

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

Mail Stop Patent Board

Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

**PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES PATENT
NO. 7,765,399 PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	REQUIREMENTS FOR IPR	2
	A. Grounds for Standing.....	2
	B. Challenge and Relief Requested Under 37 C.F.R. §42.104(b)	2
III.	THE '399 PATENT	3
	A. Brief Description.....	3
	B. Prosecution History.....	3
	C. Level of Ordinary Skill.....	4
	D. Claim Construction	4
IV.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	5
	A. [GROUND 1A] – CLAIMS 1-7 AND 9-10 WOULD HAVE BEEN OBVIOUS OVER MAREK AND SKARINE	5
	1. Marek describes a conventional mobile device having secure and non-secure processors and a cryptographic engine.....	6
	2. Skarine reveals implementation details for conventional mobile devices	10
	3. The combination of Marek and Skarine.....	12
	4. Element-by-Element Explanation of How Marek-Skarine Combination Renders Challenged Claims Obvious.....	19
	B. [GROUND 1B] – CLAIMS 4-5 WOULD HAVE BEEN OBVIOUS OVER MAREK, SKARINE, AND YOON	75
	1. Yoon describes voice command functionality on conventional mobile devices	75
	2. The combination of Marek, Skarine, and Yoon.....	76
	3. Reasons for the combination	76
	4. Element-by-Element Explanation of How Marek-Skarine-Yoon Combination Renders Challenged Claims Obvious.....	78
	C. [GROUND 1C] – CLAIMS 9-10 WOULD HAVE BEEN OBVIOUS OVER MAREK, SKARINE, AND MOON.....	79
	1. Moon describes configuring a conventional mobile device for tamper-resistance.....	79
	2. The combination of Marek, Skarine, and Moon	80
	3. Reasons for the combination	82
	4. Element-by-Element Explanation of How Marek-Skarine-Moon Combination Renders Challenged Claims Obvious.....	83

V.	PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION.....	85
A.	The <i>Fintiv</i> Factors Favor Institution—§314(a)	85
B.	The <i>Advanced Bionics</i> Test Favors Institution—§ 325(d)	88
VI.	FEES	89
VII.	CONCLUSION.....	89
VIII.	MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1).....	89
A.	Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1).....	89
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2)	89
C.	Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3).....	90
D.	Service Information	90

EXHIBITS

APPLE-1001	U.S. Patent No. 7,765,399 (“the ’399 Patent”)
APPLE-1002	Excerpts from the Prosecution History of the ’399 Patent (“the Prosecution History”)
APPLE-1003	Declaration of Dr. Sandeep Chatterjee
APPLE-1004	U.S. Patent No. 7,716,720 (“Marek”)
APPLE-1005	U.S. Patent Pub. No. 2005/0190159 (“Skarine”)
APPLE-1006	U.S. Patent No. 8,266,438 (“Orsini”)
APPLE-1007	U.S. Patent Pub. No. 2004/0082368 (“Yoon”)
APPLE-1008	U.S. Patent No. 7,571,475 (“Moon”)
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-1013	Reserved
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-1028-APPLE-1029	Reserved
APPLE-1030	Scheduling Order, <i>Speir Technologies Ltd. v. Apple Inc.</i> , Case 6:22-cv-00077-ADA (WDTX)
APPLE-1031	Complaint for Patent Infringement Against Apple Inc., <i>Speir Technologies Ltd. v. Apple Inc.</i> , Case 6:22-cv-00077-ADA (WDTX)
APPLE-1032	Amended Complaint for Patent Infringement Against Apple Inc., <i>Speir Technologies Ltd. v. Apple Inc.</i> , Case 6:22-cv-00077-ADA (WDTX)
APPLE-1033	Preliminary Disclosure of Asserted Claims and Infringement Contentions to Defendant Apple Inc., <i>Speir Technologies Ltd. v. Apple Inc.</i> , Case 6:22-cv-00077-ADA (WDTX)

APPLE-1034	Apple’s Opening Claim Construction Brief, <i>Speir Technologies Ltd. v. Apple Inc.</i> , Case 6:22-cv-00077-ADA (WDTX)
APPLE-1035	Speir’s Responsive Claim Construction Brief, <i>Speir Technologies Ltd. v. Apple Inc.</i> , Case 6:22-cv-00077-ADA (WDTX)
APPLE-1036	U.S. District Courts—Median Time Intervals From Filing to Disposition of Civil Cases Terminated, by District and Method of Disposition, During the 12-Month Period Ending September 30, 2022
APPLE-1037-APPLE-1039	Reserved
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.” <i>Proceedings of the Linux Symposium, Volume 2</i> (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”)
APPLE-1046	<i>Memorandum: Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation</i> (June 21, 2022) (“Director’s Memo”)

CLAIM LISTING

Limitation	Claim Language
[1pre]	A computer system, comprising:
[1a]	a portable mobile computing device including a secure user processor, a non-secure user processor, a communications transceiver, and a cryptographic engine;
[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;
[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;
[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
[1e]	a first data communication link communicating data between said secure processor and said cryptographic engine;
[1f]	a second data communication link communicating data between said non-secure processor and said cryptographic engine;
[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
[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;
[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.

