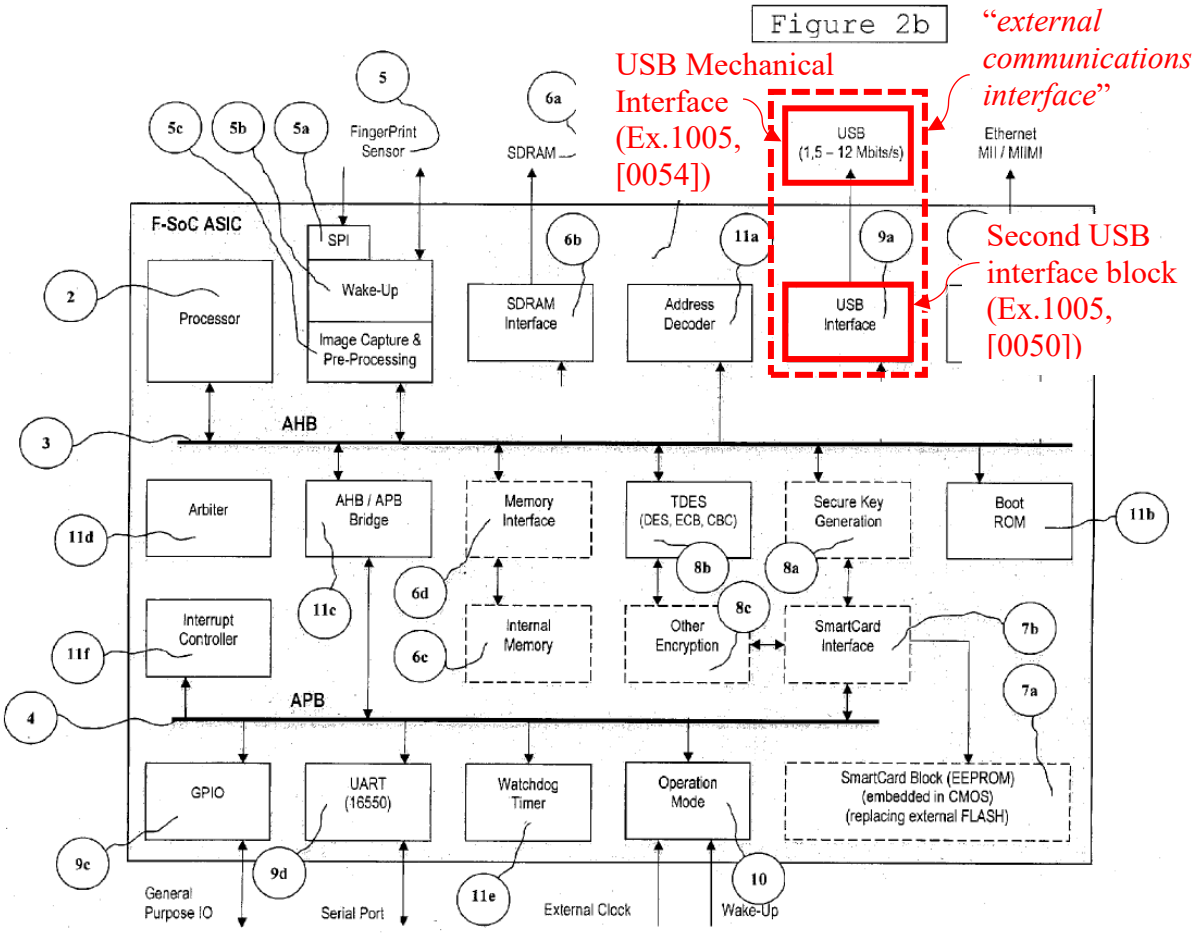
[1.1.2] further including an external communications interface;

93. 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 Fig. 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 Fig. 2b, below. Ex.1005, Fig. 2b, [0054].



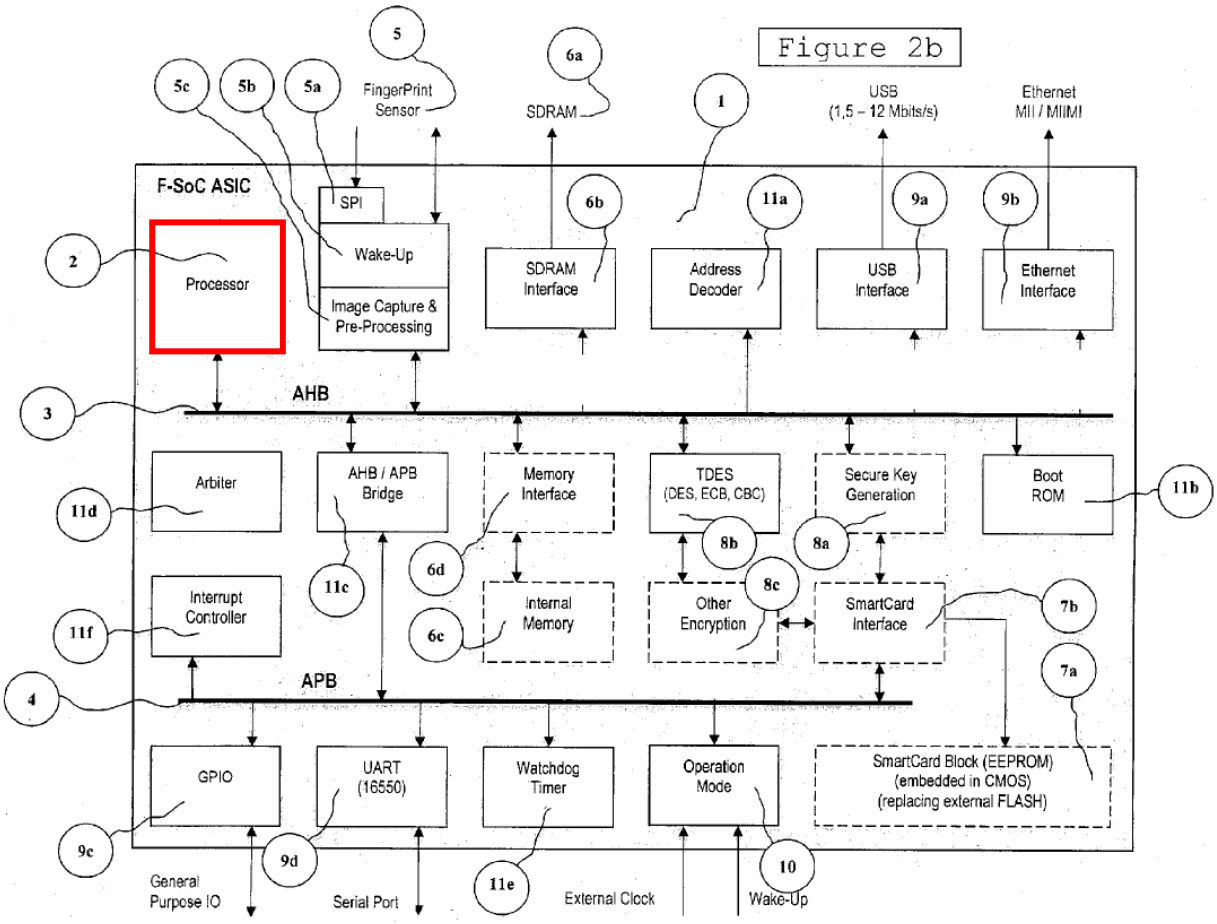
Mathiassen , Fig. 2b (annotated)

Mathiassen describes "a number of second interface blocks (9A, 9B, 9C or 9D)" which "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).").

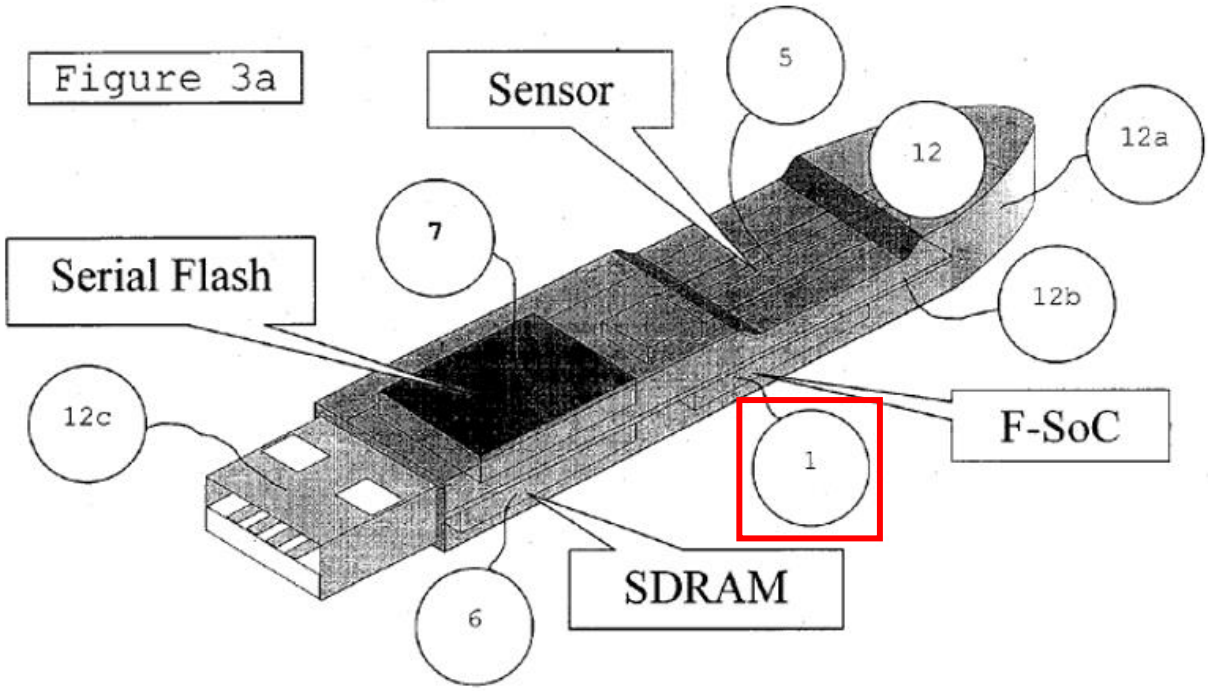
[1.2.1] at least one processor comprised within said enclosure and

94. As discussed previously with regard to limitation [1.1.1], Mathiassen discloses an *enclosure* (housing). As shown in Fig. 2b below, the integrated circuit 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. 2*b* [s]hows a second realization of an integrated circuit that is an integral part of the invention.").



