IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Terence W. O'Brien	
U.S. Patent No.:	7,765,399	Attorney Docket No.: 50095-0112IP1
Issue Date:	July 27, 2010	
Appl. Serial No.:	11/359,224	
Filing Date:	February 22, 2006	
Title:	COMPUTER ARCHITECTURE FOR A HANDHELD ELECTRONIC DEVICE	

DECLARATION OF DR. SANDEEP CHATTERJEE

TABLE OF CONTENTS

I. BACKGROUND AND QUALIFICATIONS 1

II. OVERVIEW OF CONCLUSIONS FORMED 8

III. LEVEL OF ORDINARY SKILL IN THE ART 9

IV. THE '399 PATENT 9

V. PRIOR ART ANALYSIS 11

- **A.** [GROUND 1A] – CLAIMS 1-7, 9-10, 12-13, AND 15-18 WOULD HAVE BEEN OBVIOUS OVER MAREK AND SKARINE 11
  1. Marek describes a mobile device with a secure processor, a non-secure processor, a cryptographic engine 11
  2. Skarine provides an example of a conventional mobile device 16
  3. The combination of Marek and Skarine 19
  4. Element-by-Element Explanation of How the Marek-Skarine Combination Renders the Challenged Claims Obvious 36
- **B.** [GROUND 1B] – CLAIMS 4-5 WOULD HAVE BEEN OBVIOUS OVER MAREK, SKARINE, AND YOON 171
  1. Yoon describes a mobile device providing voice command functionality 171
  2. The combination of Marek, Skarine, and Yoon 172
  3. Reasons for the combination 173
  4. Element-by-Element Explanation of How the Marek-Skarine-Yoon Combination Renders the Challenged Claims Obvious 175
- **C.** [GROUND 1C] – CLAIMS 9-10 WOULD HAVE BEEN OBVIOUS OVER MAREK, SKARINE, AND MOON 176
  1. Moon describes a tamper-resistant mobile device 176
  2. The combination of Marek, Skarine, and Moon 178
  3. Reasons for the combination 180
  4. Element-by-Element Explanation of How the Marek-Skarine-Moon Combination Renders the Challenged Claims Obvious 183

VI. LEGAL PRINCIPLES 185

- **A.** Anticipation 185
- **B.** Obviousness 186

VII. ADDITIONAL REMARKS 188

I. BACKGROUND AND QUALIFICATIONS

1. My education and experience are described more fully in the attached curriculum vitae. For ease of reference, I have highlighted certain information below.

2. I am the Chief Executive Officer of Experantis LLC ("Experantis"), a technology consulting company. Previously, I was the Co-founder, Executive Vice President and Chief Technology Officer of SourceTrace Systems, Inc., a technology and services company enabling the delivery of secure remote electronic services over landline and wireless telecommunications networks.

3. I received my Bachelor's degree in Electrical Engineering and Computer Science from the University of California, Berkeley in 1995. I received my Master's degree in Computer Science from the Massachusetts Institute of Technology (MIT) in 1997, and my Doctorate in Computer Science from MIT in 2001. I received a certificate of completion for an executive education program on global leadership from Harvard University in 2011.

4. I have extensive experience in designing, developing, and deploying end-to-end distributed systems, including communications systems. For example, as part of my doctoral research, I developed hardware and software systems for intelligent environments within homes and offices. Some of these devices included televisions, digital picture frames, refrigerators and children's toys. The hardware

architecture of this system included a high-speed backplane that could support multiple, small-sized and pluggable modules, such as Personal Computer Memory Card International Association (PCMCIA) or CardBus PC cards. These pluggable modules could contain computing processor resources or peripheral resources, such as memory, storage, user interface components, etc. My doctoral dissertation at MIT involving networked client architectures and systems, was selected as one of the top inventions in the history of MIT's Laboratory for Computer Science. This invention is showcased in a time capsule at the Museum of Science in Boston, Massachusetts. Other recipients of this honor included Bill Gates, the founder of Microsoft, and Tim Berners-Lee, inventor of the World Wide Web.

5. Thereafter, I joined Bluestone Software's Mobile Middleware Labs as a Senior Engineer developing applications and systems infrastructure for enterprise Java/J2EE, Web services, and enterprise mobile solutions. After the completion of Hewlett-Packard's ("HP") acquisition of Bluestone, I became a Senior Member of the Technical Staff at HP's Middleware Division. I was responsible for architecting and developing the company's next-generation Web services platform for enterprise as well as mobile environments, known as the Web Services Mediator. I also worked with HP's worldwide software operations to add extensions into the Java 2 Enterprise Edition (J2EE) application server to easily support mobile appli-

cations and content, as well as flexible integration with other software systems using the eXtensible Markup Language (XML) and web services technologies. I was also part of the Expert Group that developed the JSR-00172 J2ME (Java 2 Platform, Micro Edition) Web Services Specification, the worldwide industry standard for mobile web services.

6. After leaving HP and through a contract between HP and the United States Agency for International Development (USAID), I led the development of a software system that enabled customers to use mobile handsets to connect with the core banking systems of banks and other financial institutions, and perform transactions without having to travel to bank branches. This was one of the first mobile banking solutions in the world.

7. Later, after SourceTrace Systems' acquisition of this technology, I led the expansion of this solution into multiple countries and into multiple industries. Banks and other financial services companies utilized this technology to make their tellers more efficient, to provide self-service kiosks within branches, and to provide remote access to banking services. Additionally, through our licensing agreement with Telefonica, one of the largest cellular and telecommunications companies in the world, this solution was deployed in various other industries, including logistics and asset management and customer relationship management. Some of these vertical solutions supported location tracking based on GPS information,

while other vertical solutions utilized location information to provide additional levels of security and authentication for transactions. Bloomberg Television selected and featured this technology and the company I co-founded to commercialize this technology on Bloomberg TV's "Bloomberg Innovators" program.

8. Based on my professional work, in 2011, I was named Young Global Leader by the World Economic Forum. This honor, bestowed each year by the World Economic Forum, recognizes and acknowledges the top leaders – all below the age of 40 – from around the world for their professional accomplishments, commitment to society, and potential to contribute to shaping the future of the world.

9. I have been a retained expert witness for various disputes that involved significant technology issues, and I have been qualified as a technology expert by U.S. District and State Courts, including in California, Delaware, Florida and Texas, at the United States International Trade Commission (ITC) and at various U.S. and international arbitrations. I have testified in technology areas that are relevant to this case, including but not limited to: computer software and hardware systems. I have previously testified through declaration or expert report, at deposition and at trial in numerous intellectual property and commercial litigation matters, including for patent litigation, copyright and trade secret misappropriation litigation, and contract dispute cases. I have submitted more than one hundred and

forty expert declarations and expert reports, testified at deposition more than seventy times, and testified at trial or at hearings at least nine times. I have been identified as one of the top 1000 patent professionals in the world, and am listed in the IAM Patent 1000, which identifies the world's leading patent litigation and prosecution attorneys, as well as damages and technology expert witnesses. I have attached a more detailed list of my qualifications as Exhibit A to this declaration. Based on my academic and professional experiences, I believe that I am qualified in the technology fields and technology issues relevant to this matter.

10. Experantis is being compensated for my time working on this matter at my standard hourly rate plus expenses. Neither Experantis nor I have any personal or financial stake or interest in the outcome of the present proceeding, and the compensation is not dependent on the outcome of this litigation and in no way affects the substance of my statements in this declaration.

11. I have been retained on behalf of Apple Inc. to offer technical opinions relating to U.S. Patent No. 7,765,399 ("the '399 Patent") and prior art references relating to its subject matter. I have reviewed the '399 Patent, and relevant excerpts of the prosecution history of the '399 Patent. I have also reviewed the following references:

- APPLE-1004: U.S. Patent No. 7,716,720 ("Marek")
- APPLE-1005: U.S. Patent Pub. No. 2005/0190159 ("Skarine")

- APPLE-1007: U.S. Patent Pub. No. 2004/0082368 ("Yoon")
- APPLE-1008: U.S. Patent No. 7,571,475 ("Moon")

12. I have also reviewed various supporting references and other documentation, including the following list, and as further noted in my opinions below.

- APPLE-1009: U.S. Patent No. 6,671,745 ("Mathur")
- APPLE-1010: U.S. Patent No. 7,325,032 ("Zuberec")
- APPLE-1011: U.S. Patent No. 6,675,027 ("Huang")
- APPLE-1012: U.S. Patent Pub. No. 2007/0006146 ("Kwong")
- APPLE-1014: European Patent Publication No. EP 1283630 ("ITT")
- APPLE-1015: U.S. Patent No. 7,496,060 ("Ramirez")
- APPLE-1016: European Patent Publication No. EP1934879 ("SanDisk")
- APPLE-1017: U.S. Patent No. 8,442,231 ("Macchi")
- APPLE-1018: U.S. Patent No. 7,853,656 ("Yach")
- APPLE-1019: U.S. Patent No. 7,716,638 ("Thornton")
- APPLE-1020: U.S. Patent No. 8,045,958 ("Kahandaliyanage")
- APPLE-1021: U.S. Patent No. 7,607,131 ("Oe")
- APPLE-1022: U.S. Patent No. 7,596,695 ("Liao")
- APPLE-1023: U.S. Patent Pub. No. 2015/0372806 ("Carter")

- APPLE-1024: U.S. Patent Pub. No. 20070131097 ("Lu")
- APPLE-1025: U.S. Patent No. 7,394,480 ("Song")
- APPLE-1026: U.S. Patent Pub. No. 2002/0181468 ("Lucidarme")
- APPLE-1027: U.S. Patent Pub. No. 2006/0258372 ("Naegeli")
- APPLE-1040: U.S. Patent No. 6,240,303 ("Katzur")
- APPLE-1041: U.S. Patent Pub. No. 2002/0178003 ("Gehrke")
- APPLE-1042: PCT Pub. No. WO2000/028721 ("Ericsson")
- APPLE-1043: U.S. Patent Pub. No. 2005/0288063 ("Seo")
- APPLE-1044 Kylene Hall, et al. "Trusted Computing and Linux." *Proceedings of the Linux Symposium, Volume 2* (2005) ("Hall")
- APPLE-1045 "Infineon Announces Trusted Platform Module to Enhance PC Security," phys.org (2005), https://phys.org/news/2005-05-infineon-platform-module-pc.html ("Infineon")

13. Counsel has informed me that I should consider these materials through the lens of one of ordinary skill in the art related to the '399 Patent at the time of the earliest possible priority date of the '399 Patent, and I have done so during my review of these materials. The '399 Patent was filed February 22, 2006 ("the Critical Date"). Counsel has informed me that the Critical Date represents the earliest possible priority date to which the challenged claims of the '399 Patent are entitled, and I have therefore used that Critical Date in my analysis below.

14. In writing this declaration, I have considered the following: my own knowledge and experience, including my work experience as detailed above and in Appendix A, and my experience in working with others involved in those fields. In addition, I have analyzed various publications and materials, in addition to other materials I cite in my declaration.

15. My opinions, as explained below, are based on my education, experience, and expertise in the fields relating to the '399 Patent. Unless otherwise stated, my testimony below refers to the knowledge of one of ordinary skill in the art as of the Critical Date, or before. Any figures that appear within this document have been prepared with the assistance of Counsel and reflect my understanding of the '399 Patent and the prior art discussed below.

II. OVERVIEW OF CONCLUSIONS FORMED

16. This declaration explains the conclusions that I have formed based on my analysis. To summarize those conclusions, based upon my knowledge and experience and my review of the prior art publications listed above, I believe that:

- Claims 1-7, 9-10, 12, 13, and 15-18 are obvious over Marek and Skarine;
- Claims 4-5 are obvious over Marek, Skarine, and Yoon; and
- Claims 9-10 are obvious over Marek, Skarine, and Moon.

III. LEVEL OF ORDINARY SKILL IN THE ART

17. In my opinion, one of ordinary skill in the art relating to, and at the time of, the alleged invention of the ’399 Patent would have been someone a person with a Bachelor’s degree in electrical engineering, computer science, computer engineering, or a related field, and at least two years of work experience with computer architecture and system security, including cryptography. Greater education or greater experience could compensate for a deficiency in either of these criteria.

18. Based on my experiences, I have a good understanding of the capabilities of one of ordinary skill. Indeed, I have worked closely with many such persons over the course of my career. Based on my knowledge, skill, and experience, I have an understanding of the capabilities of one of ordinary skill. For example, from my professional and industry experiences, I am familiar with what an engineer would have known and found predictable in the art. Furthermore, I possess those capabilities myself.

IV. THE ’399 PATENT

19. The’399 Patent describes “a mobile PDA computer system” including “a non-secure user processor, a secure user processor, and a cryptographic engine.” APPLE-1001 (’399 Patent), 2:23-26. Each of these processors has corresponding microprocessor hardware, an operating system, and software. *See id.*, 2:25-30. The cryptographic engine “forms a bridge between the secure processing side of

the PDA and the non-secure processing side of the PDA." *Id.*, 2:32-40. Two human/machine interfaces are provided: a "secure human/machine interface" through which "[c]lassified information can be provided to the user from the secure processor," and a "non-secure human/machine interface" through which "unclassified information can be provided to the user by the non-secure processor." *Id.*, 3:4-15. However, as I will demonstrate through the analysis that follows, this architecture was not new. Specifically, a mobile device system having secure and non-secure user processors and a cryptographic engine, along with secure and non-secure human/machine interfaces, was not new in the art at the time of filing of the application leading to the '399 Patent.

20. In addition to the specific combinations of references I discuss below, I note that the trusted computing techniques and technologies described in the '399 Patent were not new. Indeed, the '399 Patent itself acknowledges as much, stating that "the basic architecture and interface systems of many commercial PDA devices may leave these devices vulnerable to intrusion. For example, COTS devices do not employ trusted microprocessors, do not employ physical separation of classified and unclassified data processing, nor do they employ physical tamper detection and subsequent memory zeroization." #399, 1:56-64 (emphasis added). These concepts, including trusted microprocessors, physical separation of classified and unclassified data processing, and physical tamper detection were well

known. For instance, Hall et al. described a platform for trusted computing which is "realized in hardware that has a small amount of both volatile and non-volatile storage and cryptographic execution engines." #Hall, 2. Infineon introduced a "Trusted Platform Module" that "features a secure chip hardware, a complete suite of embedded security and TPM system management utilities as well as application software." #Infineon, 1. Thus, while I discuss specific combinations of references in the following paragraphs, I do so noting that trusted computing was not new as of the time of filing of the '399 Patent.

V. PRIOR ART ANALYSIS

A. [GROUND 1A] – CLAIMS 1-7, 9-10, 12-13, AND 15-18 WOULD HAVE BEEN OBVIOUS OVER MAREK AND SKARINE

1. Marek describes a mobile device with a secure processor, a non-secure processor, a cryptographic engine

21. Marek relates to mobile devices, and specifically describes "a system for providing a secure and trusted commercial-off-the shelf COTS computing environment" for use with an "untrusted computing system," such as a mobile device, *e.g.*, a PDA (personal digital assistant). APPLE-1004 (Marek), Abstract, 1:7-9. Specifically, Marek describes that a "Secure COTS environment may be provided by a system including a SCM [secure computing module] as an add-on module to an untrusted host environment" such as a PDA. APPLE-1004 (Marek), 8:37-39;

see 11:53-55 ("the SCM is suitable for providing secure wireless network connections when the SCM is added on wireless devices such as PDAs, cell phones, and other mobile devices").

22. Marek's Fig. 10,which I have reproduced below, shows such an example of such a system, and specifically illustrates "a SCM 908 interfacing with an untrusted PDA 1014." *Id.*, 12:14-15. I have highlighted the secure computing module (SCM) in purple and the PDA in green. The interfacing of the SCM with the untrusted PDA allows "[o]nly authenticated COTS applications and COTS OS [to] execute on the SCM"—*i.e.*, authenticated applications and operating systems execute on the secure computing module—while "untrusted applications execute on the untrusted host environment"—*i.e.*, untrusted applications execute on the PDA. *Id.*, 8:39-41; *see* 2:21-28.

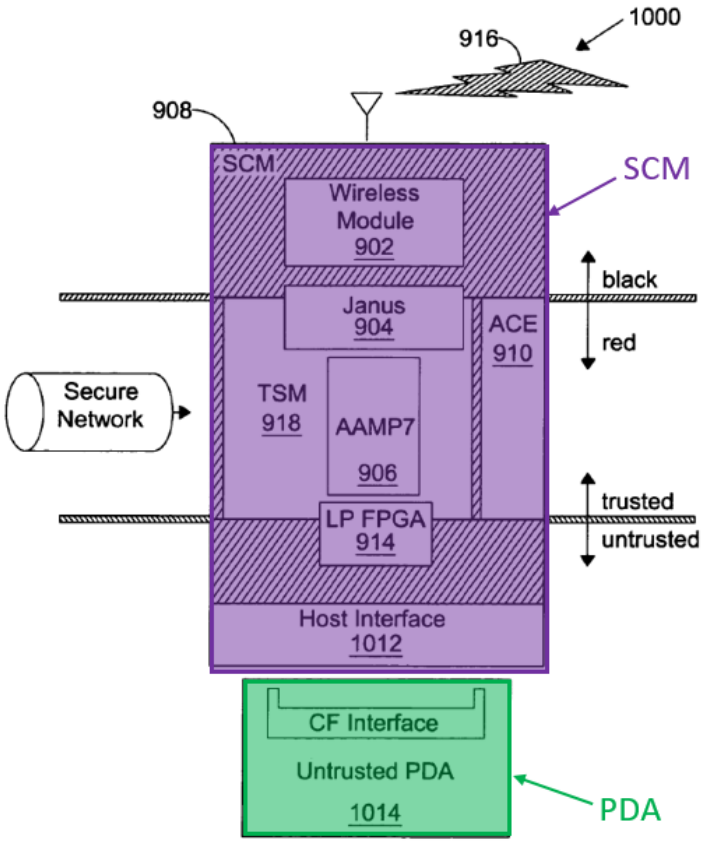


FIG. 10

Excerpt from Marek, Fig. 10 (annotated)

23. The detailed architecture of Marek's SCM is shown in Fig. 7, which I have reproduced below. Fig. 7 illustrates a computing environment "implementing SCM architecture." APPLE-1004 (Marek), 8:51-54. This environment includes a SCM 702 (which I have highlighted in orange) provided as "an add-on module to an untrusted host environment" 718, *e.g.*, a PDA (again highlighted in green). *Id.*, 8:38-39. The SCM includes an "Authenticated COTS Environment Subsystem (ACE)" (highlighted in red) that "includes an embedded COTS OS running on a

compatible embedded COTS processor." APPLE-1004 (Marek), 9:1-5. The SCM also includes a "Trusted Security Manager subsystem (TSM) 704" (highlighted in blue) that includes "a trusted processor 705 for providing a brick-wall partitioning of memory, time, and device resources, and enforcing predetermined security policies," as well as "a cryptographic engine 706 … [that] may aid the trusted processor 705 to provide a robust security interface." *Id.*, 8:67, 9:31-41; *see* 2:21-38 (the TSM "provid[es] partitioning for both memory and I/O resources on the trusted environment"). In this system, "[e]ach I/O path of the SCM 702," such as "I/O paths between the untrusted host and the SCM" (purple), "is configured to go through the TSM 704" such that each "I/O path [is] secured and authenticated." *Id.*, 9:50-54; *see* 2:25-30 ("All I/O paths of the SCM are configured to go through the TSM," with each I/O path being "subject to authentication protocols" provided by the TSM). For instance, the "I/O paths 730 between the untrusted host and the SCM 702," which go through the TSM, "are managed by a low power Field-Programmable Gate Array (FPGA) and a dedicated TSM partition," which "allow[s] for any number of strict authentication protocols." *Id.*, 10:36-39.

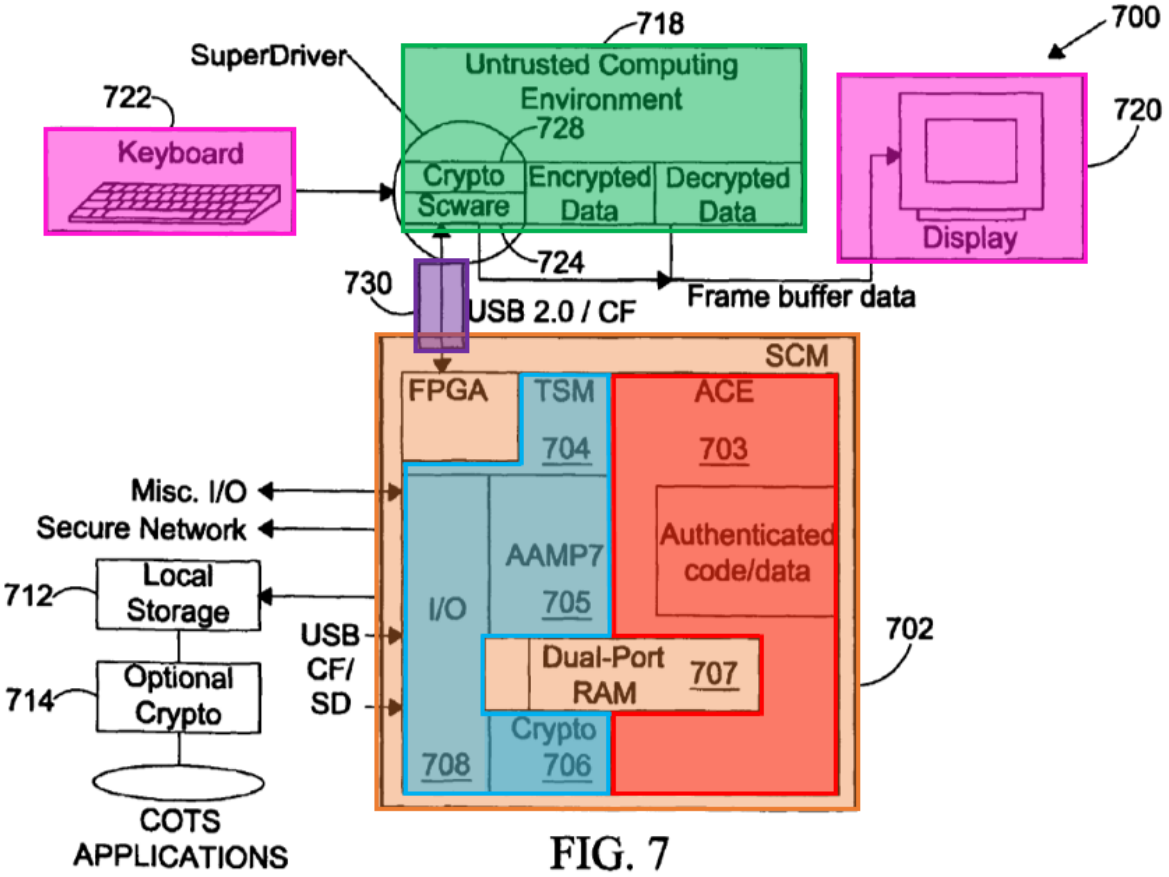


FIG. 7

Excerpt from Marek, Fig. 7 (annotated)

24. The untrusted host environment (*e.g.*, the PDA, green) includes "input and output devices 722, 720," such as a keypad and a display, which I have highlighted pink in Fig. 7. APPLE-1004 (Marek), 10:51-52; *see* 10:60-65. These input and output devices communicate with the SCM via Scware 724, which is "software that acts as a trusted agent for the SCM 702 on the untrusted host environment." *Id.*, 10:43-45. Specifically, as illustrated in Fig. 7, the Scware "resides on the untrusted host environment while the SCM 702 is operating" and "creates secure I/O

paths 730 of input and output devices 722, 720," thereby enabling input to and output from the SCM. *Id.*, 10:47-54. For instance, the Scware enables "the input and output devices 722, 720 of the untrusted host 718 [to] be utilized as a virtual input/output system 800 of the SCM." *Id.*, 10:49-54; *see* Fig. 8.

2. Skarine provides an example of a conventional mobile device

25. Skarine describes "a mobile device 202," such as "a data messaging device, a two-way pager, a cellular telephone with data messaging capabilities, a wireless Internet appliance, or a data communication device" "having at least voice and advanced data communication capabilities." APPLE-1005 (Skarine), [0034]. As shown in Skarine's Fig. 2, reproduced below, Skarine's mobile device includes a "communication subsystem 211," which I have highlighted in pink. *Id.*, [0038]. The communication subsystem 211 is connected to a microprocessor 238 (highlighted in green) of the mobile device. *Id.*, [0038]. "Communication functions, including at least data and voice communications, are performed" through the communication subsystem 211. *Id.*, [0038].

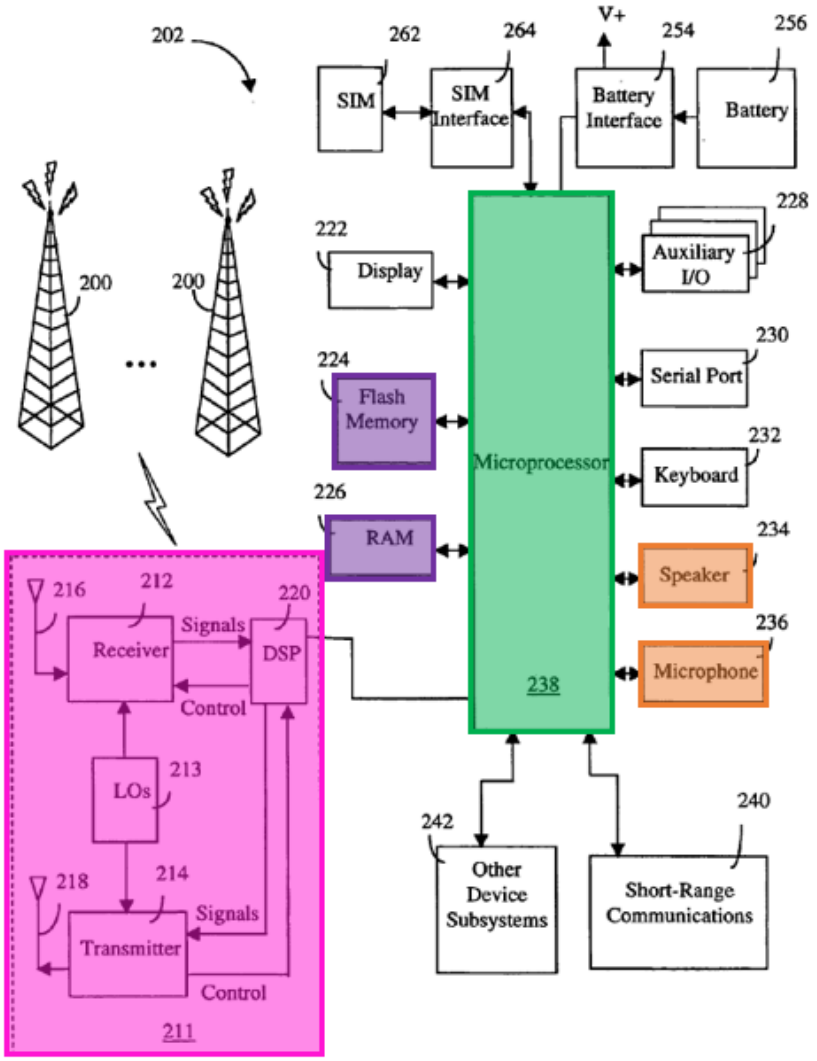


FIG. 2

Excerpt from Skarine, Fig. 2 (annotated)

26. The communication subsystem 211 "includes a receiver 212, a transmitter 214, and associated components," and is "analogous to RF transceiver circuitry 108 and antenna 110 shown in FIG. 1." APPLE-1005 (Skarine), [0035]. The RF transceiver circuitry and antenna of FIG. 1 are described as follows: "Mo-

bile device 102 sends communication signals to and receives communication signals from network 104 over a wireless link via antenna 110. RF transceiver circuitry 108 performs functions such as modulation/demodulation and possibly encoding/decoding and encryption/decryption." *Id.*, [0023]. The RF transceiver circuitry is, for instance, a cellular telephone transceiver for communication with "wireless network 104 [that] is configured in accordance with General Packet Radio Service (GPRS) and a Global Systems for Mobile (GSM) technologies." *Id.*, [0027]-[0028]; *see also* the description of the RF transceiver circuitry of FIG. 2 in paragraph [0023] ("RF transceiver circuitry 108 will be adapted to particular wireless network or networks in which mobile device 102 is intended to operate").

27. Skarine's mobile device also includes "additional device subsystems such as … a speaker 234, [and] a microphone 236," which I have highlighted orange in Fig. 2. APPLE-1005 (Skarine), [0038]. As illustrated in Fig. 2, the speaker and microphone are also connected to the microprocessor of the mobile device. *See id.*, [0038]. Skarine describes that "[f]or voice communications, … the received signals would be output to speaker 234 and signals for transmission would be generated by microphone 236." *Id.*, [0042]. Skarine's mobile device can also implement "[a]lternative voice or audio I/O subsystems, such as a voice message recording subsystem." *Id.*, [0042].

28. Skarine's mobile device also includes "a flash memory 224, [and] a random access memory (RAM) 226," in purple. *Id.*, [0038]. Skarine describes that "[o]perating system software used by microprocessor 238 is preferably stored in a persistent store such as flash memory 224, which may alternatively be a read-only memory (ROM) or similar storage element," while "the operating system, specific device applications, or parts thereof, may be temporarily loaded into a volatile store such as RAM 226." *Id.*, [0038].

3. The combination of Marek and Skarine

29. It is my opinion that a POSITA would have found it obvious to combine teachings of Marek with teachings of Skarine to produce a Marek-Skarine combination system that I describe in the following paragraphs. An example of this combination system is illustrated in the composite figure below. Generally, in the Marek-Skarine combination, a SCM, such as that described by Marek, is provided as an add-on module to a conventional mobile device, such as a PDA or cell phone (which I have highlighted in green in the composite figure below), as taught by Marek. *See* APPLE-1004 (Marek), 8:37-39, 11:44-12:21, 13:49-51.

30. For instance, in the Marek-Skarine combination, the SCM (secure computing module) includes an ACE 703 (Authenticated COTS Environment Subsystem, which I have highlighted in red) and a TSM 704 (Trusted Security Manager subsystem, highlighted in blue), consistent with the architecture of the system

described by Marek. APPLE-1004 (Marek), 8:51-67. Also consistent with the architecture of Marek's computing environment, "[o]nly authenticated applications including COTS [commercial-off-the-shelf] OS execute on the SCM while untrusted applications execute on the untrusted host environment," *e.g.*, on the untrusted host mobile device, while the TSM "provid[es] partitioning for both memory and I/O resources on the trusted environment." APPLE-1004 (Marek), 2:21-38. Additionally, and also based on the architecture of Marek's computing environment, "[a]ll I/O paths of the SCM are configured to go through the TSM," with each I/O path being "subject to authentication protocols" provided by the TSM. APPLE-1004 (Marek), 2:25-30.

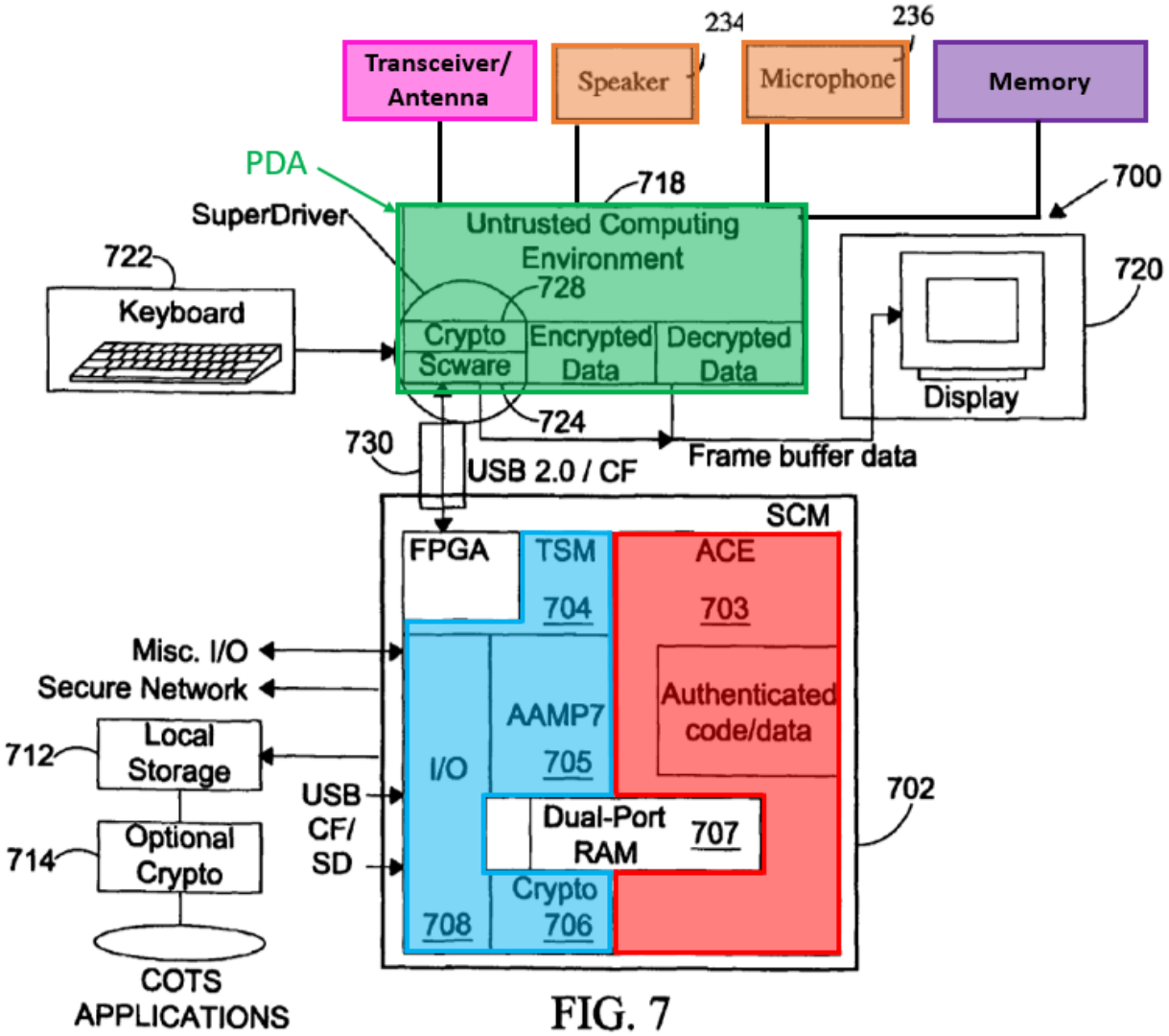


FIG. 7

Marek-Skarine composite figure[1]

[1] This figure, as well as other composite figures herein, is just one example combination that a POSITA would have found to be obvious, and is provided for illustrative purposes only. Other, similar example combinations could be conceived that also would have been obvious that that would render the challenged claims obvious for similar reasons as those discussed herein.

31. Marek states that the untrusted host mobile device can be, *e.g.*, a PDA or cell phone. *See* APPLE-1004 (Marek), 8:37-39, 11:53-55, Fig. 10. A PDA or cell phone was a conventional device as of the Critical Date, and it is my opinion that a POSITA would have understood or found obvious for such a conventional mobile device to include various conventional components. For instance, to the extent that Marek does not provide explicit description of the specific components of this untrusted host mobile device (*e.g.*, a cell phone or PDA), it is my opinion that a POSITA would have understood or found it obvious that the untrusted host mobile device—a conventional mobile device—includes common and well-known components of wireless devices. Many such conventional components are described, for example, in Skarine. I discuss in the following paragraphs one example of an obvious way to configure some of these well-known components in the untrusted host mobile device of the Marek-Skarine combination, *e.g.*, based on these teachings of Skarine.

Audio functionality in the untrusted host mobile device of the combination

32. In one example of the configuration of conventional components in the conventional untrusted host mobile device of the Marek-Skarine combination, it is my opinion that a POSITA would have understood or found obvious for the

untrusted host mobile device in the Marek-Skarine combination to include a conventional audio input and output components, such as a speaker and a microphone (highlighted in orange in the composite figure above).

33. The speaker and microphone are for audio input and output to/from the microprocessor of the mobile device (*e.g.*, for voice communications). This was well-known in the art in the context of conventional mobile devices, for instance, as demonstrated by Skarine. *See* APPLE-1005 (Skarine), [0038] ("Mobile device 202 includes a microprocessor 238 … [that] interacts with additional device subsystems such as … a speaker 234 [and], a microphone 236"), [0042] ("For voice communications, the overall operation of mobile device 202 is substantially similar, except that the received signals would be output to speaker 234 and signals for transmission would be generated by microphone 236"), Fig. 2.

34. I also refer to the following other references to corroborate that speakers and microphones were standard components in conventional mobile devices as of the Critical Date: APPLE-1018 (Yach), 3:45-50 (describing a microprocessor of a mobile device that "interacts with additional subsystems such as … a speaker 118 [and] a microphone 120"), 6:22-32; APPLE-1010 (Zuberec), 3:54-67 ("The mobile device 100 is also shown with two types of external notification mechanisms: an LED 140 and an audio interface 174. … The audio interface 174 is used to provide

audible signals to and receive audible signals from the user. For example, the audio interface 174 may be coupled to a speaker for providing audible output and to a microphone for receiving audible input, such as to facilitate a telephone conversation"); APPLE-1024 (Lu), [0004] ("a music player can be embedded in a device such as a mobile phone or a personal digital assistant (PDA). … new music selections can be … played immediately over speakers or headphones attached to the phone"); APPLE-1025 (Song), 1:18-20 ("a mobile terminal having a camera that records video and directs a microphone for recording a corresponding audio from its source is disclosed").

35. In the Marek-Skarine combination, the speaker and microphone are configured such that information is communicated from the processor of the untrusted host mobile device to the speaker, and from the microphone to the processor. I have illustrated this configuration in the composite figure above. To the extent Marek does not explicitly disclose this configuration, it is my opinion that a POSITA would have found it obvious in view of the teachings of Skarine, which describes a speaker and microphone of a mobile device coupled to a processor of that mobile device. *See* APPLE-1005 (Skarine), [0041]-[0042] ("For voice communications, the overall operation of mobile device 202 is substantially similar" to the operation in "data communication mode," where signals are communicated between a user and Skarine's mobile device processor via input and output devices),

[0038] ("Microprocessor 238 also interacts with additional device subsystems such as … a speaker 234, a microphone 236"), Fig. 2.

36. It is my opinion that a POSITA would have been motivated to have the speaker and microphone in communication with the processor of the untrusted host mobile device in the Marek-Skarine combination system for at least the following reasons.

37. One reason why a POSITA would have been motivated to have the speaker and microphone in communication with the processor of the untrusted host mobile device of the Marek-Skarine combination in this way is because doing so allows the mobile device to be used to carry out "voice communications," such as phone calls or voice mail functions, which was conventional functionality available in PDA or cell phone mobile devices as of the Critical Date, *e.g.*, as demonstrated at least by Skarine. APPLE-1005 (Skarine), [0042]; *see id.* ("a voice message recording system," "a voice call"). For instance, I believe that a POSITA would have recognized that with this configuration, the untrusted host mobile device of the Marek-Skarine combination would be able to be used for conventional mobile device functions, *e.g.*, audio communications such as phone calls.

38. A second reason why a POSITA would have been motivated to implement this configuration is because having the speaker and microphone in commu-

nication with the processor of the untrusted host mobile device of the Marek-Skarine combination allows the mobile device to be used for entertainment (*e.g.*, for playing music through the speaker) and/or for professional purposes (*e.g.*, recording interviews or meetings using the microphone), which are other examples of conventional audio functionality in standard cell phones and PDAs. *See* APPLE-1024 (Lu), [0004] ("a music player can be embedded in a device such as a mobile phone or a personal digital assistant (PDA)"); APPLE-1025 (Song), 1:18-20 ("a mobile terminal having … a microphone for recording a corresponding audio from its source"). For instance, I believe that a POSITA would have recognized that having the speaker and microphone in communication with the processor of the mobile device of the combination would enable this broad range of conventional mobile device capabilities to be readily accessible to the user.

39. It is also my opinion that a POSITA would have been motived to have the speaker and microphone in communication with the processor of the untrusted host mobile device of the Marek-Skarine combination configured in this way because this is just the application of known techniques (*e.g.*, a speaker and microphone communicatively connected to a processor in a mobile device) by a known system (*e.g.*, Marek's untrusted host mobile device) that results in a predictable outcome (*e.g.*, a mobile device with conventional audio capabilities).

40. Furthermore, it is my opinion that a POSITA would have expected success in configuring the speaker and microphone to be in communication with the processor of the untrusted host mobile device of the Marek-Skarine combination because Marek indicates that its teachings are applicable to conventional "wireless devices such as PDAs, cell phones, and other mobile devices" (APPLE-1004 (Marek), 11:55-56).

41. I also believe that a POSITA would have expected success in implementing this configuration because having a speaker and microphone of a mobile device in communication with a microprocessor of the mobile device was a standard configuration as of the Critical Date. *See* APPLE-1005 (Skarine), [0041]-[0042], Fig. 2; APPLE-1018 (Yach), 3:45-50 (describing a microprocessor of a mobile device that "interacts with additional subsystems such as … a speaker 118 [and] a microphone 120"), 6:22-32; APPLE-1010 (Zuberec), 3:54-67 ("The mobile device 100 is also shown with two types of external notification mechanisms: an LED 140 and an audio interface 174. … The audio interface 174 is used to provide audible signals to and receive audible signals from the user. For example, the audio interface 174 may be coupled to a speaker for providing audible output and to a microphone for receiving audible input, such as to facilitate a telephone conversation"); APPLE-1024 (Lu), [0004]; APPLE-1025 (Song), 1:18-20.

42. It is also my opinion that a POSITA would have expected success in pursuing this implementation because both Marek and Skarine pertain generally to the field of mobile devices. *See* APPLE-1004 (Marek), 11:44-56 ("the SCM may be utilized by various untrusted host COTS platforms such as PDAs, cell phones, laptops and the like. … Moreover, the SCM is suitable for providing secure wireless network connections when the SCM is added on wireless devices such as PDAs, cell phones, and other mobile devices"), 12:13-21 ("a block diagram of a system 1000 including a SCM 908 interfacings with an untrusted PDA 1014"), 13:49-51 ("the SCM may be packaged in a form factor suitable for various portable devices such as a PDA, a cell phone, a GPS device and the like"), 2:56-59 ("The SCM may use a Compact Flash (CF) interface for a PDA host"), 7:53-57 ("Windows CE operating system may be utilized as an embedded COTS OS on the untrusted host platform. For instance, ruggedized PDAs may employ Windows CE operating system for COTS OS 604"), 8:25-38, Figs. 10 and 11; APPLE-1005 (Skarine), [0001] ("Embodiments of the invention relate generally to mobile devices").

Wireless communications capabilities and memory components in the untrusted host mobile device of the combination

43. I discuss in the following paragraphs another example of the configuration of conventional components in the untrusted host mobile device of the Marek-Skarine combination: that this untrusted host mobile device includes conventional wireless communication components.