Limitation	Claim Language
[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.
[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.
[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.
[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.
[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.
[7]	The mobile PDA computer system 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.
[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;

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

I. INTRODUCTION

Apple Inc. (“Petitioner”) petitions for IPR of claims 1-7 and 9-10 (“the Challenged Claims”) of U.S. Patent No. 7,765,399 (“the ’399 Patent”). As will be shown here, the Challenged Claims are not inventive, but rather are directed to long-known computer system architecture.

Specifically, the ’399 Patent’s inventors claim to have developed a computer system having multiple processing elements—secure and non-secure user processors and a cryptographic engine—that purportedly “offers the combined advantages of [a] secure PDA [] and [a] commercial PDA.” APPLE-1001, claim 1, 4:37-40. But this architecture was not new. Indeed, Marek similarly configures a conventional mobile device, and it would have been obvious to a POSITA to enhance Marek’s mobile device with components/configurations known by POSITAs to enhance conventional mobile devices, *e.g.*, as disclosed by Skarine, Yoon and Moon, to resolve a device having each of the claimed features that constitute the supposedly new architecture of the ’399 Patent’s system.

Accordingly, Petitioner respectfully submits that an IPR should be instituted, and that the Challenged Claims should be canceled as unpatentable.

II. REQUIREMENTS FOR IPR

A. Grounds for Standing

Petitioner certifies that the '399 Patent is available for IPR. Petitioner is not barred or estopped from requesting this review of the Challenged Claims.

B. Challenge and Relief Requested Under 37 C.F.R. §42.104(b)

Petitioner requests IPR of the Challenged Claims on the below grounds.

APPLE-1003, ¶¶1-253.

Ground	Claims	Basis
1A	1-7, 9-10	§103: Marek, Skarine
1B	4-5	§103: Marek, Skarine, Yoon
1C	9-10	§103: Marek, Skarine, Moon

Each reference pre-dates February 22, 2006, the filing date of the '399 Patent ("Critical Date"), and thus qualifies as prior art, as shown below.

Reference	Date	Section
Marek	6/17/2005 (filed), 5/11/2010 (published)	102(e)
Skarine	2/26/2004 (filed), 9/1/2005 (published)	102(a), 102(e)
Yoon	4/29/2004 (published)	102(b)
Moon	4/5/2005 (filed) 8/4/2009 (published)	102(e)

III. THE '399 PATENT

A. Brief Description

The '399 Patent describes “a mobile PDA computer system” including “a non-secure user processor, a secure user processor, and a cryptographic engine” that “forms a bridge between the secure processing side of the PDA and the non-secure processing side of the PDA.” APPLE-1001, 2:23-40. 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; APPLE-1003, ¶19.

B. Prosecution History

The '399 Patent issued from U.S. Patent App. No. 11/359,224 (the '224 application). The independent claims were initially rejected over McPhillie (GB 2336005) and Puranik (U.S. 2006/0105740). APPLE-1002, 77-83. The applicant narrowed the claims to recite features found in limitations [1d] and [1i] of the eventually-issued claims, *e.g., inter alia*, that the cryptographic engine encrypts “any data communicated from said secure user processor to said non-secure user processor.” *Id.*, 57. The resulting combination of elements was yet again rejected as anticipated by Mauro (U.S. Patent No. 7,047,405). *Id.*, 43-46. And again,

without debating satisfaction by the prior art of limitations otherwise recited, the applicant further narrowed the claims by reciting secure and non-secure human/machine interfaces (limitations [1g] and [1h] of the eventually-issued claims). *Id.*, 22, 28-30. On these limitations, the Examiner relented and issued a Notice of Allowance. *Id.*, 7-12.

C. Level of Ordinary Skill

A person of ordinary skill in the art relating to the subject matter of the '399 Patent as of February 22, 2006 ("POSITA") would have been 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. APPLE-1003, ¶¶17-18.

D. Claim Construction

All claim terms should be construed according to the Phillips standard. *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005); 37 C.F.R. § 42.100. Here, because the Challenged Claims are obvious under any reasonable interpretation and because "claim terms need only be construed to the extent necessary to resolve the controversy," no express constructions are required in this proceeding. *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011).