Ex.1005, Fig. 2b (annotated)

95. As shown in Fig. 3a below, the IC 1, which includes the processor 2, is within the housing.

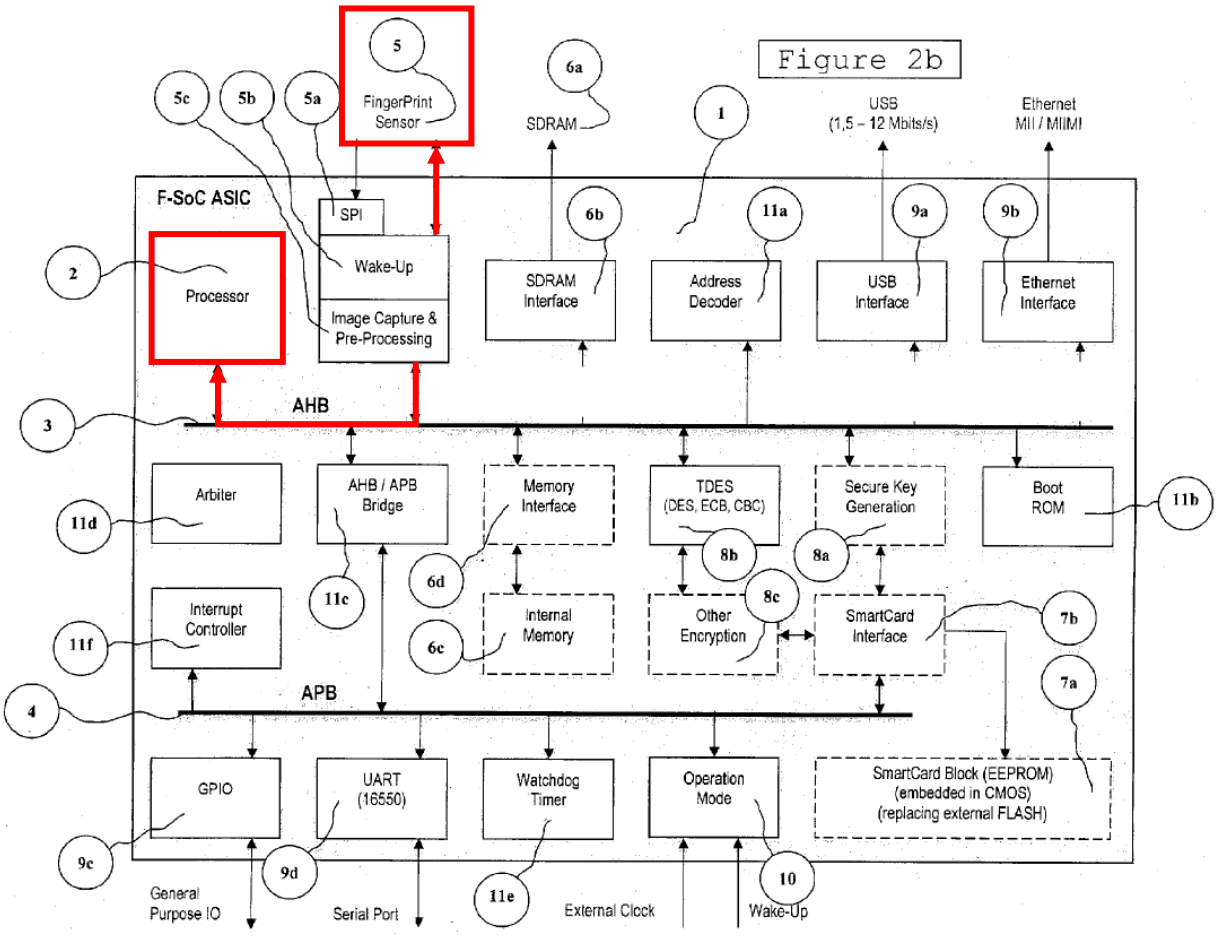


Mathiassen , Fig. 3a (annotated)

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

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

97. As shown in Fig. 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.1005, Fig. 2b (annotated)

In Mathiassen, data is transferred between the fingerprint sensor 5 and the processor 2 via the wake-up block 5B, the pre-processing block 5C, and high-speed bus 3. Ex.1005, [0066]-[0069]. Mathiassen also explains that "the biometrics processor (F) is directly connected to [t]he sensor (B)") Ex.1005, [0047]. 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 (5C) will crunch the…captured fingerprint images" (Ex.1005, [0068]) into "reduced data" that is "transferred from

the working volatile memory (5C) to the central processor (2) via the high-speed bus (3)" (Ex.1005, [0069]).

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

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

99. Mathiassen describes "administrative software" which corresponds to *transaction security software*. Ex.1005, [0050] (memory "used for storing program code, e.g., administrative software").

100. The '637 Patent's *transaction security software* includes two subsets: *biometric fingerprint authentication software* and *cryptographic transactions authentication software*. Mathiassen's administrative software corresponds to *transaction security software* because it includes two nearly identical subsets: a "matching algorithm" for fingerprint authentication (Ex.1005, [0072], *see* [1.3.2])) and an additional subset for generating cryptographic data (Ex.1005, [0091]-[0095] (describing "handshake sequences," "generating a secure key," "applying…encryption methods," and "produc[ing] secured output data"), *see* [1.3.3]).

101. Mathiassen also describes *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*.

102. Mathiassen also describes *transaction security software resident within…said at least one processor*. As discussed in Section VII.A above regarding the term *resident within*, 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).”). As explained in Section VII.A, when software is executed on a processor, it is resident within a cache memory of the processor. This understanding is consistent with the disclosure of the ’637 Patent, the disclosure of the prior art at the time, including Spear as well as other prior art references. 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. Long-term storage of software within a processor, such as within a cache memory of a processor would be highly disfavored at the time of the alleged invention because processors at the time did not have cache memories

large enough to store software, such as authentication and encryption software, long-term in addition to execute applications or perform other functions. Therefore, a POSITA at the time would have understood that software resident within a processor was not software stored long-term in the processor, but stored while it is executed.

103. In addition, the architecture of Mathiassen's portable device is substantially similar to the '637 Patent. Mathiassen's portable device includes a non-volatile memory and a central processor and a POSITA would have understood that the processor and non-volatile memory described in both the '637 patent and Mathiassen would operate in the same way. Ex.1005, Fig. 2B (illustrating memory 7a in communication with processor 2), [0050]. Mathiassen's administrative software, which is *transaction security software,* is executed by its central processor. Ex.1005, [0050]. As explained previously, as is typical in virtually all processor-based architectures, software that is stored in a non-volatile memory is transferred to the cache of the processor in small portions when it is executed. *See, e.g.*, Ex.1010, 1:20-2:47 ("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.1019, 14:46-49 ("[e]ach processor…read[s] the same line of information from main memory into its cache"). 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)."). During this process, the administrative security software is resident within the processor 2, thus teaching *transaction security software resident within…said at least one processor*.

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

104. A subset of Mathiassen's administrative software, which corresponds to *transaction security software* (*see* Section VIII.A.4.a., [1.3.1]), includes "matching algorithm" software for fingerprint authentication. Ex.1005, [0072].

105. In Mathiassen, the fingerprint sensor 5 captures the user's fingerprint and performs and the pre-processing block 5C processes the image.

> The pre-processing block is designed to perform the initial, heavy-duty processing of the captured raw images from the Sensor (5). The intermediate results are stored in the volatile memory (6A or 6C) that is interfaced via the high speed bus (3) to a first memory interface block (6B or 6D).

Ex.1005, [0049].

106. The processor 2 receives the intermediate results and reduces them into "compact fingerprint representations, called minutiae." Ex.1005, [0050]. Mathiassen then explains how a subset of the administrative software compares the received fingerprint with those previously loaded on the portable device. "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]. Mathiassen further explains that "[a]ccess 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)." Ex.1005, [0050]. Mathiassen provides additional detail regarding this same process of matching a received fingerprint with a pre-stored fingerprint to authenticate a user.

> To initiate the connection procedure, the user swipes his finger over the fingerprint Sensor (5) of the USB Dongle. This will trigger a signal to the wake-up block (5B) of the sensor interface (5A) on the IC (1).
>
> The pre-processing block (SC) will immediately start capturing the fingerprint image from the sensor (5) via a first interface block (5A), while the wake-up circuitry (5B) is powering up the remaining blocks of the IC (1).
>
> …
>
> The pre-processing block (SC) will crunch the raw data, …thus reducing them to an intermediate form….
>
> When this data reduction is completed by the pre-processing block (SC)…, the reduced data are gradually transferred from the working volatile memory (SC) to the central processor (2) via the high-speed bus (3).

> Then the central processor (2) will retrieve the compact fingerprint minutia information from a master minutiae table, created during the enrolment of the authorized user(s), stored in non-volatile memory (7, 7A or 7C), and compare it with the access minutiae table temporarily stored in working volatile memory (6A or 6C).
>
> The matching algorithm, being a subset of the administrative software, will position the minutiae points of the access attempt minutiae table over the minutiae points of the master minutiae table, and translate and rotate the upper until a best fit is established. …Thereby a comparison of the extracted features representing the captured fingerprint with features of the pre-stored master fingerprint representations is obtained.
> …
> One result of the occurrence of a positive match could be that the release of an IP address from the SmartCard block (7C) or from the external SmartCard chip (7E).

Ex.1005, [0066]-[0074].

107. As set forth above, Mathiassen clarifies that this "matching algorithm" is "a subset of the administrative software." Ex.1005, [0072].

108. Thus, Mathiassen teaches *transaction security software* (administrative software) *further comprising biometric fingerprint authentication software for authenticating authorized customers* (matching algorithm subset of administrative software).

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

109. Mathiassen's administrative software includes an additional subset of software for generating cryptographic data and encrypting data.

> A subset of the administrative software which tailors the output secure response to the target network or intranet (N) to a pre-defined format and sequence including handshake sequences, could be pre-loaded into the non-volatile memory (7A, 7E, or 7).
>
> Preferably this pre-loaded subset of administrative software is able to combine one or more of the following steps:
>
> generating a secure key or password (8 or 8A),
>
> applying any of the encryption methods at hand…,
>
> tailoring handshake sequences according to the rules of secure communication of the device, network or system (N) [and] produc[ing] secured output data which is suitable for transmission in the targeted network (C) and for processing by receiving units connected to the network (C).

Ex.1005, [0091]-[0095].

110. In Mathiassen, the secure output produced is accessed and sent by the portable device only 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].

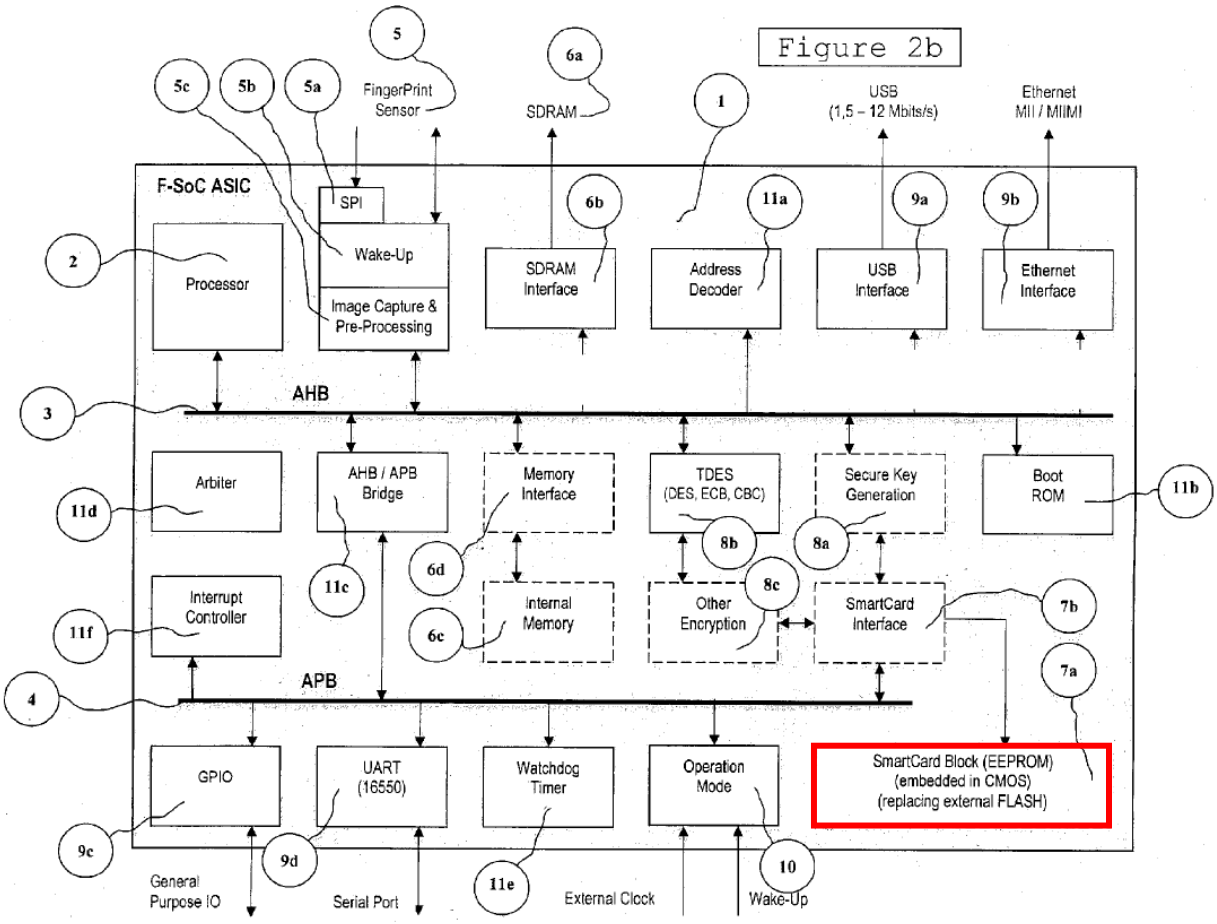
111. This generated secure output grants the user of Mathiassen's portable device access to online entities, such as "an internet bank or a corporate or government intranet." Ex.1005, Abstract. In addition, a POSITA would have understood that the same cryptographic secure output features described by Mathiassen to secure data sent to a target network for user authentication purpose would also be used to secure output data related to online transactions. 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, frequency 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]. 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.