44. As an initial point, I note that the untrusted host mobile device of Marek is a wireless device, as I have mentioned previously. *See* APPLE-1004 (Marek), 11:44-56 ("the SCM is suitable for providing secure wireless network connections when the SCM is added on ***wireless devices such as PDAs, cell phones***, and other mobile devices"), 12:13-21 ("a system 1000 including a SCM 908 interfacing with an untrusted PDA 1014"), 13:49-51 ("the SCM may be packaged in a form factor suitable for various portable devices such as a PDA, a cell phone, a GPS device and the like"), 2:56-59, 7:53-57, 8:25-38, Figs. 10 and 11.

45. It is my opinion that a POSITA would have understood or found obvious for the untrusted host mobile device (a wireless device) of the Marek-Skarine combination to include conventional wireless communication components, such as RF transceiver circuitry and an antenna (highlighted in pink in the composite figure above). The presence of such components was well-known in the art in the context of conventional mobile devices, as demonstrated, for instance, by Skarine.

See APPLE-1005 (Skarine), [0022]-[0023] ("Mobile device 102 sends communication signals to and receives communication signals from network 104 over a wireless link via antenna 110. RF transceiver circuitry 108 performs functions such as modulation/demodulation and possibly encoding/decoding and encryption/decryption."), [0027]-[0029] ("Mobile device 102 communicates in and through wireless communication network 104" which "is configured in accordance with General Packet Radio Service (GPRS) and a Global Systems for Mobile (GSM) technologies.", [0032] ("User data may be transferred transparently between mobile device 103 and the external data networks using, for example, encapsulation and tunneling. Data packets are equipped with GPRS-specific protocol information and transferred between mobile device 102 and GGSM 128"), [0034] ("Mobile device 202 is preferably a two-way communication device having at least voice and advanced data communication capabilities, including the capability to communicate with other computer systems. Depending on the functionality provided by mobile device 202, it may be referred to as a data messaging device, a two-way pager, a cellular telephone with data messaging capabilities, a wireless Internet appliance, or a data communication device (with or without telephony capabilities). Mobile device 202 may communicate with any one of a plurality of fixed transceiver stations 200 within its geographic coverage area."), ;[0035] ("Mobile device 202 will normally incorporate a communication subsystem 211, which includes a receiver

212, a transmitter 214, and associated components… Communication subsystem 211 is analogous to RF transceiver circuitry 108 and antenna 110 shown in FIG. 1. As will be apparent to those skilled in field of communications, particular design of communication subsystem 211 depends on the communication network in which mobile device 202 is intended to operate."), [0036] ("Mobile device 202 may send and receive communication signals over the network"), [0038] ("Communication functions, including at least data and voice communications, are performed through communication subsystem 211"), Figs. 1-2.

46. I also refer to the following other references to corroborate that conventional wireless communication components, such as RF transceiver circuitry and antennas, were standard components in conventional mobile devices as of the Critical Date: APPLE-1011 (Huang), 5:11-13 ("The wireless transceiver 27 transmits speech signals or intermediate speech recognition results over wireless transport 14 using antenna 11. Wireless transceiver 27 can also transmit other data over wireless transport 14. In some embodiments, transceiver 27 receives information from desktop computer 12, the information source provider 13, or from other mobile or non-mobile devices or phones. The wireless transceiver 27 is coupled to the bus 28 for communication with the processor 20 and the object store 18 to store information received from the wireless transport 14."), 4:46-59; APPLE-1015 (Ramirez), 3:11-17 ("The communication device 101, as shown, includes a

battery based power supply 109 that provides supply voltages to a WAN function or modem 111 that is the primary service access apparatus for the communication device. The WAN modem 111 includes a primary receiver and transmitter (primary transceiver) that are configured to operate on or with a first, e.g., WAN, network."; APPLE-1017 (Macchi), 10:14-18 ("The user terminal comprises … specific elements allowing radio communications with the BTSs in accordance to the GSM specifications"; APPLE-1018 (Yach), 6:33-45 ("The communication subsystem 104 comprises a receiver 150 and a transmitter 152, as well as associated components such as one or more embedded or internal antenna elements 154, 156, Local Oscillators (LOs) 158, and a processing module such as a Digital Signal Processor (DSP) 160. As will be apparent to those skilled in the field of communications, the particular design of the communication subsystem 104 is dependent upon the communication network with which the mobile device 100 is intended to operate."), 7:11-29.

47. In the Marek-Skarine combination, the wireless communication components are coupled to the processor of the untrusted host device. This configuration is illustrated in the composite figure at the beginning of this section. To the extent Marek does not explicitly disclose this configuration, it is my opinion that a POSITA would have found it obvious in view of the teachings of Skarine, which describes wireless communication components of a mobile device that are coupled

to the processor of that mobile device. *See* APPLE-1005 (Skarine), [0038] ("Communication functions, including at least data and voice communications, are performed through communication subsystem 211. Microprocessor 238 also interacts with additional device subsystems"), Fig. 2.

48. It is my opinion that a POSITA would have been motivated to implement the untrusted host mobile device of the Marek-Skarine combination such that the wireless communication components are coupled to the processor of the untrusted host mobile device at least because doing so enables the communication between the mobile device and a cellular telephone network. This was conventional functionality available in PDA or cell phone mobile devices as of the Critical Date, as demonstrated, for instance, by Skarine. *See* APPLE-1005 (Skarine), [0022]-[0023], [0027]-[0029], [0032], [0034]-[0036], [0038], Figs. 1-2; APPLE-1011 (Huang), 5:11-13; APPLE-1015 (Ramirez), 3:11-17; APPLE-1017 (Macchi), 10:14-18; APPLE-1018 (Yach), 6:33-45, 7:11-29.

49. It is also my opinion that a POSITA also would have been motivated to pursue this implementation is because this configuration is just the application of known techniques (*e.g.*, wireless communication components connected to a processor in a mobile device) by a known system (*e.g.*, Marek's untrusted host mobile device) that produces a predictable outcome (*e.g.*, a mobile device with conventional wireless communication capabilities).

50. Furthermore, it is my opinion that a POSITA would have expected success in configuring the wireless communication components of the untrusted host mobile device to be coupled to the processor of the untrusted host mobile device because Marek indicates that its teachings are applicable to conventional "wireless devices such as PDAs, cell phones, and other mobile devices" (APPLE-1004 (Marek), 11:55-56)

51. I also believe that a POSITA would have expected success in implementing this configuration because having wireless communication components in a mobile device configured to communicate with a microprocessor of that mobile device was a standard configuration as of the Critical Date. *See* APPLE-1005 (Skarine), [0022]-[0023], [0027]-[0029], [0032], [0034]-[0035], [0038], Figs. 1-2; APPLE-1011 (Huang), 5:11-13; APPLE-1015 (Ramirez), 3:11-17; APPLE-1017 (Macchi), 10:14-18; APPLE-1018 (Yach), 6:33-45, 7:11-29.

52. It is also my opinion that a POSITA would have expected success in pursuing this implementation because both Marek and Skarine pertain generally to the field of mobile devices. *See* APPLE-1004 (Marek), 11:44-56, 12:31021, 13:49-51, 2:56-59, 7:53-57, 8:25-38, Figs. 10 and 11; APPLE-1005 (Skarine), [0001].

Memory components in the untrusted host mobile device of the combination

53. In another example of the configuration of conventional components in the conventional untrusted host mobile device of the Marek-Skarine combination, it is my opinion that a POSITA would have understood or found obvious that the untrusted host mobile device in the Marek-Skarine combination to include conventional memory components (highlighted in purple in the composite figure above) such as volatile and non-volatile storage.

54. The presence of such memory components was well-known in the art as of the Critical Date in the context of conventional mobile devices, for instance, as demonstrated Skarine. *See* APPLE-1005 (Skarine), [0038] ("Microprocessor 238 also interacts with additional device subsystems such as … a flash memory 224 [and] a random access memory (RAM) 226").

55. I also refer to the following other references to corroborate that memory components such as volatile and non-volatile storage were standard components in conventional mobile devices as of the Critical Date: APPLE-1018 (Yach), 3:58-64 ("Operating system software used by the microprocessor 102 is typically stored in a persistent store such as the flash memory 108, which may alternatively be a read-only memory (ROM) or similar storage element (not shown). Those skilled in the art will appreciate that the operating system, specific device applications, or parts thereof, may be temporarily loaded into a volatile store such

as the RAM 106."); APPLE-1009 (Mathur), 1:44-46 ("the persistent storage of a typical embedded system comprising flash memory or volatile memory with a battery refresh"); APPLE-1010 (Zuberec), 3:10-39 ("The mobile device 100 has … a memory 162 … The memory 162 generally includes both volatile memory (e.g., RAM) and non-volatile memory (e.g., ROM, Flash Memory, or the like)"); APPLE-1011 (Huang), 4:46-59 ("Memory 22 is implemented as non-volatile electronic memory such as random access memory (RAM) with a battery back-up module (not shown) such that information stored in memory 22 is not lost when the general power to the mobile device 10 is shut down. A portion of memory 22 is allocated as addressable memory for program execution, while the remaining portion of memory 22 can be used for storage, such as to simulate storage on a disk drive."); APPLE-1012 (Kwong), [0013]; APPLE-1017 (Macchi), 10:14-22.

4. Element-by-Element Explanation of How the Marek-Skarine Combination Renders the Challenged Claims Obvious

(i) Claim 1

[1pre] A computer system, comprising:

56. The Marek-Skarine combination provides **a computer system**, which is illustrated in the composite figure below. For instance, a POSITA would have understood that Marek's "***computing environment 700***" implementing SCM architecture, and modified based on Skarine as I discussed above in Section VI.A.3, is **a**

computer system. APPLE-1004 (Marek), 8:51-52, Fig. 7; *see also* 8:37-39 ("Secure COTS computing environment may be provided by ***a system including a SCM as an add-on module to an untrusted host environment***."), 1:6-9 ("This invention relates generally to ***computing environments*** and more particularly to a system for providing a secure and trusted commercial-off-the-shelf COTS computing environment"), 1:43-45 ("a system provides a secure COTS computing environment through controlling COTS processor resource access"), 1:66-2:1 ("a system including a Secure Computing Module (SCM) provides a trusted environment for COTS host platforms"), 11:57-60 ("a system 900 including a SCM 908 utilized by an untrusted host platform communicating with unsecured wireless and/or wired networks"), 12:13-14 ("a system 1000 including a SCM 908 interfacing with an untrusted PDA 1014"), 12:19-21 ("a PDA computing environment 1100 utilizing the SCM shown in Fig. 10"), Figs. 9-14.

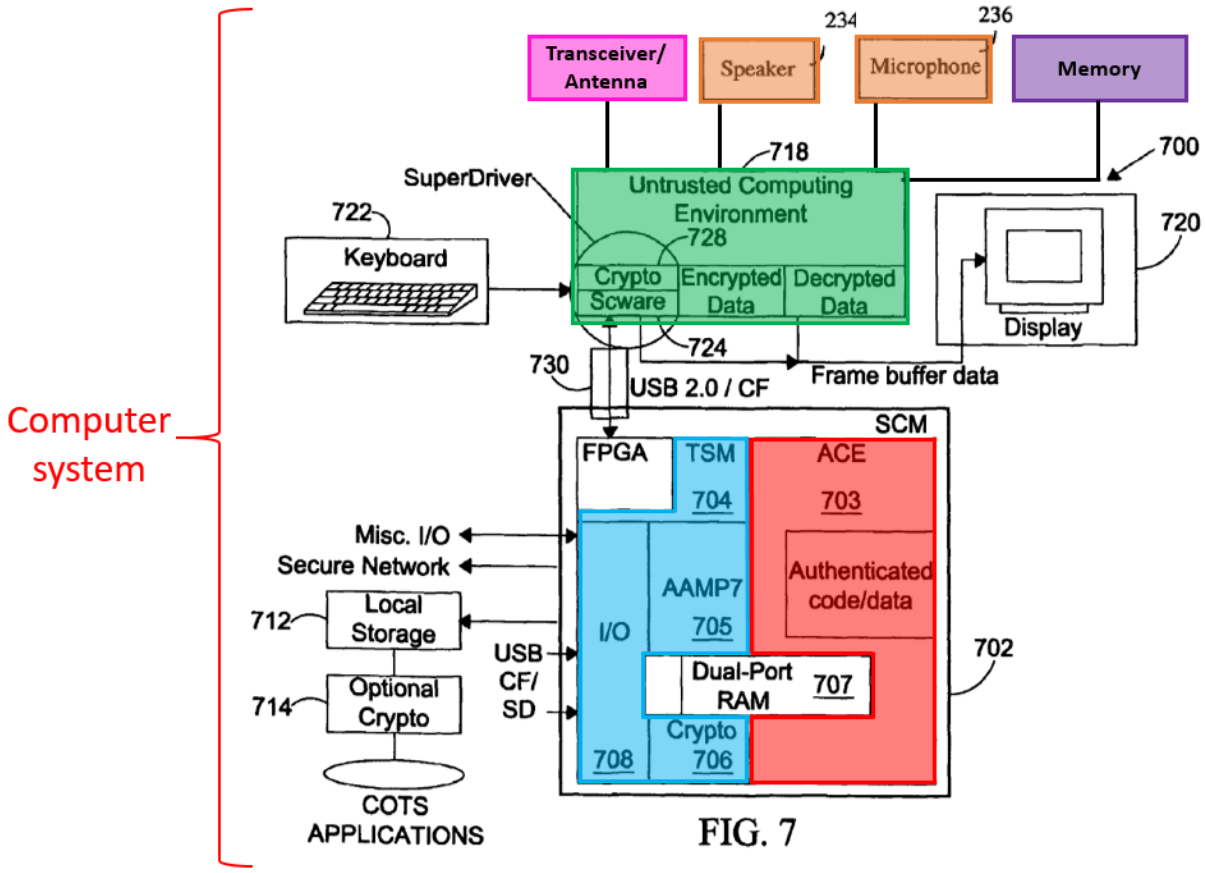


FIG. 7

Marek-Skarine composite figure

[1a] a portable mobile computing device including a secure user processor, a non-secure user processor, a communications transceiver, and a cryptographic engine;

The Marek-Skarine combination device is a portable mobile computing device

57. Marek describes that "[a] secure COTS computing environment may be provided by a system including a SCM as an add-on module to an untrusted host environment." APPLE-1004 (Marek), 10:37-39. The untrusted host 718 (which I have highlighted in green in the composite figure below) is a mobile device, such as a PDA or cell phone, as I discuss in the next paragraph. The SCM 702 (highlighted in orange) that interfaces with the untrusted mobile host 718 is

also a mobile device, which I also discuss below. Because both the untrusted host 718 and SCM 702 are mobile devices, these two mobile devices (*i.e.*, the untrusted host and the SCM) together are, or at least render obvious, **a portable mobile computing device** in the Marek-Skarine combination system. I have outlined this portable mobile computing device—which includes both the untrusted host (*e.g.*, a PDA or cell phone) and the SCM add-on module—in purple in the composite figure below.

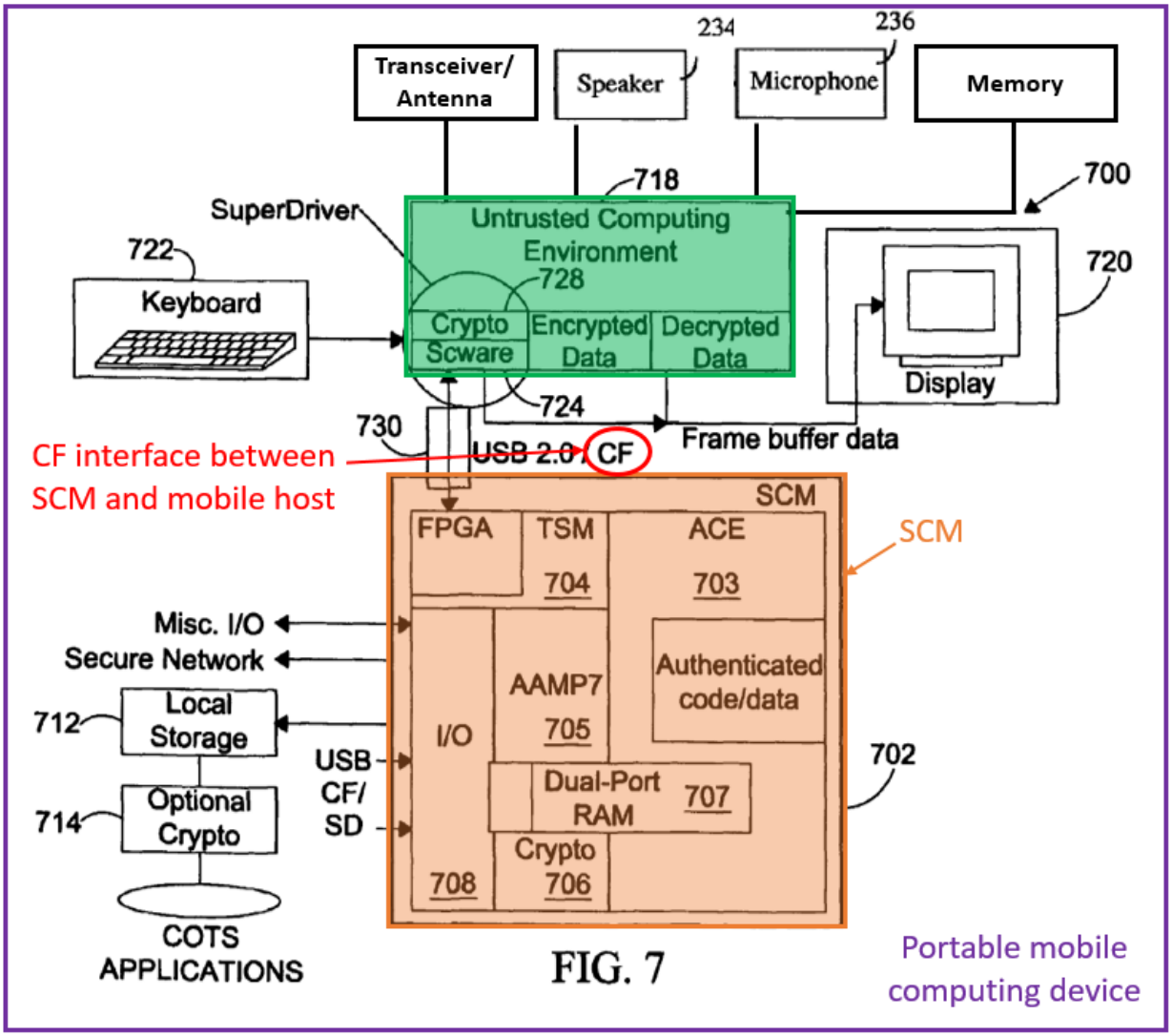


FIG. 7

Marek-Skarine composite figure

58. Marek's untrusted host 718 (highlighted green) is a mobile device, *e.g.*, a PDA or cell phone, which I discussed in more detail in the following paragraphs. I note that the combination with Skarine does not alter this form factor. Rather, as I have discussed above and will discuss in more detail in this element-by-element analysis, Skarine provides implementation details that may not necessarily have been explicitly stated by Marek.

59. Generally, Marek explains that the SCM is for use with mobile devices such as PDAs and cell phones: "the SCM may be utilized by ***various untrusted host COTS platforms such as PDAs, cell phones***, laptops and the like." APPLE-1004 (Marek), 11:44-46; *see* 11:53-56 ("the SCM is suitable for providing secure wireless network connections when the SCM is added on wireless devices such as PDAs, cell phones, and other mobile devices"), 12:13-21 ("a system 1000 including a SCM 908 interfacing with an untrusted PDA."), 13:49-51 ("the SCM may be packaged in a form factor suitable for various portable devices such as a PDA, a cell phone, a GPS device and the like"), 2:56-59 ("The SCM may use a Compact Flash (CF) interface for a PDA host"), 7:53-57, 8:25-38, Figs. 10 and 11.

60. More specifically, Marek also describes that the particular untrusted host 718 that is illustrated in Fig. 7 is a mobile device: "[t]he SCM may employ various interfaces depending on the host COTS platforms, including ***a Compact Flash (CF) interface for a PDA host platform*** and a Universal Serial Bus (USB) connection for a desktop PC platform." APPLE-1004 (Marek), 11:45-50. This CF interface is shown in Marek's Fig. 7, and I have circled the CF interface in red in the composite figure above. The presence of the CF interface connecting the SCM and the untrusted host 718 demonstrates that the specific untrusted host 718 of Marek's Fig. 7 is a mobile device such as a PDA. *See also id.*, 12:13-16 ("a block diagram of a system 1000 including a SCM 908 interfacing with an untrusted PDA

1014 … The SCM 908 may include Compact Flash (CF) interface 1012 for the host interface module."), 2:56-62 ("The SCM may use a Compact Flash (CF) interface for a PDA host"), Fig. 7.

61. Marek's SCM 702 (highlighted in orange in the composite figure above) is also a mobile device. For instance, I note that Marek describes that "the SCM may be packaged in a form factor suitable for various portable devices such as a PDA, a cell phone, a GPS device and the like." APPLE-1004 (Marek), 13:49-41. I interpret this as indicating that the SCM itself has a form factor consistent with that of a mobile device—and thus that the SCM is itself a mobile device. Additionally, as I discuss in the next two paragraphs, Marek's SCM includes a mobile device processor and a mobile device operating system, which further confirms that Marek's SCM is a mobile device.

62. Marek explains that the "Authenticated COTS Environment Subsystem" (ACE) of the SCM "includes an embedded COTS OS running on a compatible embedded COTS processor." *Id.*, 9:1-5. This embedded COTS OS is, *e.g.*, "WINDOWS® CE … or PALM OS®." APPLE-1004 (Marek), 9:5-7. Both of these operating systems are operating systems for mobile devices. *See* APPLE-1009, 1:66-2:3 ("specialized operating systems capable of running in the resource-limited environment of the embedded system have been developed. An example of such an operating system is the Windows CE™ operating system from Microsoft

Corporation."); APPLE-1010, 3:17-19 ("The mobile device 100 includes an operating system 164, such as the Windows CE operating system from Microsoft Corporation"); APPLE-1011, 4:59-61 (describing a mobile device having an "operating system … [that] is a Windows CE brand operating system commercially available from Microsoft Corporation"). The SCM—running a mobile device operating system—is thus itself a mobile device.

63. Additionally, the embedded COTS processor of Marek's ACE is likewise a processor for a mobile device: "an INTEL® cellular processor such as PXA270™ processors, mobile PENTIUM™ processors, TRANSMETA™ EFFICEON™ processors, and the like." APPLE-1004 (Marek), 9:7-10. These types of processors are mobile device processors. *See* APPLE-1012, [0012] (describing a "mobile computing platform" including a processor such as "an Intel® PXA270 XScale® processor, [or] an Intelg Pentium® M Processor"). Again, I conclude that the SCM is itself a mobile device because it includes a mobile device processor.

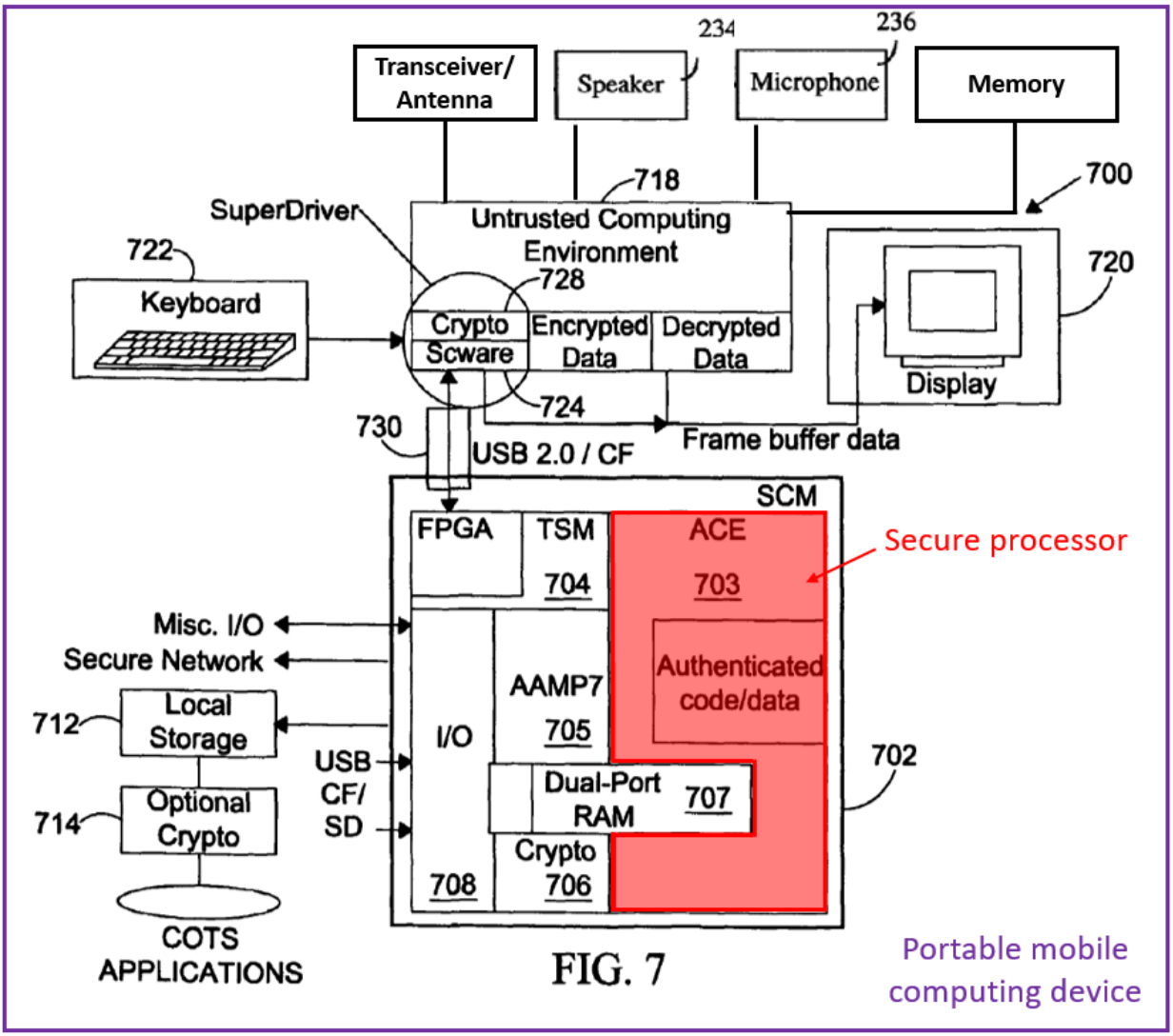
64. At least because Marek's untrusted host 718 and SCM 702 are both mobile devices, the untrusted mobile device host 718 and the SCM 702 of Marek's Fig. 7 together are, or at least render obvious, **a portable mobile computing device** in the Marek-Skarine combination system.

The combination device includes a secure user processor

65. In the Marek-Skarine combination system, the SCM 702 of the portable mobile computing device includes **a secure user processor**. Marek's SCM includes an "Authenticated COTS environment subsystem (ACE)" 703, which I have highlighted in red in the composite figure below. APPLE-1004 (Marek), 9:1-2. The ACE "includes ***an embedded COTS OS*** running on a compatible ***embedded COTS processor***" and also includes "***COTS applications***, ***manufacturer-supplied software*** and the like." APPLE-1004 (Marek), 9:4-5, 9:13-14. The embedded COTS processor of Marek's ACE 703, together with the COTS OS and software, are, or at least render obvious, **a secure user processor**.[2] For instance, these elements render obvious a secure user processor because of their role in providing a secure, trusted computing environment. *See also id.*, 8:61-62 ("The trusted environment may include ***trusted hardware and software***"), 2:12-15 ("The ACE may be secured by authenticating all code and data used for running COTS applications"), 2:33-38 ("Advantageously, the system including the SCM may provide

[2] I note that my analysis accounts for the '399 Patent's description of "a secure processor" as being "composed of trusted microprocessor hardware executing trusted operating system software and trusted application software." APPLE-1001 ('399 Patent), 4:40-43.

trusted and portable COTS computing environments against malware. Use of the ACE in conjunction with the TSM may ensure COTS applications running on the SCM to be free from malware and manufacturer-supplied software to be trusted."), 8:39-41 ("Only authenticated COTS applications and COTS OS execute on the SCM while untrusted applications execute on the untrusted host environment"), 12:18-19 ("trusted applications are implemented in the SCM 908"), 9:5-17. *See also* my further discussion in element [1b].



Marek-Skarine composite figure

66. It is my opinion that a POSITA would have found it obvious for the embedded COTS processor of Marek's ACE 703, taken alone or together with the COTS OS and software, to be a **secure** processor at least because they are included in Marek's "***Secure COTS computing environment***" provided by the SCM 702, *e.g.*, an environment that provides secure, trusted computing. APPLE-1004 (Marek), 8:37-39; *see* 8:39-45, 1:66-2:4 ("a system including a Secure Computing

Module (SCM) provides ***trusted environment*** for COTS host platforms. Only authenticated trusted applications execute on the SCM."), 2:13-20 ("The ACE may be secured by authenticating all code and data used for running COTS applications."), 2:31-38 ("the system including the SCM may provide trusted and portable COTS computing environments against malware").

67. The illustrations of Marek's Figs. 10-11 further corroborate that the embedded COTS processor of Marek's ACE 703, together with the COTS OS and software, is a **secure** processor. These figures (*see*, for instance, Fig. 10, below) show an ACE in the red domain of a portable mobile computing device system. Red and black domains are domains of a system that handles sensitive information, such as classified information. *See* APPLE-1004 (Marek), 7:25-29 ("a domain for processing possibly sensitive plain-text data, called the Red Domain, and a domain for processing non-sensitive and encrypted sensitive data, called the Black Domain"); APPLE-1014 (ITT), [0005] ("'Red/black' refers to separation of electrical and electronic circuits, components, equipment, and systems that handle national security information (red) in electrical form from those that handle non-national security information (black) in the same form, as described in the National INFOSEC Glossary. Devices and software components that operate in a red environment for processing classified data undergo extensive testing to ensure the integrity of the classified data passing through those components.").

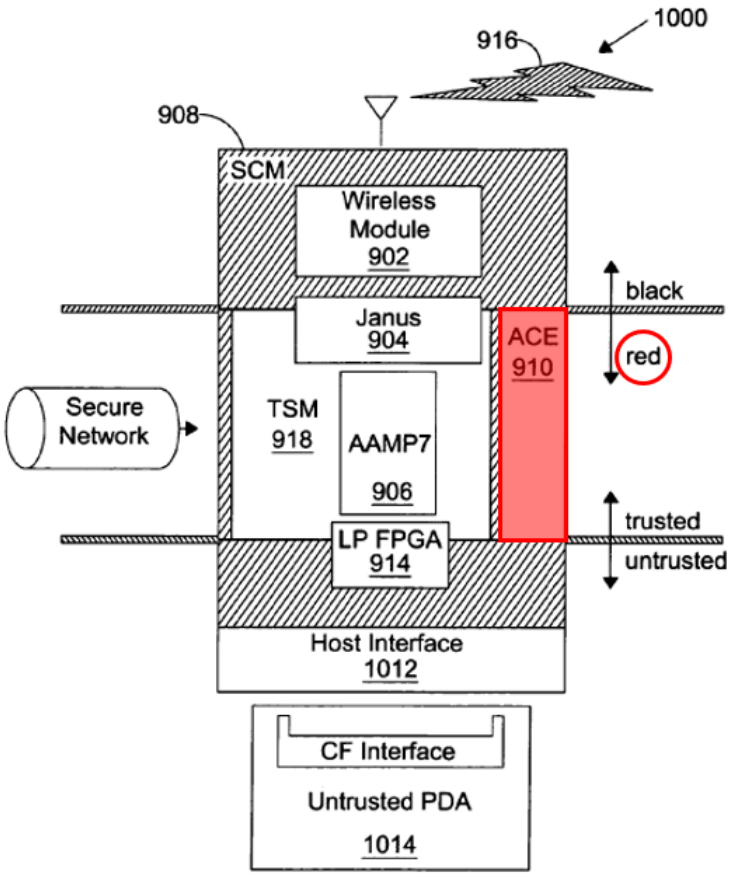


FIG. 10

Excerpt from Marek, Fig. 10 (annotated)

68. I note that Figs. 10-11 illustrate systems 1000, 1100 that show example applications for a SCM used with an untrusted host PDA. *See* APPLE-1004 (Marek), 11:43-12:21. It is my opinion that a POSITA would have understood that Marek's description of the example implementations shown in Figs. 10-11 are relevant to the SCM 702 and untrusted host mobile device 718 of the computing environment 700 of Marek's Fig. 7. For instance, this opinion is based on Marek's characterization of the systems of Figs. 10-11 as "SCM Applications" and Marek's

indication that "the SCM may be utilized by various untrusted host COTS platforms such as PDAs, cell phones, laptops, and the like." *Id.*, 11:43-46; *see* 3:33-44. This opinion is also based on the consistency of the high-level architecture illustrated in both Fig. 7 and Figs. 10-11 (*e.g.*, the presence of the various components of the SCM and its coupling to the mobile device via a CV interface).

The combination device includes a non-secure user processor

69. In the Marek-Skarine combination system, the untrusted host mobile device 718, which I have highlighted in green in the composite figure below, includes **a non-secure user processor**. Specifically, Marek describes that the untrusted host 718 includes COTS processors. *See* APPLE-1004 (Marek), 8:59-61 ("Conventionally, a host platform employing ***COTS processors*** is assumed to be untrusted."). The untrusted host 718 also includes an operating system and application software. *See* APPLE-1004 (Marek), 7:54-55 ("Windows CE operating system may be utilized as ***an embedded COTS OS on the untrusted host platform***"), 8:40-41 ("***untrusted applications execute on the untrusted host environment***"). The COTS processor(s) of the untrusted host 718, alone or taken together with the

COTS OS and the applications executing on the untrusted host, are, or at least render obvious, **a non-secure user processor**.[3] For instance, these elements render obvious a secure user processor because of their role in providing a untrusted computing environment. *See also id.*, 8:56-59 ("The untrusted host environment may include commercial software environments and applications"), 12:16-18 ("Untrusted application software and hardware may be implemented in the PDA 1014"), 2:1-4 ("untrusted applications execute on the untrusted host environment"), 2:36-38. *See also* my further discussion in element [1c].

[3] I note that my analysis accounts for the '399 Patent's description of a "[n]on-secure processor" as being "composed of untrusted microprocessor hardware executing an untrusted operating system and untrusted application software." APPLE-1001 ('399 Patent), 4:49-51.

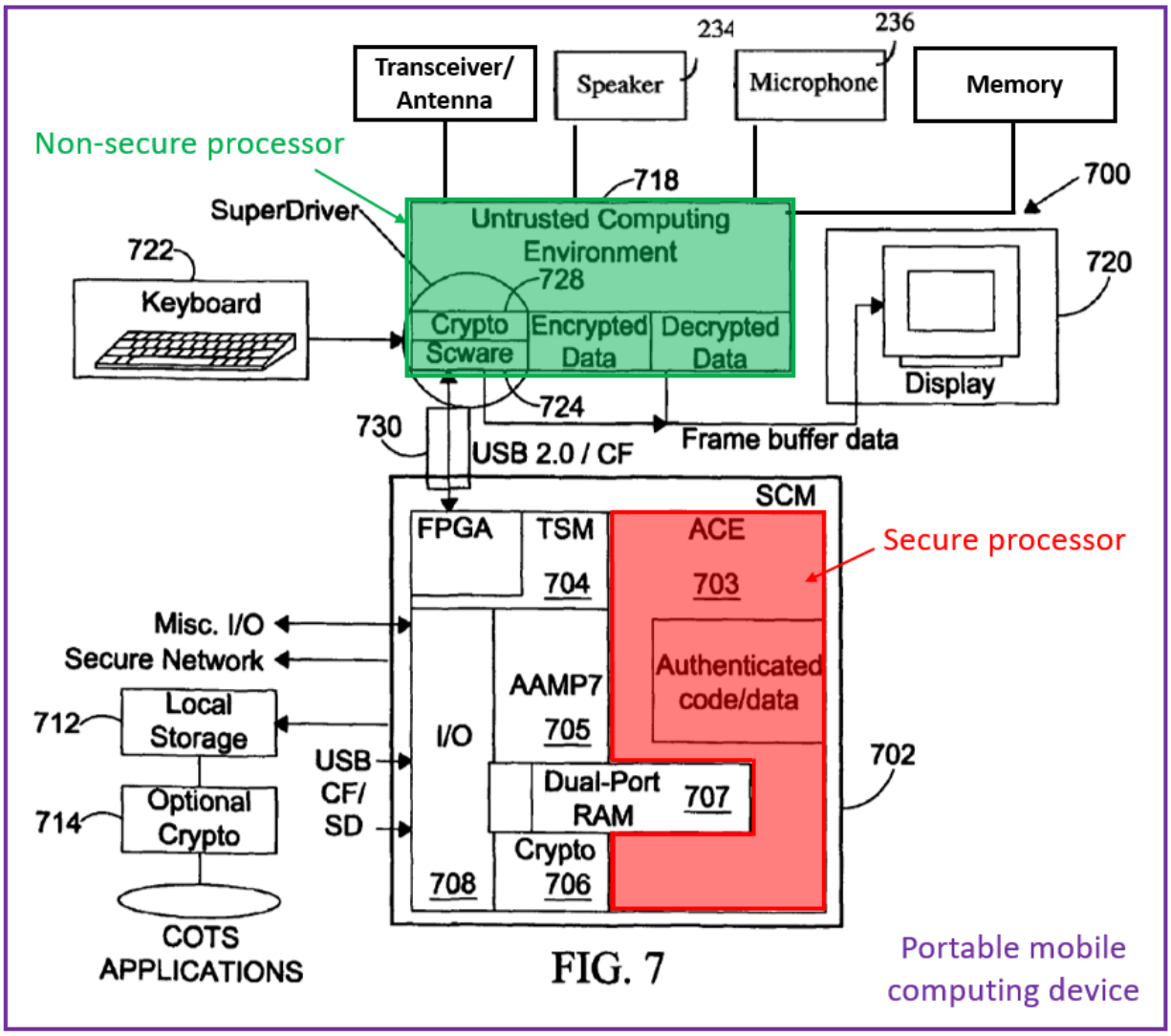


FIG. 7

Marek-Skarine composite figure

70. To the extent Marek does not explicitly state that the COTS OS is on the processor of the specific untrusted host 718, I believe that a POSITA would have understood this to be the case, or otherwise found this to be obvious, given that operating systems and their use in mobile devices were well-known as of the Critical Date. *See* APPLE-1004, 7:54-55; APPLE-1005, [0022]-[0023], [0038];

APPLE-1009, 1:64-2:3; APPLE-1010, 3:17-21; APPLE-1011, 4:54-61; APPLE-1018, 3:58-64.

71. It is my opinion that a POSITA would have found it obvious for the COTS processor(s) of the untrusted host, taken alone or together with the COTS OS and the applications, to be a **non-secure** processor at least because they are included in Marek's "untrusted host environment," *e.g.*, an environment that provides untrusted computing. APPLE-1004 (Marek), 8:40-41; *see* 8:56-59 ("a host platform employing COTS processors is assumed to be ***untrusted***"), 12:16-18 ("Untrusted application software and hardware may be implemented in the PDA"), 2:1-4, 2:36-38, Figs. 10-11 (showing a PDA in the black domain of a portable mobile computing device system).

The combination device includes a communications transceiver

72. Marek describes that "the SCM is added on ***wireless devices*** such as PDAs, cell phones, and other mobile devices," *e.g.*, the untrusted host mobile device 718 in the combination is a wireless device. APPLE-1004 (Marek), 11:53-56. It is my opinion that a POSITA would have understood—or at least found it obvious—that a "wireless device[]," (*id.*) such as the untrusted host mobile device of the combination, includes **a communications transceiver**, which I have highlighted in pink in the composite figure below. Moreover, it is also my opinion that a POSITA would have understood or found it obvious for the communications

transceiver to be coupled to the non-secure user processor of the untrusted host mobile device of the combination (still highlighted in green).

73. I hold this opinion at least because it was conventional in the art as of the Critical Date for wireless devices such as PDAs or cell phones to have communications transceivers to enable wireless communication. This is demonstrated, for instance, by Skarine. *See* APPLE-1005 (Skarine), [0022] ("signal processing operations associated with ***communication functions are typically performed in RF transceiver circuitry*** 108"), [0023] ("Mobile device 102 sends communication signals to and receives communication signals from network 104 over a wireless link via antenna 110. RF transceiver circuitry 108 performs functions such as modulation/demodulation and possibly encoding/decoding and encryption/decryption. It will be apparent to those skilled in art that ***RF transceiver circuitry 108 will be adapted to particular wireless network or networks*** in which mobile device 102 is intended to operate."), [0035] ("Mobile device 202 will normally incorporate ***a communication subsystem 211, which includes a receiver 212, a transmitter 214***, and associated components … Communication subsystem 211 is analogous to RF transceiver circuitry 108 and antenna 110"), [0027]-[0029], [0036]-[0038], Figs. 1-2.

74. I also refer to the following other references to corroborate that it was conventional for wireless devices such as PDAs or cell phones to have communication transceivers coupled to the processor of the wireless device: APPLE-1011 (Huang), 5:11-13 ("***The wireless transceiver 27 transmits speech signals … over wireless transport*** 14 using antenna 11," where "wireless transport 14 can be a paging network, cellular digital packet data (CDPD), FM-sideband, or other suitable wireless communications"), 4:46-59; APPLE-1015 (Ramirez), 3:11-17 (describing a mobile device having a "WAN modem 111 [that] includes a ***primary receiver and transmitter (primary transceiver) that are configured to operate on or with a first, e.g., WAN, network***."); APPLE-1017 (Macchi), 10:14-18; APPLE-1018 (Yach), 6:33-45, 7:11-29.