Petitioner reserves the right to address any construction proposed by Patent Owner or the Board. Petitioner also reserves the right to pursue constructions in district court that are necessary to decide matters of infringement. For example, in district court, Petitioner has proposed constructions for several terms, each opposed by Patent Owner.¹ APPLE-1034, 11-29; APPLE-1035, 9-27. While pertinent to infringement, the parties' dispute over those constructions has no bearing in this IPR because the prior art obviates the Challenged Claims under either party's interpretation.

IV. THE CHALLENGED CLAIMS ARE UNPATENTABLE

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

The sections below provide a brief introduction to Marek, Skarine, and the combination thereof.²

¹ The Court has not yet construed any claims in the district court proceeding.

² Petitioner incorporates this discussion into Grounds 1A-1C.

1. Marek describes a conventional mobile device having secure and non-secure processors and a cryptographic engine

Marek relates to mobile devices, describing “a system for providing a secure and trusted commercial-off-the shelf COTS³ computing environment” for use with an “untrusted computing system,” such as a mobile device, *e.g.*, a PDA. APPLE-1004, Abstract, 1:7-9. 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,” *e.g.*, a PDA. APPLE-1004, 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”). Annotated Fig. 10, *infra*, shows such a system, including “a SCM 908 [purple] interfacing with an untrusted PDA 1014 [green].” *Id.*, 12:14-15. With this configuration, “[o]nly authenticated COTS applications and COTS OS execute on the SCM while untrusted applications execute on the untrusted host environment.” *Id.*, 8:39-41; *see* 2:21-28; APPLE-1003, ¶¶21-22.

³ The acronym COTS is used throughout to mean “commercial-off-the-shelf.”

APPLE-1004, 1:8.

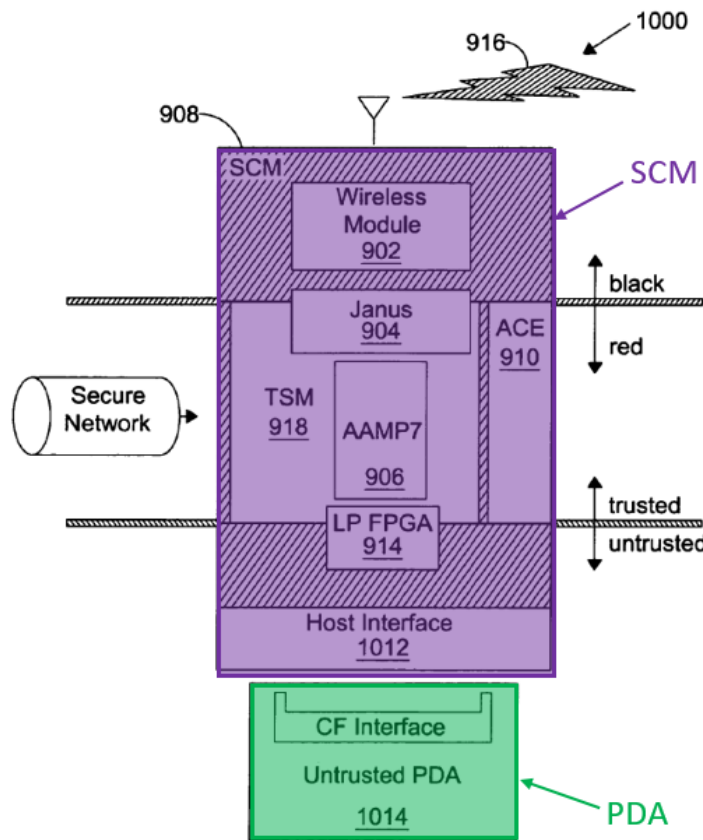
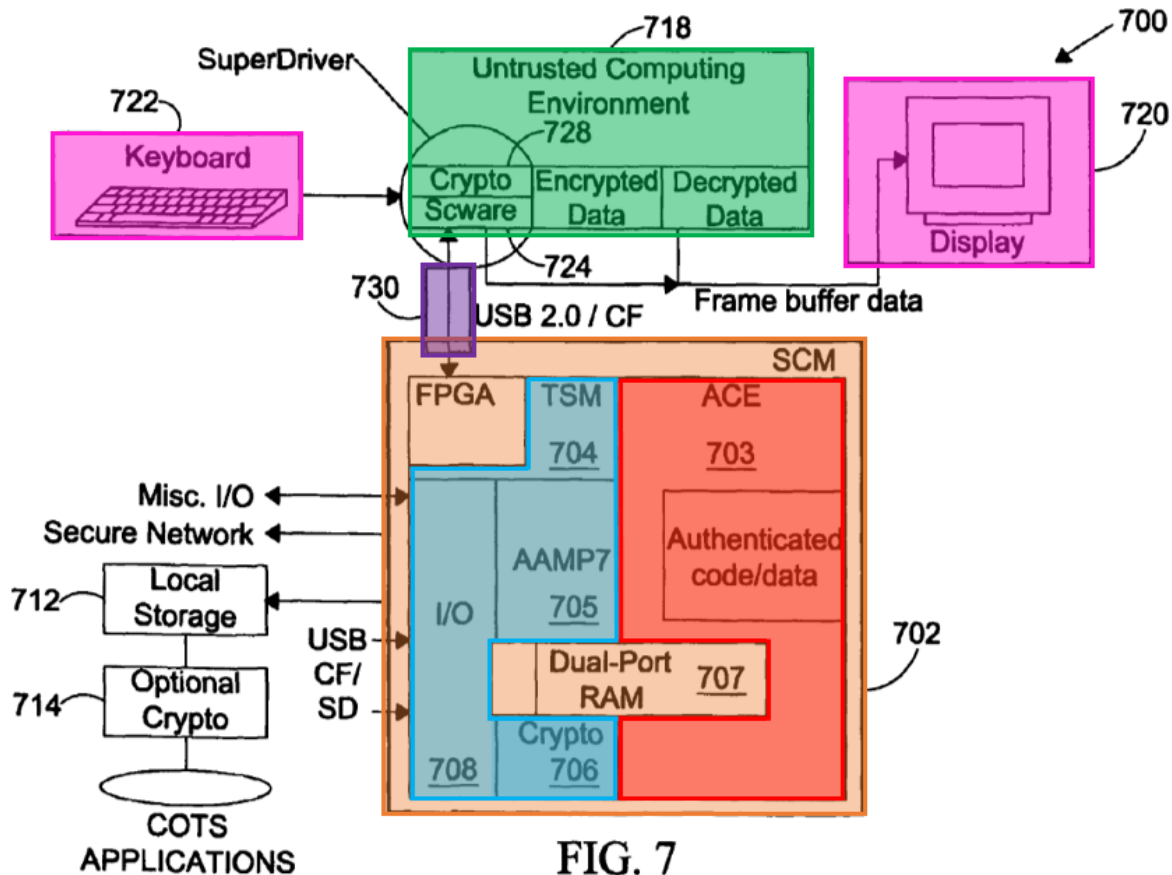