112. 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).

[1.4.1] at least one of a memory and

113. Mathiassen's portable device includes "non-volatile memory (7, 7A, or 7C)." Ex.1005, [0050]. Non-volatile memory 7A is highlighted in Mathiassen's Fig.2 below.



Ex.1005, Fig. 2b (annotated)

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

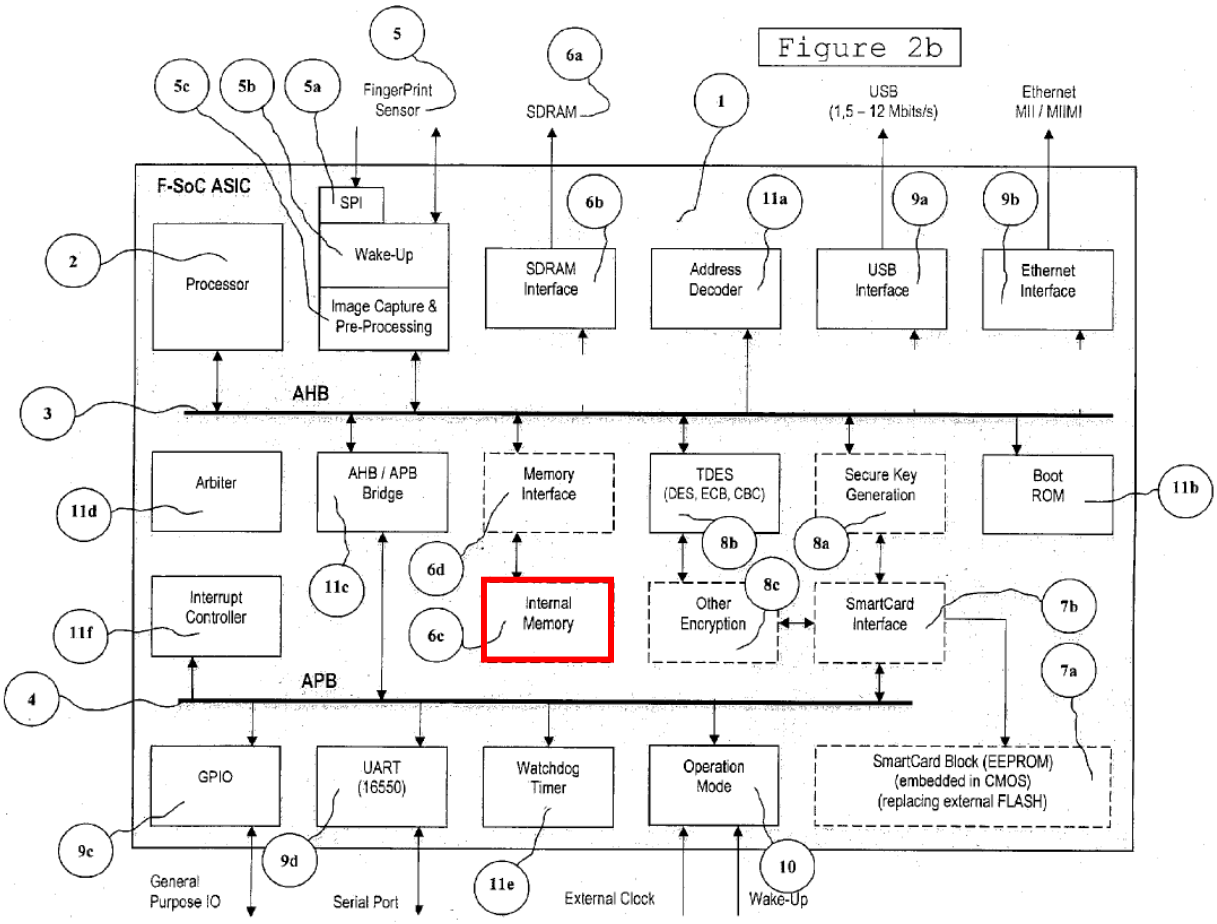
[1.4.2] a communications buffer

115. 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. This understanding is consistent with how the buffer was used in the industry to refer to a memory or storage device that temporarily stores data information. Buffers were and are commonly used to store data to be sent or received (i.e., communication data) and commonly may be volatile memory within a typical processor-based architecture.

116. Based on this understanding, a POSITA would have understood that Mathiassen's internal memory, highlighted in Fig. 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.1005, Fig. 2b (annotated)

117. 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 to and from the volatile memory itself because Mathiassen describes the volatile memory receiving "intermediate" data and transferring data from the volatile memory.

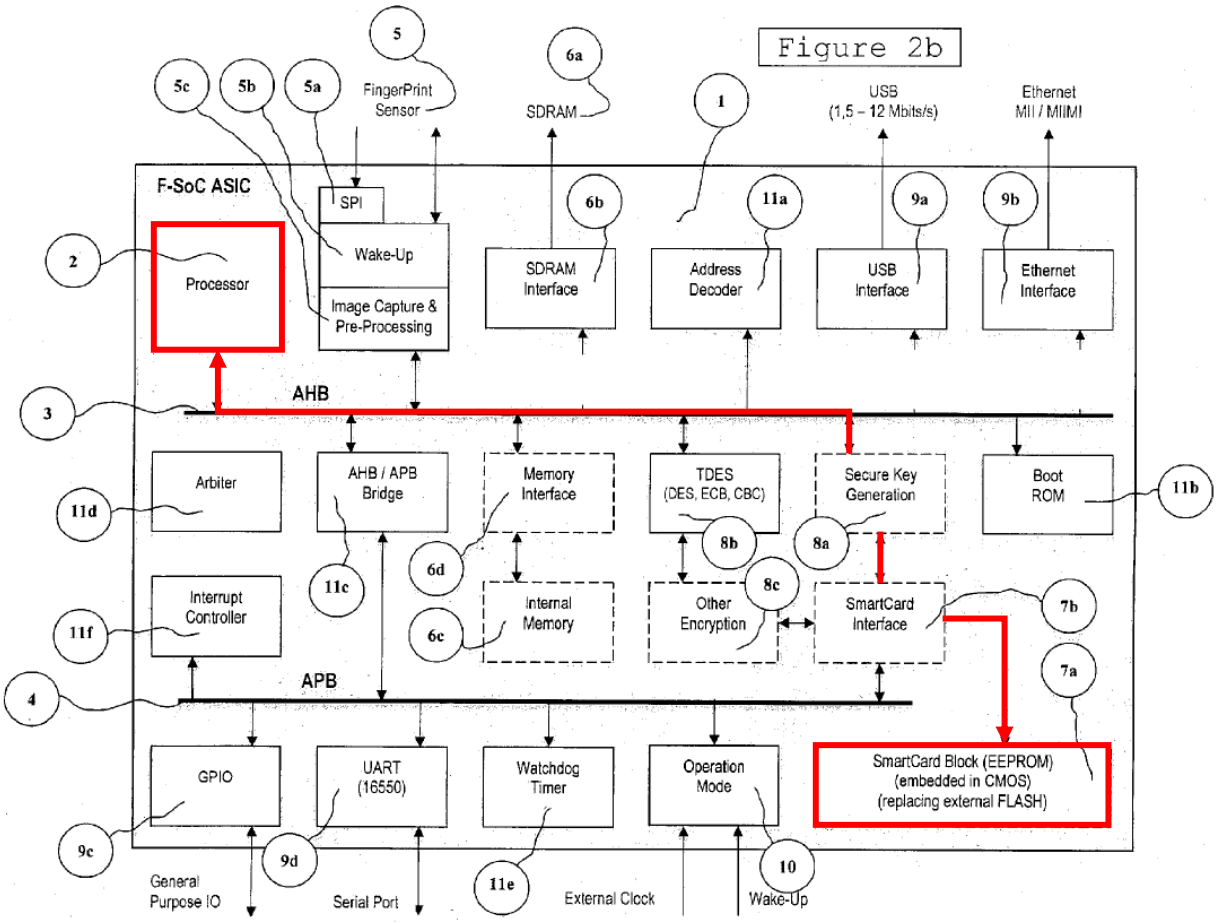
118. In addition, "[t]he volatile memory (6A or 6C)…provides working memory that is available to other modules on the IC (1)." Ex.1005, [0049]. These

modules include interfaces 9A, 9B, 9C, and 9D used for communicating external data. A POSITA would have understood that by providing working memory to external interfaces, the volatile memory 6A or 6C would receive and temporarily store data received from an external source in communication with the portable device and/or receive and temporarily store data received from the processor (2) or non-volatile memory 7 of the portable device prior to transmitting such data to an external device or network via the interface 9A, 9B, 9C, and 9D. A POSITA would have understood that the volatile memory is memory for sending and receiving external data.

119. 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.