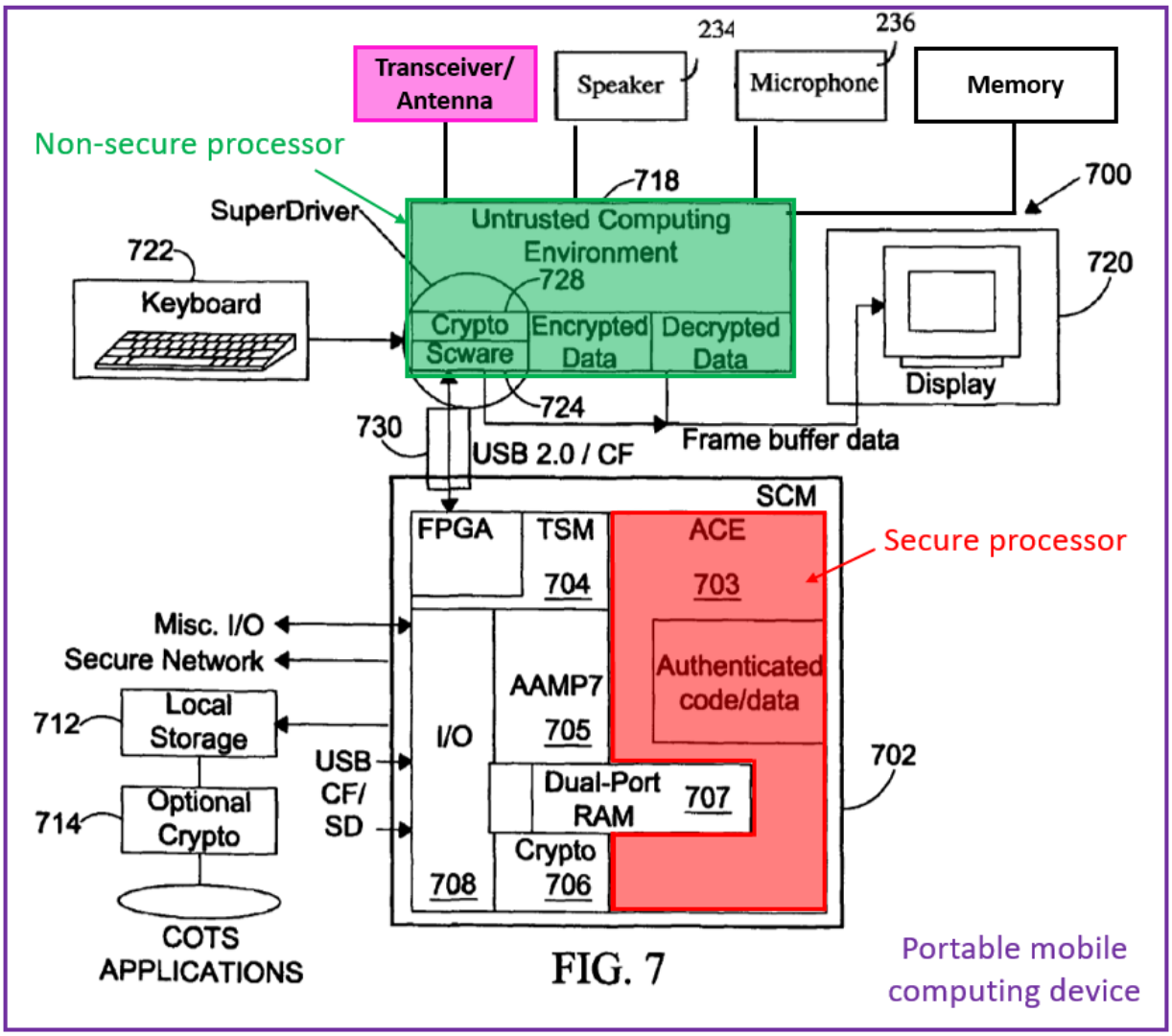


FIG. 7

Marek-Skarine composite figure

The combination device includes a cryptographic engine

75. In the Marek-Skarine combination system, the SCM 702 of the portable mobile computing device includes **a cryptographic engine**. Specifically, the SCM includes a "Trusted Security Manager subsystem (TSM) 704," as taught by Marek. APPLE-1004 (Marek), 8:67. The TSM 704 "include[s] ***a trusted proces-***

sor 705 for providing a brick-wall partitioning of memory, time, and device resources, and enforcing predetermined security policies," and "***a cryptographic engine 706*** … [that] may aid the trusted processor 705 to provide a robust security interface." APPLE-1004 (Marek), 9:31-47. The Trusted Security Manager subsystem 704, including the trusted processor 705 and cryptographic engine 706, function as, and render obvious, **a cryptographic engine**, which I have highlighted in blue in the composite figure below.

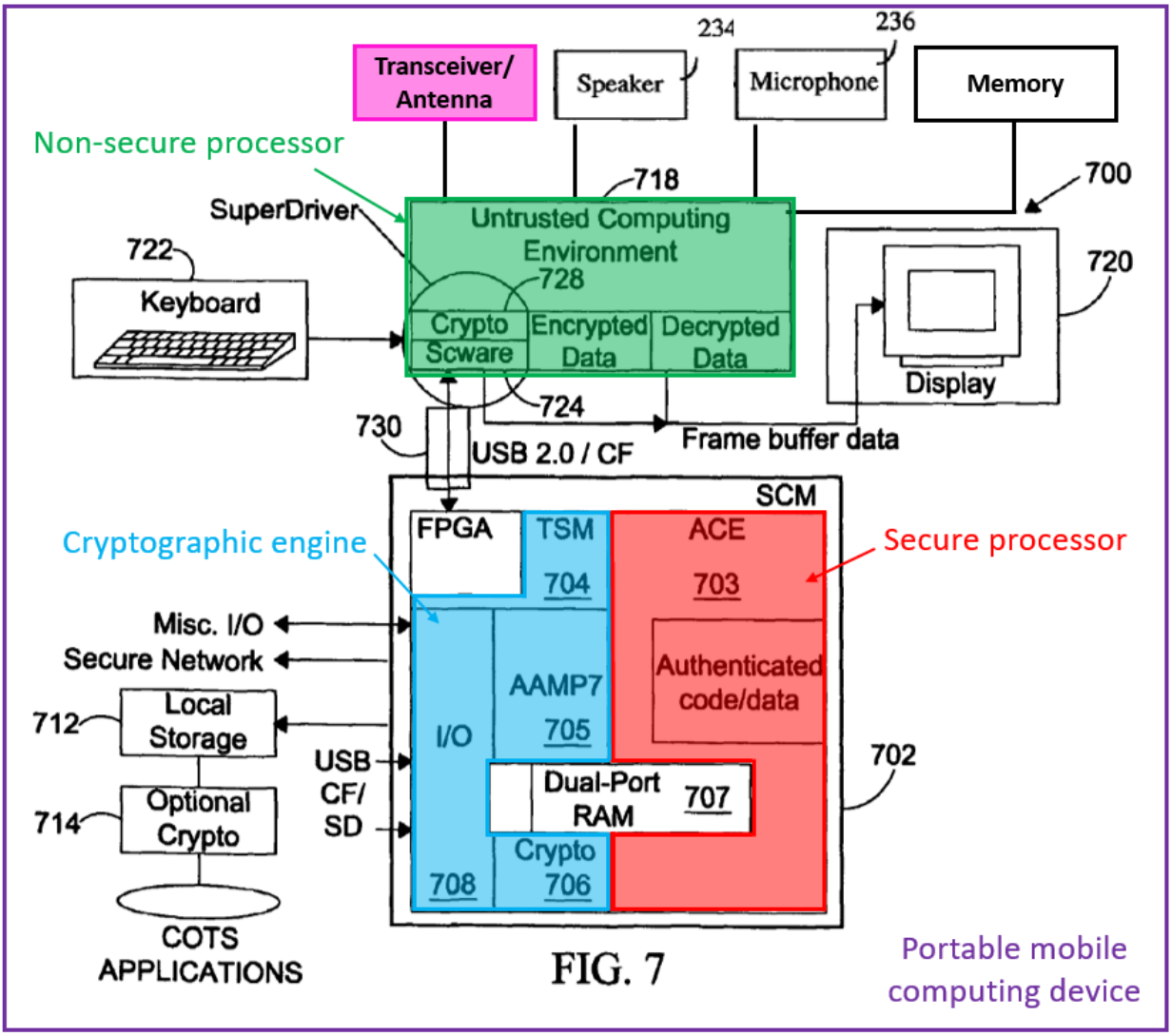


FIG. 7

Marek-Skarine composite figure

76. The TSM 704 can be considered to be a cryptographic engine at least because it "provide[s] a robust security interface" (APPLE-1004 (Marek), 9:40-41;

see 10:33-35) using cryptography.[4] *See id.*, 9:42-47 ("Conventionally, cryptography is the widely used means for protecting information confidentiality and integrity. The use of cryptography allows much of the secure communication system to be built with COTS network components."), 9:48-60 ("Memory and I/O resources in the SCM 702 are strictly partitioned and managed by several secure TSM partitions. Each I/O path of the SCM 702 is configured to go through the TSM 704 so that a corresponding TSM partition of an I/O path controls the I/O path to be secured and authenticated. … A dedicated secure TSM partition may manage each I/O path being subject to authentication protocols."), 9:31-37 ("The TSM 704 may include a trusted processor 705 for providing a brick-wall partitioning of memory, time, and device resources, and enforcing predetermined security policies. The brick-wall partitioning of memory, time and device resources may ensure that applications execute in an environment that is strictly portioned, highly protected and completely isolated from other applications.").

---

[4] I note that the functionality of Marek's TSM is consistent with the functionality of the cryptographic engine as described in the '399 Patent. *See* APPLE-1001, 8:41-49 ("the cryptographic engine can provide an encryption/decryption function for data communicated between the secure and non-secure processors").

[1b] said secure user processor comprising a trusted microprocessor, a trusted operating system executing on said trusted microprocessor, and a trusted application software executing on said trusted microprocessor;

77. The **secure user processor** of the Marek-Skarine combination system (which is contained in the ACE of the SCM, as I discussed for element [1a], above) **includes a trusted microprocessor**. For instance, the hardware of the embedded COTS processor of Marek's ACE 703 is a trusted microprocessor. *See* APPLE-1004 (Marek), 9:1-5 ("The ACE 703 includes an embedded COTS OS running on a compatible ***embedded COTS processor***"), 8:61-62 ("The trusted environment may include ***trusted hardware*** and software"), 9:7-13 ("Examples of the embedded COTS processor may include an INTEL® cellular processor such as PXA270™ processors, mobile PENTIUM™ processors, TRANSMETA™ EFFICEON™ processors, and the like."), Fig. 7.

78. The secure user processor of the Marek-Skarine combination system also includes **a trusted operating system executing on the trusted microprocessor**. For instance, the embedded COTS operating system (OS) of Marek's ACE 703 is a trusted operating system that executes on the embedded COTS processor of Marek's ACE 703 (*i.e.*, on the trusted microprocessor; *see* previous paragraph). *See* APPLE-1004 (Marek), 9:1-5 ("The ACE 703 includes ***an embedded COTS OS running on a compatible embedded COTS processor***"), 2:14-15 ("The ACE may

include ***an embedded COTS OS***"), 8:39-41 ("Only authenticated COTS applications and ***COTS OS execute on the SCM***"), 8:61-62 ("The trusted environment may include trusted hardware and software"), 9:5-7 ("***Examples of the embedded COTS OS*** include WINDOWS® CE, LINUX, or PALM OS®, or the like"), Fig. 7.

79. The secure user processor of the Marek-Skarine combination system further includes **trusted application software executing on said trusted microprocessor**. For instance, the applications included in Marek's ACE 703 are trusted application software that execute on the embedded COTS processor of Marek's ACE 703. *See* APPLE-1004 (Marek), 9:13-17 ("The ACE 703 may include ***COTS applications, manufacturer-supplied software and the like***."), 8:39-41 ("Only ***authenticated COTS applications*** … ***execute on the SCM***"), 8:61-62 ("The trusted environment may include trusted hardware and software"), 2:12-15 ("The ACE may be secured by authenticating all code and data used for running COTS applications. The ACE may include … various COTS applications."), 2:33-38 ("Use of the ACE in conjunction with the TSM may ensure ***COTS applications running on the SCM*** to be free from malware and manufacturer-supplied software to be trusted."), 12:18-19 ("trusted applications are implemented in the SCM"), 13:37-41; 2:1-4, Fig. 7.

80. One reason that the trusted microprocessor, trusted operating system, and trusted application software are **trusted** (or least that a POSITA would have found it obvious that they are trusted) is because they are part of, or execute on, the "Secure COTS computing environment" provided by the SCM 702. APPLE-1004 (Marek), 8:37-39; *see* 8:39-45, 1:66-2:4 ("a system including a Secure Computing Module (SCM) provides trusted environment for COTS host platforms. Only authenticated trusted applications execute on the SCM."), 2:13-20 ("The ACE may be secured by authenticating all code and data used for running COTS applications."), 2:31-38 ("the system including the SCM may provide trusted and portable COTS computing environments against malware"), 11:60-65 ("The SCM 908 including the TSM and the cryptographic engine resides in the red domain within a trusted environment"), Figs. 9-11 (showing an ACE in the red domain of a portable mobile computing device system).

81. Another reason that the trusted operating system and application software are **trusted** (or at least that a POSITA would have found this to be obvious) is because they are authenticated. *See* APPLE-1004 (Marek), 2:1-2 ("Only ***authenticated trusted applications*** execute on the SCM while untrusted applications execute on the untrusted host environment."), 2:13-15 ("The ACE may be secured by ***authenticating all code and data used for running COTS applications***."),

9:14-22 ("The ACE 703 including COTS applications, manufacturer-supplied software and associated data may be cleansed, optionally encrypted and then stored on a local storage 712. … It is understood that there are various ways to authenticate applications and software without departing from the scope and spirit of the invention."), 2:33-38 ("Only authenticated applications including COTS OS execute on the SCM"), 8:39-41, 9:2-4 ("The ACE 703 of the SCM 702 may be secured by authenticating all code and data used for running COTS applications").

[1c] said non-secure user processor comprising an untrusted microprocessor, an untrusted operating system executing on said untrusted microprocessor, and an untrusted application software executing on said untrusted microprocessor;

82. The **non-secure user processor** of the Marek-Skarine combination system (*i.e.*, the processor included in the untrusted host mobile device 718, as I discussed above for element [1a]) **includes an untrusted microprocessor**. For instance, the hardware of the COTS processor of the untrusted host PDA 718 is an untrusted microprocessor. *See* APPLE-1004 (Marek), 8:59-61 ("Conventionally, a host platform employing ***COTS processors*** is assumed to be untrusted."), 12:16-18 ("Untrusted application software and ***hardware*** may be implemented in the PDA 1014.").

83. The non-secure user processor of the combination also includes **an untrusted operating system executing on the untrusted microprocessor**. For instance, the operating system of the untrusted host 718 is an untrusted operating

system. For instance, in the combination, Marek describes an untrusted host platform in which "***Windows CE operating system may be utilized as an embedded COTS OS on the untrusted host platform***," *e.g.*, an operating system executing on the microprocessor of an untrusted host mobile device. APPLE-1004 (Marek), 7:54-55.

84. To the extent that Marek does not explicitly state that an operating system such as Windows CE is executed on the specific microprocessor of the untrusted mobile device host 718, it is nevertheless my opinion that a POSITA would have understood this to be the case based on Marek's disclosure of operating systems on untrusted host platforms. *See* APPLE-1004 (Marek), 7:54-55. I note that it was standard and well-known that operating systems (*e.g.*, Windows CE) execute on the microprocessors of mobile devices such as a PDAs or cell phones, *e.g.*, to control the execution of applications on the microprocessors and for resource allocation. *See* APPLE-1005 (Skarine), [0022]-[0023] ("a mobile device … includes … controller 106 [that] is embodied as a central processing unit (CPU), which runs operating system software in a memory component"), [0038] ("Operating system software used by microprocessor 238 is preferably stored in a persistent store … [and] may be temporarily loaded into a volatile store such as RAM 226."); APPLE-1009 (Mathur), 1:64-2:3 ("specialized operating systems capable of running in the resource-limited environment of the embedded system have been developed.

An example of such an operating system is the Windows CE™ operating system from Microsoft Corporation."); APPLE-1010, 3:17-21 ("The mobile device 100 includes an operating system 164, such as the Windows CE operating system from Microsoft Corporation … which is resident in the memory 162 and executes on the processor 160"); APPLE-1011 (Zuberec), 4:54-61 (describing a mobile device having an "operating system … [that] is a Windows CE brand operating system commercially available from Microsoft Corporation," where "[d]uring operation, the operating system 30 is loaded into, and executed by, the processor 20 from memory 22"); APPLE-1018 (Yach), 3:58-64 ("Operating system software used by the microprocessor 102 is typically stored in a persistent store such as the flash memory 108 … [and] may be temporarily loaded into a volatile store such as the RAM 106"). Thus, given the ubiquity of operating systems in mobile devices, it is my opinion that a POSITA would have understood or found obvious that Marek's description of an operating system executing on the processor of an untrusted host mobile device is applicable to the specific untrusted host mobile device 718 of Marek's Fig. 7, *e.g.*, that the non-secure user processor of the combination includes **an untrusted operating system**. *See* APPLE-1004 (Marek), 7:54-55.

85. Furthermore, the non-secure user processor of the combination includes **untrusted application software executing on the untrusted microprocessor**. For instance, the applications that execute on Marek's untrusted host 718 are

untrusted application software. *See* APPLE-1004 (Marek), 8:40-41 ("***untrusted applications execute on the untrusted host environment***"), 8:56-59 ("The untrusted host environment may include ***commercial software environments and applications***"), 12:16-18 ("Untrusted application software and hardware may be implemented in the PDA"), 2:1-4 ("untrusted applications execute on the untrusted host environment"), 2:36-38.

86. The untrusted microprocessor, untrusted operating system, and untrusted application software are **untrusted** (or at least a POSITA would have found this to be obvious) at least because they are part of, or execute on, "the ***untrusted*** host environment" rather than the secure environment of the SCM. APPLE-1004 (Marek), 8:40-41; *see* 8:56-59, 12:16-18, 2:1-4, 2:36-38, Figs. 9-11 (showing a PDA in the black domain of a portable mobile computing device system). Additionally, the untrusted application software is **untrusted** (or at least a POSITA would have found this to be obvious) at least because it "may include commercial software environments and applications, having minimal or no Common Criteria (CC) certification and no assurance of isolation between tasks." APPLE-1004 (Marek), 8:56-59.

[1d] said cryptographic engine configured for encrypting any data communicated from said secure user processor to said non-secure user processor, comprising a trusted cryptographic processor, and a trusted operating system executing on said trusted cryptographic processor;

The cryptographic engine of the combination device is configured for encrypting data communicated from the secure user processor to the non-secure user processor

87. In the Marek-Skarine combination system, Marek's TSM is the **cryptographic engine**, as I discussed above for element [1a]. I have highlighted the secure and non-secure user processors in red and green, respectively, in the composite figure below, and highlighted the cryptographic engine in blue. With reference to this composite figure, I now explain how Marek describes that **any data communicated from the secure user processor to the non-secure user processor** passes through the cryptographic engine.

88. Marek states that "***[e]ach I/O path of the SCM 702 is configured to go through TSM 704*** so that a corresponding TSM partition of an I/O path controls the I/O path to be secured and authenticated." APPLE-1004 (Marek), 9:50-54. "Examples of I/O paths of the SCM 702 include ***I/O paths between the untrusted host and the SCM***"—*e.g.*, I/O paths between the non-secure user processer and the SCM (which contains the secure user processor) pass through the cryptographic engine. *Id.*, 9:50-54. Further, Marek describes that "[a]ll ACE I/O's are controlled by the TSM 704 and ***any I/O from/to the ACE 703 is configured to go through the TSM 704***"— *e.g.*, all I/O paths from/to the secure user processor also

pass through the cryptographic engine. *Id.*, 9:63-66. Thus, taken together, these statements from Marek describe that any I/O path between the untrusted host and the SCM that provides I/O from/to the ACE path goes through the TSM— *e.g.*, any data communicated along an I/O path between the secure user processor and the non-secure user processor passes through the cryptographic engine. *See also id.*, 10:36-39 ("I/O paths 730 between the untrusted host and the SCM 702 are managed by a low power Field-Programmable Gate Array (FPGA) and a dedicated TSM partition"), 9:31-36 ("The TSM 704 may include a trusted processor 705 for providing a brick-wall partitioning of memory, time, and device resources, and enforcing predetermined securing policies").

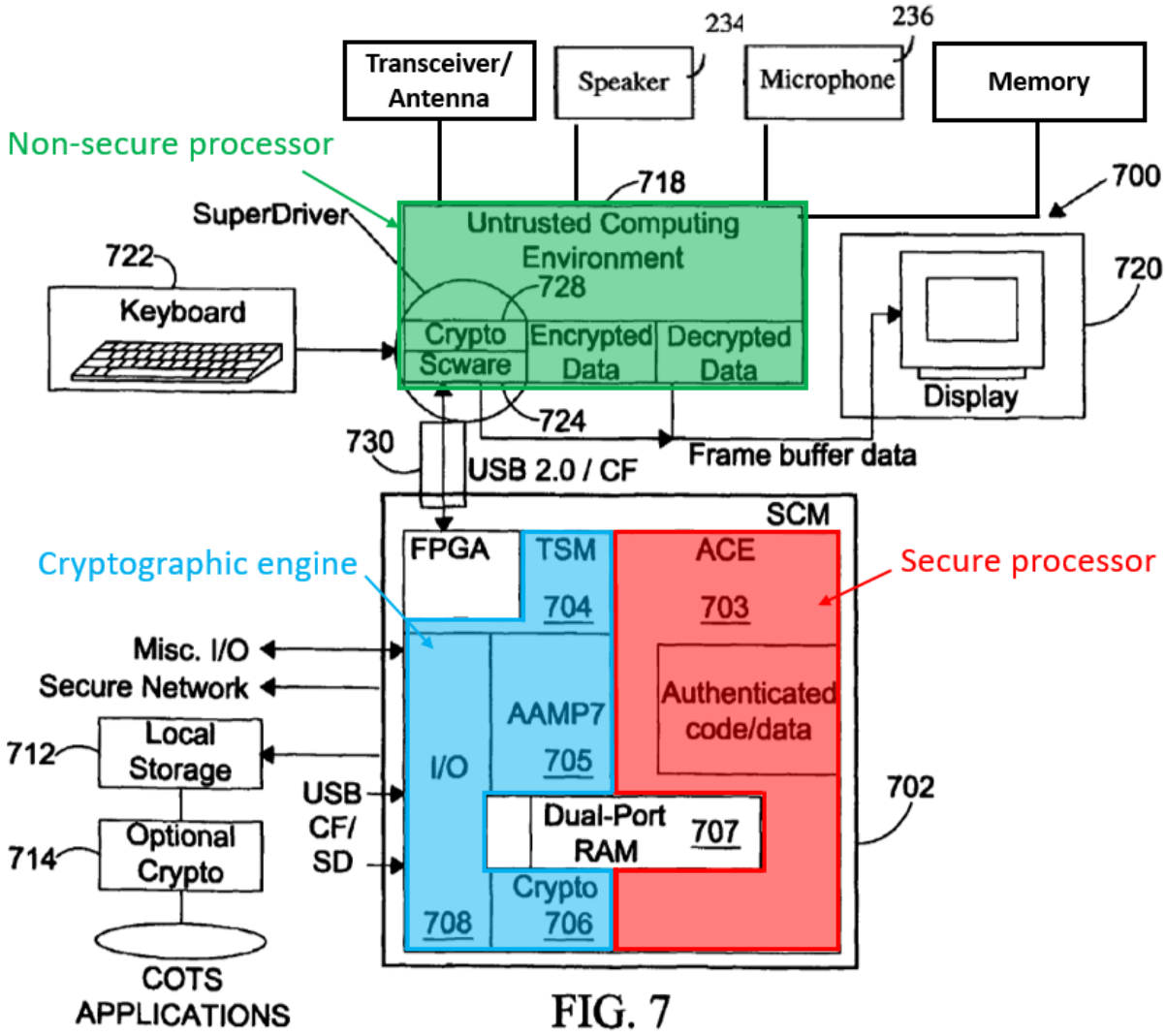


FIG. 7

Marek-Skarine composite figure

89. Also in the Marek-Skarine combination system, **the cryptographic engine is configured to encrypt any data** communicated along these I/O paths, *e.g.*, to **encrypt any data communicated between the secure user processor (red) and the non-secure user processor (green)**, as I discuss in the following paragraphs.

90. In the cryptographic engine of the Marek-Skarine combination system (*e.g.*, in Marek's TSM), Marek's trusted processor 705 "provides … partitioning" and "enforc[es] predetermined security policies," *e.g.*, such that "[e]ach I/O path … [is] secured and authenticated." APPLE-1004 (Marek), 9:31-33, 9:48-52. That is, each I/O path that passes through the TSM (including the I/O paths between the secure user processor and the non-secure processor) is "***secured and authenticated***" by Marek's TSM, *e.g.*, by the cryptographic engine of the combination. APPLE-1004 (Marek), 9:52; *see* 10:35-39 ("I/O paths 730 between the untrusted host and the SCM 702 are managed by a low power Field-Programmable Gate Array (FPGA) and a dedicated TSM partition, allowing for any number of strict ***authentication protocols***").

91. Also in the cryptographic engine of the Marek-Skarine combination system (*e.g.*, in Marek's TSM), Marek's cryptographic engine 706 "aid[s] the trusted processor 705 to provide a robust security interface" by implementing "***cryptography***," which "is the widely used means for protecting information confidentiality and integrity." APPLE-1004 (Marek), 9:40-45; *see id.* ("The cryptographic engine 706 may include a reprogrammable cryptographic engine"), 10:31-35 ("AAMP7 microprocessor provides ***a robust security interface between the red domain and the black domain through Janus Crypto Engine***").

92. A cryptographic engine encrypts data. *See* APPLE-1016 (SanDisk), [0008] ("a hardware based cryptographic engine for encrypting and/or decrypting data as it passes through the secure controller"); APPLE-1017 (Macchi), 8:23-26 ("encryption of the SMS messages is implemented, by providing the sender and the receiving MSs with an SMS message cryptographic engine capable of encrypting/decrypting the SMS messages to be sent/received, based on a specified cryptographic algorithm, working with encryption/decryption keys").

93. It is my opinion that a POSITA would have understood or at least found it obvious in light of the function of a cryptographic engine (*i.e.*, to encrypt data, as I discussed in the previous paragraph) and his/her knowledge that Marek's cryptographic engine 706 "aid[s] the trusted processor" in its securing and authenticating of the I/O paths (*see* APPLE-1004 (Marek), 9:40-52) by encrypting data communicated along those I/O paths.

94. Because these I/O paths include I/O paths between the secure user processor and the non-secure user processor, as I discussed above, the cryptographic engine of the combination (*e.g.*, Marek's TSM) thus **is configured for encrypting any data communicated from the secure user processor to the non-secure user processor**, or at least a POSITA would have found this to be obvious.

95. Alternatively or additionally, it is my opinion that a POSITA would have found it obvious for the cryptographic engine of the combination be configured specifically for encrypting **any data communicated from the secure user processor to the non-secure user processor**. For instance, I believe that configuring Marek's TSM to encrypt ***any*** data on the I/O paths would have been a straightforward design choice to, *e.g.*, maximize security, and the hardware (*e.g.*, Marek's TSM) with this capability is already in place (*e.g.*, the capability to secure and authenticate the data on every "I/O path," APPLE-1004 (Marek), 9:48-52). Indeed, I note that a cryptographic engine generally capable of encrypting data performs the same function as a cryptographic engine encrypting any data, without producing any unexpected results.

The cryptographic engine of the combination has a processor and an operating system executing on the processor

96. In the Marek-Skarine combination system, the cryptographic engine (*e.g.*, Marek's TSM 704) includes **a trusted cryptographic processor**. Specifically, Marek's TSM 704 includes "***a trusted processor 705***" and "***a cryptographic engine 706***," which "may aid the trusted processor 705 to provide a robust security interface. APPLE-1004 (Marek), 9:31-41; *see* 10:12-14 ("the trusted processor 705 may include ***ROCKWELL COLLINS AAMP7™ microprocessor*** and the like"), 10:31-35 ("The cryptographic engine 706 of the SCM 702 may include ***ROCKWELL COLLINS Janus Crypto Engine***, and the like."). Each of the

trusted processor 705 and the cryptographic engine 706 of the combination's cryptographic engine (*e.g.*, of the TSM 704) is **a trusted cryptographic processor**.

97. Moreover, it is my opinion that a POSITA would have understood or found obvious that the cryptographic engine of the combination (*e.g.*, Marek's TSM) includes **a trusted operating system executing on the trusted cryptographic processor**, as I discuss in the following paragraphs.

98. First, it is my opinion that a POSITA would have understood or found obvious that there is **an operating system executing on the cryptographic processor** (*e.g.*, on Marek's trusted processor 705) given Marek's disclosure of the functionality of the trusted processor 705. Marek states that the trusted processor "provid[es] a brick-wall partitioning of memory, time, and device resources, and enforcing predetermined security policies." APPLE-1004 (Marek), 9:31-34; *see also* 9:38-40 ("Memory and I/O resources in the SCM 702 are strictly partitioned and managed by several secure TSM partitions"), 10:14-30 ("AAMP7 microprocessor is configured to manage the untrusted host and ACE interfaces through predetermined security policies"). These functions are functions that I believe a POSITA would have understood to be provided by an operating system executing on the trusted processor 705: namely, functions that relate generally to controlling the operation and/or resources of the trusted processor. That these functions are

provided by an operating system is corroborated by at least the following references: APPLE-1009 (Mathur), 7:57-61 ("The kernel module 214 represents the ***base operating system functionality*** that must be present on all platforms. The kernel module includes ***memory management***, ***process management***, exception handling, and support for multitasking and multithreading."); APPLE-1019 (Thornton), 4:8-21 ("The term "kernel" refers to any form of ***code executing on a processor to control the operation of a computing system***, including without limitation traditional operating system kernels, such as the kernels of the WINDOWS® family of operating systems available from Microsoft Corporation."); APPLE-1020 (Kahandaliyanage), 1:23-26 ("The operating system of a mobile device provides an application programming interface (API) that provides ***access to data*** which may be sensitive and ***a task manager for controlling application execution***."); APPLE-1021 (Oe), 13:35-37 ("The general-purpose OS 201 comprises ***resources 2011 managed by the OS*** and APIs 2012 provided by the OS to the application 2021").

99. Moreover, I note that it was well known in the art as of the Critical Date for mobile device processors to have operating systems. *See* APPLE-1005 (Skarine), [0038] ("Operating system software used by microprocessor 238 is preferably stored in a persistent store such as flash memory 224, which may alternatively be a read-only memory (ROM) or similar storage element (not shown).

Those skilled in the art will appreciate that the operating system … may be temporarily loaded into a volatile store such as RAM 226"); APPLE-1009 (Mathur), 1:64-2:3 ("specialized operating systems capable of running in the resource-limited environment of the embedded system have been developed. An example of such an operating system is; the Windows CE™ operating system from Microsoft Corporation."); APPLE-1010 (Zuberec), 3:17-19 ("The mobile device 100 includes an operating system 164, such as the Windows CE operating system from Microsoft Corporation or other such operating system, which is resident in the memory 162 and executes on the processor 160."); APPLE-1011 (Huang), 4:59-61 ("During operation, the operating system 30 is loaded into, and executed by, the processor 20 from memory 22. The operating system 30, in one embodiment, is a Windows CE brand operating system commercially available from Microsoft Corporation. The operating system 30 can be designed for mobile devices"); APPLE-1018 (Yach), 3:58-64 ("Operating system software used by the microprocessor 102 is typically stored in a persistent store such as the flash memory 108").

100. Given (1) the overlap between the functionality of Marek's trusted processor 705 and the conventional functionality of an operating system, and (2) it was well known that mobile device processors have operating systems, it is my opinion that a POSITA would have understood or found obvious that Marek's trusted processor 705 has an operating system executing thereon, *e.g.*, that **the**

cryptographic engine of the combination **has a trusted operating system executing on the trusted cryptographic processor**.

101. Alternatively or additionally, it is my opinion that a POSITA would have understood or found obvious that there is **an operating system executing on the cryptographic processor** (*e.g.*, on Marek's cryptographic engine 706) given Marek's disclosure of the functionality of the cryptographic engine 706. Marek describes that the cryptographic engine 706 is "a reprogrammable cryptographic engine" implementing "cryptography … for protecting information confidentiality and integrity." APPLE-1004 (Marek), 9:40-47. This is a function that I believe a POSITA would have understood to be provided by an operating system executing on the TSM, *e.g.*, on the cryptographic engine 706. *See*, *e.g.*, APPLE-1022, 3:5-26 ("***crypto operating system 100 is capable of encrypting data*** opened by an application before storage to a device or decrypting encrypted data requested by the application after the encrypted data is read from the storage device according to the state of the application. File management system 20 instructs crypto driver 30 to perform encryption or decryption."); APPLE-1023, [0052]-[0054] (describing "an ***Encrypting Operating System (EOS)" that "encrypt[s] and decrypt[s]*** both the contents and the names of any data it is managing or storing").

102. Moreover, I note that it was well known in the art as of the Critical Date for mobile device processors to have operating systems, as I discussed earlier

in this section, and specifically it was well known for cryptographic engines in mobile devices to have operating systems. *See* APPLE-1006 (Orsini), 17:32-48 ("the cryptographic engine 220 comprises an operating system 605").

103. Thus, given (1) the overlap between the functionality of Marek's cryptographic engine 706 and the conventional functionality of an operating system, and (2) it was well known that cryptographic engines have operating systems, it is my opinion that a POSITA would have understood or found obvious that Marek's cryptographic engine 706 has an operating system executing thereon, *e.g.*, that **the cryptographic engine** of the combination **has a trusted operating system executing on the trusted cryptographic processor**.

104. The processor and operating system of the cryptographic engine of the Marek-Skarine combination system are **trusted** (or at least a POSITA would have found this to be obvious) at least because they are part of the "Secure COTS computing environment" provided by the SCM 702. APPLE-1004 (Marek), 8:37-39; *see* 8:39-45, 1:66-2:4 ("a system including a Secure Computing Module (SCM) provides trusted environment for COTS host platforms. Only authenticated trusted applications execute on the SCM."), 2:31-38 ("the system including the SCM may provide trusted and portable COTS computing environments against malware").

[1e] a first data communication link communicating data between said secure processor and said cryptographic engine;

105. In the Marek-Skarine combination system, Marek describes that "any I/O from/to the ACE 703 is configured to go through the TSM 704," and thus that data is communicated between the ACE 703 (containing the secure processor, and highlighted in red in the composite figure below) and the TSM 704 (the cryptographic engine; highlighted in blue). APPLE-1004 (Marek), 9:63-66. Given that data is communicated between the secure processor and the cryptographic engine, it is my opinion that a POSITA would have understood there to be **a first data communication link** (highlighted in purple) **communicating data between the secure processor and the cryptographic engine**. For instance, a POSITA would have understood this to be the case to enable the disclosed I/O between the ACE 703 and the TSM 704 to occur. *See* APPLE-1004 (Marek), 9:63-64 ("any I/O from/to the ACE 703 is configured to go through the TSM 704"), 9:52-54 ("All ACE I/O's are controlled by the TSM 704 and any I/O from/to the ACE 703 is configured to go through the TSM 704"), 9:50-56 ("Each I/O path of the SCM 702 is configured to go through the TSM 704").

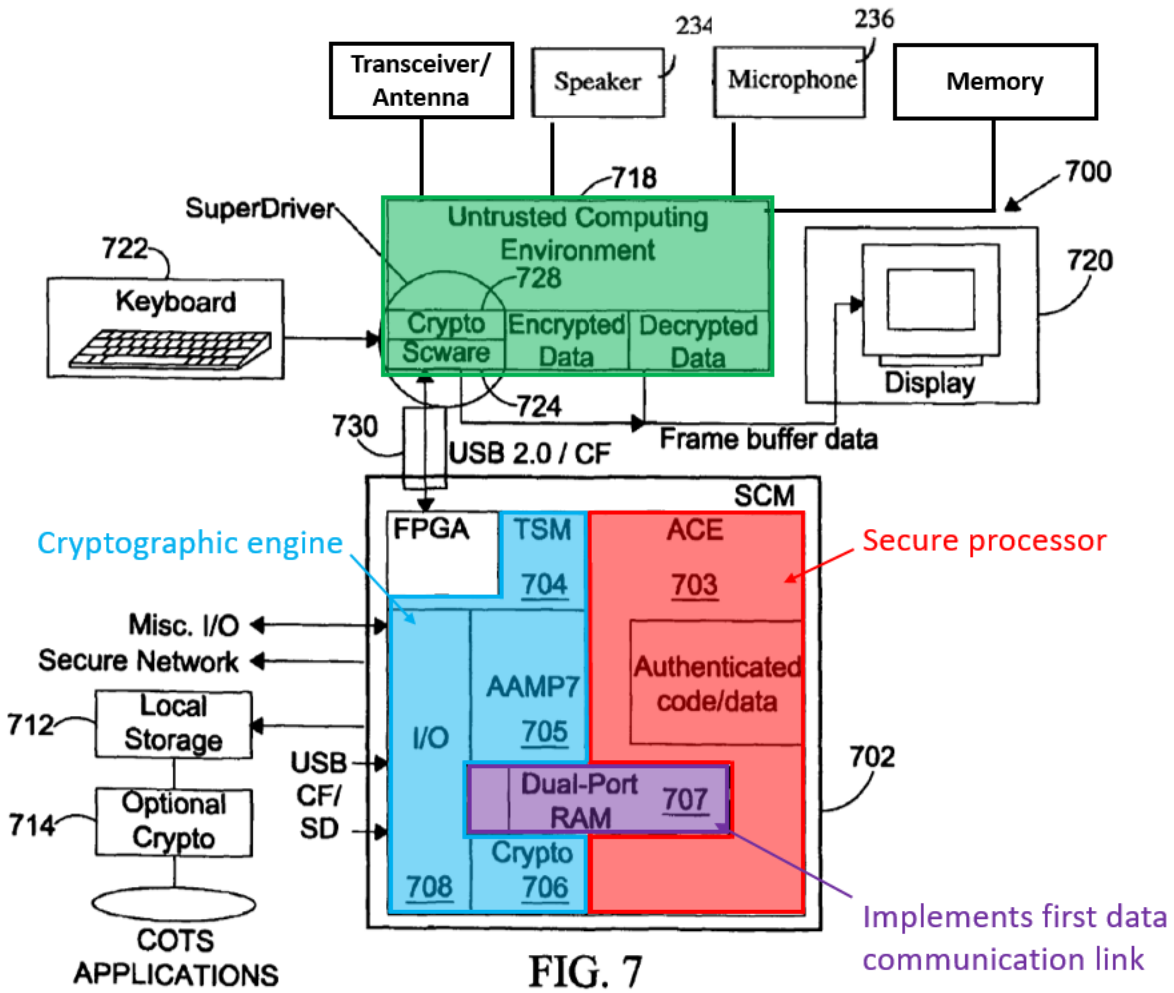


FIG. 7

Marek-Skarine composite figure

106. In a specific implementation, Marek describes that "I/O paths between the TSM 704 and the ACE 703 may include ***virtual I/O paths***." APPLE-1004 (Marek), 9:66-67. These virtual I/O paths are **a first data communication link communicating data between the secure processor** (contained in the ACE 703) **and the cryptographic engine** (the TSM 704). In particular, Marek describes that "the virtual I/O paths between the TSM and the ACE may be implemented through a dual port RAM 707," highlighted in purple, "with each I/O path and a memory-

mapped resource being controlled by a dedicated TSM partition." APPLE-1004 (Marek), 9:67-10:4. That is, in one implementation of the combination, Marek's **a first data communication link**, *e.g.*, the virtual I/O paths, **between the secure processor and the cryptographic engine** is implemented via Marek's RAM 707.

[1f] a second data communication link communicating data between said non-secure processor and said cryptographic engine;

107. Marek describes that "[e]ach I/O path of the SCM 702 is configured to ***go through the TSM 704***," *e.g.*, through the cryptographic engine of the combination. APPLE-1004 (Marek), 9:50-51. Moreover, Marek specifies that "[e]xamples of I/O paths of the SCM 702 include ***I/O paths between the untrusted host and the SCM***," such as I/O paths 730. APPLE-1004 (Marek), 9:50-54, 10:36-37. That is, the I/O paths 730 between the untrusted host (which contains the non-secure processor) and the SCM "go through the TSM 704," *e.g.*, through the cryptographic engine, and thus are I/O paths for data communication between the non-secure processor and the cryptographic engine. APPLE-1004 (Marek), 9:48-64. These I/O paths 730, highlighted in purple in the composite figure below, are **a second data communication link communicating data between the non-secure processor and the cryptographic engine**.