FIG. 10

Excerpt from Marek, Fig. 10 (annotated)

Annotated Fig. 7 of Marek, *infra*, illustrates a computing environment implementing this SCM architecture. See APPLE-1004, 8:51-54. This environment includes a SCM 702 (orange) provided as “an add-on module to an untrusted host environment” 718, *e.g.*, a PDA (green). *Id.*, 8:38-39. The SCM includes an “Authenticated COTS Environment Subsystem (ACE)” (red) and a “Trusted Security Manager subsystem (TSM) 704” (blue). *Id.*, 8:64-9:1. The TSM includes “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.” *Id.*, 9:31-41; *see* 2:21-38. In this system, “[e]ach I/O path of the SCM 702,” including “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. 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; APPLE-1003, ¶23.



Excerpt from Marek, Fig. 7 (annotated)

Marek’s untrusted host mobile device includes “input and output devices,” such as a keypad and display, pink in Fig. 7. APPLE-1004, 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. 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,” enabling “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.*, 10:47-54; *see* Fig. 8; APPLE-1003, ¶24.

2. Skarine reveals implementation details for conventional mobile devices

Skarine describes configuring a conventional mobile device with “voice and advanced data communication capabilities.” APPLE-1005, [0034]. Skarine’s mobile device includes a “communication subsystem 211,” pink in Fig. 2, *infra*, connected to its microprocessor (green). *Id.*, [0038]. The communication subsystem, which “includes a receiver 212, a transmitter 214, and associated components,” is “analogous to RF transceiver circuitry 108 and antenna 110 shown in FIG. 1.” *Id.*, [0035]; *see* [0023]; APPLE-1003, ¶¶25-26.