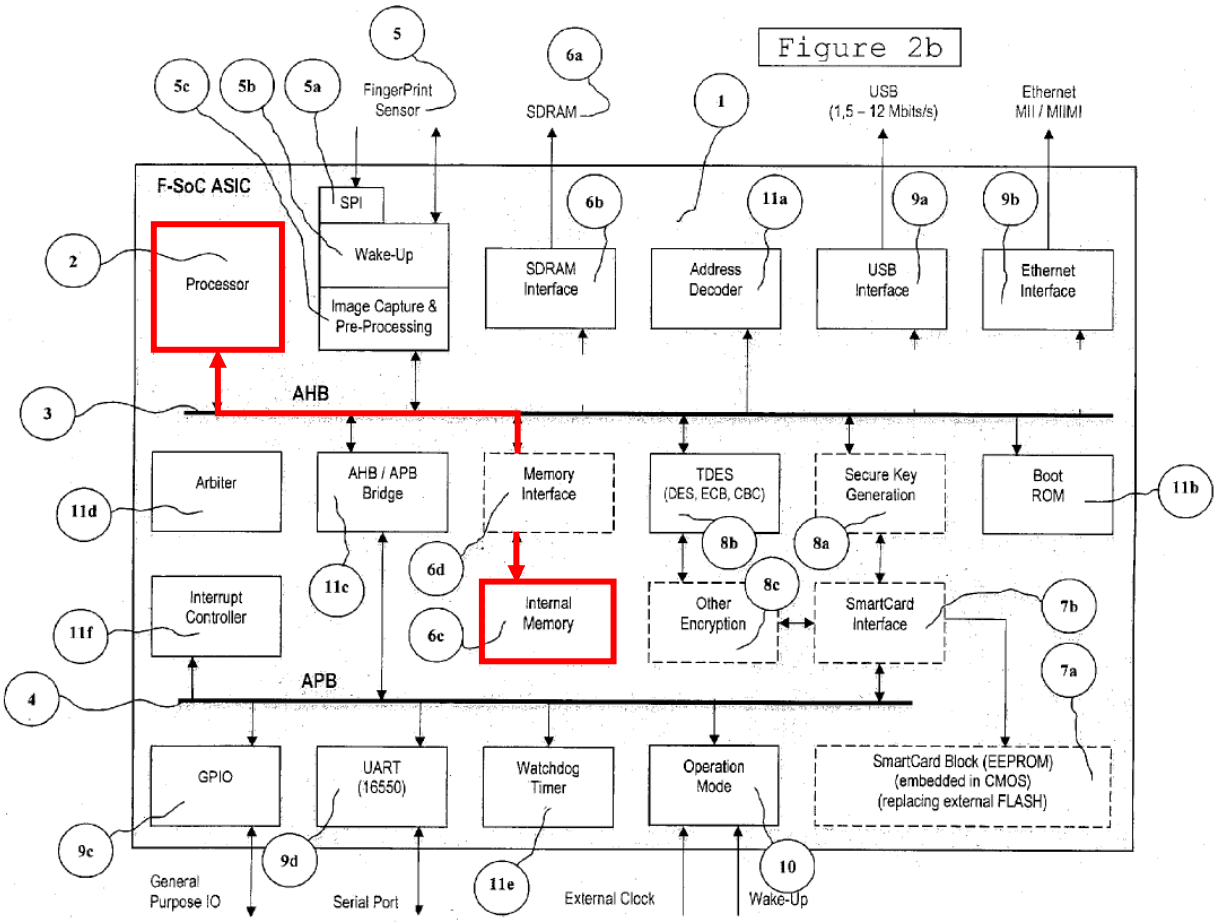
[1.4.3] at least one of a memory and a communication buffer coupled to said at least one processor and

120. 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 Fig. 2b below.



Ex.1005, Fig. 2b (annotated)

121. Mathiassen's volatile memory 6C, which corresponds to a *communications buffer* (*see* Section VIII.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 Fig. 2b below.



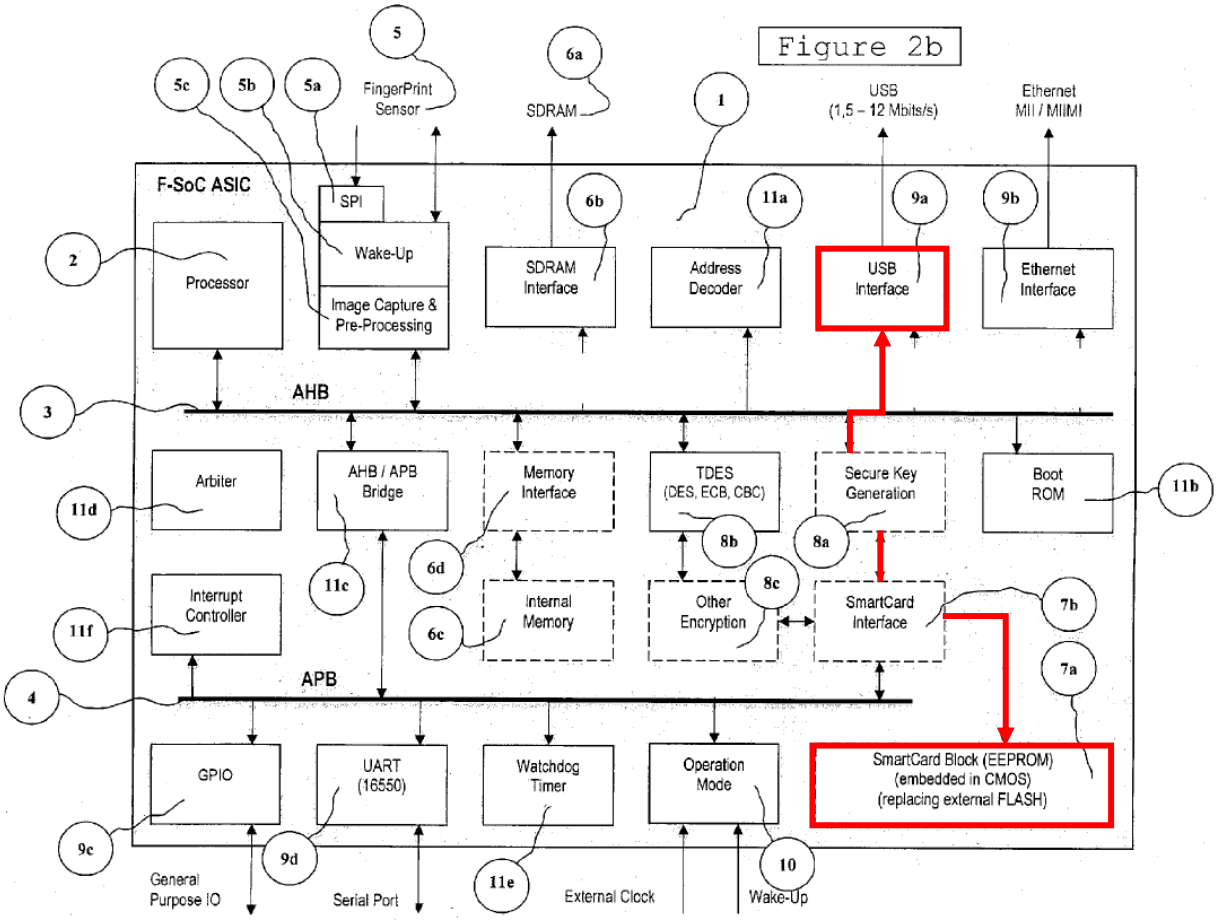
Ex.1005, Fig. 2b (annotated)

122. 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*.

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

123. Mathiassen's external communications interface includes the USB mechanical interface 12C and the USB interface block 9A in Fig. 2b. *See* Section

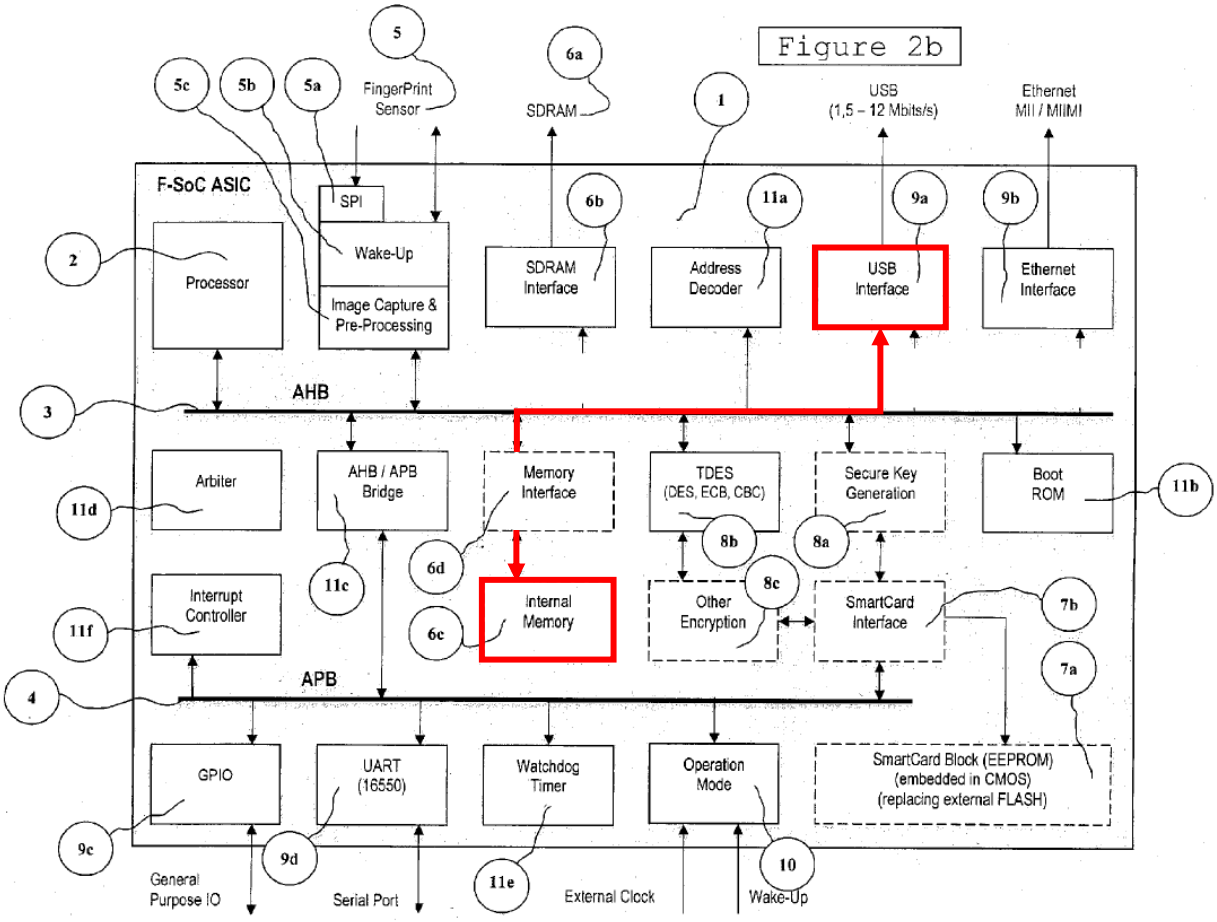
VIII.A.4.a., [1.1.2]. As shown, the non-volatile memory 7A is coupled to the USB communications interface 9A.



Ex.1005, Fig. 2b (annotated)

Mathiassen describes transferring "a Java applet from its non-volatile memory (7, 7A or 7E)…via the USB port (9A)." Ex.1005, [0075]. Because data, here a Java applet, can be transferred from the non-volatile memory 7a to the USB port 9A, Mathiassen discloses that the non-volatile memory 7a is coupled to the USB port 9A.

124. Mathiassen also shows its volatile memory 6C, which corresponds to a "communications buffer" (*see* Section VIII.A.4.a., [1.4.2]), coupled to the USB communications interface 9A, as shown in Fig. 2b below. Ex.1005, [0049]-[0050] ("The volatile memory (6A or 6C) thus provides working memory that is available modules on the IC (1)" such as "interface blocks (9A, 9B, 9C or 9D).").



Ex.1005, Fig. 2b (annotated)

125. 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).