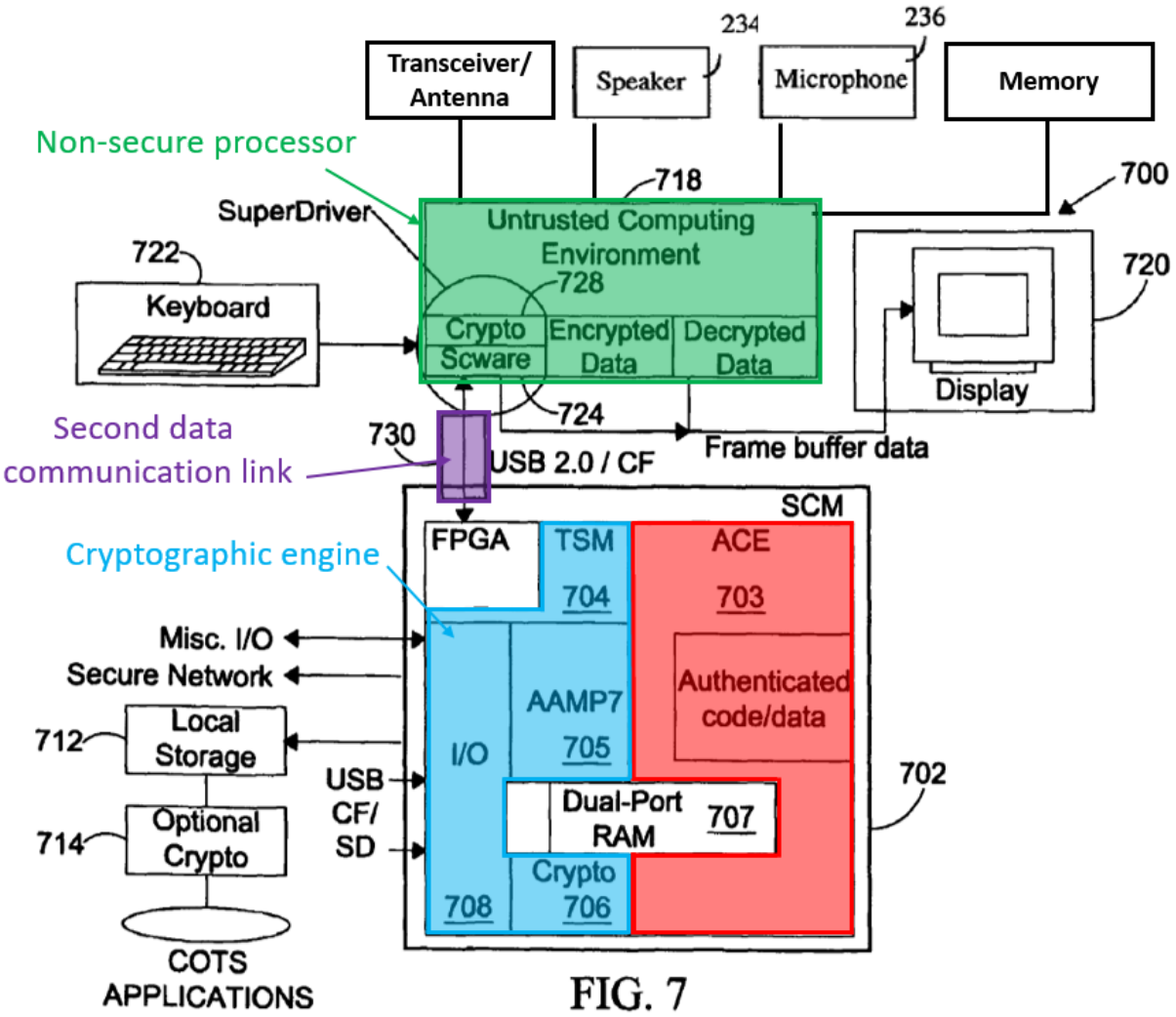


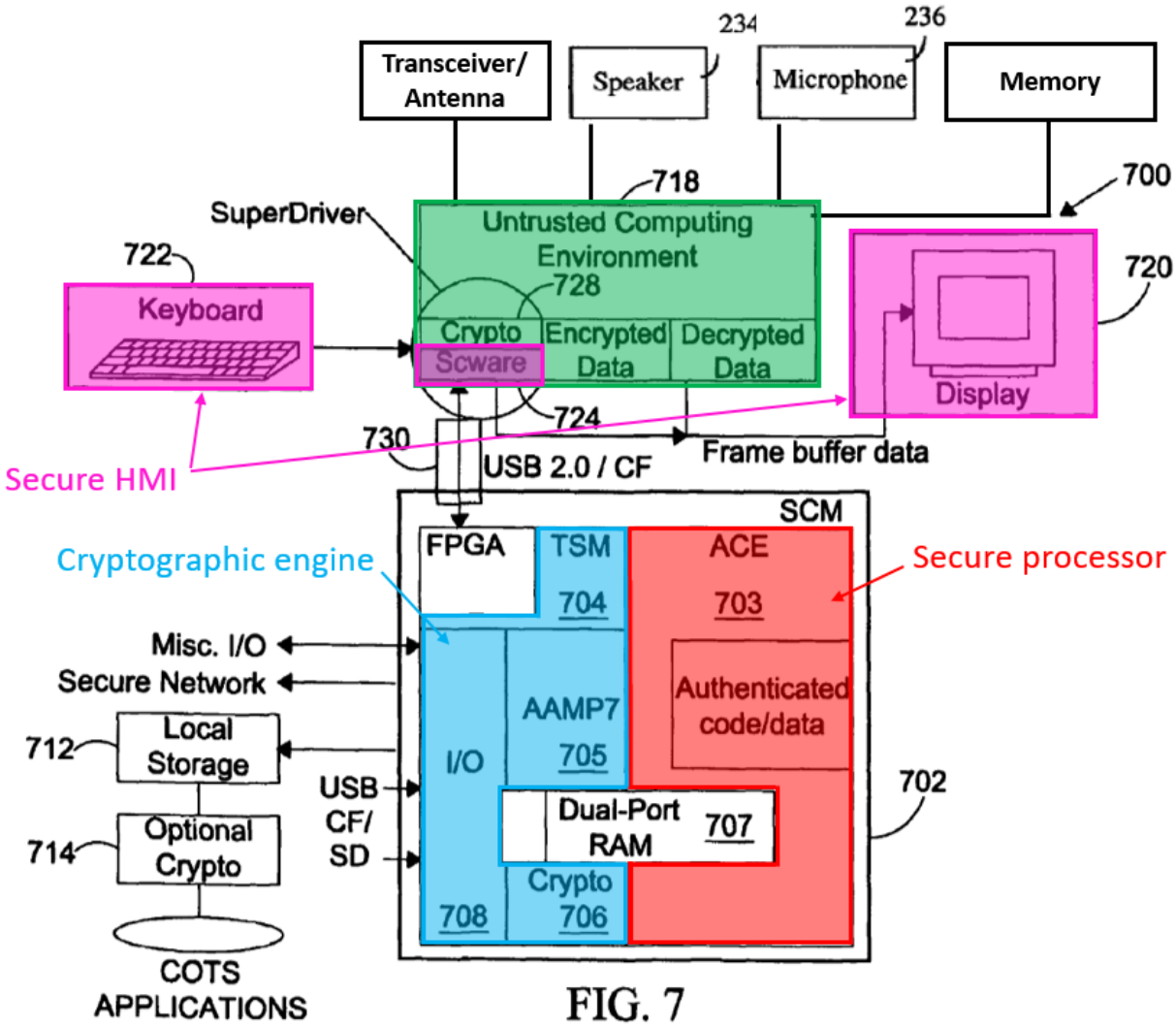
FIG. 7

Marek-Skarine composite figure

[1g] a secure human/machine interface configured for enabling bi-directional communication of classified information exclusively between a user and said secure user processor; and

108. Marek's untrusted host mobile device 718 includes "***input and output devices*** 722, 720," such as a keypad and display of the PDA or cell phone. APPLE-1004 (Marek), 10:50-51. In the Marek-Skarine combination system, the input and output devices of the mobile device 718, which I have highlighted in pink in

the composite figure below, are **a secure human/machine interface**, as I discuss in the following paragraphs.



Marek-Skarine composite figure

109. Marek's computing environment includes Scware 724, which is "software that acts as a trusted agent for the SCM 702 on the untrusted host environment." APPLE-1004 (Marek), 10:42-45. The Scware "resides on the untrusted host environment while the SCM 702 is operating" and, "in conjunction with the

TSM 704 ***creates secure I/O paths 730 of input and output devices 722, 720*** of the untrusted host 718." APPLE-1004 (Marek), 10:42-51. Specifically, "[t]he Scware 724 ***manages input from an input device*** (e.g. keyboard) ***and output to an output device*** (e.g. display device) while the host OS is completely bypassed." *Id.*, 10:60-65; *see* 10:52-54 ("the input and output devices 722, 720 of the untrusted host may be utilized as a virtual input/output system 800 of the SCM."), Fig. 7 and 8. That is, when the SCM 702 is in operation, information input into the input device 722 (*e.g.*, by a user) bypasses the untrusted host 718 and instead is provided to the SCM 702 along a secure I/O path 730; similarly, information from the SCM 702 is provided to the output device 720 (and thus to a user) via a secure I/O path 730, again bypassing the untrusted host 718.

110. In the Marek-Skarine combination system, Marek's input and output devices 722, 720 can be considered to be **a secure human/machine interface** at least because they are an interface by which a user inputs information to the SCM 702 (via the input device 722) and receives information from the SCM 702 (via the output device 720). *See* APPLE-1004 (Marek), 10:42-62, This interface enables **bi-directional communication of information**, *e.g.*, communication from the user to the SCM and from the SCM to the user. *See id.*, 10:42-62.

111. In the Marek-Skarine combination system, the secure human/machine interface enables bi-directional communication of information **between a user and**

the secure user processor, *e.g.*, between a user and the processor of the ACE 703 (highlighted in red in the composite figure above), as I discuss in the following paragraphs.

112. First, Marek generally describes that the input and output devices 722, 720, *e.g.*, the secure human/machine interface, enable communication between a user and the SCM 702, which contains the ACE. *See* APPLE-1004 (Marek), 10:49-51 ("The Scware 724 implemented in conjunction with the TSM 704 creates ***secure I/O paths 730*** of input and output devices 722, 720 of the untrusted host"), 10:52-54 ("the input and output devices 722, 720 of the untrusted host 718 may be utilized as ***a virtual input/output system 800 of the SCM***"), 11:39-41 ("a virtual keyboard and display usable for ***user interface with the SCM***"), Figs. 7 and 8.

113. Second, it is my opinion a POSITA would have understood or at least found obvious that the described communication between the user and the SCM is specifically **between the user and the secure user processor** of the ACE 703. For instance, I believe that a POSITA would have understood or at least found obvious that such communication would occur, *e.g.*, to enable information from a user to be provided as input to the "COTS applications, manufacturer-supplied software and the like" of the ACE and information generated by the applications/software of the ACE to be provided as output to a user. APPLE-1004 (Marek), 9:13-14. Additionally, I believe that a POSITA, given Marek's disclosure

that "[e]ach I/O path of the SCM 702 is configured to ***go through the TSM***," and moreover that "any I/O from/to the ACE 703 is configured to ***go through the TSM***," would have recognized or at least found obvious that the I/O paths that go through the TSM extend to the ACE, *e.g.*, the I/O paths are **between the user and the secure user processor** of the ACE. APPLE-1004 (Marek), 9:50-51, 9:63-64; *see* 10:49-51.

114. Moreover, the communication of information enabled by the secure human/machine interface is **exclusively** between the user and the secure user processor, or at least a POSITA would have found this to be obvious. In Marek's "H-mode" operation, "[t]he Scware 724 manages input from an input device (e.g. keyboard) and output to an output device (e.g. display device) ***while the host OS is completely bypassed***. As a result, the Scware 724 operates as ***a dedicated input/output device driver***." *Id.*, 10:55-65; *see* 10:65-67 ("a security critical section concept is used to implement the Scware 724 in H-mode ***to disable all applications but the Scware 724 on the host environment***"). Marek also describes that "[i]n the autonomous execution state, ***the host's only function is to provide power*** to the SCM 702. Alternatively, ***the host may not provide any functions at all*** if the SCM 702 provides its own power source." *Id.*, 11:31-36. That is, when the SCM 702 is operational, the operating system of the untrusted host device is "completely bypassed," with all functionality other than providing power being disabled. *Id.*,

10:60-65, 11:31-36. Thus, at least because the functionality of the untrusted host device is disabled, the communication enabled by the secure human/machine interface is **exclusively between the user and the secure user processor**, or at least this would have been obvious to a POSITA.

115. This secure human/machine interface is **secure** (or at least a POSITA would have found this to be obvious) at least because it is an interface to the "***Secure COTS computing environment***" provided by the SCM 702 of the combination. APPLE-1004 (Marek), 8:37-39; *see* 8:39-45, 1:66-2:4 ("a system including a Secure Computing Module (SCM) provides ***trusted environment*** for COTS host platforms. Only authenticated trusted applications execute on the SCM."), 2:13-20 ("The ACE may be secured by authenticating all code and data used for running COTS applications."), 2:31-38 ("the system including the SCM may provide trusted and portable COTS computing environments against malware").

116. The secure human/machine interface enables communication of **classified information**[5] in that the information is communicated along "secured and

[5] I understand that there is disagreement in the co-pending litigation regarding the interpretation of the term "classified." I address this term here and elsewhere in this Petition as I best understand it and without conceding that its meaning is clear.

authenticated" I/O paths and is encrypted by Marek's cryptographic engine. APPLE-1004 (Marek), 9:50-52; *see* 9:37-44. To the extent that "classified information" is interpreted to refer specifically to, *e.g.*, information designated as implicating matters of national security, Marek describes that the TSM processor 705 "provides a robust security interface between ***the red domain and the black domain*** through" the cryptographic engine 706— *e.g.*, between the SCM and the untrusted host mobile device 718. APPLE-1004 (Marek), 10:33-36. Information communicated between a user and the red domain (Marek's SCM) can be **classified information**.

[1h] a non-secure human/machine interface distinct from said secure human/machine interface and configured for enabling bi-directional communication of unclassified information exclusively between said user and said non-secure user processor;

117. In the Marek-Skarine combination system, the untrusted host mobile device 718 includes a speaker and a microphone, which I have highlighted in orange in the composite figure below. This was a well-known and conventional configuration in the art, as demonstrated, for instance, by Skarine. *See* APPLE-1005 (Skarine), [0038] ("Mobile device 202 includes a microprocessor 238 … [that] interacts with additional device subsystems such as … a speaker 234 [and], a microphone 236"), [0042] ("For voice communications, the overall operation of mobile device 202 is substantially similar, except that the received signals would be output to speaker 234 and signals for transmission would be generated by microphone

236"), Fig. 2; *see also* APPLE-1018 (Yach), 3:45-50 (describing a microprocessor of a mobile device that "interacts with additional subsystems such as … a speaker 118 [and] a microphone 120"), 6:22-32; APPLE-1010 (Zuberec), 3:54-67; APPLE-1024 (Lu), [0004]; APPLE-1025 (Song), 1:18-20.

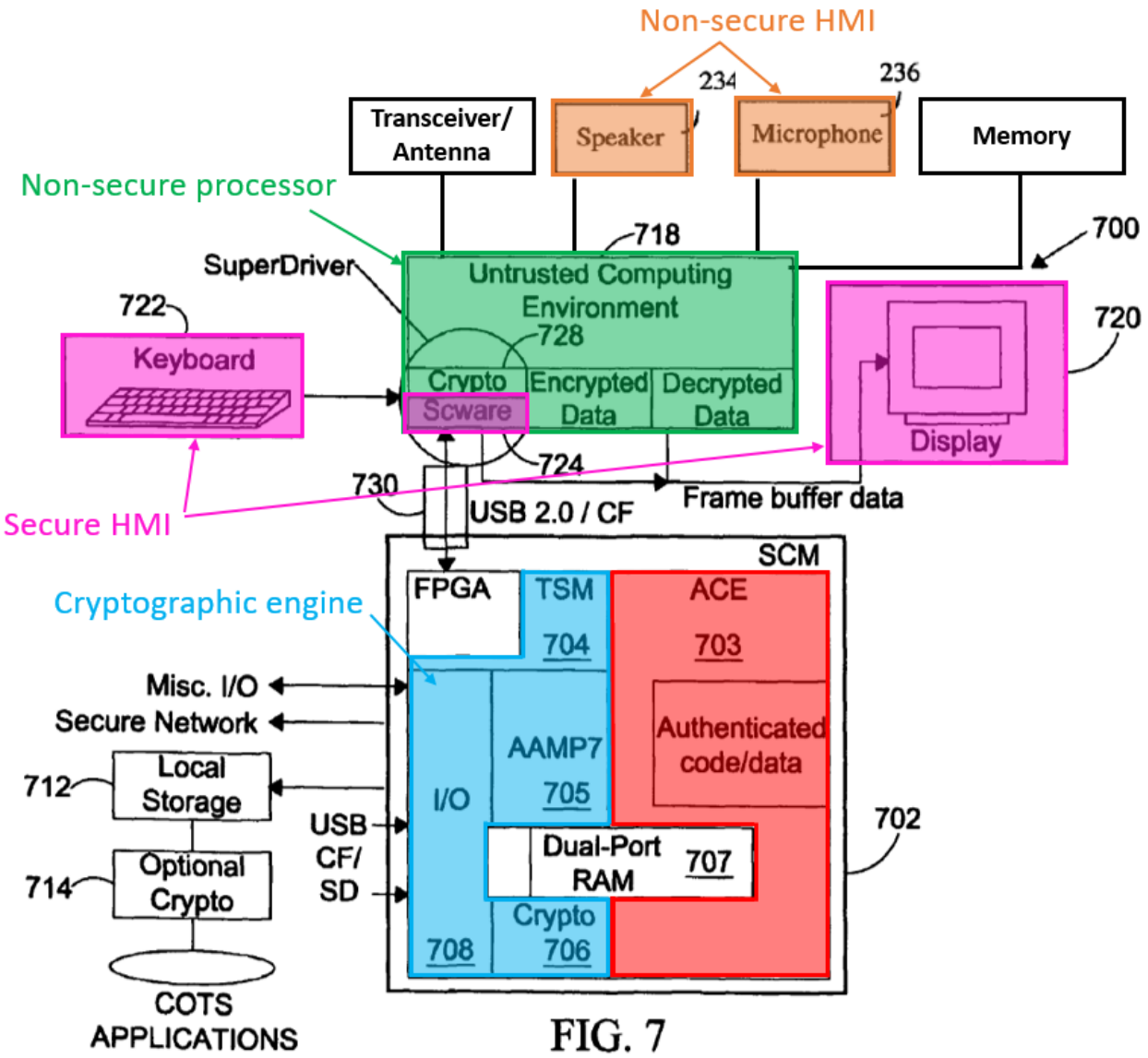


FIG. 7

Marek-Skarine composite figure

118. The speaker and microphone together are **a non-secure human/machine interface** at least because they are an interface by which a user inputs information to and receives information from the untrusted host mobile device 718 (via the microphone and speaker, respectively), as I discuss in the following paragraphs. *See* APPLE-1005 (Skarine), [0041]-[0042].

119. The non-secure human/machine interface is **distinct from the secure human/machine interface**. For instance, the speaker and microphone (the non-secure human/machine interface) are components that are distinct (*e.g.*, physically separate) from the input and output devices 722, 720 (the secure human/machine interface; *see* my analysis of element [1g]), as illustrated in the figure above.

120. The non-secure human/machine interface, *e.g.*, the speaker and microphone, is **configured for enabling bi-directional communication of information between said user and said non-secure user processor**. In the Marek-Skarine combination system, based on the teachings of Skarine, information is communicated from the processor of the untrusted host mobile device to the speaker, and from the microphone to the processor. *See* APPLE-1005 (Skarine), [0041]-[0042] ("For voice communications, the overall operation of mobile device 202 is substantially similar" to the operation in "data communication mode," where signals are communicated between a user and Skarine's mobile device processor via input and output devices.), [0038] ("Microprocessor 238 also interacts with additional

device subsystems such as … a speaker 234, a microphone 236"), Fig. 2. Additionally, signals from the speaker are communicated to a user, and audio input from a user are received by the microphone. *See* APPLE-1005 (Skarine), [0042] ("the received signals would be ***output to speaker 234*** and ***signals for transmission would be generated by microphone 236***," "voice or audio signal output is preferably accomplished primarily through speaker 234"). That is, the speaker and microphone enable **bi-directional communication of information between the user and the non-secure user processor** (*e.g.*, the processor contained in the untrusted host mobile device 718, highlighted in green).

121. Moreover, the non-secure human/machine interface, *e.g.*, the speaker and microphone, is configured for enabling communication of information **exclusively** between the user and the non-secure processor. As described by Marek, "[e]ach I/O path 702 of the SCM 702 is configured to go through the TSM 704." APPLE-1004 (Marek), 9:50-51. Based on the teachings of Skarine, the microphone and speaker are connected to the non-secure user processor of the untrusted host mobile device, and not to the SCM or the TSM. Thus, the information is not communicated between the speaker/microphone and the secure user processor; rather, it is communicated **exclusively between the user and the non-secure processor**.

122. The non-secure human/machine interface is **non-secure** (or at least a POSITA would have found this to be obvious) at least because it is part of "the untrusted host environment" of the combination. APPLE-1004 (Marek), 8:40-41; *see* 8:56-59 ("a host platform employing COTS processors is assumed to be ***untrusted***"), 12:16-18 ("Untrusted application software and hardware may be implemented in the PDA"), 2:1-4, 2:36-38.

123. The non-secure human/machine enables communication of **unclassified information**[6] because the information communicated between the speaker/microphone and the processor of the untrusted host mobile device 718 is not transmitted on the "secured and authenticated" I/O paths provided by Marek's TSM, nor is it subject to the encryption provided by Marek's cryptographic engine. *See* APPLE-1004 (Marek), 9:40-53. To the extent that "unclassified information" is interpreted to refer specifically to, *e.g.*, information designated as not implicating matters of national security, the untrusted host mobile device is in the black domain of Marek's computing environment. *See* APPLE-1004 (Marek), 10:33-36, Figs. 9-11.

[6] I understand that there is disagreement in the co-pending litigation regarding the interpretation of the term "unclassified." I address this term here and elsewhere in this Petition as I best understand it and without conceding that its meaning is clear.

Information remaining in the black domain of such an environment— *e.g.*, information communicated via the non-secure human/machine interface—can be **unclassified information**.

[1i] wherein said communications transceiver is operatively coupled to said non-secure user processor and configured for communicating data external to said portable mobile computing device.

124. In the Marek-Skarine combination system, **the communications transceiver is operatively coupled to the non-secure user processor** based on the teachings of Skarine, as I have illustrated in the composite figure below. *See* APPLE-1005 (Skarine), [0038], Fig. 2 (illustrating a mobile device, such as a cellular telephone or a PDA in which the receiver 212 and transmitter 214, *e.g.*, a communications transceiver, are coupled to the microprocessor 238).

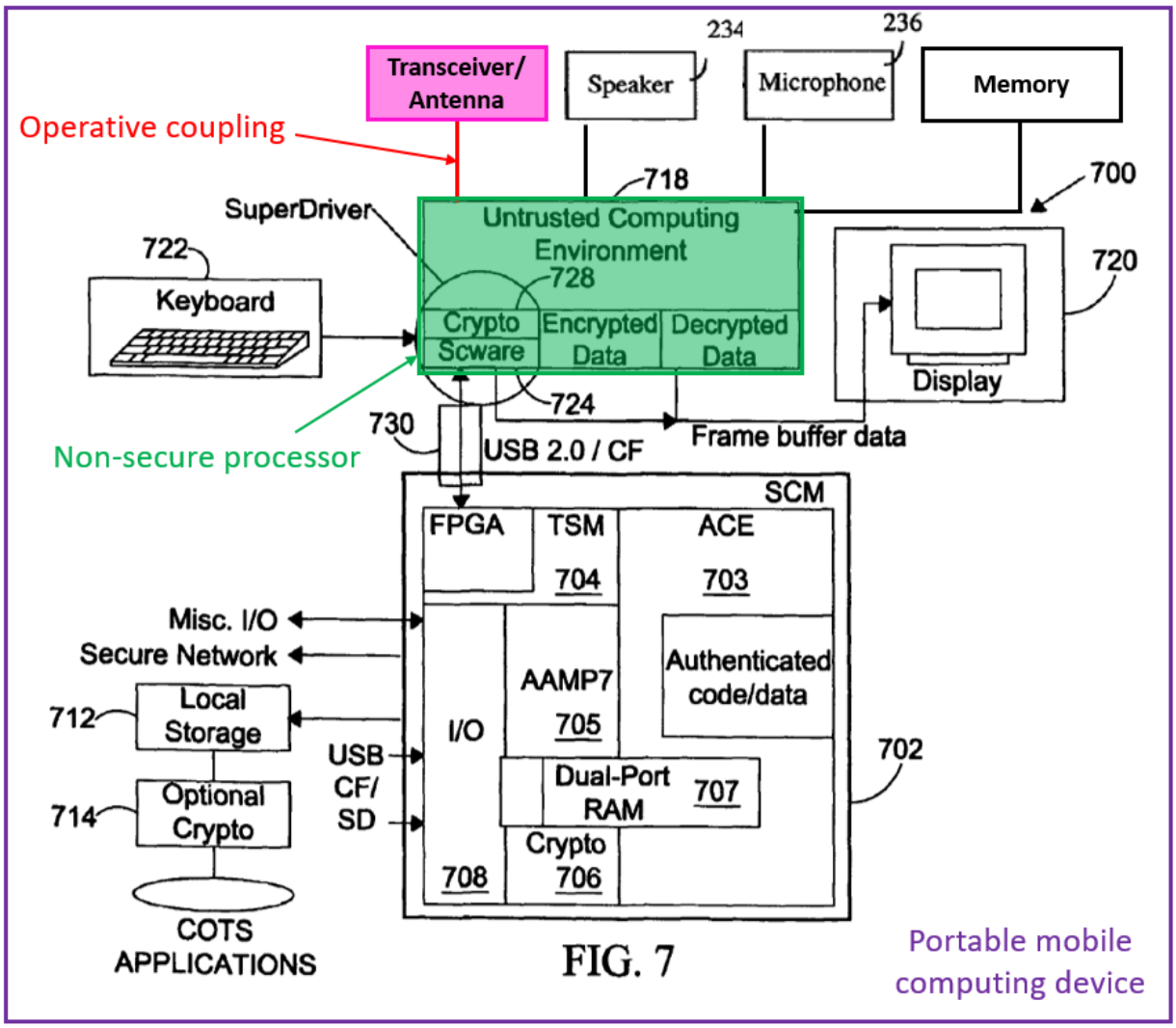


FIG. 7

Marek-Skarine composite figure

125. It is my opinion that a POSITA would have understood or found obvious that the **communications transceiver is configured for communicating data external to the portable mobile computing device**. For instance, this was a standard and well-known function of communications transceivers as of the Critical Date. *See* APPLE-1005 (Skarine), [0022] ("signal processing operations associated with ***communication functions are typically performed in RF transceiver***

circuitry 108"), [0023] ("Mobile device 102 sends communication signals to and receives communication signals from network 104 over a wireless link via antenna 110. RF transceiver circuitry 108 performs functions such as modulation/demodulation and possibly encoding/decoding and encryption/decryption. It will be apparent to those skilled in art that ***RF transceiver circuitry 108 will be adapted to particular wireless network or networks*** in which mobile device 102 is intended to operate."), [0038] ("***Communication functions, including at least data and voice communications, are performed through communication subsystem 211***," which includes a communications transceiver.), [0027]-[0029], [0035]; APPLE-1015 (Ramirez), 3:11-17 (describing a mobile device having a "WAN modem 111 [that] includes a ***primary receiver and transmitter (primary transceiver) that are configured to operate on or with a first, e.g., WAN, network***."); APPLE-1011 (Huang), 5:11-13 ("***The wireless transceiver 27 transmits speech signals … over wireless transport*** 14 using antenna 11," where "wireless transport 14 can be a paging network, cellular digital packet data (CDPD), FM-sideband, or other suitable wireless communications"), 4:46-59; APPLE-1017 (Macchi), 10:14-18 ("As known in the art, the MS 120 may be viewed as the combination of a user terminal (typically, a mobile phone) and a Subscriber Identity Module (SIM). The user terminal comprises … ***specific elements allowing radio communications with the BTSs*** [Base

Transceiver Stations] in accordance to the GSM specifications"); APPLE-1018 (Yach), 6:33-45, 7:11-29.

(ii) Claim 2

[2] The computer system according to claim 1, wherein said secure human/machine interface comprises at least one input device to allow said user to control the secure user processor.

126. In the Marek-Skarine combination system, the secure human/machine interface includes the input and output devices 722, 720 (*e.g.*, the keypad and display of the mobile device). *See* my analysis of element [1g]. The input device, *e.g.*, a keypad, is an **input device that allows the user to control the secure processor**. Input received from a user through the input device, *e.g.*, keypad, is provided to the secure user processor. *See* APPLE-1004 (Marek), 9:13-14, 9:50-64, 10:49-54, 11:39-41; *see* my analysis of element [1g]. Moreover, "COTS applications [and] manufacturer-supplied software" execute on Marek's ACE, *e.g.*, on the secure user processor. APPLE-1004 (Marek), 9:13-15; *see* 2:31-42, 12:18-19 ("trusted applications are implemented in the SCM 908"); *see* my analysis of element [1b]. It is my opinion that a POSITA would understand that when the received input is information used during execution of one of the applications or software on the secure user processor, that input **controls the secure user processor**.

(iii) Claim 3

[3] The computer system according to claim 2, wherein said secure human/machine interface comprises at least one output device to allow the secure user processor to inform said user.

127. In the Marek-Skarine combination system, the secure human/machine interface includes the "input and output devices 722, 720," such as a keypad and display of the untrusted host mobile device. APPLE-1004 (Marek), 10:50-51; *see* my analysis of element [1g]. Information output from the secure user processor is provided to the output device, *e.g.*, the display, for presentation, thereby informing the user of that information. *See* APPLE-1004 (Marek), 10:42-54; *see* [1g]. That is, the output device 720 is **an output device that allows the secure user processor to inform the user**. For instance, information communicated from the secure user processor to the user (*see* APPLE-1004 (Marek), 10:42-54) is output on the output device, *e.g.*, displayed on the display, thereby informing the user of that information.

(iv) Claim 4

[4] The computer system according to claim 1, wherein said non-secure human/machine interface comprises at least one input device to allow said user to control the non-secure user processor.

128. In the Marek-Skarine combination system, the non-secure human/machine interface includes the microphone of the untrusted host mobile device 718. *See* my analysis of element [1h]. The microphone is **an input device that allows the user to control the non-secure user processor**. For instance, it is my opinion

that a POSITA would have understood this to be the case, or otherwise found this to be obvious, based on Skarine's description of the operation of the microphone and microprocessor of its mobile device.

129. Skarine describes that "[f]or voice communications … signals for transmission would be generated by microphone 236" and are "transmitted over a communication network through communication subsystem 211." APPLE-1005 (Skarine), [0041]-[0042]. These signals that are generated by the microphone are received by Skarine's microprocessor 238 and then provided from the microprocessor to the communication subsystem 211. *See id.*, Fig. 2. That is, a user inputting an audio signal into the microphone controls Skarine's microprocessor in that, in response to receipt of that audio signal, the microprocessor operates to provide that signal to the communication subsystem for transmission.

130. In the Marek-Skarine combination, then, based on the teachings of Skarine, a user inputting an audio signal into the microphone of the untrusted host mobile device 718 causes the non-secure user processor to provide that signal to the communications transceiver of the untrusted host mobile device 718, *e.g.*, the user controls the non-secure processor by inputting an audio signal into the microphone.

131. Additionally or alternatively, it is my opinion that a POSITA would have understood or found it obvious that the untrusted host mobile device of the

combination includes "a voice message recording subsystem," *e.g.*, as taught by Skarine. APPLE-1005 (Skarine), [0042]. For instance, I believe that a POSITA would have understood that a microphone is usable in the context of voice message recording, *e.g.*, to record a voice mail greeting. Moreover, I believe that a POSITA would have understood that the microprocessor of the mobile device facilitates capturing and storing the audio data for the voice mail greeting. Thus, the user controls the microprocessor of the mobile device in that the processor coordinates storing of data responsive to receiving user input via the microphone, *e.g.*, the user controls the microprocessor using the microphone. In the combination, the use of the microphone to record a voice mail greeting thus is user control of the non-secure processor via the microphone.

(v) Claim 5

[5] The computer system according to claim 4, wherein said non-secure human/machine interface comprises at least one output device to allow the non-secure user processor to inform said user.

132. In the Marek-Skarine combination system, the non-secure human/machine interface includes the speaker of the untrusted host mobile device 718. *See* my analysis of element [1h]. The speaker is **an output device that allows the non-secure user processor to inform the user**. For instance, it is my opinion that a POSITA would have understood that audio signals are provided from the processor of the mobile device to the speaker for output to the user, thereby allowing the

processor of the mobile device to inform the user of the audio signals, *e.g.*, as evidenced by Skarine. *See* APPLE-1005 (Skarine), [0042] ("voice or audio signal output is preferably accomplished primarily through speaker 234"), *id.* ("received signals would be output to speaker 234"), [0041]; APPLE-1009, [0033] (describing a mobile device in which "received signals are preferably be [sic] output to the speaker"); APPLE-1010, 6:5-32 ("received signals are output to the speaker").

(vi) Claim 6

[6] The computer system according to claim 1, wherein said communications transceiver is selected from the group consisting of a wireless LAN transceiver and a cellular telephone transceiver.

133. In the Marek-Skarine combination system, the communications transceiver (*see* [1a]) is **a cellular telephone transceiver**, *e.g.*, based on the teachings of Skarine. Skarine describes RF transceiver circuitry 108 that is "adapted to particular wireless network or networks in which mobile device 102 is intended to operate." APPLE-1005 (Skarine), [0023]; *see* [0035] ("particular design of communication subsystem 211 depends on the communication network in which mobile device 202 is intended to operate"). Moreover, Skarine's mobile device is "intended to operate" in a cellular telephone network. *Id.*, [0023]; *see* [0027]-[0028] ("wireless network 104 is configured in accordance with General Packet Radio Service (GPRS) and a Global Systems for Mobile (GSM) technologies," *i.e.*, cellu-

lar telephone networks (*see* APPLE-1026 (Lucidarme), [0011] ("Some second generation cellular networks (GSM, Global System for Mobile communications) now include a packet transmission service called CPRS (General Packet Radio Service)"), APPLE-1027 (Naegeli), Abstract ("Global System for Mobile Communications (GSM/GPRS) cellular telephone network"))), [0026] ("a cellular telephone"), [0034] ("a cellular telephone … [that] may communicate with any one of a plurality of fixed transceiver stations 200 within its geographic coverage area"). In the combination, the communications transceiver is designed for operation in a cellular telephone network, *i.e.*, it is a cellular telephone transceiver.

134. It is my opinion that a POSITA would have been motivated to implement the communications transceiver as a cellular telephone transceiver, *e.g.*, based on the teachings of Skarine, for at least the following reasons.

135. One reason why a POSITA would have been motivated to implement the communications transceiver as a cellular telephone transceiver is because doing so would enable the PDA to be used for communications via a cellular network, *e.g.*, to send or receive phone calls, SMS messages, or data communications. *See* APPLE-1005 (Skarine), [0032] (a cellular telephone can "receive, for example, pages via SGSN, notifications of incoming GPRS data, or SMS messages over GPRS"); [0034] ("Mobile device 202 is preferably a two-way communication device having at least voice and advanced data communication capabilities, including

the capability to communicate with other computer systems."). It is my opinion that a POSITA would have recognized that providing such communication functionality is desirable in that it enables the PDA to be used not only for self-contained computing, but also for various types of two-way mobile communications with other devices.

136. Another reason why a POSITA would have been prompted to implement the communications transceiver of the combination as a cellular telephone transceiver is because this is just the implementation of known techniques (*e.g.*, a cellular telephone transceiver) by a known system (*e.g.*, a wireless device) that results in a predictable outcome (*e.g.*, a wireless device with conventional cellular network communication capability).

137. It is also my opinion that a POSITA would have expected success in implementing the communications transceiver as a cellular telephone transceiver because Marek specifically indicates that its PDA can be capable of wireless communications: "an untrusted host platform communicating with unsecured wireless and/or wired networks." APPLE-1004 (Marek), 11:58-59; *see* Fig. 9. Moreover, I also believe that a POSITA would have expected success because wireless communication components such as cellular telephone transceivers were standard components in mobile devices as of the Critical Date. *See* APPLE-1005 (Skarine), [0022]-[0023], [0027]-[0029], [0035], [0038], Figs. 1-2; APPLE-1011 (Huang),

5:11-13; APPLE-1015 (Ramirez), 3:11-17; APPLE-1017 (Macchi), 10:14-18; APPLE-1018 (Yach), 6:33-45, 7:11-29.

(vii) Claim 7

[7] The mobile PDA computer system[7] according to claim 1, further comprising a first file system exclusively accessible to said secure user processor for storing classified data and a second file system for storing unclassified data, said second file system distinct from said first file system so as to provide physical separation of said classified data from said unclassified data within said portable mobile computing device.

138. In the Marek-Skarine combination system, Marek's SCM includes "a local storage 712" (highlighted in orange in the composite figure below), *e.g.*, **a first file system**.[8] APPLE-1004 (Marek), 9:14-19. This first file system is **for**

[7] I note that the phrase "The mobile PDA computer system" as recited in the preamble of claim 7 does not find antecedent basis in claim 1. I address this claim as best understood.

[8] The phrase "The mobile PDA computer system" can be interpreted as referred to either the computer system or to the portable mobile computing device. I note that Marek's SCM is part of both the computer system of the combination (*see* my analysis of element [1pre]) and the portable mobile computing device of the combination (*see* my analysis of element [1a]). Thus, regardless of which interpretation of this phrase is adopted, Marek's SCM satisfies the features of claim [7].

storing classified data. *See id.*, 9:14-24 ("The ACE 703 including COTS applications, manufacturer-supplied software and associated data may be cleansed, optionally encrypted and then stored on a local storage 712."), 2:16-17 ("The ACE may be cleansed and encrypted and then stored on a local encrypted storage."). To the extent that "classified data" is interpreted to refer specifically to, *e.g.*, information designated as implicating matters of national security, data stored in the red domain in the combination— *e.g.*, data stored in the first file system of Marek's SCM—can be **classified data**. *See* APPLE-1004 (Marek), 10:33-36; [1g], *supra*.

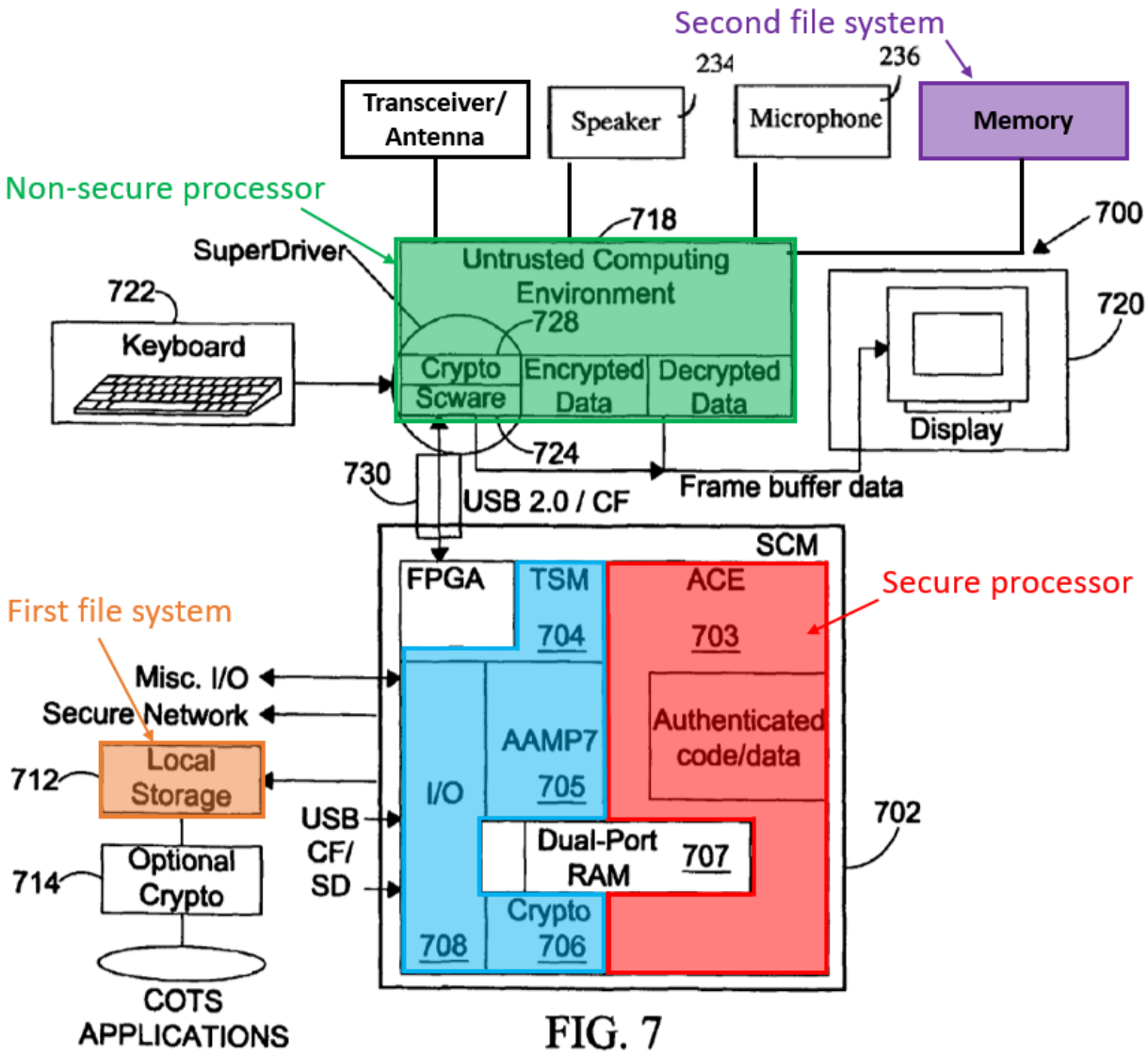


FIG. 7

Marek-Skarine composite figure

139. The first file system, *e.g.*, the local storage 712, is **exclusively accessible to the secure processor**, *e.g.*, the processor of Marek's ACE 703. For instance, Marek describes that "[a]ll secure resources," including the local storage 712, are "maintained on the trusted side of the plug-in module interface." APPLE-1004 (Marek), 2:5-7; *see* 2:40-41. Moreover, Marek describes that the secure processor accesses the local storage 712: "The ACE 703 including COTS applications,

manufacturer-supplied software and associated data may be … stored on a local storage 712." *Id.*, 9:14-17; *see* 9:22-25, 10:4-5.

140. As I discussed in my analysis of element [1c], the untrusted host mobile device of the Marek-Skarine combination system includes an operating system and application program software. *See* APPLE-1004 (Marek), 7:54-55 ("Windows CE operating system may be utilized as an embedded COTS OS on the untrusted host platform"), 8:56-59 ("The untrusted host environment may include ***commercial software environments and applications***"), 8:40-41, 12:16-18). It is my opinion that a POSITA would have understood or at least found obvious that the untrusted host mobile device 718 includes **a second file system**, *e.g.*, memory including non-volatile and volatile memory (highlighted in purple in the composite figure above), *e.g.*, for storage of the operating system, applications, and associated application data. This was well-known and conventional in the art as of the Critical Date, as demonstrated, for instance, by Skarine. *See* APPLE-1005 (Skarine), [0038] ("Operating system software used by microprocessor 238 is preferably stored in a persistent store such as flash memory 224, which may alternatively be a read-only memory (ROM) or similar storage element … the operating system, specific device applications, or parts thereof, may be temporarily loaded into a volatile store such as RAM 226"), [0040] ("Additional applications may also be loaded onto mobile device 202 … and installed by a user in RAM 226 or preferably a non-

volatile store (not shown) for execution by microprocessor 238"), [0050]-[0053] ("Mobile device 410 comprises … a memory 430 coupled to CPU 420 (e.g. RAM 226 of FIG. 2) … In the operation of mobile device 410, CPU 420 is controlled by one or more processing modules 470 embodying instructions for CPU 420, loaded into memory 430. Intermediate calculations and data may also be stored in memory 430 during operation of mobile device 410.").

141. That the existence of a file system in a conventional mobile device, *e.g.*, for storage of operating systems, applications, and associated data, was itself conventional is corroborated by the following additional references: APPLE-1018 (Yach), 3:58-61 ("Operating system software used by the microprocessor 102 is typically stored in a persistent store such as the flash memory 108, which may alternatively be a read-only memory (ROM) or similar storage element"); APPLE-1009 (Mathur), 5:26-30 ("A number of program modules may be stored on the hard disk, magnetic disk 29, optical disk 31, ROM 24, or RAM 25, including an operating system 35, one or more application programs 36, other program modules 37, and program data"); APPLE-1010 (Zuberec), 3:17-21 ("The mobile device 100 includes an operating system 164 … which is resident in the memory 162 and executes on the processor 160," where "[t]he memory 162 generally includes both volatile memory (e.g., RAM) and non-volatile memory (e.g., ROM, Flash Memory, or the like)"), 3:28-39 ("One or more application programs 166 are loaded into

memory 162 and run on the operating system 164. … The applications 166 may use and store information in the [non-volatile] storage 168" "within the memory"); APPLE-1011 (Huang), 4:54 ("Memory 22 includes an operating system 30, the application programs 16 … and the object store 18. During operation, the operating system 30 is loaded into, and executed by, the processor 20 from memory 22."); APPLE-1012 (Kwong), [0013] ("The memory 114 may store, for example, applications, programs, procedures, and/or modules that store instructions to be executed by the processor 112."); APPLE-1017 (Macchi), 10:14-22 (describing a mobile phone "with dynamic and non-volatile memory resources").