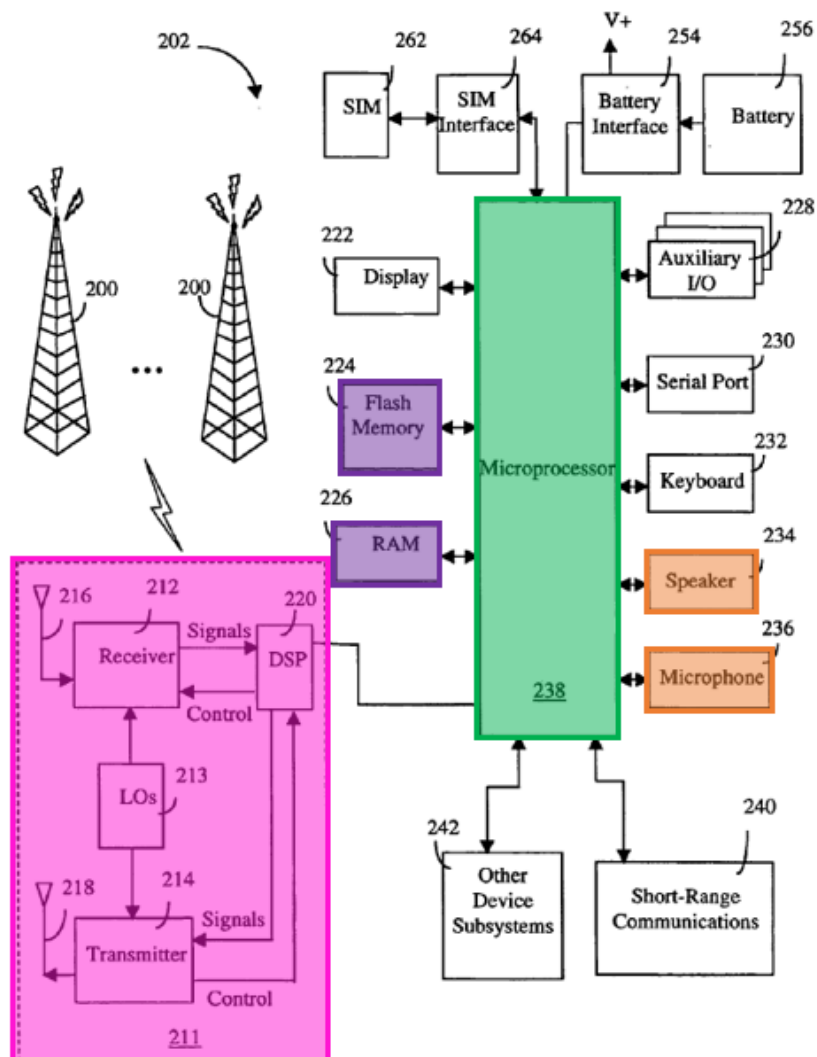


FIG. 2

Excerpt from Skarine, Fig. 2 (annotated)

Skarine's mobile device includes "additional device subsystems such as ... a speaker 234, [and] a microphone 236," orange in Fig. 2, also connected to the mobile device microprocessor. APPLE-1005, [0038]. "For voice communications, ... the received signals would be output to speaker 234 and signals for transmission would be generated by microphone 236." *Id.*, [0042].

Additionally, Skarine's mobile device includes "a flash memory 224, [and] a random access memory (RAM) 226," purple. *Id.*, [0038]. "Operating system software used by microprocessor 238 is preferably stored in a persistent store such as flash memory 224." *Id.*, [0038]; APPLE-1003, ¶¶27-28.