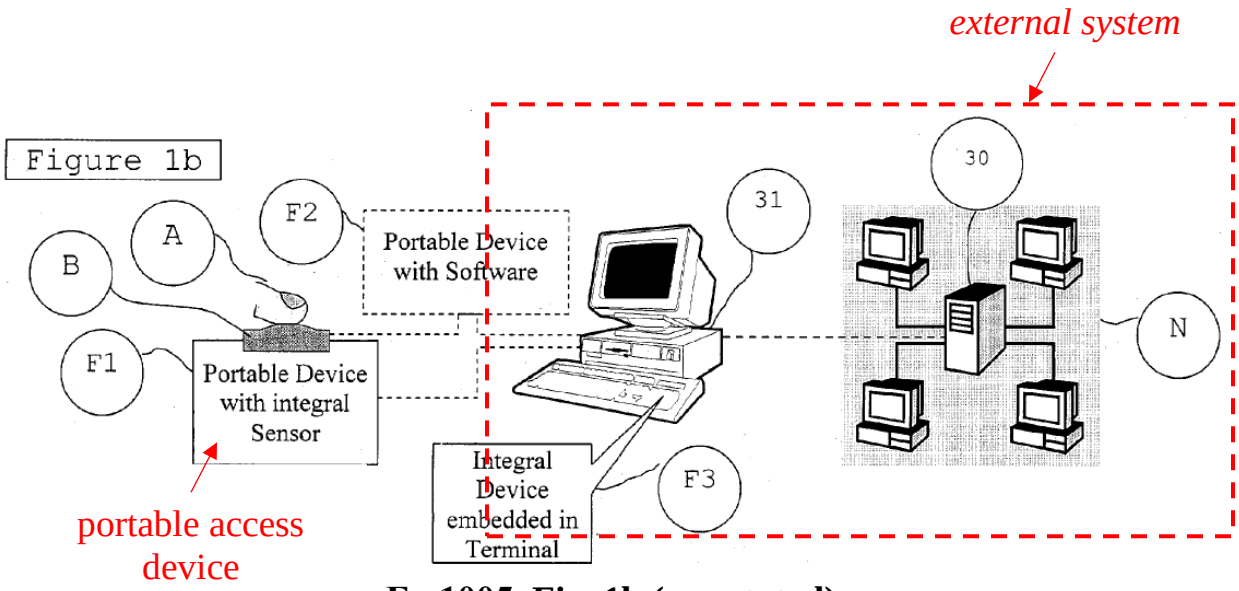
[1.5] a communications subsystem coupled into said external communications interface for relaying data messages between at least one external system and said apparatus.

126. The term "*communications subsystem*" is a very generic term to refer to generic electronic components that relate to communication. In that regard, a POSITA would have understood that *a communications subsystem* that is *coupled into said external communications interface* may refer to any one or more components (i.e., a subset) of the external communication interface that facilitate communications with external devices.

127. As explained in Section VIII.A.4.a., [1.1.2] above, Mathiassen's external communications interface includes the USB mechanical interface 12C and USB interface block 9A. As one or more components of the external communications interface, either of these components may correspond to a *subsystem coupled into said external communications interface*. For example, the USB interface block 9A may correspond to a *subsystem coupled into said external communications interface*.

128. 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 Fig. 1b below. Ex.1005, [0053] ("a server (30) in a network" and "a terminal (31) of the network.").



Ex.1005, Fig. 1b (annotated)

Fig. 1b 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]).

129. 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).

130. Due to the generic nature of the claim terms "*communications subsystem*" and "*external communications interface*" of claim element [1.5], various arguments could be made that any number of components could be mapped to these claim elements. However, even if other components of the '637 Patent were to be mapped to the "*communications subsystem*" and "*external communications interface*" claimed, Mathiassen and Ryan would certainly disclose the same features. As a result, claim limitation [1.5] is rendered obvious. At best, the '637 Patent provides two embodiments of an interface that communicates with an external device or system, i.e., an *external communications interface* including a *communications subsystem*. These include a standard USB plug, as shown in Fig. 1A of the '637 Patent and a standard wireless antenna, as shown in Fig. 1B of the '637 Patent. Nothing about these interfaces is novel. A USB plug is a universal external communications interface that must adhere to predetermined standards of compatibility. Similarly, the wireless antenna described in the '637 Patent is only ever described as complying with similar communications standards (i.e., "a Bluetooth or ZigBee chip" (Ex.1001, 6:54)) that are also not only well known, but must comply with predetermined standards to be universally compatible. 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 and complying with the same USB standards of universal

communication. Ex.1005, [0054], Fig. 3a; §§ VIII.A.4.b-c. Ryan's "compact personal token apparatus comprises a wireless interface" that similarly complies with well-known and established standards. Ex.1006, [0124], Fig. 1A, Fig. 2B; §§ VIII.A.2., VIII.A.4.d. For example, Ryan provides a wireless interface such as a "Bluetooth compatible interface, WLAN 812.11, UWB, and any similar interface." Ex.1006, [0134].

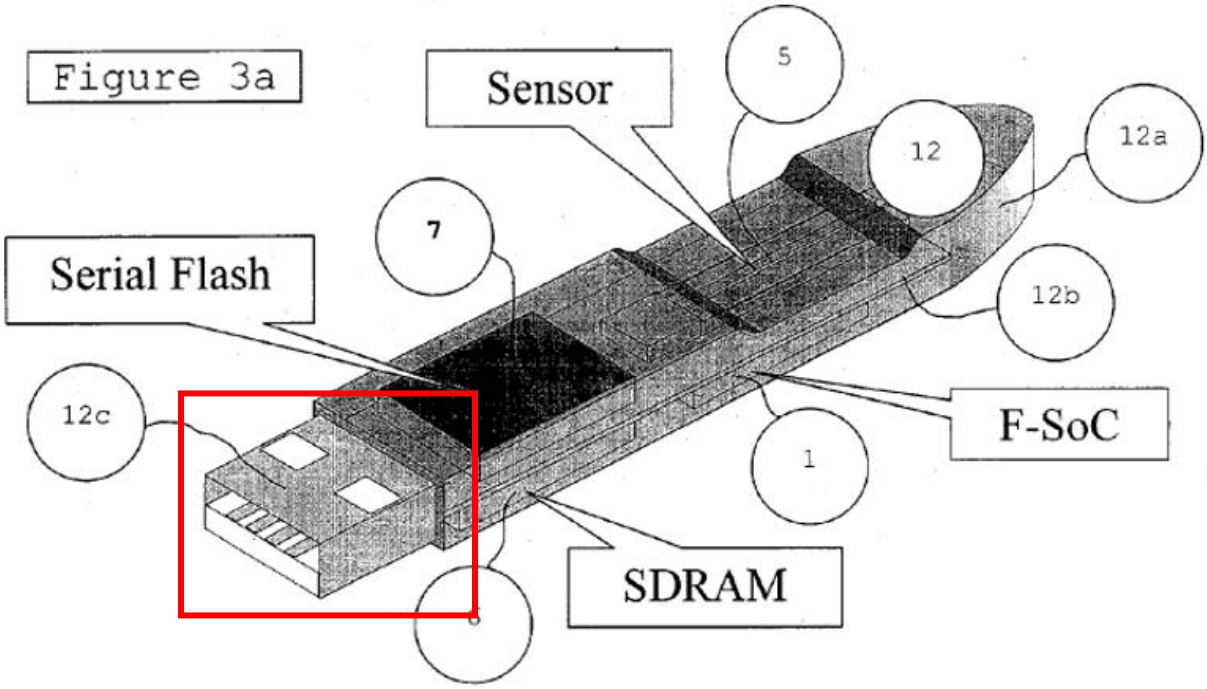
131. The '637 Patent never alleges that its communications interfaces (the USB plug or wireless antenna) are anything more than the same conventional USB connectors and antennas described in Mathiassen and Ryan. Thus, to the extent the claim terms *external communications interface* or *communications subsystem* may be mapped to other components within the '637 Patent, Mathiassen and Ryan disclose the same components and these mappings would also be disclosed or rendered obvious.

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.

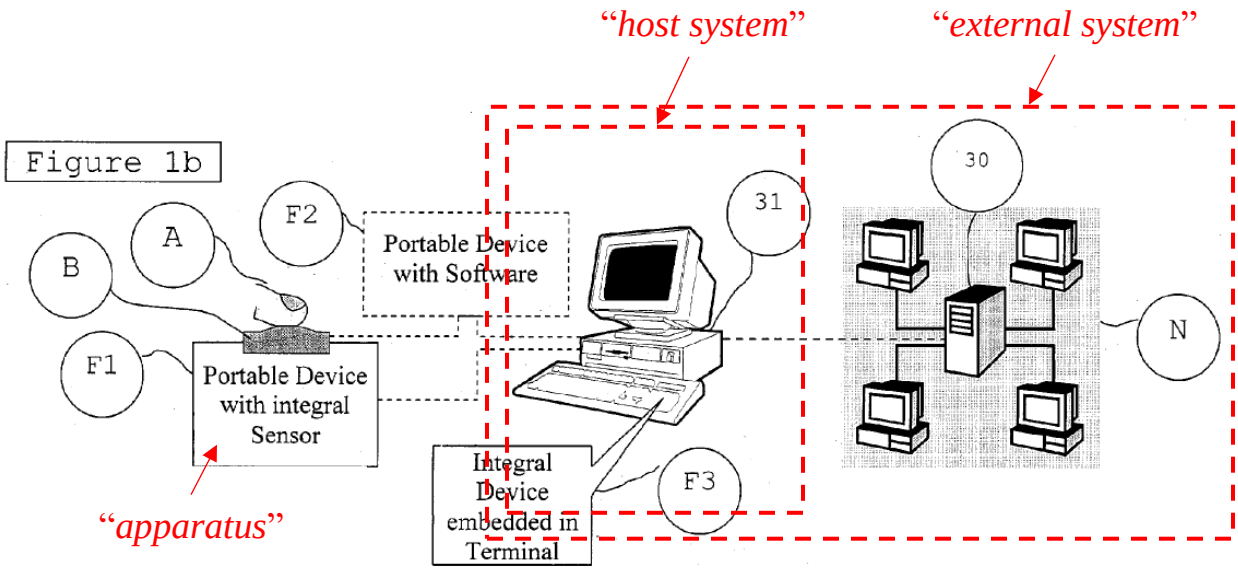
132. Mathiassen's USB mechanical interface 12C and USB interface block 9A correspond to an *external communications interface*. Mathiassen's USB mechanical interface 12C, illustrated in Fig. 3a, is a *physical interface connector*.

This is shown in that it is physically inserted into a USB port. "The user will insert the portable device (12 or 13) into [a] USB port." Ex.1005, [0065].



Mathiassen , Fig. 3a (annotated)

133. 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 Fig. 1b.



Ex.1005, Fig. 1b (annotated)

134. 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*. Mathiassen's network N corresponds to *said external system. See* Section VIII.A.4.a., [1.5]. The computer terminal 31 is a part of the network N. Ex.1005, [0053] ("a terminal (31) of the network."). The computer terminal 31 corresponds to the *host system* claimed and is described in Mathiassen as a "host device." Ex.1005, claim 9.

135. 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).

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.

136. Claim 3 further defines the *physical interface connector* of claim 2 to a more specific *USB connector*. The physical interface connector of Mathiassen described at claim 2 is a USB connector. Ex.1005, [0054] ("USB interface (12C)"), [0065] ("[t]he user will insert the portable device (12 or 13) into [a] USB port."). Thus, for the same reasons that Mathiassen renders obvious claim 2, Mathiassen also renders obvious claim 3. Specifically, Mathiassen's external communications interface *further comprises a USB connector for insertion into an external port disposed upon one of a said host system at said at least one external system* as claimed.