142. In the Marek-Skarine combination system, the **second file system is for storing unclassified data**, *e.g.*, for storing the untrusted operating system of the untrusted host mobile device. *See* APPLE-1005 (Skarine), [0038] ("Operating system software used by [the] microprocessor" of the untrusted host mobile device 718 is "stored in a persistent store such as flash memory 224 … a read-only memory (ROM) or similar storage element"), [0022]-[0023]; APPLE-1004 (Marek), 7:54-55; APPLE-1010, 3:17-21 ("The mobile device 100 includes an operating system 164 … which is resident in the memory 162 and executes on the processor 160"); APPLE-1011, 4:54-59 (describing a mobile device having

"[m]emory 22 [that] includes an operating system 30 … During operating, the operating system 30 is loaded into, and executed by, the processor 20 from memory 22"); APPLE-1018, 3:58-64. *See* my analysis of element [1c].

143. Data stored in the untrusted host mobile device 718, such as the unstrusted operating system software, can be considered to be **unclassified** at least because it is not transmitted on the "secured and authenticated" I/O paths provided by Marek's TSM, nor is it subject to the encryption provided by Marek's cryptographic engine. APPLE-1004 (Marek), 9:40-53; *see* 2:36-37 ("untrusted applications execute on the untrusted host environment"). To the extent that "unclassified data" is interpreted to refer specifically to, *e.g.*, information designated as not implicating matters of national security, data stored in the black domain in the combination— *e.g.*, data stored in the second file system of the untrusted host mobile device—can be **unclassified data**. *See* APPLE-1004 (Marek), 10:33-36. *See also* my analysis of element [1g].

144. The second file system is **distinct from the first file system**, *e.g.*, the persistent storage of the untrusted host mobile device 718 is distinct (*e.g.*, physically separate) from the local storage 712 in the SCM, as illustrated in the composite figure above. Because the second file system is distinct from the first file system, the classified data are stored in a different physical location than the unclassi-

fied data, *e.g.*, the distinctness of the two file systems **provides physical separation of the classified data from the unclassified data within the portable mobile computing device**.

(viii) Claim 9

[9pre] A computer system, comprising:

[9a] a portable mobile computing device including a secure user processor, a non-secure user processor, a communications transceiver, and a cryptographic engine,

[9b] said communications transceiver operatively coupled to said non-secure user processor and configured for communicating data external to said portable mobile computing device,

[9c] said secure user processor comprising a trusted microprocessor, a trusted operating system executing on said trusted microprocessor, and a trusted application software executing on said trusted microprocessor;

[9d] said non-secure user processor comprising an untrusted microprocessor, an untrusted operating system executing on said untrusted microprocessor, and an untrusted application software executing on said untrusted microprocessor;

[9e] said cryptographic engine configured for encrypting data communicated from said secure user processor to said non-secure user processor, comprising a trusted cryptographic processor, and a trusted operating system executing on said trusted cryptographic processor;

[9f] a first data communication link communicating data between said secure user processor and said cryptographic engine;

[9g] a second data communication link communicating data between said non-secure user processor and said cryptographic engine;

145. *See* my analysis of elements [1pre]-[1f], [1i] of Ground 1A.

[9h] a secure human/machine interface communicatively coupled to said secure user processor and configured to enable bi-directional communication of

classified information exclusively between a user and said secure user processor, at least a portion of said secure human/machine interface located in a physically secure enclosure; and

146. The Marek-Skarine combination system includes a secure human/machine interface configured to enable bi-directional communication of classified information exclusively between a user and the secure user processor. *See* my analysis of element [1g]. The secure human/machine interface (Marek's input and output devices 722, 720) is communicatively coupled to the secure user processor (contained in the ACE) in that they are coupled such that there is communication of information therebetween, *e.g.*, via Marek's TSM. *See* APPLE-1004 (Marek), 9:13-14, 9:50-64, 10:49-54, 11:39-41.

147. Moreover, I note that it was well known that at least a portion of both the keypad and the display of a mobile device (*e.g.*, PDA or cell phone, such as Marek's untrusted host mobile device) are located in a housing of the mobile device. *See* APPLE-1011 (Huang), 5:28-6:7 ("[I]n addition to antenna 11 and microphone 17, mobile device 10 includes a miniaturized keyboard 32 [and] a display 34," with "microphone 17 positioned on antenna 11 and speaker 86 positioned on the housing of the device"), 1:8-25, Figs. 3-4. In the Marek-Skarine combination, the housing of the untrusted host mobile device 718 is **a physically secure enclosure** that houses at least a portion of the keypad and the display (the secure human/machine interface; *see* my analysis of element [1g])— *e.g.*, **at least a portion**

of the secure human/machine interface is located in a physically secure enclosure.

[9i] a non-secure human/machine interface communicatively coupled to said non-secure user processor and configured to enable bi-directional communication of unclassified information exclusively between said user and said non-secure user processor, said non-secure human/machine interface distinct from said secure human/machine interface.

148. The Marek-Skarine combination system includes a non-secure human/machine interface configured to enable bi-directional communication of unclassified information exclusively between the user and the non-secure user processor and distinct from said secure human/machine interface. *See* my analysis of element [1h]. The non-secure human/machine interface (the speaker and microphone) is communicatively coupled to the non-secure user processor (the processor of the untrusted host mobile device 718) in that they are coupled such that there is communication of information therebetween. *See* APPLE-1005 (Skarine), [0038], Fig. 2.

(ix) Claim 10

[10] The computer system according to claim 9, wherein said non-secure user processor is operatively connected to said communications transceiver.

149. *See* my analysis of element [1i].

(x) Claim 12

[12pre] A method for managing classified and unclassified data on a portable mobile computing device of a computer system, comprising:

150. The Marek-Skarine combination provides **a computer system**, which is illustrated in the composite figure below. For instance, Marek's "***computing environment 700***" implementing SCM architecture, and modified based on Skarine as I discussed above in Section VI.A.3, is **a computer system**. APPLE-1004 (Marek), 8:51-52; *see* 8:37-39 ("Secure COTS computing environment may be provided by ***a system including a SCM as an add-on module to an untrusted host environment***."), 1:6-9 ("This invention relates generally to ***computing environments*** and more particularly to a system for providing a secure and trusted commercial-off-the-shelf COTS computing environment"), 1:43-45, 1:66-2:1, 11:57-60, 12:13-14, 12:19-21, Fig. 7, Figs. 9-14; *see* ¶56 of this declaration.

The Marek-Skarine combination device is a portable mobile computing device

151. Marek describes that "[a] secure COTS computing environment may be provided by a system including a SCM as an add-on module to an untrusted host environment." APPLE-1004, 10:37-39. In the Marek-Skarine combination, the untrusted host 718 (green in the figure below) and the SCM 702 (orange), which each is a mobile device as I discuss below, together are (or render obvious) **a portable mobile computing device** (outlined in purple). *See* ¶57 of this declaration.

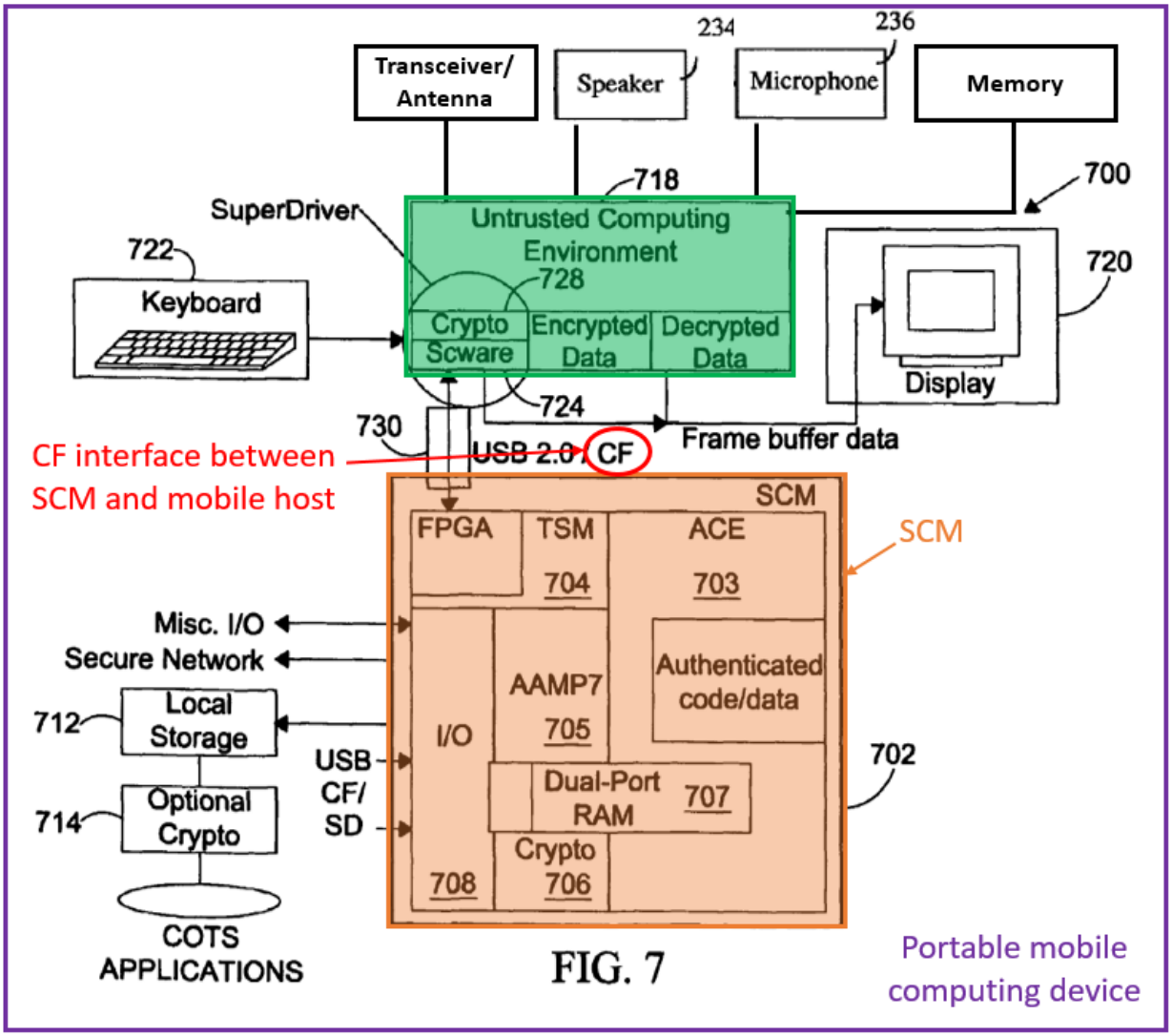


FIG. 7

Marek-Skarine composite figure

152. First, Marek's untrusted host (highlighted in green) is a mobile device, *e.g.*, a PDA or cell phone. I note that the combination with Skarine does not alter this form factor. Rather, as I have discussed above and will discuss in more detail in this element-by-element analysis, Skarine provides implementation details that may not necessarily have been explicitly stated by Marek. *See* ¶58 of this declaration.

153. Generally, Marek explains that "the SCM may be utilized by ***various untrusted host COTS platforms such as PDAs, cell phones***, laptops and the like." APPLE-1004, 11:44-46; *see* 11:53-56 ("the SCM is suitable for providing secure wireless network connections when the SCM is added on ***wireless devices such as PDAs, cell phones, and other mobile devices***"), 13:49-51 ("the SCM may be packaged in a form factor suitable for various portable devices such as a PDA, a cell phone, a GPS device and the like"), 2:56-59, 7:53-57, 8:25-38, 12:13-21, Figs. 10-11. *See* ¶59 of this declaration.

154. More specifically, Marek also describes that the particular untrusted host 718 that is illustrated in Fig. 7 is a mobile device: "[t]he SCM may employ various interfaces depending on the host COTS platforms, including ***a Compact Flash (CF) interface for a PDA host platform***." *Id.*, 11:45-50 (CF interface circled in red in the figure *supra*); *see* 12:13-16, 2:56-62, Fig. 7. As I discussed above in ¶60 of this declaration, at least when the SCM employs the illustrated CF interface, the untrusted host is a mobile device. *See* APPLE-1004, 11:45-50. *See* ¶60 of this declaration.

155. Marek's SCM (orange) is also a mobile device. For instance, I note that Marek describes that "the SCM may be packaged in a form factor suitable for various portable devices such as a PDA, a cell phone, a GPS device and the like." APPLE-1004, 13:49-41. Moreover, Marek explains that the "Authenticated COTS

Environment Subsystem" (ACE) of the SCM "includes an embedded COTS OS running on a compatible embedded COTS processor." APPLE-1004, 9:1-5. This embedded COTS OS is, *e.g.*, "WINDOWS® CE … or PALM OS®," both of which are operating systems for mobile devices. APPLE-1004, 9:5-7; *see* APPLE-1010, 3:17-19; APPLE-1011, 4:59-61; APPLE-1009, 1:66-2:3. The embedded COTS processor of Marek's ACE is likewise a processor for a mobile device: "an INTEL® cellular processor such as PXA270™ processors, mobile PENTIUM™ processors, TRANSMETA™ EFFICEON™ processors, and the like." APPLE-1004, 9:7-10; *see* APPLE-1012, [0012]. Because Marek's SCM has a mobile device form factor, and because it includes a mobile device processor and operating system, I conclude that Marek's SCM is a mobile device. *See* ¶¶61-64 of this declaration.

156. At least because Marek's untrusted host 718 and SCM 702 are both mobile devices, the untrusted mobile device host 718 and the SCM 702 of Marek's Fig. 7 together are, or at least render obvious, **a portable mobile computing device** in the Marek-Skarine combination system. *See* ¶¶64 of this declaration.

The Marek-Skarine combination device manages classified and unclassified data

157. Marek describes that a "secure communication system for military applications is required to have high bandwidth and support users who operate at ***dif-***

ferent security levels." APPLE-1004, 1:10-12. "For example, a network connecting real time embedded military multi-level applications must support communications between diverse groups with ***different clearance levels***." APPLE-1004, 1:15-17. Thus, I believe that a POSITA would have understood or at least found it obvious from these teachings that the system described by Marek and of the Marek-Skarine combination would need to be able to manage data and communications at different security/clearance levels. *See* APPLE-1004, 1:10-37, 4:33-50, 5:36-47, 8:37-67. For instance, I believe that a POSITA would have recognized, or at least found obvious, that the different security/clearance levels to which Marek refers are related to various levels of classified and unclassified data. *Id.* Indeed, I note that Marek teaches that its system provides new mechanisms for enforcing security policies and that "prevent compromising ***classified data***" without the complicated separation mechanisms of prior art systems. *See* APPLE-1004, 4:15-61. With respect to the example shown in FIG. 7, Marek describes that the "trusted environment may include trusted hardware and software ensuring access to certain resources, or parts of shared resources to be controlled in a structured manner to prevent compromising ***classified data***." APPLE-1004, 8:61-64.

158. As I will discuss further with respect to elements [12a] and [12g], Marek's computing environment includes Scware, which is "software that acts as a trusted agent for the SCM 702 on the untrusted host environment." APPLE-1004,

10:42-45. The Scware "resides on the untrusted host environment while the SCM 702 is operating" and, "in conjunction with the TSM 704 creates secure I/O paths 730 of input and output devices 722, 720 of the untrusted host 718." APPLE-1004, 10:42-51. **The secure human/machine interface enables communication of classified information**: the information is encrypted and communicated along "secured and authenticated" I/O paths. APPLE-1004, 9:50-52; *see* 9:37-44. Thus, at least the Scware and TSM of the Marek-Skarine combination manage classified data on the portable mobile computing device. *See* ¶¶109, 116 of this declaration.

159. As I will discuss further with respect to elements [12c] and [12h], the untrusted host mobile device of the Marek-Skarine combination includes a speaker and a microphone, orange in the figure *infra*, as was conventional in the art and as evidenced, *e.g.*, by Skarine. *See* APPLE-1005, [0038], [0042], Fig. 2; *see* APPLE-1018, 3:45-50; APPLE-1010, 3:54-67; APPLE-1024, [0004]; APPLE-1025, 1:18-20. The speaker and microphone together are a non-secure human/machine interface at least because they are an interface by which a user inputs information to and receives information from the untrusted host mobile device (via the microphone and speaker, respectively). *See* APPLE-1005, [0041]-[0042]. **The non-secure human/machine interface enables communication of unclassified information** because the information communicated between the speaker/microphone and the non-secure processor is not transmitted on the "secured and authenticated"

I/O paths provided by the TSM, nor is it subject to the encryption provided by the cryptographic engine. *See* APPLE-1004, 9:40-53. *See* ¶¶117-118 of this declaration.

[12a] processing said classified data exclusively using a secure processor of said portable mobile computing device,

The combination device includes a secure processor

160. In the Marek-Skarine combination system, the SCM 702 of the portable mobile computing device includes **a secure processor**. Marek's SCM includes an "Authenticated COTS environment subsystem (ACE)" 703, red in the figure *infra*. APPLE-1004, 9:1-2. The ACE "includes an embedded COTS OS running on a compatible ***embedded COTS processor***" and also includes "COTS applications, manufacturer-supplied software and the like." APPLE-1004, 9:4-5, 9:13-14; *see* 8:61-62 ("The trusted environment may include ***trusted hardware and software***"), 2:12-15, 2:33-38, 8:39-41, 9:5-17, 12:18-19; *see* [12b]. Alone or in combination, the embedded COTS processor of Marek's ACE, together with the COTS OS and software, are, or at least render obvious, **a secure processor**. For instance, these elements render obvious a secure user processor because of their role in providing a secure, trusted computing environment. *See* ¶65 of this declaration.

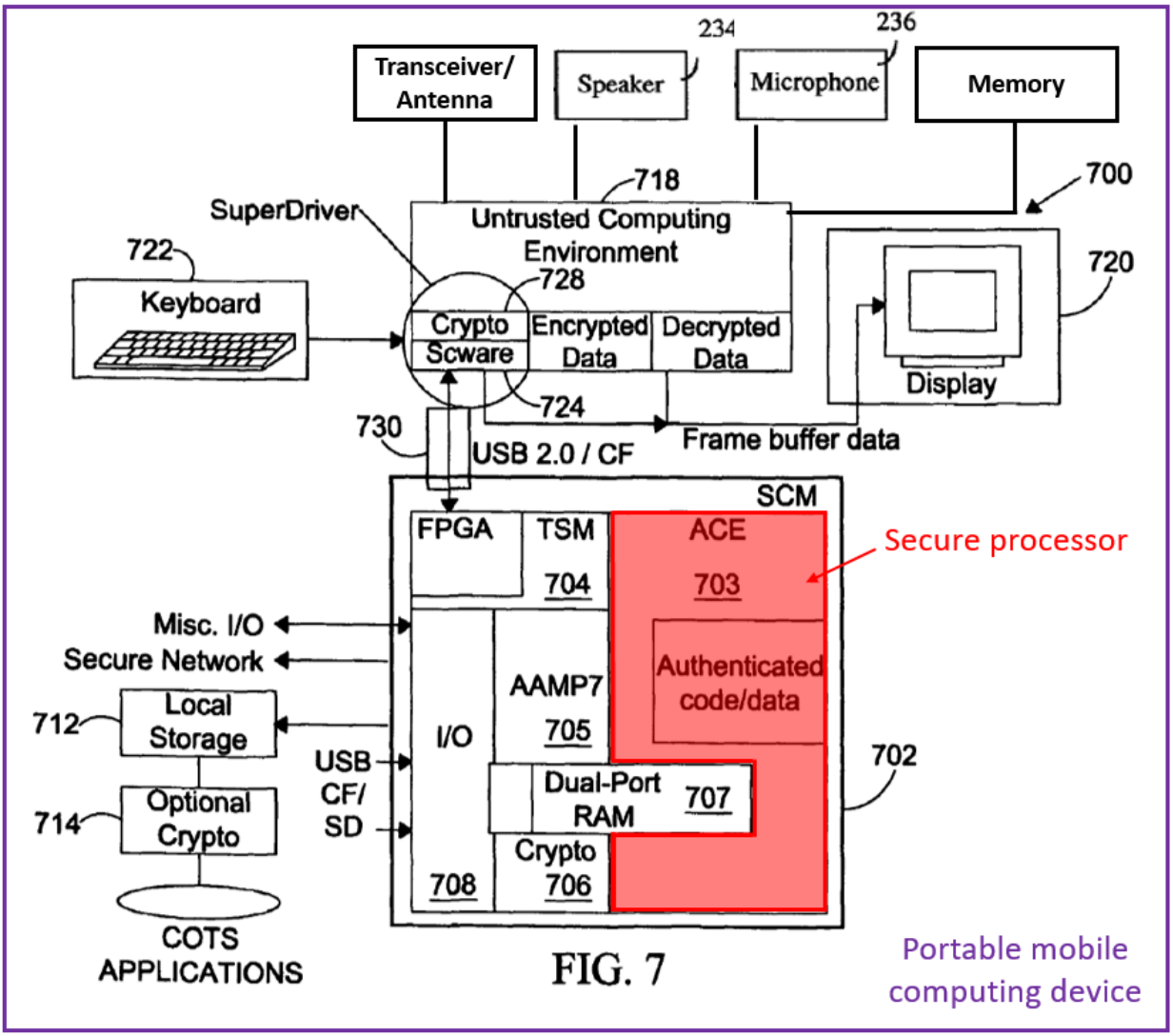


FIG. 7

Marek-Skarine figure

161. It is my opinion that a POSITA would have found it obvious for the embedded COTS processor, taken alone or together with the COTS OS, and software of Marek's ACE, to be a **secure** processor, at least because they are included in Marek's "***Secure COTS computing environment***" provided by the SCM, *e.g.*, an environment that provides secure, trusted computing. APPLE-1004, 8:37-39; *see* 8:39-45, 1:66-2:4 ("a system including a Secure Computing Module (SCM)

provides ***trusted environment*** for COTS host platforms. Only authenticated trusted applications execute on the SCM."), 2:13-20 ("The ACE may be secured by authenticating all code and data used for running COTS applications."), 2:31-38 ("the system including the SCM may provide trusted and portable COTS computing environments against malware"), Figs. 10-11 (showing an ACE in the red domain[9] of a portable mobile computing device system). *See* ¶¶66-71 of this declaration.

The secure processor of the combination exclusively processes said classified data

162. In the embodiment of FIG. 7, Marek describes that "[o]nly authenticated COTS applications and COTS OS execute on the SCM while untrusted applications execute on the untrusted host environment." APPLE-1004, 8:39-41. As a result ***"[a]ll secure resources*** may be maintained ***on the trusted side*** of the plug-in module interface" (i.e., within the SCM 702). APPLE-1004, 8:43-45. "The trusted environment may include trusted hardware and software ensuring access to certain resources, or parts of shared resources to be controlled in a structured manner to ***prevent compromising classified data***." APPLE-1004, 8:61-64. It is my

[9] Red and black domains are secure and non-secure domains, respectively, of a system that handles sensitive information, such as classified information. *See* APPLE-1004, 7:25-29; APPLE-1014, [0005].

opinion that a POSITA would have recognized or at least found it obvious from these disclosures that, in the Marek-Skarine combination, the classified data would have been processed exclusively using the ACE 704 of the SCM 702 (*e.g.*, the claimed "secure processor"), for instance, to enable compliance with the "stringent standards" required by "[g]overnment and military applications." *Id.*, 1:24-25.

163. I also believe that to have classified data processed **exclusively** by the secure processor would have been a straightforward design choice that a POSITA would have found to be obvious, *e.g.*, to provide security for the processed data. A secure processor that is generally capable of processing classified data—such as Marek's secure processor—would operate in the same way regardless of whether or not classified data is processed exclusively on that processor, and with no unexpected results. Indeed, I note that the '399 Patent itself appears to indicate that having classified data processed exclusively by the secure processor is just a design choice, stating that "The invention can also concern a method for managing classified and unclassified on a mobile PDA computer system. The method can include processing classified data exclusively using a secure processor. The method can also include processing unclassified data exclusively using a non-secure processor." APPLE-1001 ('399 Patent), 2:57-63.

[12b] said secure processor comprising a trusted microprocessor and a trusted operating system executing on said trusted microprocessor;

164. The **secure processor** of the Marek-Skarine combination system (which is contained in the ACE of the SCM, as I discussed for element [12a], above) **includes a trusted microprocessor**. For instance, the hardware of the embedded COTS processor of Marek's ACE is a trusted microprocessor. *See* APPLE-1004, 9:1-5 ("The ACE 703 includes an embedded COTS OS running on a compatible ***embedded COTS processor***"), 8:61-62 ("The trusted environment may include ***trusted hardware*** and software"), 9:7-13, Fig. 7. *See* ¶77 of this declaration.

165. The secure processor of the Marek-Skarine combination system also includes **a trusted operating system executing on the trusted microprocessor**. For instance, the embedded COTS operating system (OS) of Marek's ACE is a trusted operating system that executes on the embedded COTS processor of Marek's ACE 703 (*i.e.*, on the trusted microprocessor; *see* previous paragraph). . *See* APPLE-1004, 9:1-5 ("The ACE 703 includes ***an embedded COTS OS running on a compatible embedded COTS processor***"), 2:14-15 ("The ACE may include ***an embedded COTS OS***"), 8:39-41 ("Only authenticated COTS applications and ***COTS OS execute on the SCM***"), 8:61-62, 9:5-7 ("***Examples of the embedded COTS OS*** include WINDOWS® CE, LINUX, or PALM OS®, or the like"), Fig. 7. *See* ¶78 of this declaration.

166. The secure processor of the Marek-Skarine combination system further includes trusted application software executing on said trusted microprocessor. For instance, the applications included in Marek's ACE 703 are trusted application software that execute on the embedded COTS processor of Marek's ACE 703. *See* APPLE-1004, 9:13-17 ("The ACE 703 may include COTS applications, manufacturer-supplied software and the like."), 8:39-41 ("Only authenticated COTS applications … execute on the SCM"), 8:61-62 ("The trusted environment may include trusted hardware and software"), 2:12-15, 2:33-38, 12:18-19, 13:37-41; 2:1-4, Fig. 7. *See* ¶79 of this declaration.

167. One reason that the trusted microprocessor, trusted operating system, and trusted application software are **trusted** (or least that a POSITA would have found it obvious that they are trusted) is because they are part of, or execute on, the "Secure COTS computing environment" provided by the SCM. APPLE-1004, 8:37-39; *see* 8:39-45, 1:66-2:4 ("a system including a Secure Computing Module (SCM) provides trusted environment for COTS host platforms. Only authenticated trusted applications execute on the SCM."), 2:13-20 ("The ACE may be secured by authenticating all code and data used for running COTS applications."), 2:31-38, 11:60-65 ("The SCM 908 including the TSM and the cryptographic engine resides in the red domain within a trusted environment"), Figs. 10-11 (showing an ACE in

the red domain of a portable mobile computing device system). *See* ¶80 of this declaration.

168. Another reason that the trusted operating system and application software are **trusted** (or at least that a POSITA would have found this to be obvious) is because they are authenticated. *See* APPLE-1004, 2:1-2 ("Only ***authenticated trusted applications*** execute on the SCM"), 2:13-15, 9:14-22 ("The ACE 703 including COTS applications, manufacturer-supplied software and associated data may be cleansed, optionally encrypted and then stored on a local storage 712."), 2:33-38, 8:39-41, 9:2-4. *See* ¶81 of this declaration.

[12c] processing unclassified data exclusively using a non-secure processor of said portable mobile computing device,

The combination device includes a non-secure processor

169. In the Marek-Skarine combination system, the untrusted host mobile device 718, which I have highlighted in green in the composite figure below, includes **a non-secure user processor**. Marek describes that the untrusted host includes COTS processors. *See* APPLE-1004, 8:59-61 ("Conventionally, a host platform employing ***COTS processors*** is assumed to be untrusted."). The untrusted host also includes an operating system and application software. *See* APPLE-1004, 7:54-55 ("Windows CE operating system may be utilized as ***an embedded COTS OS on the untrusted host platform***"), 8:40-41 ("***untrusted applications ex-***

ecute on the untrusted host environment"), 8:56-59 ("The untrusted host environment may include commercial software environments and applications"), 12:16-18, 2:1-4, 2:36-38; *see* [12d]. The COTS processor(s) of the untrusted host 718, alone or taken together with the COTS OS and the applications executing on the untrusted host, are, or at least render obvious, **a non-secure user processor**. For instance, these elements render obvious a secure user processor because of their role in providing a untrusted computing environment. *See* ¶69 of this declaration.

170. To the extent Marek does not explicitly state that the COTS OS is on the processor of the specific untrusted host 718, I believe that a POSITA would have understood this to be the case, or otherwise found this to be obvious, given that operating systems in mobile devices were well-known as of the Critical Date. *See* APPLE-1004, 7:54-55; APPLE-1005, [0022]-[0023], [0038]; APPLE-1009, 1:64-2:3; APPLE-1010, 3:17-21; APPLE-1011, 4:54-61; APPLE-1018, 3:58-64. *See* ¶70 of this declaration.

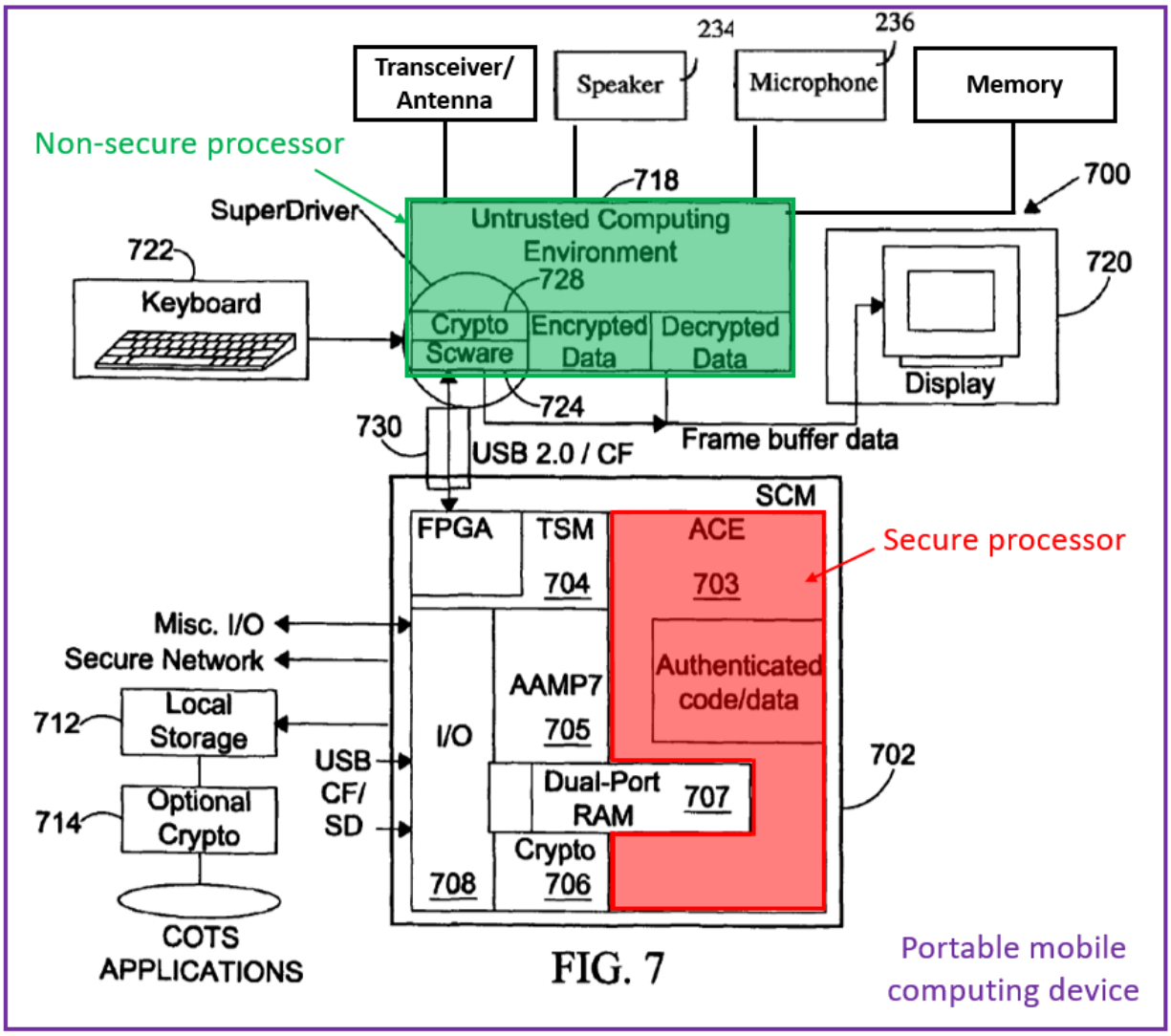


FIG. 7

Marek-Skarine composite figure

171. It is my opinion that a POSITA would have found it obvious for the COTS processor(s) of the untrusted host, taken alone or together with the COTS OS and the applications, to be a **non-secure** processor at least because they are included in Marek's "untrusted host environment," *e.g.*, an environment that provides untrusted computing. APPLE-1004 (Marek), 8:40-41; *see* 8:56-59 ("a host platform employing COTS processors is assumed to be ***untrusted***"), 12:16-18

("Untrusted application software and hardware may be implemented in the PDA"), 2:1-4, 2:36-38, Figs. 10-11 (showing a PDA in the black domain of a portable mobile computing device system). *See* ¶71 of this declaration.

The non-secure processor of the combination exclusively processes said unclassified data

172. In the example shown in FIG. 7, Marek describes that the "untrusted host environment [718] may include commercial software environments and applications, having minimal or no Common Criteria (CC) certification and no assurance of isolation between tasks." APPLE-1004, 8:56-59. According to Marek, "[o]nly authenticated COTS applications and COTS OS execute on the SCM ***while untrusted applications execute on the untrusted host environment***." APPLE-1004, 8:39-41. When the secure computing module embodiment is implemented on a PDA, "***[u]ntrusted application software and hardware may be implemented in the PDA 1014*** while trusted applications are implemented in the SCM 908." APPLE-1004, 12:16-19. Moreover, when the Scware operates in a "higher level of security" mode, "all applications but the Scware 724" are disabled on the host environment, *e.g.*, indicating that when stringent security is required (*e.g.*, when classified information is to be processed), only the secure user processor is operational—and thus the non-secure processor does not process classified data, but rather exclusively processes unclassified data. *Id.*, 10:55-67. It is my opinion that a POSITA would have recognized or at least found it obvious from these disclosures

that, in the Marek-Skarine combination, the unclassified data would have been processed exclusively using the COTS processors of the untrusted host 718 (that is, the claimed "unsecure processor").

[12d] said non-secure processor comprising an untrusted microprocessor and an untrusted operating system executing on said untrusted microprocessor;

173. The **non-secure user processor** of the Marek-Skarine combination system (*i.e.*, the processor included in the untrusted host mobile device 718, as I discussed above for element [1a]) **includes an untrusted microprocessor**. For instance, the hardware of the COTS processor of the untrusted host PDA 718 is an untrusted microprocessor. *See* APPLE-1004 (Marek), 8:59-61 ("Conventionally, a host platform employing ***COTS processors*** is assumed to be untrusted."), 12:16-18 ("Untrusted application software and ***hardware*** may be implemented in the PDA 1014."). *See* ¶82 of this declaration.

174. The non-secure user processor of the combination also includes **an untrusted operating system executing on the untrusted microprocessor**. For instance, the operating system of the untrusted host 718 is an untrusted operating system. For instance, in the combination, Marek describes an untrusted host platform in which "***Windows CE operating system may be utilized as an embedded COTS OS on the untrusted host platform***," *e.g.*, an operating system executing on the microprocessor of an untrusted host mobile device. APPLE-1004 (Marek), 7:54-55. *See* ¶83 of this declaration.

175. To the extent that Marek does not explicitly state that an operating system such as Windows CE is executed on the specific microprocessor of the untrusted mobile device host 718, it is nevertheless my opinion that a POSITA would have understood this to be the case based on Marek's disclosure of operating systems on untrusted host platforms. *See* APPLE-1004 (Marek), 7:54-55. I note that it was standard and well-known that operating systems (*e.g.*, Windows CE) execute on the microprocessors of mobile devices such as a PDAs or cell phones, *e.g.*, to control the execution of applications on the microprocessors and for resource allocation. *See* APPLE-1005 (Skarine), [0022]-[0023] ("a mobile device … includes … controller 106 [that] is embodied as a central processing unit (CPU), which runs operating system software in a memory component"), [0038] ("Operating system software used by microprocessor 238 is preferably stored in a persistent store … [and] may be temporarily loaded into a volatile store such as RAM 226."); APPLE-1009 (Mathur), 1:64-2:3 ("specialized operating systems capable of running in the resource-limited environment of the embedded system have been developed. An example of such an operating system is the Windows CE™ operating system from Microsoft Corporation."); APPLE-1010, 3:17-21 ("The mobile device 100 includes an operating system 164, such as the Windows CE operating system from Microsoft Corporation … which is resident in the memory 162 and executes on the processor 160"); APPLE-1011 (Zuberec), 4:54-61 (describing a mobile device

having an "operating system … [that] is a Windows CE brand operating system commercially available from Microsoft Corporation," where "[d]uring operation, the operating system 30 is loaded into, and executed by, the processor 20 from memory 22"); APPLE-1018 (Yach), 3:58-64 ("Operating system software used by the microprocessor 102 is typically stored in a persistent store such as the flash memory 108 … [and] may be temporarily loaded into a volatile store such as the RAM 106"). Thus, given the ubiquity of operating systems in mobile devices, it is my opinion that a POSITA would have understood or found obvious that Marek's description of an operating system executing on the processor of an untrusted host mobile device is applicable to the specific untrusted host mobile device 718 of Marek's Fig. 7, *e.g.*, that the non-secure user processor of the combination includes **an untrusted operating system**. *See* APPLE-1004 (Marek), 7:54-55. *See* ¶84 of this declaration.

176. Furthermore, the non-secure user processor of the combination includes **untrusted application software executing on the untrusted microprocessor**. For instance, the applications that execute on Marek's untrusted host 718 are untrusted application software. *See* APPLE-1004 (Marek), 8:40-41 ("***untrusted applications execute on the untrusted host environment***"), 8:56-59 ("The untrusted host environment may include ***commercial software environments and ap-***

plications"), 12:16-18 ("Untrusted application software and hardware may be implemented in the PDA"), 2:1-4 ("untrusted applications execute on the untrusted host environment"), 2:36-38. *See* ¶85 of this declaration.

177. The untrusted microprocessor, untrusted operating system, and untrusted application software are **untrusted** (or at least a POSITA would have found this to be obvious) at least because they are part of, or execute on, "the ***untrusted*** host environment" rather than the secure environment of the SCM. APPLE-1004 (Marek), 8:40-41; *see* 8:56-59, 12:16-18, 2:1-4, 2:36-38, Figs. 9-11 (showing a PDA in the black domain of a portable mobile computing device system). Additionally, the untrusted application software is **untrusted** (or at least a POSITA would have found this to be obvious) at least because it "may include commercial software environments and applications, having minimal or no Common Criteria (CC) certification and no assurance of isolation between tasks." APPLE-1004 (Marek), 8:56-59. *See* ¶86 of this declaration.

[12e] communicating encrypted and decrypted classified data between said secure processor and a cryptographic engine of said portable mobile computing device using a first data communication link;

The combination device includes a cryptographic engine

178. In the Marek-Skarine combination system, the SCM 702 of the portable mobile computing device includes **a cryptographic engine**. Specifically, the SCM includes a "Trusted Security Manager subsystem (TSM) 704," as taught by

Marek. APPLE-1004 (Marek), 8:67. The TSM 704 "include[s] ***a trusted processor 705*** for providing a brick-wall partitioning of memory, time, and device resources, and enforcing predetermined security policies," and "***a cryptographic engine 706*** … [that] may aid the trusted processor 705 to provide a robust security interface." APPLE-1004 (Marek), 9:31-47. The Trusted Security Manager subsystem 704, including the trusted processor 705 and cryptographic engine 706, function as, and render obvious, **a cryptographic engine**, which I have highlighted in blue in the composite figure below. *See* ¶¶75, 87-88 of this declaration.

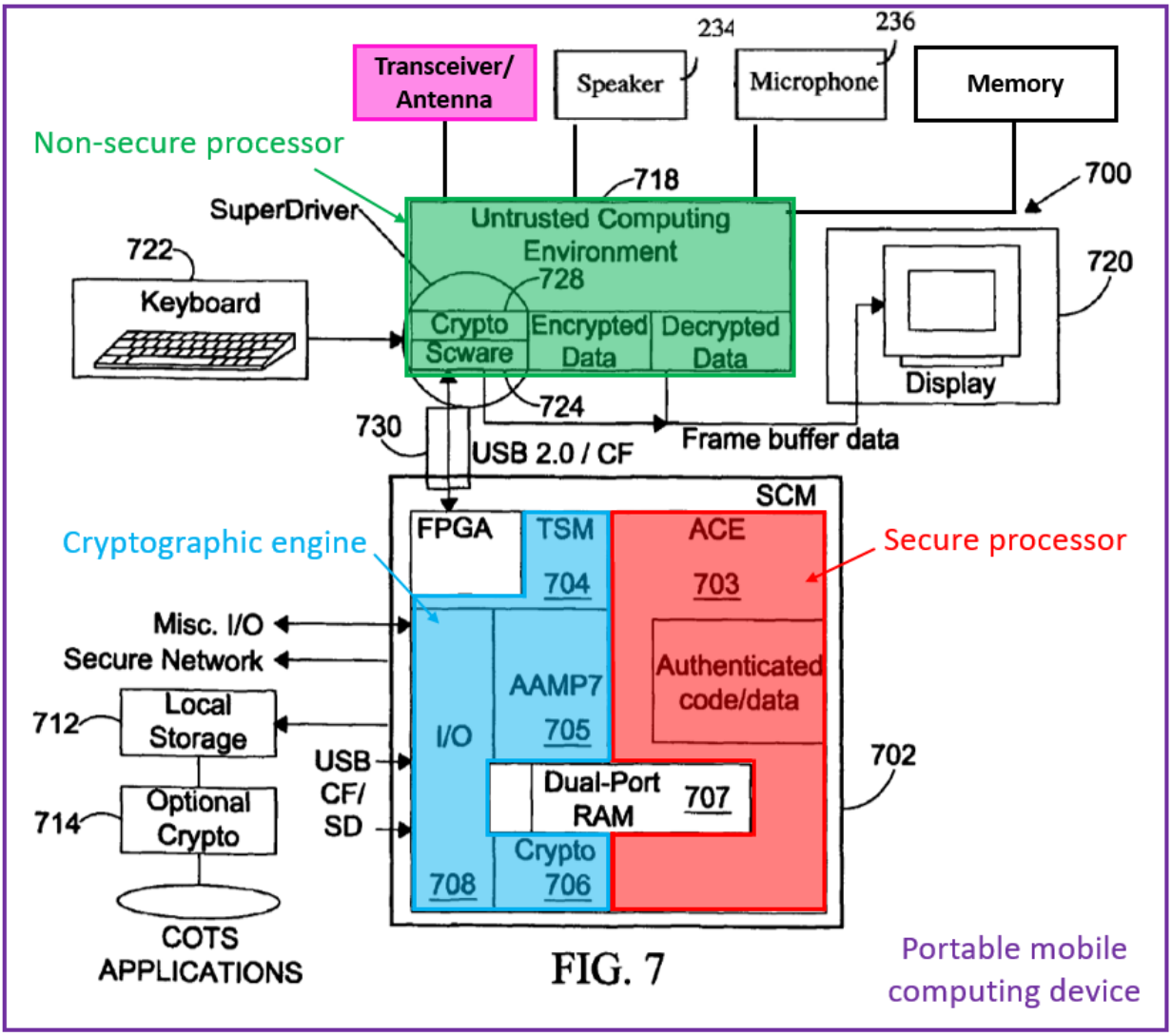


FIG. 7

Marek-Skarine composite figure

179. The TSM 704 can be considered to be a cryptographic engine at least because it "provide[s] a robust security interface" (APPLE-1004 (Marek), 9:40-41; *see* 10:33-35) using cryptography. *See id.*, 9:42-47 ("Conventionally, cryptography is the widely used means for protecting information confidentiality and integrity. The use of cryptography allows much of the secure communication system

to be built with COTS network components."), 9:48-60 ("Memory and I/O resources in the SCM 702 are strictly partitioned and managed by several secure TSM partitions. Each I/O path of the SCM 702 is configured to go through the TSM 704 so that a corresponding TSM partition of an I/O path controls the I/O path to be secured and authenticated. … A dedicated secure TSM partition may manage each I/O path being subject to authentication protocols."), 9:31-37 ("The TSM 704 may include a trusted processor 705 for providing a brick-wall partitioning of memory, time, and device resources, and enforcing predetermined security policies. The brick-wall partitioning of memory, time and device resources may ensure that applications execute in an environment that is strictly portioned, highly protected and completely isolated from other applications."). *See* ¶76 of this declaration.