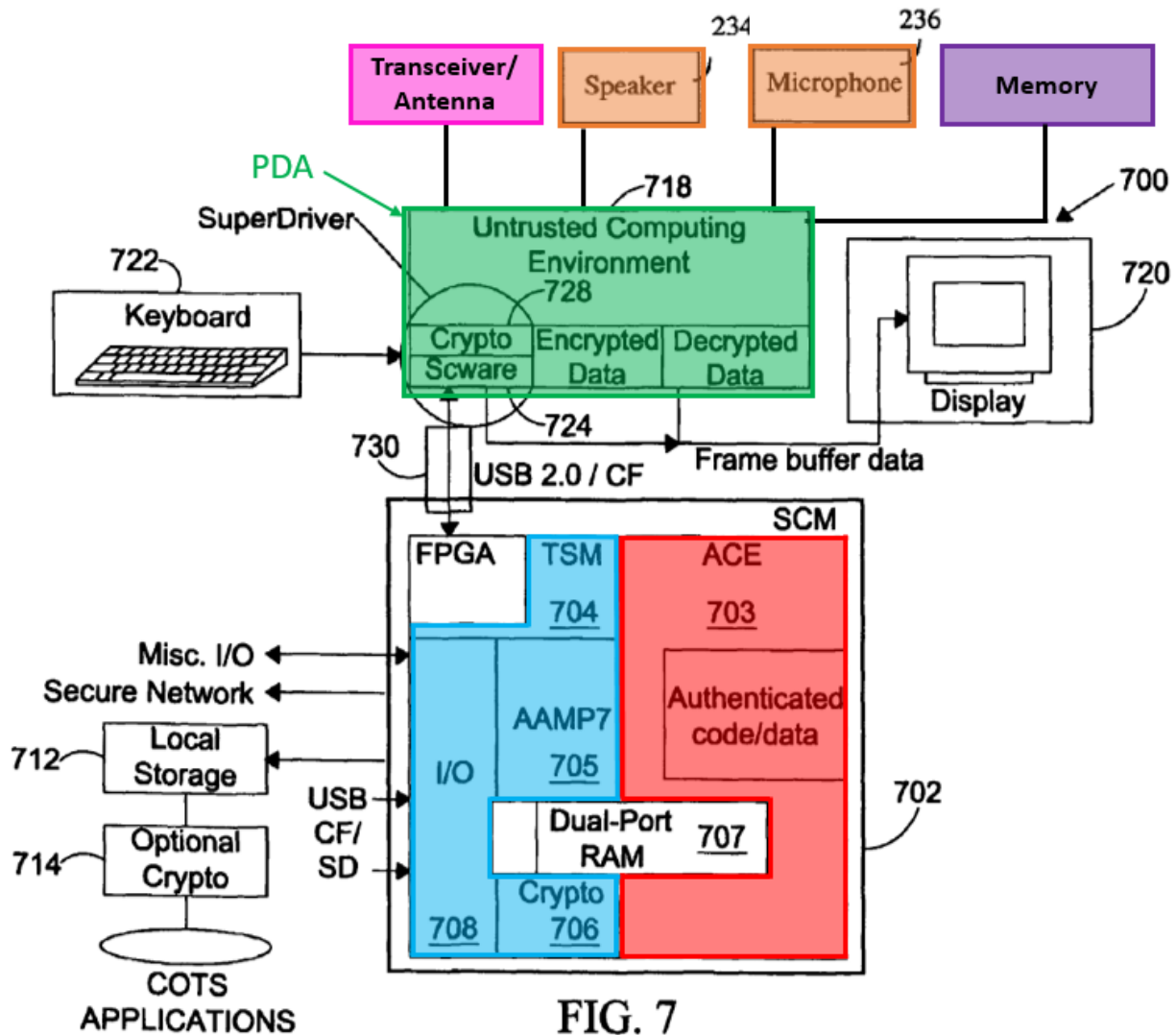
3. The combination of Marek and Skarine

In the Marek-Skarine combination, a SCM interfaces with a mobile device, *e.g.*, a PDA or cell phone (green in the composite figure *infra*), as taught by Marek. *See* APPLE-1004, 8:37-39, 11:44-12:21, 13:49-51; APPLE-1003, ¶29.

In the combination, the SCM (secure computing module) includes an ACE (Authenticated COTS Environment Subsystem, red) and a TSM (Trusted Security Manager subsystem, blue), as also taught by Marek. APPLE-1004, 8:51-67.

"Only 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 PDA, while the TSM "provid[es] partitioning for both memory and I/O resources on the trusted environment." APPLE-1004, 2:21-38.

"All I/O paths of the SCM are configured to go through the TSM," with each I/O path "subject to authentication protocols" provided by the TSM. APPLE-1004, 2:25-30; APPLE-1003, ¶30.



Marek-Skarine composite rendering⁴

⁴ 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 combinations also would have been obvious to a POSITA. APPLE-1003, ¶30.

To the extent that Marek omits details regarding its untrusted host mobile device and components thereof, a POSITA would have understood or found it obvious that the untrusted host mobile device of the combination includes common and well-known components of mobile devices many of which are described, *e.g.*, in Skarine. APPLE-1003, ¶31.

Audio functionality in the untrusted host mobile device of the combination

For instance, a POSITA would have understood or found obvious that the combination's untrusted host mobile device includes conventional audio input and output components, *e.g.*, a speaker and a microphone (orange in the figure *supra*), for audio input and output to/from the mobile device microprocessor (*e.g.*, for voice communications), as was well-known 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; APPLE-1003, ¶32.

In the 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. APPLE-1003, ¶¶33-35. To the extent Marek does not explicitly disclose this configuration, a POSITA would have found it obvious in view of Skarine. *See* APPLE-1005, [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; APPLE-1003, ¶¶33-35.

A POSITA would have been motivated to implement this configuration for at least the following reasons. APPLE-1003, ¶¶36-42.

First, a POSITA would have been motivated to pursue this implementation because doing so enables the mobile device to be used to carry out "voice communications," *e.g.*, phone calls or voicemail, which was conventional mobile device functionality, *e.g.*, as evidenced by Skarine. APPLE-1005, [0042]; *see id.* ("a voice message recording system," "a voice call"); APPLE-1003, ¶37. A POSITA would have recognized that with this configuration, the untrusted host mobile device of the combination can be used for conventional mobile device audio communications functions. APPLE-1003, ¶37.