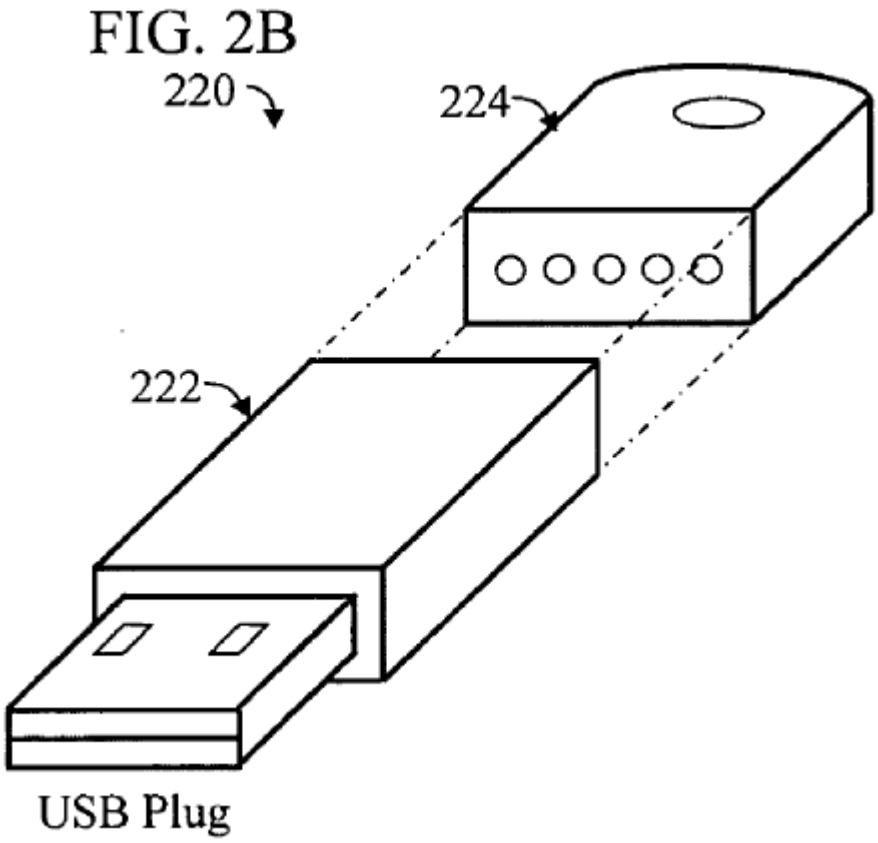
d) Claim 4

[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.

137. Implementing a wireless transceiver into Mathiassen's portable device would have been a straightforward and routine modification, as shown by Ryan. Mathiassen's portable device includes an external communications interface. *See* Section VIII.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), PCMCI/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* Section VIII.A.3.

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



Ex.1006, Fig. 2B

As shown in Fig. 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's wireless interface "enabl[es] communication with a personal device" external to the smart fob. Ex.1006, [0038]. That personal device "also comprises means for wireless communication." Ex.1006, [0038].

139. Ryan's smart fob has similar processing capabilities as Mathiassen's portable device and is intended to perform very similar functions. *See* § VII.A.3. Given the similarity, the benefits of a wireless interface, and the open-ended list of external interfaces disclosed in Mathiassen, a POSITA would have understood that Mathiassen's device would be readily modified to include a wireless interface. *See* § VIII.A.3.

140. 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* (means for wireless communication of external device) *communications interface aboard one of a host system* (computer terminal 31) *and said at least one external system* (network N).

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.

141. Mathiassen's "non-volatile memory (7, 7A, or 7C)" (Ex.1005, [0050]) corresponds to the *memory* claimed. *See* Section VIII.A.4.a. [1.4.1]. Mathiassen's non-volatile memory 7A *is…adapted for storing and retrieving data*. Specifically, Mathiassen explains:

> The non-volatile memory (7, 7A or 7C) being coupled to the high-speed bus (3) via a second memory interface block (7B or 7D) 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.

Ex.1005, [0050]. Similarly, the non-volatile memory 7A is for "data exchange." Ex.1005, [0052] (explaining how the "demand for data exchange" is reduced by incorporating the "volatile memory (6C) and non-volatile memory (7A) as integrated blocks in the IC (1).").

142. 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, as mentioned above, 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 SecureCard 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*.

143. Mathiassen's "volatile memory (6C)" (Ex.1005, [0052]) corresponds to the claimed *communications buffer*. *See* Section VIII.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 minutia table." Ex.1005, [0070].

144. 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.

145. 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).

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.

146. Mathiassen's portable device compiles and encrypts a message that is then sent to an external system, i.e., network N. This message includes at least "[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].

147. This secure data message/communication is sent to the network N, which corresponds to *said…external system*.

> This message/communication is encrypted to form a secure output in a predefined format and sequence (e.g. handshake procedures) and **transferred to an external unit, network or system** through one of the communication interfaces.

Ex.1005, [0084].

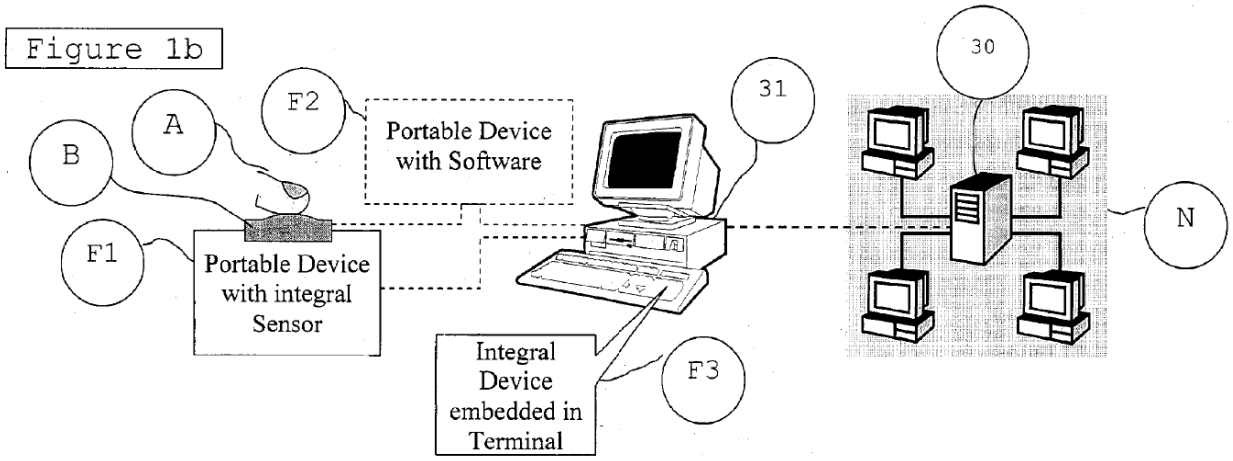
148. Similarly, Mathiassen explains that "this information is received by e.g. the target server (30) of the network (N)." Ex.1005, [0086]. Mathiassen also explains that this transmission of the "message/communication" is done after the user is biometrically authenticated. Ex.1005, [0084]-[0085] (the "response is thus a result depending on the above comparison of fingerprints").

149. Thus, Mathiassen discloses *cryptographically encapsulating said data messages* (compiling and encrypting a secure message) *into secure data messages* (encrypted message) *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* (biometric user authentication) *by said customer initiating said transaction* (initiated by the user swiping their finger over the sensor), as claimed.

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:

150. I have been informed that the preamble of claim 21 is not limiting. To the extent that the preamble is limiting, Mathiassen and Ryan discloses or at least renders it obvious. Mathiassen illustrates *[a] system* in Fig. 1b.



Ex.1005, Fig. 1b

In describing Fig. 1b, Mathiassen describes:

> In an access-limited apparatus, device, network or **system** (N), e.g. a computer terminal, an internet bank or a corporate or government intranet, a portable access device for allowing only authorized users access is preferably arranged as shown schematically in FIG. 1B.

Ex.1005, [0047].

The biometrics processor of the portable access device "is exemplified in FIGS. 2A and 2B." Ex.1005, [0047].

151. Mathiassen explains that the system shown in Fig. 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 how a user may securely accessing the server to initiate a transaction. Ex.1005, [0050] (describing how "[t]he encryption blocks (8, 8B or 8C) may also be used to encrypt general information transactions between the IC (1) and the network server (30), if desirable."). To access the server, the user "insert[s] 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].

152. Mathiassen also explains that the system shown in Fig. 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]). A POSITA would be motivated to implement this process to encrypt data transferred as part of an online transaction, as taught by Ryan. See §§ VIII.A.3., VIII.A.4.a. [1.0], [1.3.3].

153. 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, Fig. 1b of Mathiassen illustrates a customer interacting with the biometric authentication apparatus by her finger A shown in Fig. 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).").

154. 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* (portable device).

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

155. Mathiassen describes enrolling a user with the portable device.

> The network administrator, or persons he has delegated authority to, will then enroll the user who will be the "owner" of the portable device (12 or 13). Such delegation may be performed by the administrator enrolling new sub-administrators on the server, with privilege to enroll new users. When the administrator has enrolled a sub-administrator, including capturing one or more of the sub-administrator's fingerprints, the administrator must counter-sign with his own pre-approved fingerprint, before the sub-administrator privilege to enroll new users is authorized by the software on the server (30). Thereby a delegation hierarchy is maintained, enabling tracking of administrator and sub-administrator authorizations, to check for non-intended use of the administrator rights, to detect any unfaithful servants in the hierarchy.

Ex.1005, [0061].

156. The process also 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].

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

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

158. 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]. *See* § VIII.A.4.a.[1.1.1].

159. 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, Fig. 2b of Mathiassen illustrates the processor 2 within the IC 1 of the portable device and explains that "the portable device has an IC (1)." Ex.1005, [0053]. In addition, "the IC (1)" includes "the central processor (2)." Ex.1005, [0050]; *see* § VIII.A.4.a.[1.2.1].

160. 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 Fig. 2b of Mathiassen. Ex.1005, Fig. 2b; *see* § VIII.A.4.a.[1.2.2].

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

161. 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]. *See* § VIII.A.4.a.[1.1.2].

162. 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* § VIII.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*.

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

163. Limitation [21.2.3] is substantially similar to limitation [1.3.1]. In particular, limitation [1.3.1] recites *transaction security software resident within and executing on said at least one processor*. Limitation [21.2.3] recites *transaction security software resident within and executing on said processor*. Because the

claimed *said processor* of limitation [21.2.3] is also *at least one processor* as recited in limitation [1.3.1], the Mathiassen-Ryan combination render limitation [21.2.3] obvious for at least the same reasons as the described with reference to limitation [1.3.1]. *See* § VIII.A.4.a [1.3.1].

[21.2.4] biometric fingerprint authentication software for authenticating authorized customers

164. Limitation [21.2.4] is identical to limitation [1.3.2]. For the same reasons described at claim limitation [1.3.2], the Mathiassen-Ryan combination renders obvious claim limitation [21.2.4]. *See* § VIII.A.4.a [1.3.1].

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

165. Limitation [21.2.5] is identical to limitation [1.3.3], respectively. Therefore, the Mathiassen-Ryan combination discloses or renders obvious limitation [21.2.5] for the same reasons as described with reference to limitation [1.3.3]. *See* § VIII.A.4.a [1.3.3].

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

166. 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 an *external system* including the server 30 and computer terminal 31. Ex.1005, [0053], Fig. 1b; *see* § VIII.A.4.b.

167. 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 is "plugged into a terminal (31) of the network" in order to communicate with the network N. 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]).

168. 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*.

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

169. 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*. Limitation [3.0] recites *a USB connector for insertion into an external interface port*. As explained with regard to limitations [2.0] and [3.0], Mathiassen's portable device includes a USB connector. Ex.1005, [0054]. This USB connector is configured to be inserted into the USB port of the terminal 31 of the network N. Ex.1005, [0065] (to access "the network (N)," "[t]he user will insert the portable device (12 or 13) into [a] USB port."). The physical USB port of the

network N is *a physical external communication interface 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.

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

170. Limitation [21.3.3] is similar to limitation [4.0]. 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* Section VIII.A.4.d. Similarly, if a POSITA would have understood how to modify Mathiassen's portable device to include a wireless interface, a POSITA would similarly have understood that the system with which the portable device would communicate wirelessly would also include a wireless interface. Therefore, a POSITA would have also understood that the Network N, including any of the devices of the Network N, would also include a wireless communications interface.