The combination device includes a first data communication link between said secure processor and the cryptographic engine for communicating data

180. In the Marek-Skarine combination system, Marek describes that "any I/O from/to the ACE 703 is configured to go through the TSM 704," and thus that data is communicated between the ACE 703 (containing the secure processor, and highlighted in red in the composite figure below) and the TSM 704 (the cryptographic engine; highlighted in blue). APPLE-1004 (Marek), 9:63-66. Given that data is communicated between the secure processor and the cryptographic engine, it is my opinion that a POSITA would have understood there to be **a first data**

communication link (highlighted in purple) **communicating data between the secure processor and the cryptographic engine**. For instance, a POSITA would have understood this to be the case to enable the disclosed I/O between the ACE 703 and the TSM 704 to occur. *See* APPLE-1004 (Marek), 9:63-64 ("any I/O from/to the ACE 703 is configured to go through the TSM 704"), 9:52-54 ("All ACE I/O's are controlled by the TSM 704 and any I/O from/to the ACE 703 is configured to go through the TSM 704"), 9:50-56 ("Each I/O path of the SCM 702 is configured to go through the TSM 704"). *See* ¶¶87-88, 105 of this declaration.

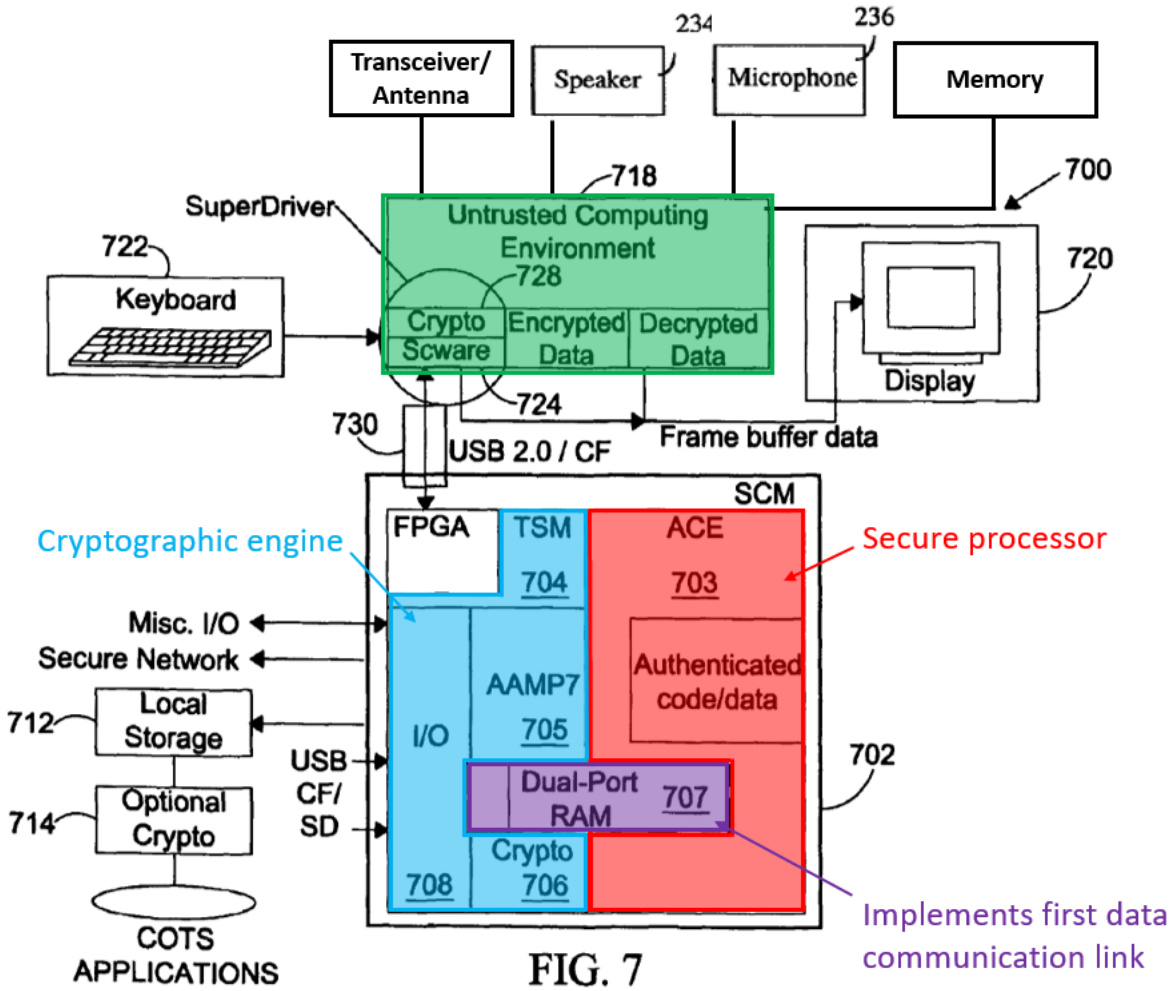


FIG. 7

Marek-Skarine composite figure

181. In a specific implementation, Marek describes that "I/O paths between the TSM 704 and the ACE 703 may include ***virtual I/O paths***." APPLE-1004 (Marek), 9:66-67. These virtual I/O paths are **a first data communication link communicating data between the secure processor** (contained in the ACE 703) **and the cryptographic engine** (the TSM 704). In particular, Marek describes that "the virtual I/O paths between the TSM and the ACE may be implemented through a dual port RAM 707," highlighted in purple, "with each I/O path and a memory-

mapped resource being controlled by a dedicated TSM partition." APPLE-1004 (Marek), 9:67-10:4. That is, in one implementation of the combination, Marek's **a first data communication link**, *e.g.*, the virtual I/O paths, **between the secure processor and the cryptographic engine** is implemented via Marek's RAM 707. *See* ¶106 of this declaration.

Encrypted and decrypted classified data are communicated via the first data communication link between the secure processor and the cryptographic engine in the combination

182. Marek describes that data communicated to or from the secure processor (red in the figure *infra*) passes through the cryptographic engine (blue), *e.g.*, through Marek's TSM—*e.g.*, **data is communicated between the secure processor and the cryptographic engine**. Specifically, Marek states that "***[e]ach I/O path of the SCM 702 is configured to go through TSM 704*** so that a corresponding TSM partition of an I/O path controls the I/O path to be secured and authenticated," where "[e]xamples of I/O paths of the SCM 702 include ***I/O paths between the untrusted host and the SCM***"—*e.g.*, I/O paths between the non-secure processor and the SCM (which contains the secure processor) pass through the cryptographic engine. APPLE-1004, 9:50-54. Further, "[a]ll ACE I/O's are controlled by the TSM 704 and ***any I/O from/to the ACE 703 is configured to go through the TSM 704***"— *e.g.*, all I/O paths from/to the secure processor also pass through the cryptographic engine. *Id.*, 9:63-66. Thus, any I/O path to or from the ACE of

the SCM goes through the TSM—*e.g.*, **data is communicated between the secure processor and the cryptographic engine**. *See id.*, 10:36-39 ("I/O paths 730 between the untrusted host and the SCM 702 are managed by … a dedicated TSM partition"), 9:31-36. *See* ¶¶88, 107 of this declaration.

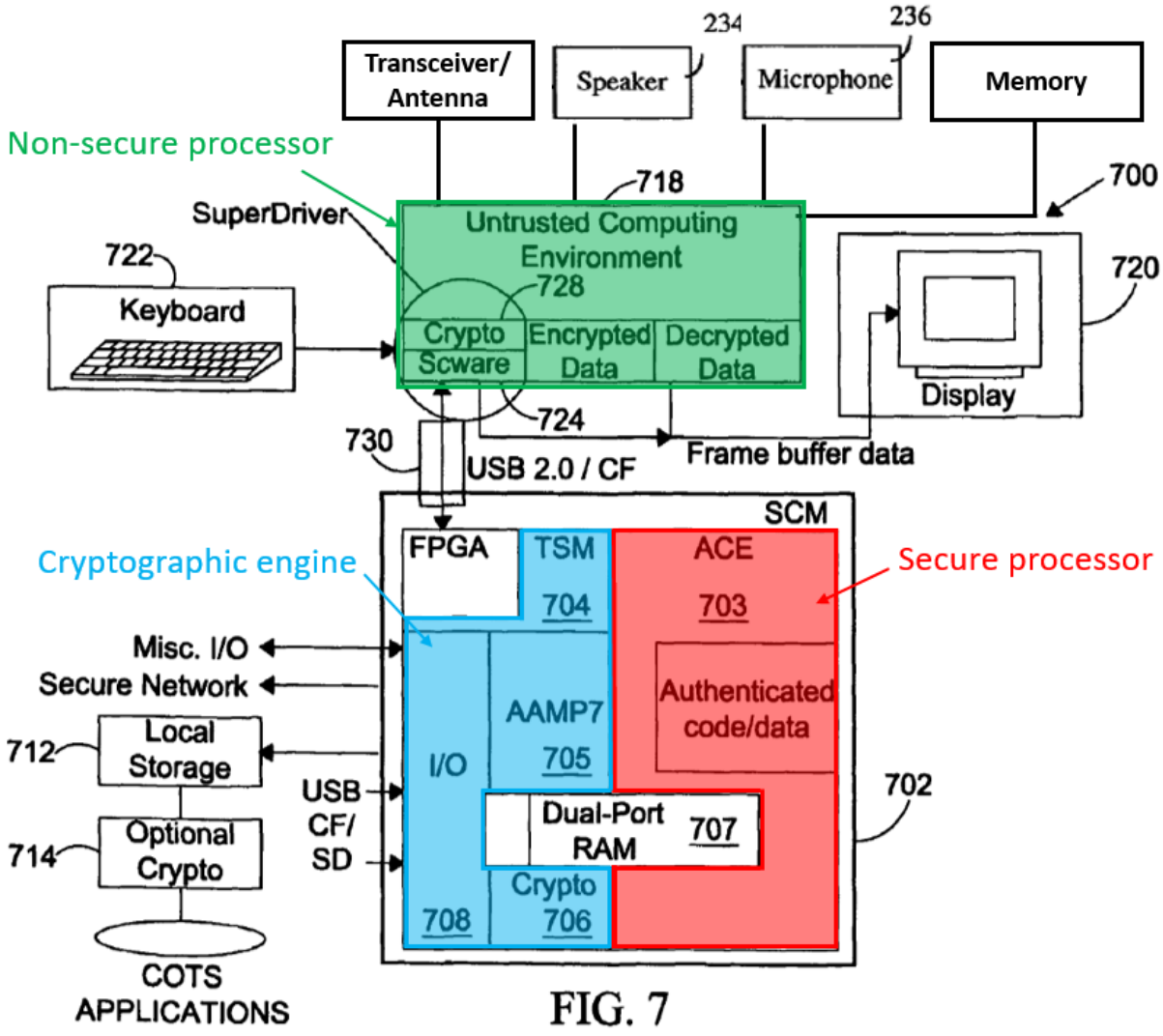


FIG. 7

Marek-Skarine composite figure

183. Also in the Marek-Skarine combination system, **the cryptographic engine is configured to encrypt any data** communicated along these I/O paths,

e.g., to **encrypt any data communicated between the secure user processor (red) and the non-secure user processor (green)**, as I discuss in the following paragraphs. *See* ¶89 of this declaration.

184. In the cryptographic engine of the Marek-Skarine combination system (*e.g.*, in Marek's TSM), Marek's trusted processor 705 "provides … partitioning" and "enforc[es] predetermined security policies," *e.g.*, such that "[e]ach I/O path … [is] secured and authenticated." APPLE-1004 (Marek), 9:31-33, 9:48-52. That is, each I/O path that passes through the TSM (including the I/O paths between the secure user processor and the non-secure processor) is "***secured and authenticated***" by Marek's TSM, *e.g.*, by the cryptographic engine of the combination. APPLE-1004 (Marek), 9:52; *see* 10:35-39 ("I/O paths 730 between the untrusted host and the SCM 702 are managed by a low power Field-Programmable Gate Array (FPGA) and a dedicated TSM partition, allowing for any number of strict ***authentication protocols***"). *See* ¶90 of this declaration.

185. Also in the cryptographic engine of the Marek-Skarine combination system (*e.g.*, in Marek's TSM), Marek's cryptographic engine 706 "aid[s] the trusted processor 705 to provide a robust security interface" by implementing "***cryptography***," which "is the widely used means for protecting information confidentiality and integrity." APPLE-1004 (Marek), 9:40-45; *see id.* ("The cryptographic engine 706 may include a reprogrammable cryptographic engine"), 10:31-

35 ("AAMP7 microprocessor provides ***a robust security interface between the red domain and the black domain through Janus Crypto Engine***"). *See* ¶91 of this declaration.

186. A cryptographic engine encrypts data. *See* APPLE-1016 (SanDisk), [0008] ("a hardware based cryptographic engine for encrypting and/or decrypting data as it passes through the secure controller"); APPLE-1017 (Macchi), 8:23-26 ("encryption of the SMS messages is implemented, by providing the sender and the receiving MSs with an SMS message cryptographic engine capable of encrypting/decrypting the SMS messages to be sent/received, based on a specified cryptographic algorithm, working with encryption/decryption keys"). *See* ¶92 of this declaration.

187. It is my opinion that a POSITA would have understood or at least found it obvious in light of the function of a cryptographic engine (*i.e.*, to encrypt data, as I discussed in the previous paragraph) and his/her knowledge that Marek's cryptographic engine 706 "aid[s] the trusted processor" in its securing and authenticating of the I/O paths (*see* APPLE-1004 (Marek), 9:40-52) by encrypting data communicated along those I/O paths. *See* ¶93 of this declaration.

188. Because these I/O paths include I/O paths between the secure user processor and the non-secure user processor, as I discussed above, the crypto-

graphic engine of the combination (*e.g.*, Marek's TSM) thus **is configured for encrypting any data communicated from the secure user processor to the non-secure user processor**, or at least a POSITA would have found this to be obvious. *See* ¶94 of this declaration.

189. Alternatively or additionally, it is my opinion that a POSITA would have found it obvious for the cryptographic engine of the combination be configured specifically for encrypting **any data communicated from the secure user processor to the non-secure user processor**. For instance, I believe that configuring Marek's TSM to encrypt ***any*** data on the I/O paths would have been a straightforward design choice to, *e.g.*, maximize security, and the hardware (*e.g.*, Marek's TSM) with this capability is already in place (*e.g.*, the capability to secure and authenticate the data on every "I/O path," APPLE-1004 (Marek), 9:48-52). Indeed, I note that a cryptographic engine generally capable of encrypting data performs the same function as a cryptographic engine encrypting any data, without producing any unexpected results. *See* ¶95 of this declaration.

190. It is my opinion that a POSITA would have understood or at least found it obvious that the data communicated between the secure processor in the

ACE and the cryptographic engine are encrypted[10] and decrypted classified data, as claimed. For instance, a POSITA would have understood or found this obvious, *e.g.*, given the above-discussed role of the cryptographic engine in communications to and from the ACE and given the role of the ACE (the secure processor) in processing encrypted data. Marek describes that the "ACE 703 of the SCM 702 may be secured by ***authenticating all code and data*** used for running COTS applications." APPLE-1004, 9:2-4. "The ACE 703 including COTS applications, manufacturer-supplied software and associated data may be cleansed, ***optionally encrypted*** and then stored on a local storage 712." APPLE-1004, 9:14-17.

191. As described with respect to [12a], it is my opinion that a POSITA would have recognized or at least found it obvious from these disclosures that, in

[10] I note that the '399 Patent describes that the "[c]lassified data ***for encryption*** and classified decrypted data can be communicated between the secure processor via the cryptographic engine using a first data communication link." APPLE-1001, 2:62-65. Thus, assuming for the sake of this proceeding only that this limitation is enabled by the brief disclosure related to it in the specification, I believe that a POSITA would understand that first data communication link need not communicate encrypted data, but instead communicate classified data for encryption by the cryptographic engine.

the Marek-Skarine combination, the classified data would have been processed exclusively using the ACE 704 of the SCM 702 (*i.e.*, the claimed "secure processor"). Because the secure processor exclusively processes the classified data within the Marek-Skarine combination and all data communicated to and processed by the secure processor is communicated via the first data communication link (*e.g.*, the virtual I/O paths implemented through dual port RAM 707), a POSITA would have understood or at least found it obvious that **the first data communication link communicates encrypted and decrypted classified data between said secure processor and a cryptographic engine**, at least in the same manner that the first data communication link 303 described in the '399 Patent communicates classified data.

[12f] communicating data from said secure processor and said cryptographic engine to said non-secure processor exclusively in an encrypted form using a second data communication link between said cryptographic engine and said non-secure processor;

192. Marek describes that "[e]ach I/O path of the SCM 702 is configured to ***go through the TSM 704***," *e.g.*, through the cryptographic engine of the combination. APPLE-1004 (Marek), 9:50-51. Moreover, Marek specifies that "[e]xamples of I/O paths of the SCM 702 include ***I/O paths between the untrusted host and the SCM***," such as I/O paths 730. APPLE-1004 (Marek), 9:50-54, 10:36-37. That is, the I/O paths 730 between the untrusted host (which contains the non-secure processor) and the SCM "go through the TSM 704," *e.g.*, through the cryptographic

engine, and thus are I/O paths for data communication between the non-secure processor and the cryptographic engine. APPLE-1004 (Marek), 9:48-64. These I/O paths 730, highlighted in purple in the composite figure below, are **a second data communication link communicating data between the non-secure processor and the cryptographic engine**. *See* ¶107 of this declaration.

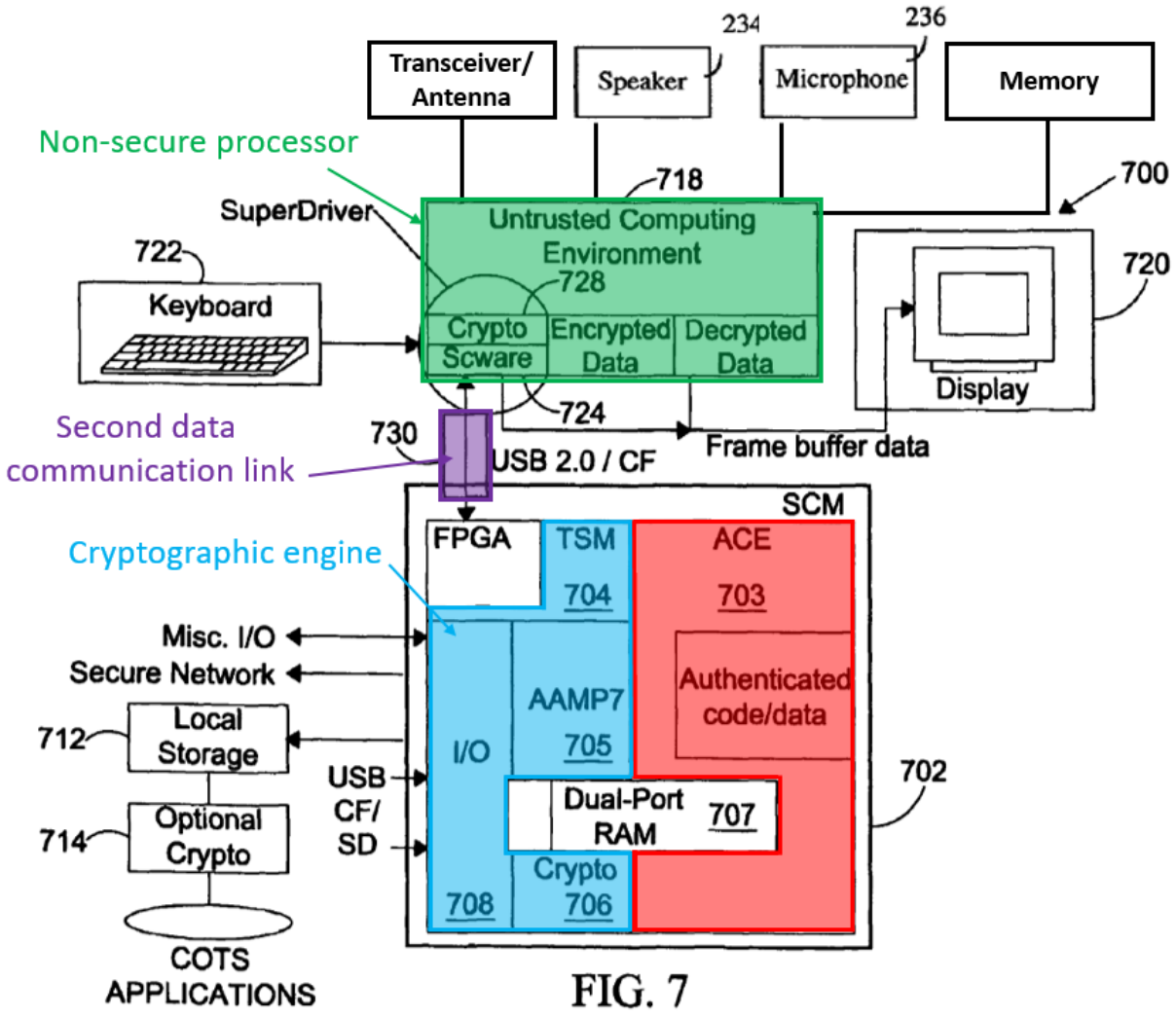


FIG. 7

Marek-Skarine composite figure

193. As I discussed above in [12e], in Marek's system, data communicated between the secure processor and the non-secure processor passes through and is encrypted by the cryptographic engine. *See* APPLE-1004, 9:31-54, 9:63-66, 10:35-39. Thus, data is **communicated from the secure processor and the cryptographic engine to the non-secure processor**.

194. It is my opinion that a POSITA would have understood or found obvious that this data communicated from the secure processor and the cryptographic engine to the non-secure processor is communicated **exclusively in an encrypted form**. For instance, Marek describes that, in one implementation, "AAMP7 microprocessor provides a robust security interface between the red domain and the black domain through Janus Crypto Engine." APPLE-1004, 10:33-35. In this implementation, "I/O paths 730 between the untrusted host and the SCM 702 are managed by a low power Field-Programmable Gate Array (FPGA) and a dedicated TSM partition, allowing for any number of strict authentication protocols." APPLE-1004, 10:35-39. Because Marek teaches that "parts of shared resources to be controlled in a structured manner to ***prevent compromising classified data***," I believe that a POSITA would have understood or at least found it obvious that the second data communication link would have communicated data from the secure processor and the cryptographic engine to the non-secure processor exclusively in an encrypted form, because the non-secure processor of the untrusted host 718 is

necessarily untrusted. For instance, in order prevent classified data from being comprised, a POSITA would have found it obvious for these data to be encrypted, *e.g.*, for the data to be communicated **exclusively in an encrypted form**.

[12g] communicating classified information to and from said secure processor using a secure human/machine interface that is configured for enabling bi-directional communication of classified information exclusively between a user and said secure processor; and

195. Marek's untrusted host mobile device 718 includes "***input and output devices*** 722, 720," such as a keypad and display of the PDA or cell phone. APPLE-1004 (Marek), 10:50-51. In the Marek-Skarine combination system, the input and output devices of the mobile device 718, which I have highlighted in pink in the composite figure below, are **a secure human/machine interface**, as I discuss in the following paragraphs. *See* ¶108 of this declaration.

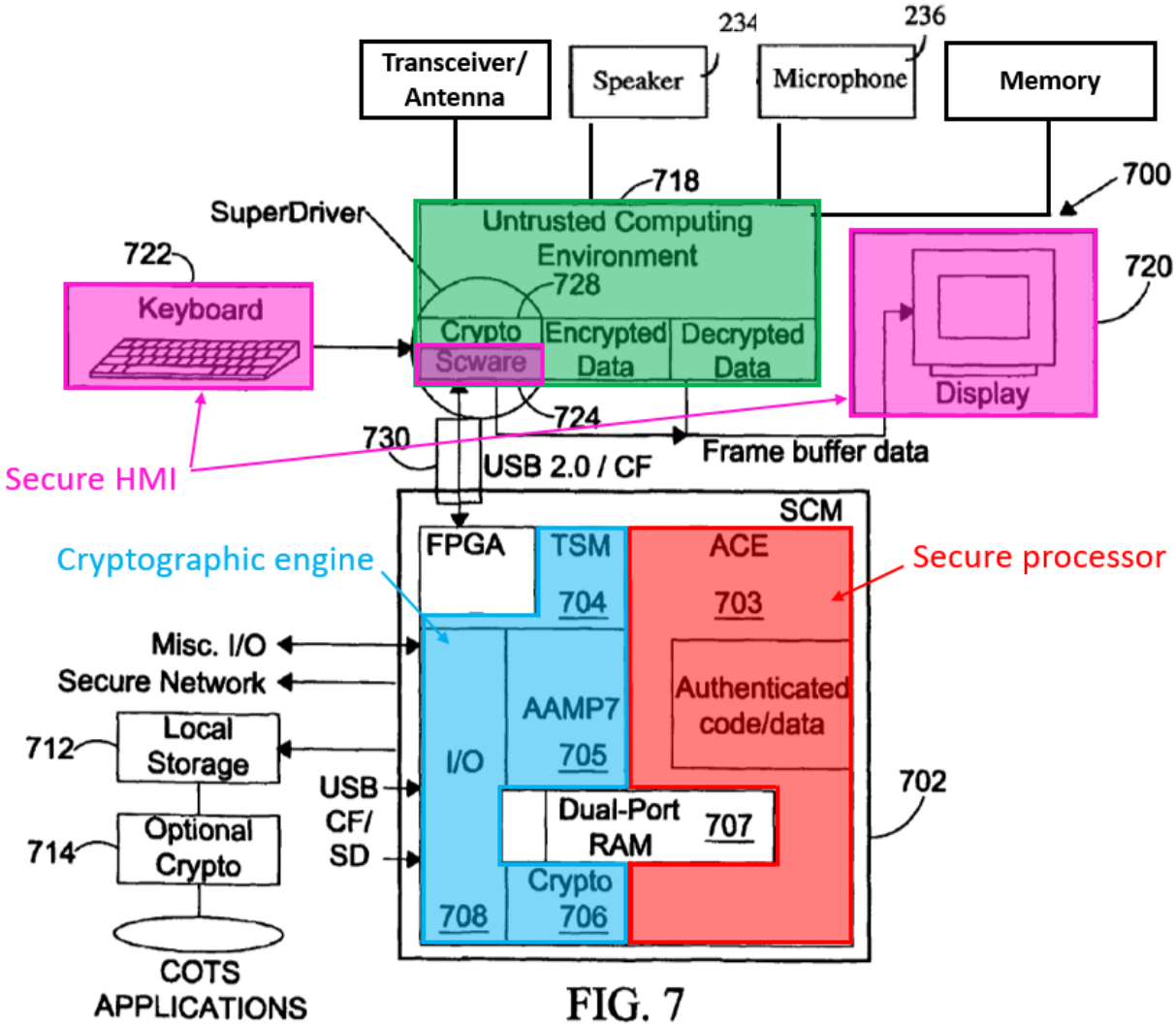


FIG. 7

Marek-Skarine composite figure

196. Marek's computing environment includes Scware 724, which is "software that acts as a trusted agent for the SCM 702 on the untrusted host environment." APPLE-1004 (Marek), 10:42-45. The Scware "resides on the untrusted host environment while the SCM 702 is operating" and, "in conjunction with the TSM 704 ***creates secure I/O paths 730 of input and output devices 722, 720*** of the untrusted host 718." APPLE-1004 (Marek), 10:42-51. Specifically, "[t]he

Scware 724 ***manages input from an input device*** (e.g. keyboard) ***and output to an output device*** (e.g. display device) while the host OS is completely bypassed." *Id.*, 10:60-65; *see* 10:52-54 ("the input and output devices 722, 720 of the untrusted host may be utilized as a virtual input/output system 800 of the SCM."), Fig. 7 and 8. That is, when the SCM 702 is in operation, information input into the input device 722 (*e.g.*, by a user) bypasses the untrusted host 718 and instead is provided to the SCM 702 along a secure I/O path 730; similarly, information from the SCM 702 is provided to the output device 720 (and thus to a user) via a secure I/O path 730, again bypassing the untrusted host 718. *See* ¶109 of this declaration.

In the Marek-Skarine combination system, Marek's input and output devices 722, 720 can be considered to be **a secure human/machine interface** at least because they are an interface by which a user inputs information to the SCM 702 (via the input device 722) and receives information from the SCM 702 (via the output device 720). *See* APPLE-1004 (Marek), 10:42-62, This interface enables **bi-directional communication of information**, *e.g.*, communication from the user to the SCM and from the SCM to the user. *See id.*, 10:42-62. *See* ¶110 of this declaration.

197. In the Marek-Skarine combination system, the secure human/machine interface enables bi-directional communication of information **between a user and the secure user processor**, *e.g.*, between a user and the processor of the ACE 703

(highlighted in red in the composite figure above), as I discuss in the following paragraphs. *See* ¶111 of this declaration.

198. First, Marek generally describes that the input and output devices 722, 720, *e.g.*, the secure human/machine interface, enable communication between a user and the SCM 702, which contains the ACE. *See* APPLE-1004 (Marek), 10:49-51 ("The Scware 724 implemented in conjunction with the TSM 704 creates ***secure I/O paths 730*** of input and output devices 722, 720 of the untrusted host"), 10:52-54 ("the input and output devices 722, 720 of the untrusted host 718 may be utilized as ***a virtual input/output system 800 of the SCM***"), 11:39-41 ("a virtual keyboard and display usable for ***user interface with the SCM***"), Figs. 7 and 8. *See* ¶112 of this declaration.

199. Second, it is my opinion a POSITA would have understood or at least found obvious that the described communication between the user and the SCM is specifically **between the user and the secure user processor** of the ACE 703. For instance, I believe that a POSITA would have understood or at least found obvious that such communication would occur, *e.g.*, to enable information from a user to be provided as input to the "COTS applications, manufacturer-supplied software and the like" of the ACE and information generated by the applications/software of the ACE to be provided as output to a user. APPLE-1004 (Marek), 9:13-14. Additionally, I believe that a POSITA, given Marek's disclosure

that "[e]ach I/O path of the SCM 702 is configured to ***go through the TSM***," and moreover that "any I/O from/to the ACE 703 is configured to ***go through the TSM***," would have recognized or at least found obvious that the I/O paths that go through the TSM extend to the ACE, *e.g.*, the I/O paths are **between the user and the secure user processor** of the ACE. APPLE-1004 (Marek), 9:50-51, 9:63-64; *see* 10:49-51. *See* ¶113 of this declaration.

200. Moreover, the communication of information enabled by the secure human/machine interface is **exclusively** between the user and the secure user processor, or at least a POSITA would have found this to be obvious. In Marek's "H-mode" operation, "[t]he Scware 724 manages input from an input device (e.g. keyboard) and output to an output device (e.g. display device) ***while the host OS is completely bypassed***. As a result, the Scware 724 operates as ***a dedicated input/output device driver***." *Id.*, 10:55-65; *see* 10:65-67 ("a security critical section concept is used to implement the Scware 724 in H-mode ***to disable all applications but the Scware 724 on the host environment***"). Marek also describes that "[i]n the autonomous execution state, ***the host's only function is to provide power*** to the SCM 702. Alternatively, ***the host may not provide any functions at all*** if the SCM 702 provides its own power source." *Id.*, 11:31-36. That is, when the SCM 702 is operational, the operating system of the untrusted host device is "completely bypassed," with all functionality other than providing power being disabled. *Id.*,

10:60-65, 11:31-36. Thus, at least because the functionality of the untrusted host device is disabled, the communication enabled by the secure human/machine interface is **exclusively between the user and the secure user processor**, or at least this would have been obvious to a POSITA. *See* ¶114 of this declaration.

This secure human/machine interface is **secure** (or at least a POSITA would have found this to be obvious) at least because it is an interface to the "***Secure COTS computing environment***" provided by the SCM 702 of the combination. APPLE-1004 (Marek), 8:37-39; *see* 8:39-45, 1:66-2:4 ("a system including a Secure Computing Module (SCM) provides ***trusted environment*** for COTS host platforms. Only authenticated trusted applications execute on the SCM."), 2:13-20 ("The ACE may be secured by authenticating all code and data used for running COTS applications."), 2:31-38 ("the system including the SCM may provide trusted and portable COTS computing environments against malware"). *See* ¶115 of this declaration.

The secure human/machine interface enables communication of **classified information** in that the information is communicated along "secured and authenticated" I/O paths and is encrypted by Marek's cryptographic engine. APPLE-1004 (Marek), 9:50-52; *see* 9:37-44. To the extent that "classified information" is interpreted to refer specifically to, *e.g.*, information designated as implicating matters of national security, Marek describes that the TSM processor 705 "provides a robust

security interface between ***the red domain and the black domain*** through" the cryptographic engine 706— *e.g.*, between the SCM and the untrusted host mobile device 718. APPLE-1004 (Marek), 10:33-36. Information communicated between a user and the red domain (Marek's SCM) can be **classified information**. *See* ¶116 of this declaration.

[12h] communicating unclassified information to and from said non-secure processor using a non-secure human/machine interface that is distinct from said secure human/machine interface and configured for enabling bi-directional communication of unclassified information exclusively between said user and said non-secure processor.

201. In the Marek-Skarine combination system, the untrusted host mobile device 718 includes a speaker and a microphone, which I have highlighted in orange in the composite figure below. This was a well-known and conventional configuration in the art, as demonstrated, for instance, by Skarine. *See* APPLE-1005 (Skarine), [0038] ("Mobile device 202 includes a microprocessor 238 … [that] interacts with additional device subsystems such as … a speaker 234 [and], a microphone 236"), [0042] ("For voice communications, the overall operation of mobile device 202 is substantially similar, except that the received signals would be output to speaker 234 and signals for transmission would be generated by microphone 236"), Fig. 2; *see also* APPLE-1018 (Yach), 3:45-50 (describing a microprocessor of a mobile device that "interacts with additional subsystems such as … a speaker

118 [and] a microphone 120"), 6:22-32; APPLE-1010 (Zuberec), 3:54-67; APPLE-1024 (Lu), [0004]; APPLE-1025 (Song), 1:18-20. *See* ¶117 of this declaration.

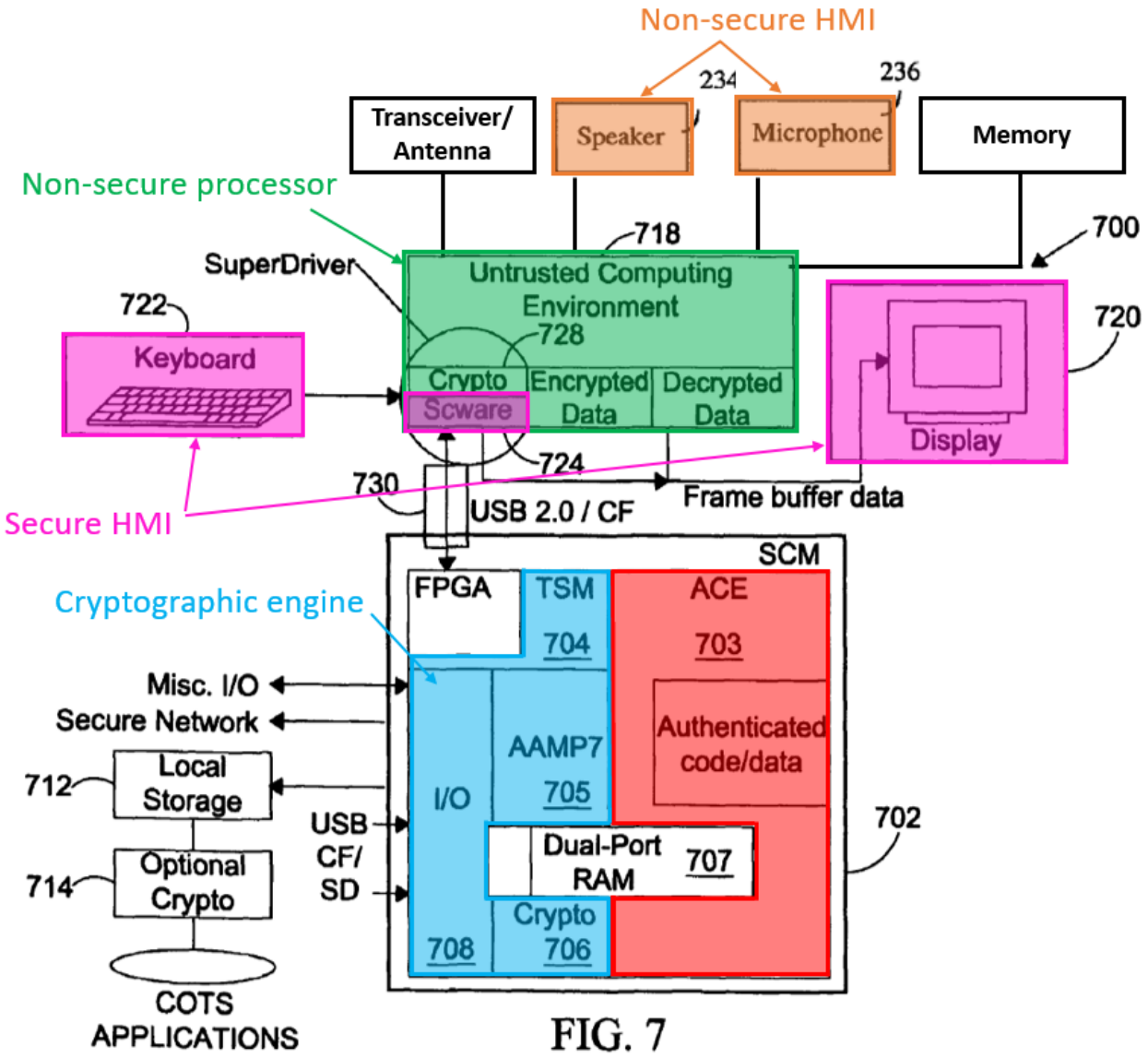


FIG. 7

Marek-Skarine composite figure

202. The speaker and microphone together are **a non-secure human/machine interface** at least because they are an interface by which a user inputs information to and receives information from the untrusted host mobile device 718 (via

the microphone and speaker, respectively), as I discuss in the following paragraphs. *See* APPLE-1005 (Skarine), [0041]-[0042]. *See* ¶118 of this declaration.

203. The non-secure human/machine interface is **distinct from the secure human/machine interface**. For instance, the speaker and microphone (the non-secure human/machine interface) are components that are distinct (*e.g.*, physically separate) from the input and output devices 722, 720 (the secure human/machine interface), as illustrated in the figure above. *See* ¶119 of this declaration.

204. The non-secure human/machine interface, *e.g.*, the speaker and microphone, is **configured for enabling bi-directional communication of information between said user and said non-secure user processor**. In the Marek-Skarine combination system, based on the teachings of Skarine, information is communicated from the processor of the untrusted host mobile device to the speaker, and from the microphone to the processor. *See* APPLE-1005 (Skarine), [0041]-[0042] ("For voice communications, the overall operation of mobile device 202 is substantially similar" to the operation in "data communication mode," where signals are communicated between a user and Skarine's mobile device processor via input and output devices.), [0038] ("Microprocessor 238 also interacts with additional device subsystems such as … a speaker 234, a microphone 236"), Fig. 2. Additionally, signals from the speaker are communicated to a user, and audio input from a user are received by the microphone. *See* APPLE-1005 (Skarine), [0042]

("the received signals would be ***output to speaker 234*** and ***signals for transmission would be generated by microphone 236***," "voice or audio signal output is preferably accomplished primarily through speaker 234"). That is, the speaker and microphone enable **bi-directional communication of information between the user and the non-secure user processor** (*e.g.*, the processor contained in the untrusted host mobile device 718, highlighted in green). *See* ¶120 of this declaration.

205. Moreover, the non-secure human/machine interface, *e.g.*, the speaker and microphone, is configured for enabling communication of information **exclusively** between the user and the non-secure processor. As described by Marek, "[e]ach I/O path 702 of the SCM 702 is configured to go through the TSM 704." APPLE-1004 (Marek), 9:50-51. Based on the teachings of Skarine, the microphone and speaker are connected to the non-secure user processor of the untrusted host mobile device, and not to the SCM or the TSM. Thus, the information is not communicated between the speaker/microphone and the secure user processor; rather, it is communicated **exclusively between the user and the non-secure processor**. *See* ¶121 of this declaration.

206. The non-secure human/machine interface is **non-secure** (or at least a POSITA would have found this to be obvious) at least because it is part of "the untrusted host environment" of the combination. APPLE-1004 (Marek), 8:40-41; *see*

8:56-59 ("a host platform employing COTS processors is assumed to be ***un-trusted***"), 12:16-18 ("Untrusted application software and hardware may be implemented in the PDA"), 2:1-4, 2:36-38. *See* ¶122 of this declaration.

The non-secure human/machine enables communication of **unclassified information**[11] because the information communicated between the speaker/microphone and the processor of the untrusted host mobile device 718 is not transmitted on the "secured and authenticated" I/O paths provided by Marek's TSM, nor is it subject to the encryption provided by Marek's cryptographic engine. *See* APPLE-1004 (Marek), 9:40-53. To the extent that "unclassified information" is interpreted to refer specifically to, *e.g.*, information designated as not implicating matters of national security, the untrusted host mobile device is in the black domain of Marek's computing environment. *See* APPLE-1004 (Marek), 10:33-36, Figs. 9-11. Information remaining in the black domain of such an environment— *e.g.*, information communicated via the non-secure human/machine interface—can be **unclassified information**. *See* ¶123 of this declaration.