Second, a POSITA would have been motivated to pursue this implementation because having the speaker and microphone in communication with the processor of the mobile device enables the mobile device to be used for entertainment (*e.g.*, for playing music) and/or for professional purposes (*e.g.*, recording interviews or meetings), which are other examples of conventional audio functionality in standard mobile devices. *See* APPLE-1024, [0004] ("a music

player can be embedded in a device such as a mobile phone or a personal digital assistant (PDA)"); APPLE-1025, 1:18-20 ("a mobile terminal having ... a microphone for recording a corresponding audio"); APPLE-1003, ¶38. A POSITA would have recognized that having the speaker and microphone in communication with the processor of the mobile device enables this broad range of conventional mobile device capabilities to be readily accessible to the user. APPLE-1003, ¶38.

Third, a POSITA would have been prompted to pursue this implementation because doing so is merely the application of known techniques (*e.g.*, a speaker and microphone communicatively connected to a mobile device processor) by a known system (*e.g.*, Marek's untrusted host mobile device) to yield predictable results (*e.g.*, a mobile device with conventional audio capabilities). APPLE-1003, ¶39; *see KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007) (a supposed invention that "simply arranges old elements with each performing the same function it had been known to perform" is obvious).

A POSITA would have expected success in pursuing this implementation because Marek's teachings are applicable to conventional "wireless devices such as PDAs, cell phones, and other mobile devices" (APPLE-1004, 11:55-56), and because speakers and microphones in communication with mobile device microprocessors was a standard configuration. *See* APPLE-1018, 3:45-50; APPLE-1010, 3:54-67; APPLE-1024, [0004]; APPLE-1025, 1:18-20; APPLE-

1003, ¶¶40-41. Furthermore, a POSITA would have expected success because both Marek and Skarine pertain generally to mobile devices. *See* APPLE-1004, 11:44-56, 12:13-21, 13:49-51, 2:56-59, 7:53-57, 8:25-38, Figs. 10-11; APPLE-1005, [0001]; APPLE-1003, ¶42.

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

The untrusted host mobile device of the combination is a wireless device, as taught by Marek (*see* APPLE-1004, 11:44-56, 12:13-21, 13:49-51, 2:56-59, 7:53-57, 8:25-38). A POSITA would have understood or found obvious that this wireless device includes conventional wireless communication components, such as RF transceiver circuitry and an antenna (pink in the figure *supra*), as was well-known and as evidenced, *e.g.*, by Skarine. *See* APPLE-1003, ¶¶43-46; APPLE-1005, [0022]-[0023], [0027]-[0029], [0032], [0034]-[0036], [0038], Figs. 1-2; *see* APPLE-1011, 5:11-13; APPLE-1015, 3:11-17; APPLE-1017, 10:14-18; APPLE-1018, 6:33-45, 7:11-29.

In the Marek-Skarine combination, the wireless communication components are coupled to the processor of the untrusted host device. APPLE-1003, ¶47. To the extent Marek does not explicitly disclose this configuration, a POSITA would have found it obvious in view of Skarine. *See* APPLE-1005, [0038], Fig. 2; APPLE-1003, ¶47.

A POSITA would have been motivated to have the wireless communication components coupled to the processor of the combination's untrusted host mobile device at least because doing so enables communication between the mobile device and a cellular telephone network, which was conventional mobile device functionality, *e.g.*, as evidenced by Skarine. *See* APPLE-1003, ¶48; APPLE-1005, [0022]-[0023], [0027]-[0029], [0032], [0034]-[0035], [0038], Figs. 1-2; APPLE-1011, 5:11-13; APPLE-1015, 3:11-17; APPLE-1017, 10:14-18; APPLE-1018, 6:33-45, 7:11-29.

A POSITA also would have been motivated to pursue this implementation because doing so is merely the application of known techniques (*e.g.*, wireless communication components connected to a mobile device processor) by a known system (*e.g.*, Marek's untrusted host mobile device) to yield predictable results (*e.g.*, a mobile device with conventional wireless communication capabilities). APPLE-1003, ¶49; *see KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

A POSITA would have expected success in pursuing this implementation because Marek's teachings are applicable to conventional "wireless devices" (APPLE-1004, 11:55-56), and because wireless communication components in communication with mobile device microprocessors was a standard configuration. *See* APPLE-1003, ¶¶50-51; APPLE-1005, [0022]-[0023], [0027]-[0029], [0032], [0034]-[0035], [0038], Figs. 1-2; APPLE-1011, 5:11-13; APPLE-1015, 3:11-17;

APPLE-1017, 10:14-18; APPLE-1018, 6:33-45, 7:11-29. Furthermore, a POSITA would have expected success because both Marek and Skarine pertain generally to mobile devices. *See* APPLE-1004, 11:44-56, 12:31021, 13:49-51, 2:56-59, 7:53-57, 8:25-38, Figs. 10 and 11; APPLE-1005, [0001]; APPLE-1003, ¶52.