171. This understanding is also supported by the teachings in Ryan. Ryan explicitly teaches components of an external system that include 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 describes a scenario in which "the user takes the smart fob to the event where it connects wirelessly with a reader at the venue." Ex.1006, [0223]. 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. *See* § VIII.A.4.d.

172. A POSITA would also understand that the network N described in Mathiassen includes a wireless communication interface based on prevailing technology of the time. In particular, the terminal 31 in Mathiassen is depicted and described as a standard computer. Ex.1005, Fig. 1b, [0100]. Standard computers at the time of the '637 Patent included wireless interfaces. For example, U.S. Patent No. 6,760,017 to Banerjee et al. ("Banerjee"), which was filed over 10 years prior to the '637 Patent's filing date, explains how wireless systems were common to standard computers at that time.

> **Wireless LAN systems are known in the art**. Such systems enable various desktop and/or portable personal computers to be connected in a local area network in order to share resources. Such wireless LAN

> systems obviate the need to provide a direct wire connection between the various desktop and/or portable personal computers connected to the LAN. **Such personal computers are normally equipped with a wireless LAN card and a radio interface** which typically includes a spread-spectrum type radio to reduce interference.

Ex.1013, 1:54-63.

Similarly, U.S. Patent No. 6,092,117 to Gladwin et al. ("Gladwin"), also filed over 10 years prior to the '637 Patent's filing date and a coinventor of Banerjee, also shows that it was common knowledge for standard computers at the time to include a wireless interface.

> When the remote host computer 101 is in a stand-alone configuration, as illustrated in FIG. 1, **communication between the remote host computer 101 and the wireless interface device 100 is by way of a wireless communication link**, provided by a communication subsystem 118 in which the remote host computer 101 is provided with a transceiver 115 for radio communication with a transceiver 116 in the wireless interface device 100. For example, the desktop or remote host computer 101 can be provided with a PCMCIA interface which can be used with a wireless transceiver card to communicate with the transceiver 116 in the wireless interface device 100.

Ex.1014, 4:13-25.

173. Thus, a POSITA would have understood that Mathiassen's network N, which includes a terminal 31 illustrated as a standard computer in Fig. 1a, would

include a wireless communications interface like the external systems that interact with the wireless communications interface of Ryan's smart fob. Thus, the combination of Mathiassen and Ryan teach the *wireless communications interface* of limitation [21.3.3].

174. In addition, Mathiassen teaches that its network N is *for receiving secure data message*s. 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].

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

[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.

176. Mathiassen's network N includes at least the computer terminal 31 and servers 30. *See* § VIII.A.4.b. Describing the network N, Mathiassen also explains that its portable device is integrated into the network N.

> It is a second object of the present invention to overcome the above limitations by providing an embedded access device for **integration into peripherals of networked computers or communication terminals**, to allow only authorized users access to all types of proprietary networks (LAN, WAN, etc.) typically represented by **internet banking applications**, corporate and government intranets, and similar.

Ex.1005, [0017].

Mathiassen's network includes "internet banking applications" which corresponds to *at least one external system including at least one part of a web application*. In addition, Mathiassen explains these proprietary networks may include "an internet bank or a corporate or government intranet." Ex.1005, [0047]. An internet banking application is a transaction processing application and resides within the network N.

177. In addition, a POSITA would have understood that Mathiassen's network N would include a transaction processing application based on the teachings of Ryan. In particular, Ryan describes several "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 also describes how these e-commerce applications reside on "remote servers and networks" accessed by the smart fob via a "personal computer…apparatus, or other appliance." Ex.1006, [0175]. The remote servers and network described by Ryan are substantially the same as Mathiassen's network N and the '637 Patent's external system. Ryan also 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]).

178. In addition, a POSITA at the time would have understood that Mathiassen's banking application, described as an "internet banking application," included *at least one part of a web application*, based on the disclosures of Ryan. Ex.1005, [0017]; *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"). Similarly, any of the e-commerce applications described in Ryan

would have also included *at least one part of a web application*. Ex.1006, [0223]-[0236].

179. The web applications described in Mathiassen and Ryan are *accessed by said at least one external system*. For example, Ryan explains that the PC into which the smart fob is inserted, which a POSITA would understand to be part of the external system, accesses the web application. Specifically, "[t]he device is capable of loading and storing information from the Internet, via the PC to its flash memory." Ex.1006, [0168]. Similarly, a POSITA would understand that when the portable device in Mathiassen is inserted into the terminal 31, for example to connect "to the Intranet server (30) of the network (N) from an Internet Café or a Business Center," the terminal 31 accesses a web application. Ex.1005, [0065]. For example, a user would access a banking website through the terminal 31, and then biometrically authenticate themselves via the portable device.

180. Ryan also describes how its smart fob "is capable of loading and storing information from the Internet, via the PC to its flash memory." Ex.1006, [0168]. The PC thus accesses the internet, which includes *at least one part of a web application.* The PC described in Ryan, like the terminal 31 of Ex.1005, is part of an external system. Ex.1006, [0168] (smart fob is "inserted into a personal computer (PC) connected to the Internet"), [0258] ("external Internet connected PC"). Mathiassen's terminal 31 and network N operate in a very similar way. For example, Mathiassen

provides an example scenario in which "a user traveling, wanting to connect to the Intranet server (30) of the network (N) from an Internet Café or a Business Center at a hotel[,] will insert the portable device (12 or 13) into the USB port" of the computer terminal 31. Thus, the computer terminal 31 accesses the website the user wishes to access, after which the portable device and the website of the external system may begin to communicate. includes the computer terminal 31 to which the portable device is connected.

181. Mathiassen explains how its network N, as well as any web applications residing within the network N, are *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.

182. The web applications described as part of Ryan's external system are also *adapted for transmitting and receiving requests and responses to and from said customer authentication apparatus*. For example, the web applications of Ryan's

external system transmit information to the smart fob. Ex.1006, Abstract ("The apparatus is capable of loading and storing information from the Internet."); *see also* [0168]. Similarly, the smart fob can upload information to the web application. Ex.1006, [0223] ("In use, for example, the user plugs the smart fob into his PC, or other Internet capable device (appliance), connects to the Internet, and interacts with a service or content provider to upload and/or download information.").

183. Thus, the Mathiassen-Ryan combination renders obvious *at least one transaction processing application* (internet banking application of network N) *residing within said at least one external system* (network N) *including at least one part of a web application* (website of internet bank of network N) *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* (portable device).

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.

184. As explained previously, Mathiassen describes authenticating users to provide access to restricted systems or networks. *See* § VIII.A.4.a.[1.3.2]-[1.3.3]. For example, Mathiassen describes acquiring a fingerprint of the user and comparing it with a master fingerprint. Ex.1005, [0049]-[0050]. If the acquired fingerprint

matches the master fingerprint, the user is authenticated and allowed to access the network N. Ex.1005, [0049]-[0050]. While this authentication is performed within the IC 1 of the portable device itself, Mathiassen describes an alternative embodiment in which this authentication procedure is performed either on the computer terminal 31 or another machine of the network 30.

> The User places, or swipes his finger (A) over the access/input device with a fingerprint sensor (B). **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) acquires the sensor signals and processes them to reconstruct a 2-dimensional fingerprint image, and thereafter extracts the particulars of the fingerprint, and finally either perform a matching locally at the PC (C).

Ex.1005, [0046].

Thus, Mathiassen anticipates that user authentication may be performed on various devices or systems other than the portable device.

185. Similarly, Ryan explains that authentication may be performed by devices or systems other than its smart fob, including a trusted third party as claimed.

> The client user can be authenticated by the ISP **or by a trusted third party** through a digital signature or a unique MAC (Media Access Control) address, or through the implementation of public key infrastructure in order to validate the client's identity.

Ex.1006, [0245].

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

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.

187. 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.

188. For example, as explained with reference to claim 2, Mathiassen illustrates the USB mechanical interface 12C in Fig. 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* claimed. 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).").

189. 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).

j) 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.

190. 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 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.

191. As explained at Sections VIII.A.2 and VIII.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 aboard the smart fob and external system form a "wireless communications link" because the two wireless transceivers are for wireless communication. Ex.1006, [0038] (The wireless interface "enabl[es] communication with a personal device" external to the smart fob.).

192. 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*.

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

1. Overview of Lim

193. Lim describes a portable device for biometrically authenticating a user.

> Apparatus and method for implementing biometrics-based access control to a restricted resource. In a preferred embodiment, the present invention is realized using a portable device. Specifically, in one embodiment, the portable device includes a microprocessor, a non-volatile memory coupled thereto, and a biometrics-based authentication module controlled by the microprocessor. Preferably, the biometrics technology used is fingerprint authentication technology.

Ex.1007, Abstract.

Lim's device is shown in Figs. 2-9. Fig. 2 is shown below.

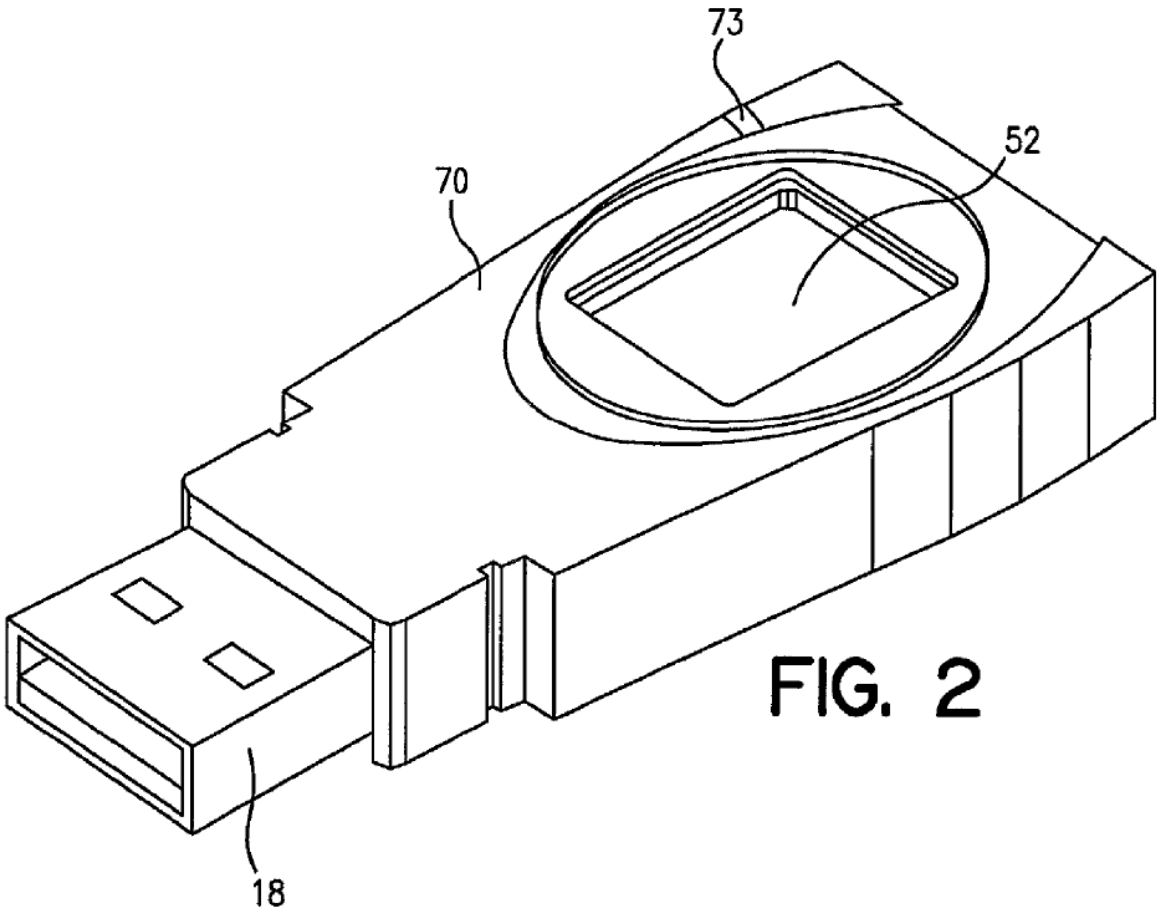


FIG. 2

Ex.1007, Fig. 2

Lim's device includes a fingerprint sensor 52 "disposed on the top side of portable device 70." Ex.1007, Fig. 2, [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]. As shown in Fig. 2, Lim's device includes a USB connector 18. Ex.1007, Fig. 2, [0035] ("Portable device 70 is shown with USB connector 18 protruding from its front end.").