[11] I understand that there is disagreement in the co-pending litigation regarding the interpretation of the term "unclassified." I address this term here and elsewhere in this Petition as I best understand it and without conceding that its meaning is clear.

207. I thus conclude that the speaker and microphone communicate unclassified information to and from said non-secure processor and enable bi-directional communication of unclassified information exclusively between said user and said non-secure processor, because the data communicated between the speaker/microphone and the non-secure processor is not transmitted on the "secured and authenticated" I/O paths and is therefore not subject to the encryption provided by the cryptographic engine.

(xi) Claim 13

[13] The method according to claim 12, further comprising controlling said secure processor exclusively using said secure human/machine interface.

208. In the Marek-Skarine combination system, the secure human/machine interface includes the input and output devices 722, 720 (*e.g.*, the keypad and display of the mobile device). *See* my analysis of element [1g]. The input device, *e.g.*, a keypad, is an **input device that allows the user to control the secure processor**. Input received from a user through the input device, *e.g.*, keypad, is provided to the secure user processor. *See* APPLE-1004 (Marek), 9:13-14, 9:50-64, 10:49-54, 11:39-41; *see* my analysis of element [1g]. Moreover, "COTS applications [and] manufacturer-supplied software" execute on Marek's ACE, *e.g.*, on the secure user processor. APPLE-1004 (Marek), 9:13-15; *see* 2:31-42, 12:18-19 ("trusted applications are implemented in the SCM 908"); *see* my analysis of ele-

ment [1b]. It is my opinion that a POSITA would understand that when the received input is information used during execution of one of the applications or software on the secure user processor, that input **controls the secure user processor**. *See* ¶126 of this declaration.

209. I note that Marek describes an implementation in which "[t]he Scware 724 manages input from an input device (e.g. keyboard) and output to an output device (e.g. display device) ***while the host OS is completely bypassed***. As a result, the Scware 724 operates as ***a dedicated input/output device driver***." *Id.*, 10:55-65; *see* 10:65-67 ("a security critical section concept is used to implement the Scware 724 in H-mode ***to disable all applications but the Scware 724 on the host environment***"). Marek also describes that "[i]n the autonomous execution state, ***the host's only function is to provide power*** to the SCM 702. Alternatively, ***the host may not provide any functions at all*** if the SCM 702 provides its own power source." *Id.*, 11:31-36. Thus, at least because the functionality of the untrusted host device is disabled when the SCM is operational, a POSITA would have found obvious that in this operational state, the secure user processor is controlled **exclusively using the secure human/machine interface**, *e.g.*, at least because all other functionality of the host device is disabled, thus rendering the secure human/machine interface the only (*e.g.*, exclusive) means for controlling the secure processor.

210. I also believe that to having the secure processor controlled exclusively using the secure human/machine interface would have been a straightforward design choice that a POSITA would have found to be obvious, *e.g.*, to provide security to the operation of the secure processor. A secure human/machine interface that is generally capable of controlling a secure processor—such as Marek's secure human/machine interface —would operate in the same way regardless of whether or not it exclusively controls that processor, and would have no unexpected results.

(xii) Claim 15

[15] The method according to claim 12, further comprising performing wireless data communication of unclassified data from said non-secure processor using a wireless communications transceiver.

The combination device includes a communications transceiver

211. Marek describes that "the SCM is added on ***wireless devices*** such as PDAs, cell phones, and other mobile devices," *e.g.*, the untrusted host mobile device 718 in the combination is a wireless device. APPLE-1004 (Marek), 11:53-56. It is my opinion that a POSITA would have understood—or at least found it obvious—that a "wireless device[]," (*id.*) such as the untrusted host mobile device of the combination, includes **a communications transceiver**, which I have highlighted in pink in the composite figure below. Moreover, it is also my opinion that a POSITA would have understood or found it obvious for the communications transceiver to be coupled to the non-secure user processor of the untrusted host

mobile device of the combination (still highlighted in green). *See* ¶¶72-74 of this declaration.

212. I hold this opinion at least because it was conventional in the art as of the Critical Date for wireless devices such as PDAs or cell phones to have communications transceivers to enable wireless communication. This is demonstrated, for instance, by Skarine. *See* APPLE-1005 (Skarine), [0022] ("signal processing operations associated with ***communication functions are typically performed in RF transceiver circuitry*** 108"), [0023] ("Mobile device 102 sends communication signals to and receives communication signals from network 104 over a wireless link via antenna 110. RF transceiver circuitry 108 performs functions such as modulation/demodulation and possibly encoding/decoding and encryption/decryption. It will be apparent to those skilled in art that ***RF transceiver circuitry 108 will be adapted to particular wireless network or networks*** in which mobile device 102 is intended to operate."), [0035] ("Mobile device 202 will normally incorporate ***a communication subsystem 211, which includes a receiver 212, a transmitter 214***, and associated components … Communication subsystem 211 is analogous to RF transceiver circuitry 108 and antenna 110"), [0027]-[0029], [0036]-[0038], Figs. 1-2. *See* ¶¶72-74 of this declaration.

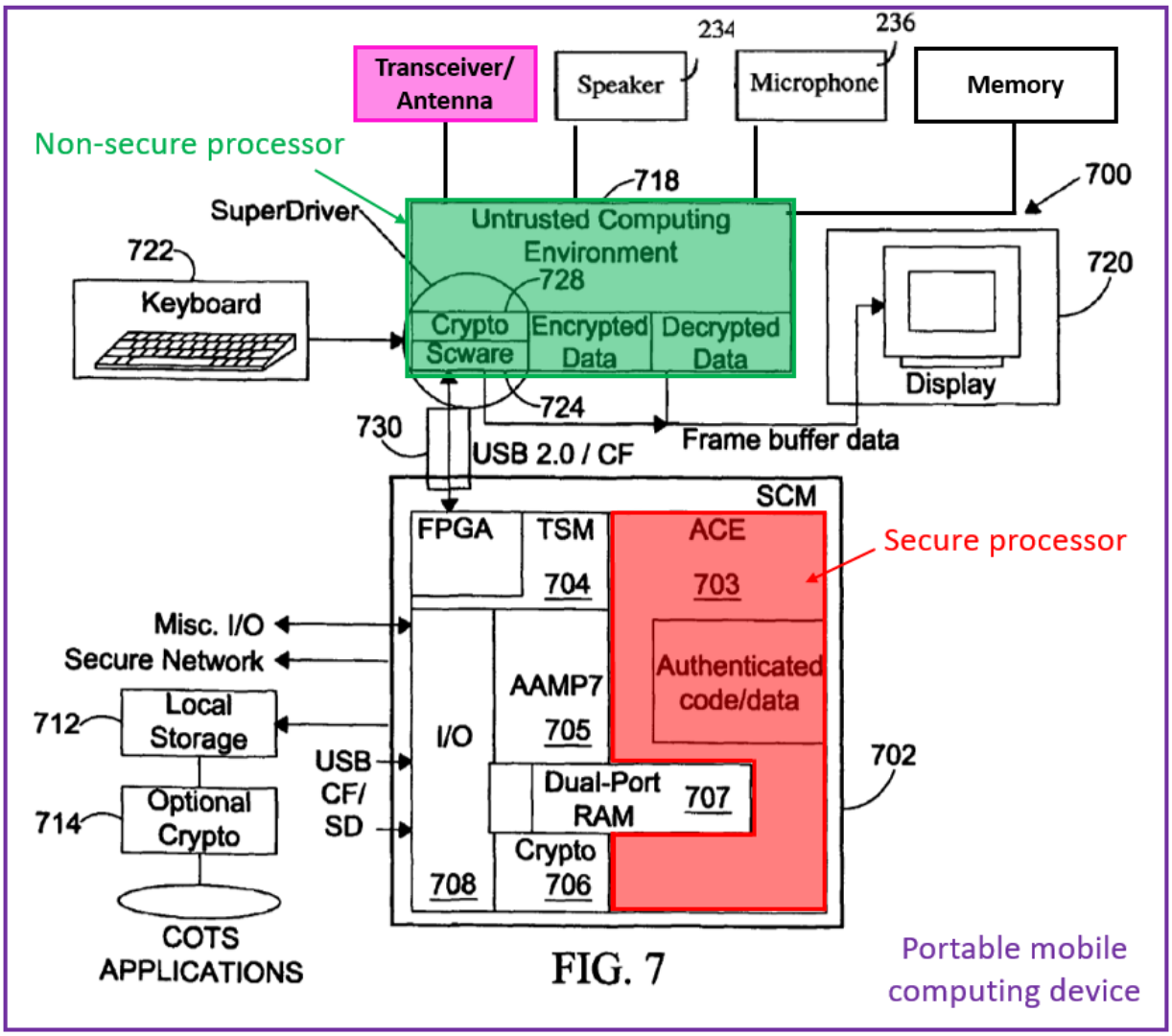


FIG. 7

Marek-Skarine figure

The communications transceiver of the combination performs wireless data communication of unclassified data from said non-secure processor

213. In the Marek-Skarine combination system, **the communications transceiver is operatively coupled to the non-secure user processor** based on the teachings of Skarine, as I have illustrated in the composite figure below. *See* APPLE-1005 (Skarine), [0038], Fig. 2 (illustrating a mobile device, such as a cellular telephone or a PDA in which the receiver 212 and transmitter 214, *e.g.*, a

communications transceiver, are coupled to the microprocessor 238). *See* ¶124 of this declaration.

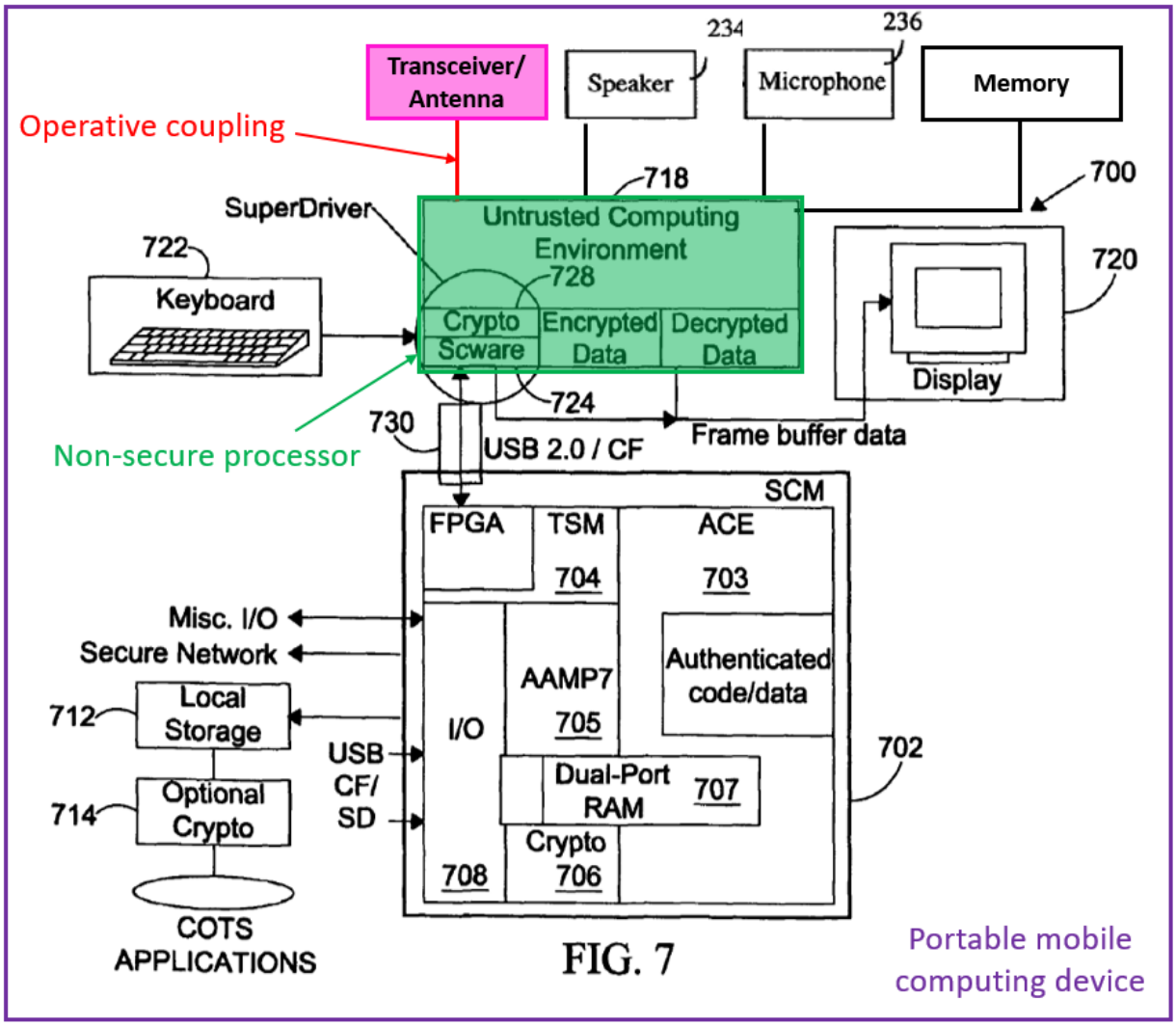


FIG. 7

Marek-Skarine figure

It is my opinion that a POSITA would have understood or found obvious that the **communications transceiver is configured for communicating data from the non-secure processor**, *e.g.*, to a destination external to the portable mo-

bile computing device, *e.g.*, given the coupling between the communications transceiver and the non-secure user processor. For instance, this was a standard and well-known function of communications transceivers as of the Critical Date. *See* APPLE-1005, [0022] ("signal processing operations associated with ***communication functions are typically performed in RF transceiver circuitry*** 108"), [0023], [0038], [0027]-[0029], [0035]; APPLE-1015, 3:11-17 (describing a mobile device having a "WAN modem 111 [that] includes a ***primary receiver and transmitter (primary transceiver) that are configured to operate on or with a first, e.g., WAN, network***."); APPLE-1011, 5:11-13, 4:46-59; APPLE-1017, 10:14-18; APPLE-1018, 6:33-45, 7:11-29. *See* ¶125 of this declaration.

214. Furthermore, it is my opinion that a POSITA would have understood or found obvious that any data communicated from the non-secure processor would have been **unclassified data**. As I noted above with respect to [12c], Marek describes that "[o]nly authenticated COTS applications and COTS OS execute on the SCM while ***untrusted applications execute on the untrusted host environment***." APPLE-1004, 8:39-41. It is my opinion that a POSITA would have understood or found obvious that any data communicated via the communications transceiver from the untrusted applications execute on the untrusted host environment would necessarily be unclassified data.

(xiii) Claim 16

[16] The method according to claim 15, further comprising communicating encrypted classified data from said secure processor using said wireless communications transceiver.

215. As illustrated in FIG. 10, which I have reproduced below, Marek describes the SCM "may interface between a black domain and a red domain through a wireless network module 902 and the cryptographic engine 904." APPLE-1004, 11:60-63. "A trusted processor 906 such as AAMP7 microprocessor may provide a robust security interface between red domain and wireless networks (black domain) through the cryptographic engine 904 such as Janus Crypto Engine and the secure wireless module 902." APPLE-1004, 12:1-6. Based on these teachings, it is my opinion that a POSITA would have understood or found obvious that the secure processor (contained in the ACE of the combined system, highlighted in red below) would have been capable of communicating using the wireless network module 902 (highlighted in blue) via the AAMP7 microprocessor and Janus Crypto Engine, which would have encrypted any classified data.

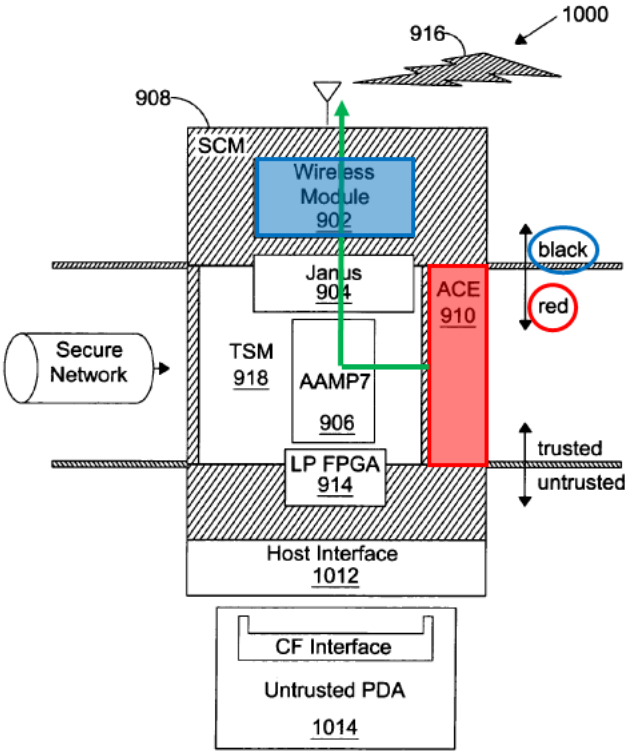


FIG. 10

Marek, Fig. 10 (annotated)

216. While Marek describes and illustrates the wireless module 902 as part of the SCM 908, it is also my opinion that a POSITA would have found it obvious to utilize the wireless transceiver contained in the untrusted host wireless device of the combination for communication from the secure processor. Marek describes that the "trusted environment may include trusted hardware and software ensuring access to certain resources, or ***parts of shared resources to be controlled in a structured manner to prevent compromising classified data***." APPLE-1004,

8:61-64. Marek further describes that "[e]xamples of I/O paths of the SCM 702 include I/O paths between the untrusted host and the SCM . . . ." APPLE-1004, 10:53-56. A POSITA would have found it obvious that, like the input and output devices 722, 720 of the untrusted host 718, the Scware 7242 could be used to completely bypass the host OS and control the wireless transceiver of the untrusted host 718 such that the wireless transceiver of the untrusted host 718 in the same manner as described with respect to the wireless module 902. Moreover, Marek contemplates that use of the wireless transceiver of the untrusted host 718 could be subject to security protocols, *e.g.*, in its indication that "all network accesses require[e] authentication." *Id.*, 8:49-50.

(xiv) Claim 17

[17] The method according to claim 15, further comprising selecting said wireless communications transceiver from the group consisting of a wireless LAN transceiver and a cellular telephone transceiver.

217. In the Marek-Skarine combination system, the communications transceiver (*see* [1a]) is **a cellular telephone transceiver**, *e.g.*, based on the teachings of Skarine. Skarine describes RF transceiver circuitry 108 that is "adapted to particular wireless network or networks in which mobile device 102 is intended to operate." APPLE-1005 (Skarine), [0023]; *see* [0035] ("particular design of communication subsystem 211 depends on the communication network in which mobile

device 202 is intended to operate"). Moreover, Skarine's mobile device is "intended to operate" in a cellular telephone network. *Id.*, [0023]; *see* [0027]-[0028] ("wireless network 104 is configured in accordance with General Packet Radio Service (GPRS) and a Global Systems for Mobile (GSM) technologies," *i.e.*, cellular telephone networks (*see* APPLE-1026 (Lucidarme), [0011] ("Some second generation cellular networks (GSM, Global System for Mobile communications) now include a packet transmission service called CPRS (General Packet Radio Service)"), APPLE-1027 (Naegeli), Abstract ("Global System for Mobile Communications (GSM/GPRS) cellular telephone network"))), [0026] ("a cellular telephone"), [0034] ("a cellular telephone … [that] may communicate with any one of a plurality of fixed transceiver stations 200 within its geographic coverage area"). In the combination, the communications transceiver is designed for operation in a cellular telephone network, *i.e.*, it is a cellular telephone transceiver. *See* ¶133 of this declaration.

218. It is my opinion that a POSITA would have been motivated to implement the communications transceiver as a cellular telephone transceiver, *e.g.*, based on the teachings of Skarine. It is also my opinion that a POSITA would have expected success in doing so. *See* ¶¶134-137 of this declaration.

(xv) Claim 18

[18] The method according to claim 12, further comprising storing classified data in a first file system accessible only to said secure user processor and

storing unclassified data in a second file system distinct from said first file system which is accessible to said non-secure user processor, thereby providing physical separation of said classified data from said unclassified data within said portable mobile computing device.

219. In the Marek-Skarine combination system, Marek's SCM includes "a local storage 712" (highlighted in orange in the composite figure below), *e.g.*, **a first file system**. APPLE-1004 (Marek), 9:14-19. This first file system is **for storing classified data**. *See id.*, 9:14-24 ("The ACE 703 including COTS applications, manufacturer-supplied software and associated data may be cleansed, optionally encrypted and then stored on a local storage 712."), 2:16-17 ("The ACE may be cleansed and encrypted and then stored on a local encrypted storage."). To the extent that "classified data" is interpreted to refer specifically to, *e.g.*, information designated as implicating matters of national security, data stored in the red domain in the combination— *e.g.*, data stored in the first file system of Marek's SCM—can be **classified data**. *See* APPLE-1004 (Marek), 10:33-36. *See* ¶138 of this declaration.

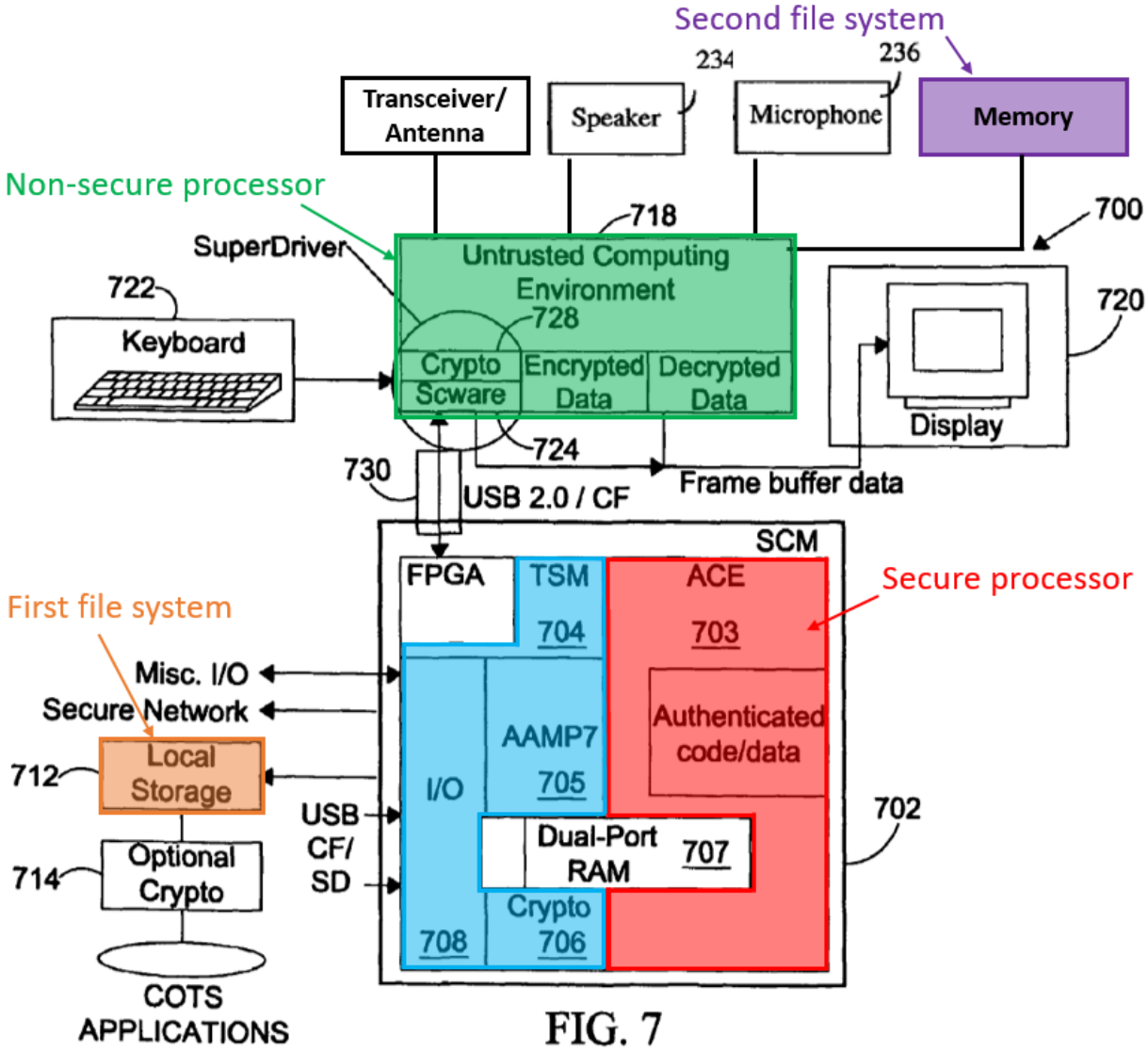


FIG. 7

Marek-Skarine composite figure

220. The first file system, *e.g.*, the local storage 712, is **accessible only to the secure processor**, *e.g.*, the processor of Marek's ACE. For instance, Marek describes that "[a]ll secure resources," including the local storage 712, are "maintained on the trusted side of the plug-in module interface." APPLE-1004 (Marek), 2:5-7; *see* 2:40-41. Moreover, Marek describes that the secure processor accesses the local storage 712: "The ACE 703 including COTS applications, manufacturer-

supplied software and associated data may be … stored on a local storage 712." *Id.*, 9:14-17; *see* 9:22-25, 10:4-5. *See* ¶139 of this declaration.

The combination includes a second file system for storing unclassified data

221. As discussed in [12b], the untrusted host mobile device of the combination includes an operating system and application software. *See* APPLE-1004, 7:54-55, 8:56-59, 8:40-41, 12:16-18. It is my opinion that a POSITA would have understood or at least found obvious that the untrusted host mobile device 718 includes **a second file system**, *e.g.*, memory including non-volatile and volatile memory (highlighted in purple in the composite figure above), *e.g.*, for storage of the operating system, applications, and associated application data. This was well-known and conventional in the art as of the Critical Date, as demonstrated, for instance, by Skarine. *See* APPLE-1005, [0038] ("Operating system software used by microprocessor 238 is preferably stored in a persistent store such as flash memory 224, which may alternatively be a read-only memory (ROM) or similar storage element … the operating system, specific device applications, or parts thereof, may be temporarily loaded into a volatile store such as RAM 226"), [0040], [0050]-[0053]; APPLE-1018, 3:58-64; APPLE-1011, 4:54-59 ("Memory 22 includes an operating system 30, the application programs 16 … and the object store 18. During operation, the operating system 30 is loaded into, and executed by, the processor 20

from memory 22."); APPLE-1009, 5:26-30; APPLE-1010, 3:17-39; APPLE-1012, [0013]; APPLE-1017, 10:14-22. *See* ¶¶140-141 of this declaration.

222. In the Marek-Skarine combination system, the **second file system is for storing unclassified data**, *e.g.*, for storing the untrusted operating system of the untrusted host mobile device. *See* APPLE-1005 (Skarine), [0038] ("Operating system software used by [the] microprocessor" of the untrusted host mobile device 718 is "stored in a persistent store such as flash memory 224 … a read-only memory (ROM) or similar storage element"), [0022]-[0023]; APPLE-1004 (Marek), 7:54-55; APPLE-1010, 3:17-21 ("The mobile device 100 includes an operating system 164 … which is resident in the memory 162 and executes on the processor 160"); APPLE-1011, 4:54-59 (describing a mobile device having "[m]emory 22 [that] includes an operating system 30 … During operating, the operating system 30 is loaded into, and executed by, the processor 20 from memory 22"); APPLE-1018, 3:58-64. *See* ¶142 of this declaration.

223. Data stored in the untrusted host mobile device 718, such as the unstrusted operating system software, can be considered to be **unclassified** at least because it is not transmitted on the "secured and authenticated" I/O paths provided by Marek's TSM, nor is it subject to the encryption provided by Marek's cryptographic engine. APPLE-1004 (Marek), 9:40-53; *see* 2:36-37 ("untrusted applications execute on the untrusted host environment"). To the extent that "unclassified

data" is interpreted to refer specifically to, *e.g.*, information designated as not implicating matters of national security, data stored in the black domain in the combination— *e.g.*, data stored in the second file system of the untrusted host mobile device—can be **unclassified data**. *See* APPLE-1004 (Marek), 10:33-36. *See* ¶143 of this declaration.

224. The second file system is **distinct from the first file system**, *e.g.*, the persistent storage of the untrusted host mobile device 718 is distinct (*e.g.*, physically separate) from the local storage 712 in the SCM, as illustrated in the composite figure above. Because the second file system is distinct from the first file system, the classified data are stored in a different physical location than the unclassified data, *e.g.*, the distinctness of the two file systems **provides physical separation of the classified data from the unclassified data within the portable mobile computing device**. *See* ¶144 of this declaration.

B. [GROUND 1B] – CLAIMS 4-5 WOULD HAVE BEEN OBVIOUS OVER MAREK, SKARINE, AND YOON

1. Yoon describes a mobile device providing voice command functionality

225. Yoon describes "a mobile communication terminal," such as a "cellular phone," "provided with a hands-free function capable of originating a call or receiving a call by a user's voice command." APPLE-1007 (Yoon), [0002], [0004]. Yoon's mobile communication terminal includes "a microphone 140 for inputting

a user's voice … and a micro computer 120 for controlling an operation of the mobile communication terminal according to a user's voice inputted to the microphone 140 in controlling an operation for calling." *Id.*, [0030]. The micro computer 120 implements "a voice-dialing function for recognizing calling party's information inputted by the user's voice, thereby searching from the telephone directory, and guiding the search result by voice," and "a voice command function for recognizing a calling command such as a calling connection, a calling finishing, and etc. by a voice command." *Id.*, [0032]. For instance, "[w]hen the user of the mobile communication terminal inputs a calling party's name through the microphone 140 (S403), the micro computer 140 searches a mounted telephone directory (S404) thus to certify whether the calling party's name inputted by the user's voice exists," and ultimately "originates a calling with the selected telephone number thus to perform a calling connection." *Id.*, [0043]-[0047].

2. The combination of Marek, Skarine, and Yoon

226. In the Marek-Skarine-Yoon combination system, the untrusted host mobile device 718 (*e.g.*, a PDA or cell phone, as I have discussed previously) implements voice command functionality based on the teachings of Yoon. For instance, the non-secure microprocessor of the untrusted host mobile device 718 has "a voice dialing function" and "a voice command function" to search for a calling party and to carry out a call-related command based on the user's voice input

through the microphone of the combination device. *See* APPLE-1007 (Yoon), [0032]-[0032], [0043]-[0047].

3. Reasons for the combination

227. It is my opinion that a POSITA would have been motivated to pursue the Marek-Skarine-Yoon combination, in which voice command functionality is incorporated into the untrusted host mobile device, for at least the following reasons.

228. One reason why a POSITA would have been motivated to incorporate voice command functionality into the untrusted host mobile device of the combination is that the hands-free calling functionality that is enabled by this modification expands the scope of the situations in which the user can use the mobile device, thus making the mobile device more accessible. For instance, I believe that a POSITA would have recognized that hands-free calling functionality allows the user to make calls while driving without compromising safety and while complying with relevant driving regulations. *See* APPLE-1007 (Yoon), [0005] ("it is regulated to directly use the mobile communication terminal at the time of driving since it may cause an unexpected accident due to an attention lowering. That is, when the user receives a call at the time of driving, the user has to press a button of the mobile communication terminal or open a folder by using hands, and when the

user originates a call, eyes of the user have to be towards the mobile communication terminal with hands thus to lower the user's attention.”).

229. Another reason why a POSITA would have been motivated to incorporate a voice command functionality into the untrusted host mobile device of the combination is because this is just the implementation of known techniques (*e.g.*, voice commands) by a known system (*e.g.*, the untrusted host mobile device of the combination) that results in a predictable outcome (*e.g.*, a mobile device with conventional voice command capabilities).

230. It is also my opinion that a POSITA would have expected to be successful in incorporating voice command functionality into the untrusted host mobile device of the combination given that a POSITA would have understood or found obvious for the relevant hardware components (*e.g.*, microphone and speakers) to be included in the Marek-Skarine combination untrusted host mobile device, as I have already discussed. *See*, *e.g.*, my analysis of element [1h].

231. I also believe that a POSITA would have expected to be successful in pursuing this implementation because voice recognition and voice command technology was widespread in the context of mobile devices as of the Critical Date. *See* APPLE-1040 (Katzur), Abstract (“a mobile telephone having a voice recognition system which receives and acts on voice commands”); APPLE-1041 (Gehrke), Abstract (“A wireless communication system employs a method and apparatus for

providing voice recognition service to a wireless communication device"); APPLE-1042 (Ericsson), Abstract ("A wireless mobile station having voice recognition capabilities to determine authorized user of the mobile station"); APPLE-1043 (Seo), Abstract ("a method for initiating a mode for performing a function through voice recognition on a mobile device, which comprises the steps of … shifting to a voice dialing mode for making a call through voice recognition").

232. Additionally, I believe that a POSITA would have expected success because Yoon, like Marek and Skarine, generally pertains to the field of mobile devices. *See* APPLE-1004 (Marek), 11:44-56, 12:31021, 13:49-51, 2:56-59, 7:53-57, 8:25-38, Figs. 10 and 11; APPLE-1005 (Skarine), [0001]; APPLE-1007 (Yoon), Abstract ("a mobile communication terminal provided with a hands-free function").

4. Element-by-Element Explanation of How the Marek-Skarine-Yoon Combination Renders the Challenged Claims Obvious

(i) Claim 4

[4] The computer system according to claim 1, wherein said non-secure human/machine interface comprises at least one input device to allow said user to control the non-secure user processor.

233. In the Marek-Skarine-Yoon combination system, a user can input a voice command via the microphone of the untrusted host mobile device 718, *e.g.*, via the non-secure human/machine interface, based on the teachings of Yoon. *See*

APPLE-1007 (Yoon), [0030]-[0032], [0043]-[0047]. The non-secure user processor of the untrusted host mobile device performs, *e.g.*, "a voice-dialing function for recognizing calling party's information inputted by the user's voice" or "a voice command function for recognizing a calling command … by a voice command," as taught by Yoon. APPLE-1007 (Yoon), [0032], [0043]-[0047]. That is, the user's voice command input through the microphone controls the non-secure user processor to execute a voice-dialing function or a voice command function. Thus, in the Marek-Skarine-Yoon combination system, the microphone of the non-secure human/machine interface is **an input device to allow the user to control the non-secure user processor**.

(ii) Claim 5

[5] The computer system according to claim 4, wherein said non-secure human/machine interface comprises at least one output device to allow the non-secure user processor to inform said user.

234. *See* my analysis of element [5] of Ground 1A.

C. [GROUND 1C] – CLAIMS 9-10 WOULD HAVE BEEN OBVIOUS OVER MAREK, SKARINE, AND MOON

1. Moon describes a tamper-resistant mobile device

235. Moon describes "[a] method and apparatus for initiating a zeroization process in an electronic device," such as a "cellular telephone phone, … [or] portable computing device such as a PDA," "if the electronic appears to have been com-

promised." APPLE-1008 (Moon), Abstract, 2:36-41. As shown in Fig. 3, reproduced below, Moon's electronic device "includes a zeroization circuit 302 [and] a monitor 304" (both in highlighted in blue), "a plurality of sensors 306" (highlighted in orange) and "storage sub-systems where sensitive information is stored or retained" (highlighted in purple). *Id.*, 4:23-26. The "monitor 304 receives input from sensors 306 and, whenever a sensor indicates a problem, monitor 304 activates zeroization circuit 302 to zero out storage locations in sub-systems 308 where sensitive information is otherwise stored." *Id.*, 4:33-37; *see* 6:1-39. Among other sensors, Moon describes a "[t]amper sensor" that "monitors the enclosure in which the electronic device is housed and if forced entry is detected, an interrupt is generated for monitor 304." *Id.*, 6:1-3.

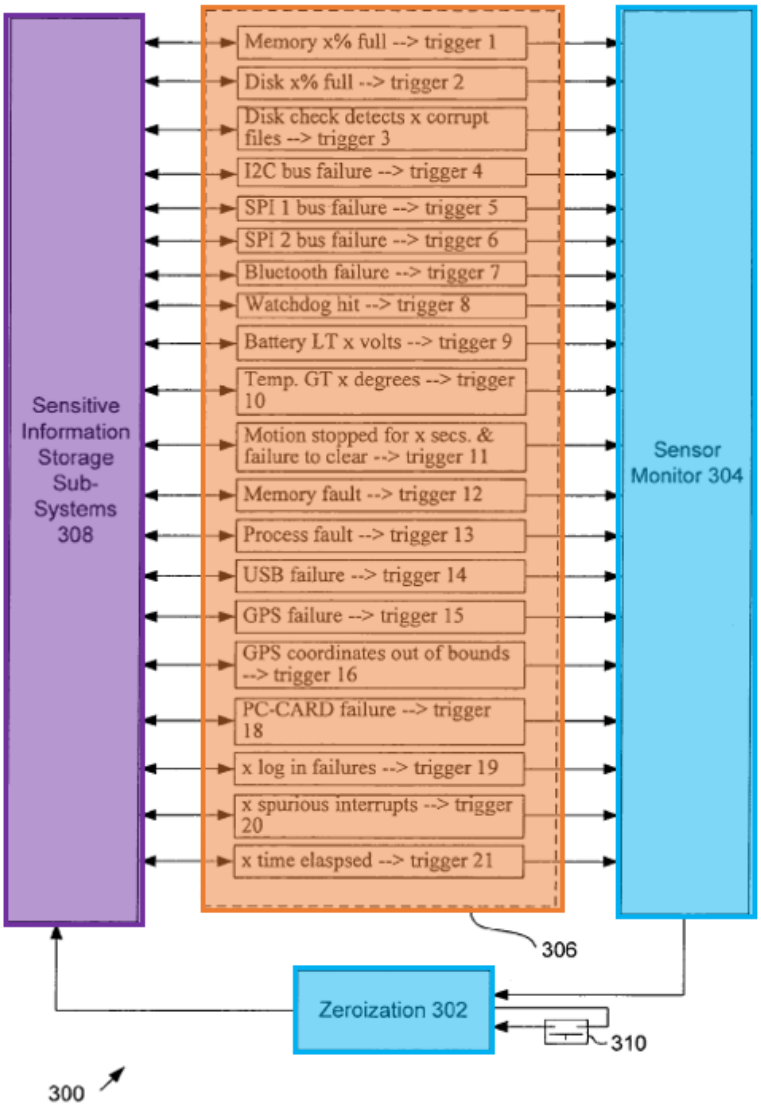


FIGURE 3

Moon, Fig. 3 (annotated)

2. The combination of Marek, Skarine, and Moon

236. In the Marek-Skarine-Moon combination system, tamper detection and zeroization functionality, such as that described by Moon, is incorporated into the untrusted host mobile device 718 of the combination. As illustrated in the

composite figure below, the untrusted host mobile device 718 is modified to include a "[t]amper sensor" (highlighted in orange) integrated into its housing, as well as tamper detection and zeroization elements (highlighted in blue) such as "a zeroization circuit" and "a monitor," *e.g.*, based on the teachings of Moon. APPLE-1008 (Moon), 6:1, 4:23-26. In operation, the tamper sensor "monitors the enclosure" (*e.g.*, the housing) of the untrusted host mobile device. *Id.*, 6:1-2. "[I]f forced entry is detected, an interrupt is generated for monitor 304." *Id.*, 6:2-3. As a result, "monitor 304 activates zeroization circuit 302 to zero out storage locations," *e.g.*, storage locations in the memory (purple) of the untrusted host mobile device 718 (*see* my analysis of claim [7]), "where sensitive information is otherwise stored." *Id.*, 4:33-37; *see* 6:12-39.

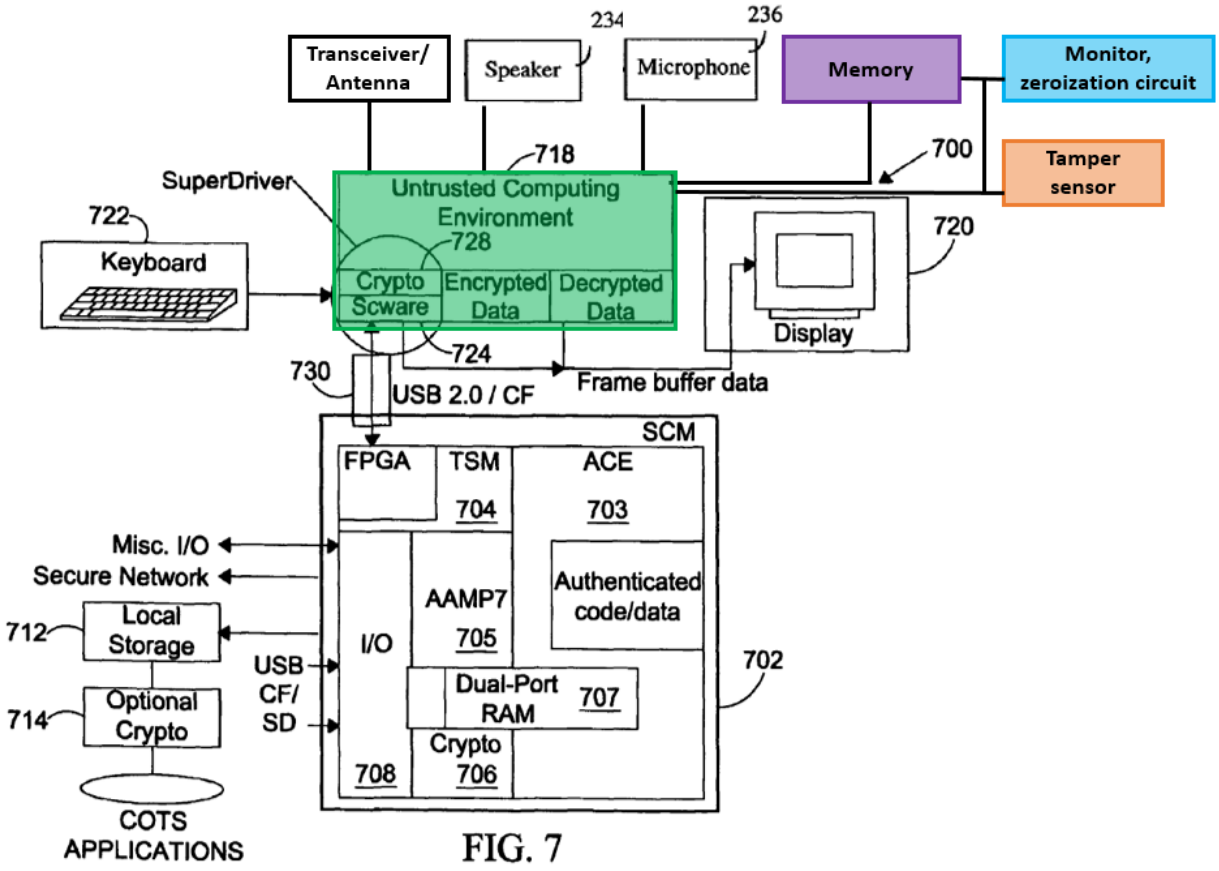


FIG. 7

Marek-Skarine-Moon composite figure

3. Reasons for the combination

237. It is my opinion that A POSITA would have been motivated to implement the Marek-Skarine-Moon combination, including implementing tamper detection and zeroization functionality in the untrusted host mobile device of the combination, for at least the following reasons.