194. Lim's authentication module is software described as an authentication engine 12.

> In a currently preferred embodiment, an authentication engine 12 is included in integrated circuit 10. Authentication engine 12 in turns 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 explains that this authentication software may be located in any location within the device, including the microprocessor 11. Ex.1007, [0025].

2. Motivation to Combine Mathiassen and Ryan with Lim

195. Lim's portable device is analogous to the ITA apparatus of 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]. In addition, Lim is reasonably pertinent to a particular problem with which the inventor is 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").

196. As described at Section VIII.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 basic circuit architecture, including the location for software storage, as taught by Lim. Lim's software, "authentication engine 12," is similar to the transaction security software of the '637 Patent and administrative software of Mathiassen in that includes at least two subsets for biometric authentication and encryption respectively *See* Ex.1007, Abstract; § VIII.A.4.a [1.3.1]. Lim explains that its software 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 where it was feasible would also enhance security and speed of the device.

197. 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). 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"). Storing software within the processor as explained by Lim would greatly increase speed of operation because the software would not need to be transferred to the processor from the memory.

198. 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. In addition, as previously mentioned, Lim's software is strikingly similar to that of the '637 Patent and Mathiassen. A POSITA

would have recognized that similar software could be stored in a similar processor as described by Lim.

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" (Mathiassen , [0054]), as well as "extra capacity beyond the 256 Kbytes minimum" (Mathiassen , [0058]). Lim similarly describes a device with a "RISC processor" (Ex.1007, [0024]) and "a storage capacity between 8 MB and 512 MB" (Lim , [0023]).

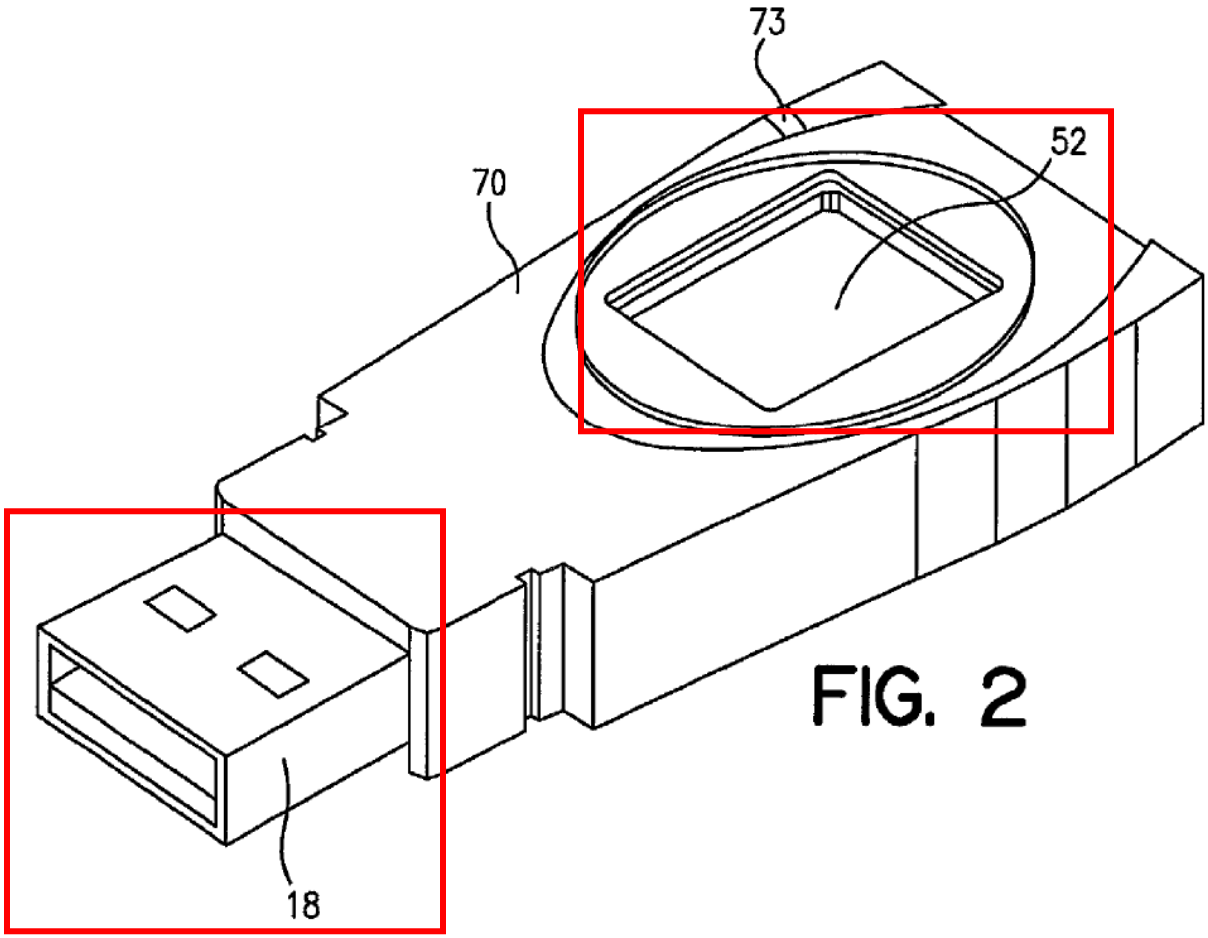
3. Analysis

a) Claim 1

200. The Mathiassen-Ryan combination renders obvious limitations [1.0]-[1.2] and [1.3.2]-[1.5] for the reasons described above in Ground 1. Claim 1 is included in Ground 2 to show that limitation [1.3.1] also would have been obvious over the Mathiassen-Ryan combination in view of Lim ("the Mathiassen-Ryan-Lim combination").

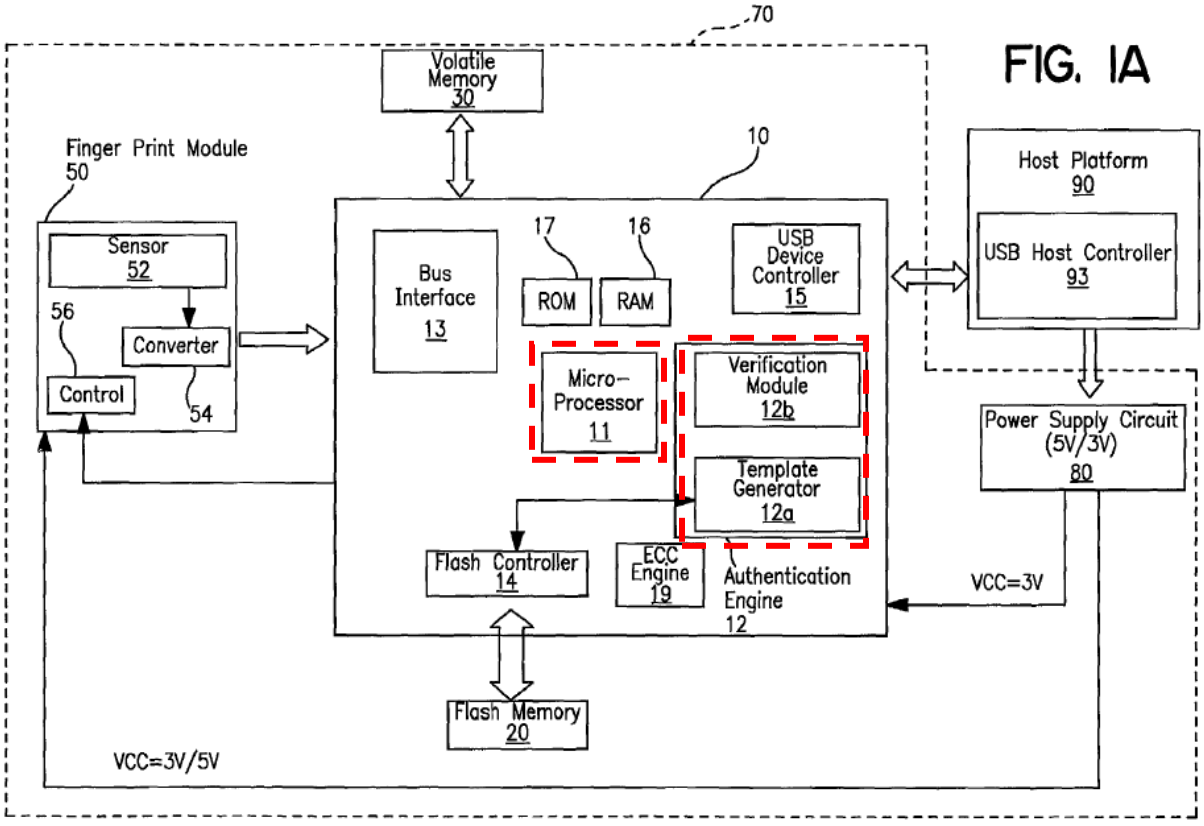
[1.3.1] transaction security software resident within and executing on said at least one processor further comprising

201. Lim describes a "portable device 70" that includes a "USB connector 18" and a "[f]ingerprint module 50…with sensor 52 on the top side of the portable device 70" for biometrically authenticating users. Ex.1007, [0035]. Lim's portable device is illustrated in Fig. 2 (reproduced below).



Ex.1007, Fig. 2 (annotated)

202. The portable device includes an "[i]ntegrated circuit 10 [that] comprises a microprocessor 11" and an "authentication engine 12." Ex.1007, [0024], Fig. 1A (reproduced below). Lim's authentication engine 12 is software similar to Mathiassen's administrative software which corresponds to the claimed *transaction security software*. *See* §§ VIII.A.4.a [1.3.1]-[1.3.3]; Ex.1007, [0024] ("Authentication engine 12 in turns comprises a template generator 12a and a verification module 12b.").



Ex.1007, Fig. 1A (annotated)

203. Lim's authentication engine 12 is *resident within and executing on said at least one processor* as claimed. As previously explained in Section VII.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. Therefore, a POSITA would have understood that the terms *resident within* mean temporary storage of the software while the software is being executed. However, even if the terms *resident within…at least one processor* are interpreted to require software to be permanently stored within the processor, contrary to the prevailing principles of circuit architecture at the time, 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).

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

b) Claim 21

205. The Mathiassen-Ryan combination renders obvious limitations [21.0]-[21.2.2] and [21.2.4]-[21.4] for the reasons in Ground 1. Claim 21 is included in Ground 2 to show that Limitation [21.2.3] also would have been obvious over the Mathiassen-Ryan combination in view of Lim ("the Mathiassen-Ryan-Lim combination").

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

206. 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 limitations [1.3.1]. *See* Section VIII.B.3.a.

IX. AVAILABILITY FOR CROSS-EXAMINATION

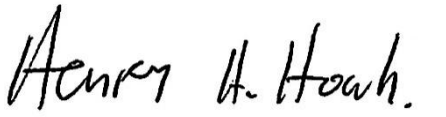
207. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross examination in the case and that cross examination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

X. CONCLUSION

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

Date: May 16, 2024

Respectfully submitted,



Henry Houh