238. One reason why a POSITA would have been motivated to implement tamper detection and zeroization functionality in the mobile device of the combination is because this would enhance data security by "protect[ing] stored sensitive

information from being wrongfully acquired," consistent with the security-focused objectives of Marek's mobile device environment. APPLE-1008 (Moon), 1:10-12; *see* APPLE-1004 (Marek), 1:5-37 ("a system suitable for highly assured military applications employing widely available and cost effective commercial off-the-shelf (COTS) components is necessary").

239. Another reason why a POSITA would have been motivated to implement tamper detection and zeroization functionality based specifically on the teachings of Moon is to achieve the advantages of Moon's "automated mechanism that monitors the condition of the electronic device and initiates the zeroization process … without operator intervention." APPLE-1008 (Moon), 1:57-62. I believe that a POSITA would have recognized the advantages of this approach in terms of rapid response speed. *See id.*, 1:48-57 ("Thus, the immediate zeroization of sensitive information means that upon detection of tampering, the electronic device must drop everything and perform zeroization."). I also believe that a POSITA also would have recognized that this approach advantageously allows for tamper detection and zeroization to occur even if the device user is "unable to activate [a] key or button or is, for some reason, incapacitated and unable to enter the code," thereby providing robust and broadly applicable device security. *Id.*, 1:29-42.

240. Another reason why a POSITA would have been prompted to incorporate tamper detection and zeroization sensors and circuitry into the mobile device of the combination is because this is just the implementation of known techniques (*e.g.*, tamper detection and zeroization) in a known system (*e.g.*, the untrusted host mobile device of the combination) that results in a predictable outcome (*e.g.*, a mobile device capable of performing conventional tamper detection and zeroization of stored sensitive information).

241. It is also my opinion that a POSITA would have expected to be successful in incorporating tamper detection and zeroization functionality into the mobile device of the combination because that zeroization is a well known feature provided in "mission critical electronic devices." APPLE-1008 (Moon), 1:14-23.

242. I also believe that a POSITA would have expected success because Moon, like Marek and Skarine, generally pertains to the field of mobile devices. *See* APPLE-1004 (Marek), 11:44-56, 12:31021, 13:49-51, 2:56-59, 7:53-57, 8:25-38, Figs. 10 and 11; APPLE-1005 (Skarine), [0001]; APPLE-1008, 2:36-42 ("Various embodiments of the invention provide a method and system for triggering zeroization in an electronic device. The electronic device may be a … cellular telephone phone … portable computing device such as a PDA or notebook").

4. Element-by-Element Explanation of How the Marek-Skarine-Moon Combination Renders the Challenged Claims Obvious

(i) Claim 9

[9pre] A computer system, comprising:

[9a] a portable mobile computing device including a secure user processor, a non-secure user processor, a communications transceiver, and a cryptographic engine,

[9b] said communications transceiver operatively coupled to said non-secure user processor and configured for communicating data external to said portable mobile computing device,

[9c] said secure user processor comprising a trusted microprocessor, a trusted operating system executing on said trusted microprocessor, and a trusted application software executing on said trusted microprocessor;

[9d] said non-secure user processor comprising an untrusted microprocessor, an untrusted operating system executing on said untrusted microprocessor, and an untrusted application software executing on said untrusted microprocessor;

[9e] said cryptographic engine configured for encrypting data communicated from said secure user processor to said non-secure user processor, comprising a trusted cryptographic processor, and a trusted operating system executing on said trusted cryptographic processor;

[9f] a first data communication link communicating data between said secure user processor and said cryptographic engine;

[9g] a second data communication link communicating data between said non-secure user processor and said cryptographic engine;

243. *See* [1pre]-[1f], [1i] of Ground 1A.

[9h] a secure human/machine interface communicatively coupled to said secure user processor and configured to enable bi-directional communication of

classified information exclusively between a user and said secure user processor, at least a portion of said secure human/machine interface located in a physically secure enclosure; and

244. The Marek-Skarine-Moon combination system renders obvious a secure human/machine interface communicatively coupled to said secure user processor and configured to enable bi-directional communication of classified information exclusively between a user and the secure user processor. *See* my analysis of elements [1g] and [9h] of Ground 1A.

245. In the Marek-Skarine-Moon combination system, the housing of the untrusted host mobile device houses at least a portion of the keypad and the display (*e.g.*, the secure human/machine interface, as I discussed in my analysis of element [1g] and [9h] of Ground 1A). Moreover, in the Marek-Skarine-Moon combination system, the housing of the untrusted host mobile device incorporates a tamper sensor to "monitor the enclosure," *e.g.*, to monitor the housing of the mobile device. APPLE-1008 (Moon), 6:1-2. If the tamper sensor detects a forced entry into the housing, storage locations in the untrusted host mobile device are zeroed out. *See* APPLE-1008 (Moon), 6:1-39, 4:23-37. The housing of the untrusted host mobile device, including the tamper sensor, is **a physically secure enclosure**, *e.g.*, in that it provides physical security by detecting physical tampering or intrusion into the housing. Thus, **at least a portion of the secure human/machine interface is located in a physically secure enclosure**.

[9i] a non-secure human/machine interface communicatively coupled to said non-secure user processor and configured to enable bi-directional communication of unclassified information exclusively between said user and said non-secure user processor, said non-secure human/machine interface distinct from said secure human/machine interface.

246. *See* [1h], [9i] of Ground 1A.

(ii) Claim 10

[10] The computer system according to claim 9, wherein said non-secure user processor is operatively connected to said communications transceiver.

247. *See* [9b] of Ground 1A.

VI. LEGAL PRINCIPLES

A. Anticipation

248. I have been informed that a patent claim is invalid as anticipated under 35 U.S.C. § 102 if each and every element of a claim, as properly construed, is found either explicitly or inherently in a single prior art reference. Under the principles of inherency, if the prior art necessarily functions in accordance with, or includes the claimed limitations, it anticipates.

249. I have been informed that a claim is invalid under 35 U.S.C. § 102(a) if the claimed invention was known or used by others in the U.S., or was patented or published anywhere, before the applicant's invention. I further have been informed that a claim is invalid under 35 U.S.C. § 102(b) if the invention was patented or published anywhere, or was in public use, on sale, or offered for sale in this country, more than one year prior to the filing date of the patent application

(critical date). And a claim is invalid, as I have been informed, under 35 U.S.C. § 102(e), if an invention described by that claim was described in a U.S. patent granted on an application for a patent by another that was filed in the U.S. before the date of invention for such a claim.

B. Obviousness

250. I have been informed that a patent claim is invalid as "obvious" under 35 U.S.C. § 103 in light of one or more prior art references if it would have been obvious to a POSITA, taking into account (1) the scope and content of the prior art, (2) the differences between the prior art and the claims, (3) the level of ordinary skill in the art, and (4) any so called "secondary considerations" of non-obviousness, which include: (i) "long felt need" for the claimed invention, (ii) commercial success attributable to the claimed invention, (iii) unexpected results of the claimed invention, and (iv) "copying" of the claimed invention by others.

251. I have been informed that a claim can be obvious in light of a single prior art reference or multiple prior art references. To be obvious in light of a single prior art reference or multiple prior art references, there must be a reason to modify the single prior art reference, or combine two or more references, in order to achieve the claimed invention. This reason may come from a teaching, suggestion, or motivation to combine, or may come from the reference or references themselves, the knowledge or "common sense" of one skilled in the art, or from

the nature of the problem to be solved, and may be explicit or implicit from the prior art as a whole. I have been informed that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. I also understand it is improper to rely on hindsight in making the obviousness determination.

VII. ADDITIONAL REMARKS

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

253. I hereby declare 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 further declare that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of the Title 18 of the United States Code.

Dated: 1/31/2023 By: _____

APPENDIX A

EXPERANTIS
Expert Services for Commercial Litigation

Harvard University
Exec. Ed., Global Leadership

Massachusetts Institute of Technology
Ph.D., Computer Science
M.S., Electrical Engineering & Computer Science

University of California at Berkeley
B.S., Electrical Engineering & Computer Science

Sandeep Chatterjee, Ph.D.

Chief Executive Officer

Professional Summary

Sandeep Chatterjee, Ph.D. is a seasoned technology expert and business professional with almost two decades of hands-on contributions as a thought leader, technologist, consultant, entrepreneur, and author. He is an expert in computer software and hardware systems, with particular emphasis on distributed systems and architectures, service-oriented architectures (SOAs), software-as-a-service (SaaS) and Web Services, end-to-end security, quality-of-service (QoS), communications and telecommunications systems, location-based services, social network services and social media, as well as mobile and wireless systems and applications. He is the co-author of a book on developing enterprise computing systems, which has been adopted by over 100 universities worldwide.

Dr. Chatterjee also has extensive experience with providing expert testimony for intellectual property and commercial litigation, including for high stakes patent litigation, copyright and trade secret misappropriation, contract disputes and patent licensing cases. He has testified at trial, and has had his deposition taken more than 60 times. Dr. Chatterjee combines strong experience with expert testimony within the context of litigation together with worldwide experience in designing, architecting and implementing complex computing systems.

Honors & Achievements

- Named a **Young Global Leader** by the **World Economic Forum** for professional accomplishments, commitment to society and potential to contribute to shaping the future of the world.
- Doctoral dissertation at the Massachusetts Institute of Technology (MIT) was selected as one of the **most important inventions in computing**, and the invention is preserved and showcased in a time-capsule at the Museum of Science in Boston, Massachusetts. Other recipients of this honor include **Bill Gates** (founder of Microsoft) and **Tim Berners-Lee** (inventor of the World Wide Web).
- Technology solution designed by Dr. Chatterjee was identified as a Bloomberg Innovation, and the company he co-founded to commercialize that technology solution was featured on Bloomberg TV's "**Bloomberg Innovators**" program.
- Member of the **JSR 172 Expert Group** that defined the worldwide standard for J2ME mobile Web services.

sandeep@experantis.com
+1 650-759-6523

Professional Experience

From: 2013
To: present
Organization: Experantis LLC
Title: Chief Executive Officer
Summary: Experantis LLC provides consultation and services in all facets of commercial litigation.

From: 2016
To: 2019
Organization: International Institute of Digital Technologies
Title: Dean, Mobility Center of Excellence
Summary: International Institute of Digital Technologies (IIDT) is a leading institute of higher education, focused on digital technologies.

From: 2013
To: present
Organization: S3G Technology LLC
Title: Member
Summary: S3G Technology LLC provides consultation, products and services related to mobile and wireless solutions that deliver critical services to semi-urban, rural and remote populations across the world.

From: 2011
To: present
Organization: World Economic Forum
Title: Young Global Leader; Member of the Expert Network
Summary: The World Economic Forum is an international institution for public-private cooperation, and its mission is cited as "committed to improving the state of the world by engaging business, political, academic, and other leaders of society to shape global, regional, and industry agendas."

From: 2007
To: present
Organization: Shuv Gray LLC
Title: Chief Executive Officer
Summary: Shuv Gray LLC provides information technology and intellectual property consultation and services.

From: 2007
To: 2012
Organization: SourceTrace Systems, Inc.
Title: Chief Technology Officer & Executive Vice President
Summary: SourceTrace Systems is a leading vendor of end-to-end mobile and wireless distributed transactional systems for the financial services, agricultural commodities, and product distribution markets around the world.

From: 2004
To: 2007
Organization: Cyndeo LLC
Title: Chief Executive Officer
Summary: Founded Cyndeo to be a leading provider of enterprise integration and mobilization solutions as well as technology strategy consulting and outsourcing services to global corporations, government agencies, and major not-for-profit organizations. Cyndeo provides consulting, software engineering development, and management services to companies and organizations of all sizes, from Fortune Global 100 corporations to small organizations in developing countries.

From: 2001
To: 2002
Organization: Hewlett-Packard (Palo Alto, CA)
Title: Senior Member of Technical Staff
Summary: Independently identified a need in the mobile and e-Business marketplace for a more flexible Web Services platform. Invented a patent-pending (applied) solution, and led the development as well as the initial sales and marketing efforts.

- This next-generation J2EE (HP/Bluestone app server) Web Services solution ties together the emerging Web Services standards, end-to-end transactions, and optimized mobile services & applications.
- Led and managed the entire lifecycle of the product from conception, architectural design, product development, QA, documentation, senior management approval, patent filing, preparation for marketing launch at JavaOne, as well as interfacing with early adopter customers and strategic partners.
- Managed relationships with multiple HP organizations and teams that contributed to the overall solution.
- Positioned the product, targeted key early adopters and partners, and leveraged my own contacts to build successful strategic relationships.
- Selected to provide support to HP/Bluestone's top sales manager, and helped land a strategic account in the Asia-Pac market.
- Selected as the representative for Hewlett Packard to the JSR 172 Expert Group that is defining the worldwide standard for J2ME mobile Web Services.

From: 1999
To: 2000
Organization: Satora Networks
Title: Founder & Chief Technology Officer
Summary: Founded Satora Networks to create wireless platforms and services for Internet devices based on the technologies invented by Dr. Chatterjee as part of his Ph.D. research at MIT Lab for Computer Science.

- Raised venture funding, recruited the management and core engineering teams, set corporate and product strategy, handled customer and partner relations, and managed overall corporate affairs.

- Architected and led the development of the StrongARM-based mobile hardware platform, Linux-based mobile OS, client-side services, and server-side J2EE environment.
- Landed key customer and partner wins, managed revenue and burn rate to become profitable early on, and oversaw the growth of the company.

From: 1995
To: 2001
Organization: MIT Lab for Computer Science
Title: Doctoral Researcher
Summary: Designed a modular system architecture that supports the cost-effective development of network devices and services. The system consists of Lego-like commodity hardware and standards-based software components that are quickly composed together through a development environment into optimized end-user devices as well as client-side services.

- Architected and implemented the entire system: a Linux-based client software environment, a wireless network and StrongARM processor-based device hardware platform, as well as a Web-based design and optimization environment and tool.
- Successfully mentored and managed a research group of 6 Masters and Bachelors students.
- The technology underlying Dr. Chatterjee's thesis was selected as one of the top inventions in thirty-five year history of MIT Laboratory for Computer Science.

From: 1997
To: 1999
Organization: FidelityCAPITAL (Boston, MA)
Title: Entrepreneur-In-Residence
Summary: Worked with Fidelity senior management and FidelityCAPITAL partners to source, analyze, and fund technology start-ups strategic to Fidelity interests.

- Evaluated business plans submitted to Fidelity for venture funding, and analyzed emerging market and technology trends to identify opportunities for internal spin-offs in the telecom and eBusiness spaces.
- Founded and served as President & CTO of a wireless devices and services company (Satora Networks) that was seed funded by Fidelity.

Litigation Support Experience

Expert Engagement:

Type of Matter: Enterprise Software Patent Infringement
Law Firm: Morrison & Foerster
Case Name: Software AG and Software AG v. BEA Systems
Services Provided: Retained as BEA's expert; submitted two expert reports; deposed twice; prepared for trial (exhibits, testimony, cross examination).
Date: 2004

sandeep@experantis.com
+1 650-759-6523

Expert Engagement:

Type of Matter:	Enterprise software intellectual property litigation.
Law Firm:	Morrison & Foerster
Case Name:	
Services Provided:	Consultant to attorney
Date:	2004-2005

Expert Engagement:

Type of Matter:	Mobile software intellectual property litigation.
Law Firm:	Perkins Coie
Case Name:	Esmertec v. Tao Group
Services Provided:	Retained as Esmertec's expert; submitted two expert reports.
Date:	2006

Expert Engagement:

Type of Matter:	Enterprise and mobile software intellectual property litigation.
Law Firm:	McDermott Will & Emery
Case Name:	Metrologic Instruments v. Symbol Technologies
Services Provided:	Retained as Metrologic's expert
Date:	2006-2007

Expert Engagement:

Type of Matter:	Distributed and mobile computing trade secret litigation.
Law Firm:	Haralson, Miller, Pitt, Feldman & McAnally
Case Name:	Modular Mining Systems (Komatsu Ltd.) v. Jigsaw Systems et al.
Services Provided:	Retained as Modular's expert; submitted two expert reports; deposed.
Date:	2006-2008

Expert Engagement:

Type of Matter:	Distributed systems, mobile computing and object oriented programming intellectual property litigation.
Law Firm:	Kirkland & Ellis
Case Name:	
Services Provided:	Consultant to attorney
Date:	2007

Expert Engagement:

Type of Matter:	Communications software and systems intellectual property litigation.
Law Firm:	Carey Rodriguez Greenberg & Paul
Case Name:	Catch Curve v. Venali
Services Provided:	Retained as Venali's expert; submitted two expert reports
Date:	2008

sandeep@experantis.com
+1 650-759-6523

Expert Engagement:

Type of Matter:	Distributed computing and network routing systems intellectual property litigation.
Law Firm:	Vinson & Elkins
Case Name:	WebXChange v. Dell
Services Provided:	Retained as Dell's expert
Date:	2008-2010

Expert Engagement:

Type of Matter:	Communications systems intellectual property litigation.
Law Firm:	Kirkland & Ellis
Case Name:	Motorola, Inc. et al. v. Rembrandt Technologies, LP
Services Provided:	Retained as the plaintiffs' expert; submitted expert report
Date:	2009

Expert Engagement:

Type of Matter:	Database and object mapping intellectual property litigation.
Law Firm:	Kirkland & Ellis
Case Name:	DataTern v. United Airlines
Services Provided:	Retained as United Airlines' expert
Date:	2009

Expert Engagement:

Type of Matter:	Control systems intellectual property litigation.
Law Firm:	Morgan Lewis & Bockius
Case Name:	Finisar v. Source Photonics
Services Provided:	Retained as Finisar's expert; source code review
Date:	2010

Expert Engagement:

Type of Matter:	Mobile systems intellectual property litigation.
Law Firm:	Morgan Lewis & Bockius
Case Name:	OpenWave v. 724 Solutions
Services Provided:	Retained as OpenWave's expert; source code review
Date:	2010

Expert Engagement:

Type of Matter:	Mobile systems intellectual property litigation.
Law Firm:	Winston Strawn
Case Name:	Ganas v. Charles Schwab et al
Services Provided:	Retained as Charles Schwab's expert
Date:	2011

Expert Engagement:

Type of Matter:	Mobile systems trade secret misappropriation litigation.
Law Firm:	Berliner Cohen
Case Name:	Damodharan Ulagaratchalan v Dhyan Infotech
Services Provided:	Retained as Dhyan's expert; source code review
Date:	2011

Expert Engagement:

Type of Matter:	Control systems intellectual property litigation.
Law Firm:	Morgan Lewis & Bockius
Case Name:	Finisar v. Oplink
Services Provided:	Retained as Finisar's expert; source code review
Date:	2011

Expert Engagement:

Type of Matter:	Mobile systems intellectual property litigation.
Law Firm:	Ropes & Gray
Case Name:	Motorola Mobility (Google) v. Microsoft
Services Provided:	Retained as Google's expert; source code review
Date:	2011-2012

Expert Engagement:

Type of Matter:	Wireless networking & management intellectual property litigation.
Law Firm:	Kirkland & Ellis
Case Name:	Netgear v. Ruckus Wireless
Services Provided:	Retained as Netgear's expert; source code review
Date:	2012-2013

Expert Engagement:

Type of Matter:	Mobile systems intellectual property litigation.
Law Firm:	Morgan Lewis & Bockius
Case Name:	XpertUniverse v. Cisco Systems
Services Provided:	Retained as Cisco's expert; submitted expert report; source code review; deposition; trial
Date:	2012-2013

Expert Engagement:

Type of Matter:	Distributed computing systems contract litigation.
Law Firm:	Berliner Cohen
Case Name:	Skillnet Solutions v. Entertainment Publications
Services Provided:	Retained as Entertainment's expert
Date:	2013

sandeep@experantis.com
+1 650-759-6523

Expert Engagement:

Type of Matter:	Mobile systems intellectual property litigation.
Law Firm:	Mayer Brown
Case Name:	Aeritas v. US Airways, Inc., Delta Airlines, Inc., Alaska Air Group
Services Provided:	Retained as the airlines' expert; submitted 3 expert reports; source code review; depositions
Date:	2013

Expert Engagement:

Type of Matter:	Distributed systems intellectual property litigation.
Law Firm:	Ropes & Gray
Case Name:	Wellogix v. ADP et. al.
Services Provided:	Retained as ADP's expert
Date:	2013

Expert Engagement:

Type of Matter:	Trade secret misappropriation litigation.
Law Firm:	Hopkins & Carley
Case Name:	Bradford Technologies v. NCV Software et al.
Services Provided:	Retained as Bradford's expert; submitted expert report; mediation
Date:	2013

Expert Engagement:

Type of Matter:	Mobile systems intellectual property litigation.
Law Firm:	Fish & Richardson P.C.
Case Name:	Ericsson Inc. v. Samsung Electronics Co., Ltd. et al.
Services Provided:	Retained as Samsung's expert; source code review
Date:	2013

Expert Engagement:

Type of Matter:	Contract dispute litigation.
Law Firm:	Morgan Lewis & Bockius
Case Name:	AMC Technologies v. Cisco Systems
Services Provided:	Retained as Cisco's expert; submitted expert report; deposition
Date:	2013

Expert Engagement:

Type of Matter:	Trade secret misappropriation litigation.
Law Firm:	Lexanalytica
Case Name:	PQ Labs v. Qi et. al.
Services Provided:	Retained as defendants' expert; source code review; deposition
Date:	2013

Expert Engagement:

Type of Matter:	Distributed systems and security intellectual property litigation.
Law Firm:	Troutman Sanders
Case Name:	Media Rights Technologies, Inc. v. Capital One Financial Corporation
Services Provided:	Retained as Capital One's expert; source code review; expert reports; declaration
Date:	2013

Expert Engagement:

Type of Matter:	Distributed computing intellectual property litigation.
Law Firm:	Rothwell, Figg, Ernst & Manbeck, P.C.
Case Name:	SecureBuy v. CardinalCommerce
Services Provided:	Retained as SecureBuy's expert; *inter partes* review; declarations
Date:	2013

Expert Engagement:

Type of Matter:	Distributed computing intellectual property litigation.
Law Firm:	Mayer Brown LLP
Case Name:	American Airlines , Inc. et al. v. Loyalty Conversion Systems Corporation
Services Provided:	Retained as the airlines' expert; covered business method petitions; declarations
Date:	2014

Expert Engagement:

Type of Matter:	Mobile computing and security intellectual property litigation.
Law Firm:	Dickstein Shapiro, LLP
Case Name:	Tierra Intellectual Borinquen, Inc. v. Toshiba Corporation et. al.
Services Provided:	Retained as Toshiba's expert; declaration; expert report
Date:	2014

Expert Engagement:

Type of Matter:	Distributed computing systems and software intellectual property litigation.
Law Firm:	Reed Smith, LLP
Case Name:	Kroy IP Holdings, LLC v. Safeway, Inc. and The Kroger Co.
Services Provided:	Retained as the defendants' expert; expert report
Date:	2014

Expert Engagement:

Type of Matter:	Secure mobile computer hardware and software intellectual property litigation.
Law Firm:	White & Case LLP
Case Name:	Maxim Integrated Products, Inc. v. JPMorgan Chase & Co.
Services Provided:	Retained as JPMorgan Chase's expert; 3 expert reports
Date:	2014

sandeep@experantis.com
+1 650-759-6523

Expert Engagement:

Type of Matter:	Computer hardware and software antitrust litigation.
Law Firm:	Morgan Lewis & Bockius LLP
Case Name:	In Re: Keurig Green Mountain Single Serve Coffee Antitrust Litigation.
Services Provided:	Retained as plaintiffs' expert; declarations
Date:	2014

Expert Engagement:

Type of Matter:	Mobile computer and location-based systems intellectual property litigation.
Law Firm:	Morgan Lewis & Bockius LLP
Case Name:	Unwired Planet LLC v. Square, Inc.
Services Provided:	Retained as plaintiffs' expert; source code review; declarations
Date:	2014

Expert Engagement:

Type of Matter:	Distributed computing systems intellectual property litigation.
Law Firm:	Morrison & Foerster LLP
Case Name:	AirWatch LLC v. Good Technology Corporation et al.
Services Provided:	Retained as plaintiff's expert; declaration
Date:	2014

Expert Engagement:

Type of Matter:	Mobile computer and location-based systems intellectual property litigation.
Law Firm:	Goodwin Procter LLP
Case Name:	Unwired Planet LLC v. Square, Inc.
Services Provided:	Retained as plaintiff/patent owner's expert; source code review; covered business methods review; *inter partes* review; declarations; deposition
Date:	2015

Expert Engagement:

Type of Matter:	Distributed computing systems intellectual property litigation.
Law Firm:	Morrison & Foerster LLP
Case Name:	Good Technology Corporation et al. v. AirWatch LLC
Services Provided:	Retained as defendant's expert; *inter partes* review; declaration
Date:	2015

Expert Engagement:

Type of Matter:	Mobile computer and location-based systems intellectual property litigation.
Law Firm:	Schwegman Lundberg & Woessner
Case Name:	Square, Inc. v. Unwired Planet LLC
Services Provided:	Retained as patent owner's expert; CBM declaration
Date:	2015

sandeep@experantis.com
+1 650-759-6523

Expert Engagement:

Type of Matter:	Mobile computer and location-based systems intellectual property litigation.
Law Firm:	EIP
Case Name:	Square, Inc. v. Unwired Planet LLC
Services Provided:	Retained as patent owner's expert; *inter partes* review; declaration
Date:	2015

Expert Engagement:

Type of Matter:	Software systems intellectual property litigation.
Law Firm:	Mayer Brown LLP
Case Name:	American Express Company et al. v. Signature Systems, LLC
Services Provided:	Retained as petitioner's expert; covered business methods review; declaration
Date:	2015

Expert Engagement:

Type of Matter:	Software and backup systems intellectual property litigation.
Law Firm:	Morrison & Foerster LLP
Case Name:	Farstone Technology, Inc. v. Apple, Inc.
Services Provided:	Retained as Apple's expert; source code review; expert reports (2); declarations; deposition
Date:	2015

Expert Engagement:

Type of Matter:	Distributed computing systems intellectual property litigation.
Law Firm:	Baker Botts LLP
Case Name:	MobileIron, Inc. v. Good Technology Corporation
Services Provided:	Retained as petitioner's expert; *inter partes* review; declaration
Date:	2015

Expert Engagement:

Type of Matter:	Data management intellectual property litigation.
Law Firm:	Mayer Brown
Case Name:	Olivistar v. Regions Bank et al.
Services Provided:	Retained as defendant's expert; declaration
Date:	2015

Expert Engagement:

Type of Matter:	Cloud computing and data migration intellectual property litigation.
Law Firm:	Ropes & Gray
Case Name:	BitTitan v. SkyKick
Services Provided:	Retained as defendant's expert; declarations; deposition
Date:	2015

Expert Engagement:

Type of Matter:	Breach of contract, fraud litigation involving large scale enterprise software.
Law Firm:	Orrick
Case Name:	State of Oregon v. Oracle et al.
Services Provided:	Retained as defendants' expert
Date:	2016

sandeep@experantis.com
+1 650-759-6523

Expert Engagement:

Type of Matter:	Document processing intellectual property litigation.
Law Firm:	Mayer Brown
Case Name:	Capital Security Systems v. NCR et al.
Services Provided:	Retained as defendants' expert; expert report
Date:	2016

Expert Engagement:

Type of Matter:	Web page intellectual property litigation.
Law Firm:	Cooley
Case Name:	Tele-Publishing, Inc. v. Facebook et al.
Services Provided:	Retained as Facebook's expert; expert report; declarations; deposition
Date:	2016

Expert Engagement:

Type of Matter:	Intellectual property litigation.
Law Firm:	Cooley
Case Name:	Sound View Innovations, LLC v. Facebook, Inc.
Services Provided:	Retained as Facebook's expert; *inter partes* review; declarations
Date:	2017

Expert Engagement:

Type of Matter:	Intellectual property litigation.
Law Firm:	Cooley
Case Name:	Zkey Investments, LLC v. Facebook, Inc.
Services Provided:	Retained as Facebook's expert; *inter partes* review; declaration
Date:	2017

Expert Engagement:

Type of Matter:	Intellectual property litigation.
Law Firm:	Young Basile
Case Name:	Mantissa Corp. v. Ondot Systems, Inc. et al
Services Provided:	Retained as plaintiff's expert; declaration
Date:	2017

Expert Engagement:

Type of Matter:	Intellectual property litigation.
Law Firm:	Cooley
Case Name:	Vaporstream, Inc. v. Snap, Inc.
Services Provided:	Retained as Snap's expert; *inter partes* review; declarations
Date:	2017

Expert Engagement:

Type of Matter:	Intellectual property litigation.
Law Firm:	Baker Botts
Case Name:	Symantec Corporation v. Zscaler, Inc.
Services Provided:	Retained as Symantec's expert; *inter partes* reviews; declarations
Date:	2017

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Klarquist
Case Name: American Express Company et al. v. Signature Systems, LLC
Services Provided: Retained as Petitioner's expert; covered business method petition; declaration
Date: 2017

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Miller Law
Case Name: Apogee Telecom, Inc. v. Brian Rosenblatt
Services Provided: Retained as Defendant's expert
Date: 2017

Expert Engagement:
Type of Matter: Intellectual property arbitration.
Law Firm: Morgan Lewis & Bockius
Case Name: Trupanion, Inc. v. Veterinary Data Services, Inc.
Services Provided: Retained as Defendant's expert
Date: 2017

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Goodwin
Case Name: Leftsnrights, Inc. v. 33Across, Inc.
Services Provided: Retained as Defendant's expert; *inter partes* review; declaration; deposition
Date: 2018

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Cooley
Case Name: Ameranth, Inc. v. Mobo Systems, Inc. (Olo)
Services Provided: Retained as Defendant's expert; expert reports
Date: 2018

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Cooley
Case Name: Facebook, Inc. and Instagram, LLC v. Search and Social Media Partners, LLC
Services Provided: Retained as Facebook's expert; *inter partes* review; declarations; deposition
Date: 2018

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Cooley
Case Name: Facebook, Inc. v. Hyper Search LLC
Services Provided: Retained as Facebook's expert; *inter partes* review; declaration
Date: 2018

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Goodwin
Case Name: Touchstream Technologies, Inc. v. Vizbee, Inc.
Services Provided: Retained as Vizbee's expert; expert report; source code analysis; deposition
Date: 2018

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Cooley
Case Name: Facebook, Inc., Instagram, LLC and WhatsApp, Inc. v. Blackberry Limited
Services Provided: Retained as Petitioners' expert; *inter partes* reviews; declarations; depositions
Date: 2018

Expert Engagement:
Type of Matter: Litigation.
Law Firm: Morgan Lewis & Bockius
Case Name: Roger Hogan et al. v. Toyota Motor Sales, U.S.A., Inc.
Services Provided: Retained as defendant's expert; expert report; deposition
Date: 2019

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Baker Botts
Case Name: Blue Spike LLC v. DISH Network Corp.
Services Provided: Retained as DISH's expert; inter partes review; declarations
Date: 2018

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: King & Spalding
Case Name: NCR Corp. v. Pendum, LLC and Burroughs, Inc.
Services Provided: Retained as NCR's expert; expert reports; source code analysis; depositions
Date: 2019

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Paul Hastings
Case Name: Snap, Inc. v. Blackberry Limited
Services Provided: Retained as Snap's expert; *inter partes* reviews; declarations
Date: 2019

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: King & Spalding
Case Name: Lufthansa Technik and Certified Aviation Services, LLC v. EcoServices, LLC
Services Provided: Retained as Lufthansa's expert; ex parte reexamination; declaration
Date: 2019

sandeep@experantis.com
+1 650-759-6523

Expert Engagement:

Type of Matter:	Intellectual property litigation.
Law Firm:	Davis Polk & Wardwell; Winston & Strawn
Case Name:	Rovi Guides, Inc. v. Comcast Corp. et al., ITC Inv. No. 337-TA-1158 (2019)
Services Provided:	Retained as Comcast's expert; expert report; deposition; trial
Date:	2019

Expert Engagement:

Type of Matter:	Intellectual property litigation.
Law Firm:	Cooley
Case Name:	Microsoft Corporation, Google LLC, Asustek Computer Inc., Acer Incorporated, HTC Corporation v. Mimzi, LLC
Services Provided:	Retained as Petitioners' expert; *inter partes* review; declaration
Date:	2019

Expert Engagement:

Type of Matter:	Intellectual property litigation.
Law Firm:	Fish & Richardson
Case Name:	Rain Computing, Inc. v. Samsung Electronics Co., Ltd.; Samsung Electronics America, Inc.; and Samsung Research America, Inc.
Services Provided:	Retained as Samsung's expert; declaration
Date:	2019

Expert Engagement:

Type of Matter:	Intellectual property litigation.
Law Firm:	Goodwin
Case Name:	JBF Interlude 2009 Ltd. - Israel v. Quibi Holdings LLC
Services Provided:	Retained as JBF Interlude's expert; declaration
Date:	2020

Expert Engagement:

Type of Matter:	Intellectual property litigation.
Law Firm:	Winston & Strawn; Quinn Emanuel
Case Name:	Warner Records, Inc., et al. v. Charter Communications, Inc.
Services Provided:	Retained as Charter's expert; declarations
Date:	2020

Expert Engagement:

Type of Matter:	Intellectual property litigation.
Law Firm:	Winston & Strawn; Quinn Emanuel
Case Name:	UMG Recordings, Inc., et al. v. Bright House Networks, LLC
Services Provided:	Retained as Bright House Networks' expert; declarations
Date:	2020

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Ropes & Gray
Case Name: Dolby Laboratories, Inc. v. Intertrust Technologies Corporation
Services Provided: Retained as Dolby's expert; *inter partes* review; declarations
Date: 2020

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Barclay Damon, LLP
Case Name: Document Dynamics, LLC v. Xerox Corporation
Services Provided: Retained as Xerox's expert; declarations; re-exam
Date: 2020

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Goodwin
Case Name: Thaddeus Gabara v. Facebook, Inc.
Services Provided: Retained as Facebook's expert; *inter partes* reviews; declarations
Date: 2020

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Wilmer Cutler Pickering Hale and Dorr LLP
Case Name: NexStep, Inc. v. Comcast Cable Communications, LLC
Services Provided: Retained as Comcast's expert; declaration
Date: 2020

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Cooley
Case Name: Facebook, Inc. v. USC IP Partnership, L.P.
Services Provided: Retained as Petitioner's expert; *inter partes* review; declaration
Date: 2020

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Locke Lord
Case Name: Cloudofchange, LLC v. NCR Corp.
Services Provided: Retained as NCR's expert; expert reports; declaration; depositions; trial
Date: 2020

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Cooley
Case Name: CommVault Systems, Inc. v. Rubrik Inc.
Services Provided: Retained as Rubrik's expert; *inter partes* reviews; declarations
Date: 2020

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Paul Hastings
Case Name: Google LLC v. Express Mobile, Inc.
Services Provided: Retained as Google's expert; *inter partes* reviews; declarations
Date: 2021

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Paul Hastings
Case Name: Uber Technologies, Inc. v. AGIS Software Development LLC
Services Provided: Retained as Uber's expert; *inter partes* reviews; re-exam; declarations
Date: 2021

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Baker Botts
Case Name: Broadband iTV, Inc. v. AT&T Services, Inc. and AT&T Communications LLC
Services Provided: Retained as AT&T's expert; expert report; deposition
Date: 2021

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Baker Botts
Case Name: Broadband iTV, Inc. v. DIRECTV, LLC
Services Provided: Retained as DIRECTV's expert; expert report; deposition
Date: 2021

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: Kirkland & Ellis
Case Name: Samsung Electronics Co., Ltd. v. Blaze Mobile, Inc. and Michelle Fisher
Services Provided: Retained as Samsung's expert; *inter partes* reviews; declarations
Date: 2021

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: King & Spalding
Case Name: Proven Networks, LLC v F5 Networks, Inc.
Services Provided: Retained as F5's expert; declaration
Date: 2021

Expert Engagement:
Type of Matter: Intellectual property litigation.
Law Firm: King & Spalding
Case Name: WSOU Investments, LLC v F5 Networks, Inc.
Services Provided: Retained as F5's expert; declaration; deposition
Date: 2021

sandeep@experantis.com
+1 650-759-6523

Expert Engagement:

Type of Matter:	Intellectual property litigation.
Law Firm:	King & Spalding
Case Name:	People.AI, Inc. v SetSail Technologies, Inc.
Services Provided:	Retained as SetSail's expert; declaration
Date:	2021

Expert Engagement:

Type of Matter:	Intellectual property litigation.
Law Firm:	Orrick
Case Name:	IGT and IGT Canada Solutions ULC v Zynga Inc.
Services Provided:	Retained as Zynga's expert; declarations
Date:	2021

Expert Engagement:

Type of Matter:	Intellectual property litigation.
Law Firm:	Baker Botts
Case Name:	Express Mobile, Inc. v Booking Holdings, Inc.
Services Provided:	Retained as Booking Holdings' expert; declarations
Date:	2021

Expert Engagement:

Type of Matter:	Intellectual property litigation.
Law Firm:	Winston & Strawn
Case Name:	Wapp Tech Limited Partnership v. Wells Fargo Bank, N.A.
Services Provided:	Retained as Wells Fargo's expert
Date:	2022

Expert Engagement:

Type of Matter:	Intellectual property litigation.
Law Firm:	Goodwin
Case Name:	Trident Holdings, Inc. v. HubSpot, Inc.
Services Provided:	Retained as HubSpot's expert
Date:	2022

Expert Engagement:

Type of Matter:	Intellectual property litigation.
Law Firm:	Faegre Drinker; Hogan Lovells
Case Name:	Hafeman v. LG Electronics, Inc.
Services Provided:	Retained as LG's expert
Date:	2022

sandeep@experantis.com
+1 650-759-6523

Non-Litigation Consulting Projects

Consulting Engagement:

Type of Matter:	Enterprise software architecture and development
Client:	Sevak Solutions, Inc.
Services Provided:	Architect, specify, and develop enterprise-class software for secure financial transactioning in multiple markets and countries around the world
Date:	2005-2006

Consulting Engagement:

Type of Matter:	Enterprise software architecture and development
Client:	United States Agency for International Development (USAID)
Services Provided:	Specify and develop financial transactioning and tracking software
Date:	2004-2005

Consulting Engagement:

Type of Matter:	Training services
Client:	South Korean Ministry of Information and Communications
Services Provided:	Conducted a workshop to train selected university professors and corporate researchers on properly using mobile and distributed technology for strategic and financial growth.
Date:	2004

Consulting Engagement:

Type of Matter:	Product and service strategy and development
Client:	Hewlett-Packard Company
Services Provided:	Analyze market opportunities for new, market-specific technology product and service offerings
Date:	2004

Consulting Engagement:

Type of Matter:	Mobile enterprise software
Client:	ACCION International
Services Provided:	Specified, architected, and developed a mobile enterprise software system for optimizing wireless transactioning.
Date:	2003

Consulting Engagement:

Type of Matter:	Market, technology and services strategy development
Client:	Hewlett-Packard Laboratories
Services Provided:	Analyzed multiple country-specific market needs and opportunities, and proposed technology and service offerings
Date:	2003

Publications

sandeep@experantis.com
+1 650-759-6523

1. Chatterjee, Sandeep and Webber, James, Developing Enterprise Web Services: An Architect's Guide (Pearson Education Korea Ltd. and Hong Reung Science Pub. Co. 2005), Korean Trans.
2. Chatterjee, Sandeep and Webber, James, Developing Enterprise Web Services: An Architect's Guide (Prentice Hall 2004).
3. Chatterjee, Sandeep and Webber, James, Developing Enterprise Web Services: An Architect's Guide (Pearson Education Singapore Pvt. Ltd. 2004), Indian Reprint.
4. Chatterjee, Sandeep, "Enterprise Technology: Web Services: The Next Revolution in IT," in *Dataquest* (March 2004).
5. Chatterjee, Sandeep, "Enterprise 2004 Trends: On A Cautious Note," *Dataquest* (Feb. 2004).
6. Chatterjee, Sandeep, "A Real-World Web Services-Based Application," *JavaBoutique* (http://javaboutique.internet.com/articles/WSApplications/realWorld3_1.html).
7. Chatterjee, Sandeep, "Write Once, Run Anywhere Web Services," *JavaBoutique* (http://javaboutique.internet.com/articles/WSApplications/realWorld2_1.html).
8. Chatterjee, Sandeep, "Developing Real World Web Services-Based Applications," *JavaBoutique* (http://javaboutique.internet.com/articles/WSApplications/).
9. Chatterjee, Sandeep, Doctoral Thesis Dissertation, "Composable System Resources As An Architecture For Networked Systems," Massachusetts Institute of Technology (2001).
10. Keckler, Stephen W., Chang, Andrew, Lee, Whay Sing, Chatterjee, Sandeep, and Dally, William J., "Concurrent Event Handling Through Multithreading," *IEEE Trans. Computers* 48(9), pages 903-916 (1999).
11. Chatterjee, Sandeep and Devadas, Srinivas, "MASC Composable Computing Infrastructure For Intelligent Environments," *Proceedings of the Industrial Electronics Conference*, pages 132-138 (1999).
12. Chatterjee, Sandeep, "SANI: A Seamless and Non-Intrusive Framework and Agent for Creating Intelligent Interactive Homes," *Second International Conference on Autonomous Agents*, pages 436-440 (1998).
13. Chatterjee, Sandeep, "Towards A MASC Appliances-Based Educational Paradigm," *ACM Symposium on Applied Computing*, pages 112-116 (1998).
14. Chatterjee, Sandeep, "Towards Rapidly Deployable Intelligent Environments," *American Association for Artificial Intelligence Symposium on Intelligent Environments*, pages 31-36 (1998).
15. Chatterjee, Sandeep, "The ModuleC Network Architecture: A Novel Approach Of Computing Through Information Appliances," *IEEE International Symposium on Consumer Electronics* (1997).
16. Chatterjee, Sandeep, Masters Thesis, "Asynchronous Event Handling," Massachusetts Institute of Technology Technical Report (May 1997).
17. Tennenhouse, David L. and Chatterjee, Sandeep, "The First 10 Feet: The Missing Story For Encouraging User Investment In Universal Broadband Connectivity" (October 1996).
18. Chatterjee, Sandeep and Faraboschi, Paolo, "The VLIW Trace Scheduling Compiler Visual Analysis System," Hewlett-Packard Laboratories Internal Technical Report (September 1995).

sandeep@experantis.com
+1 650-759-6523

19. Chatterjee, Sandeep and Donohue, Richard J., "Electron Gamma Shower Windows 2," *International Conference on Monte Carlo Simulations in Nuclear & High Energy Physics* (February 1993).