Additionally, a POSITA would have understood or found obvious that the untrusted host mobile device of the combination includes conventional memory components (purple) such as volatile and non-volatile storage, as was also well-known in the art as of the Critical Date and as evidenced, *e.g.*, by Skarine. *See* APPLE-1003, ¶¶53-55; APPLE-1005, [0038]; APPLE-1018, 3:58-64; APPLE-1009, 1:44-46; APPLE-1010, 3:10-39; APPLE-1011, 4:46-59; APPLE-1012, [0013]; APPLE-1017, 10:14-22.

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

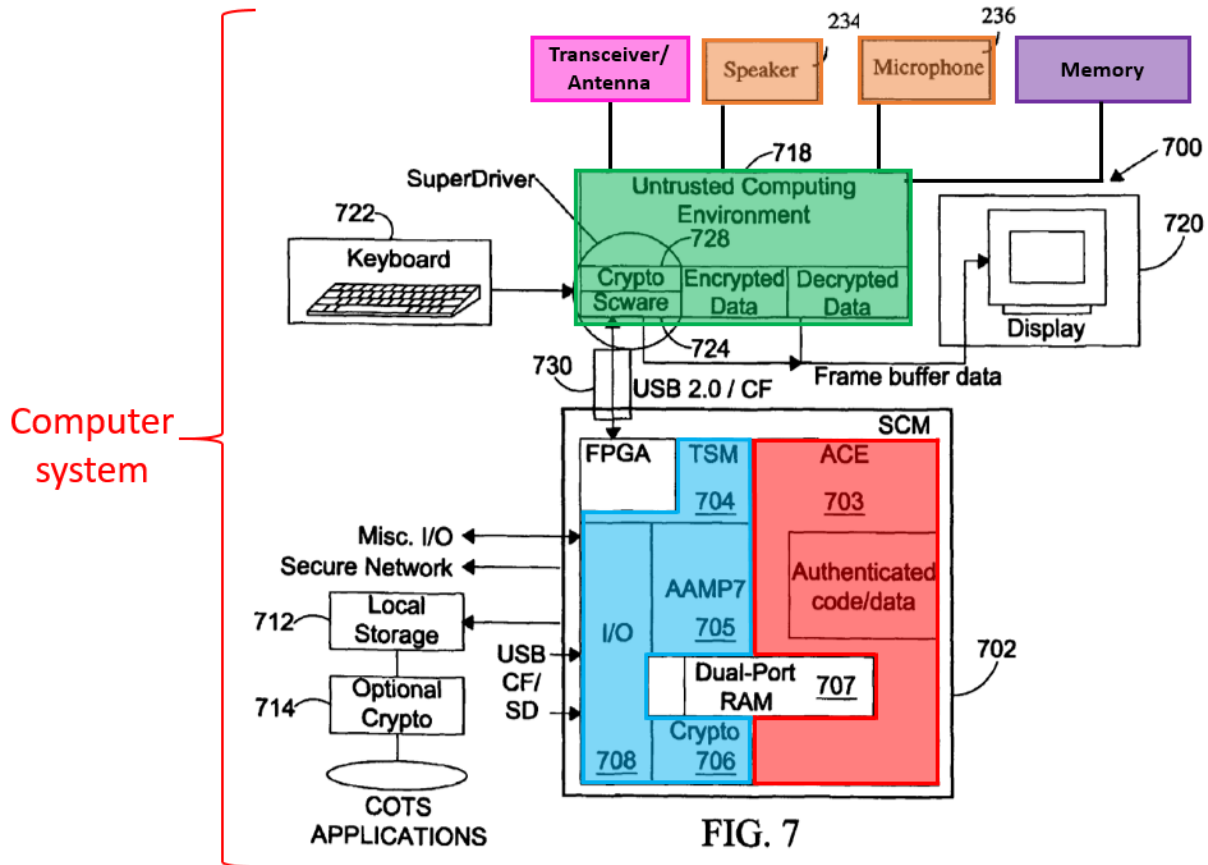
(i) Claim 1

[1pre]

To the extent the preamble is deemed to be limiting, the Marek-Skarine combination renders it obvious. APPLE-1003, ¶56.

Marek-Skarine provides **a computer system**, shown in the figure *infra*. Marek's "**computing environment 700**" implementing SCM architecture, modified based on Skarine as discussed in §IV.A.3, is **a computer system**, or at least a POSITA would have understood it to be a computer system. APPLE-1004, 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; APPLE-1003, ¶56.

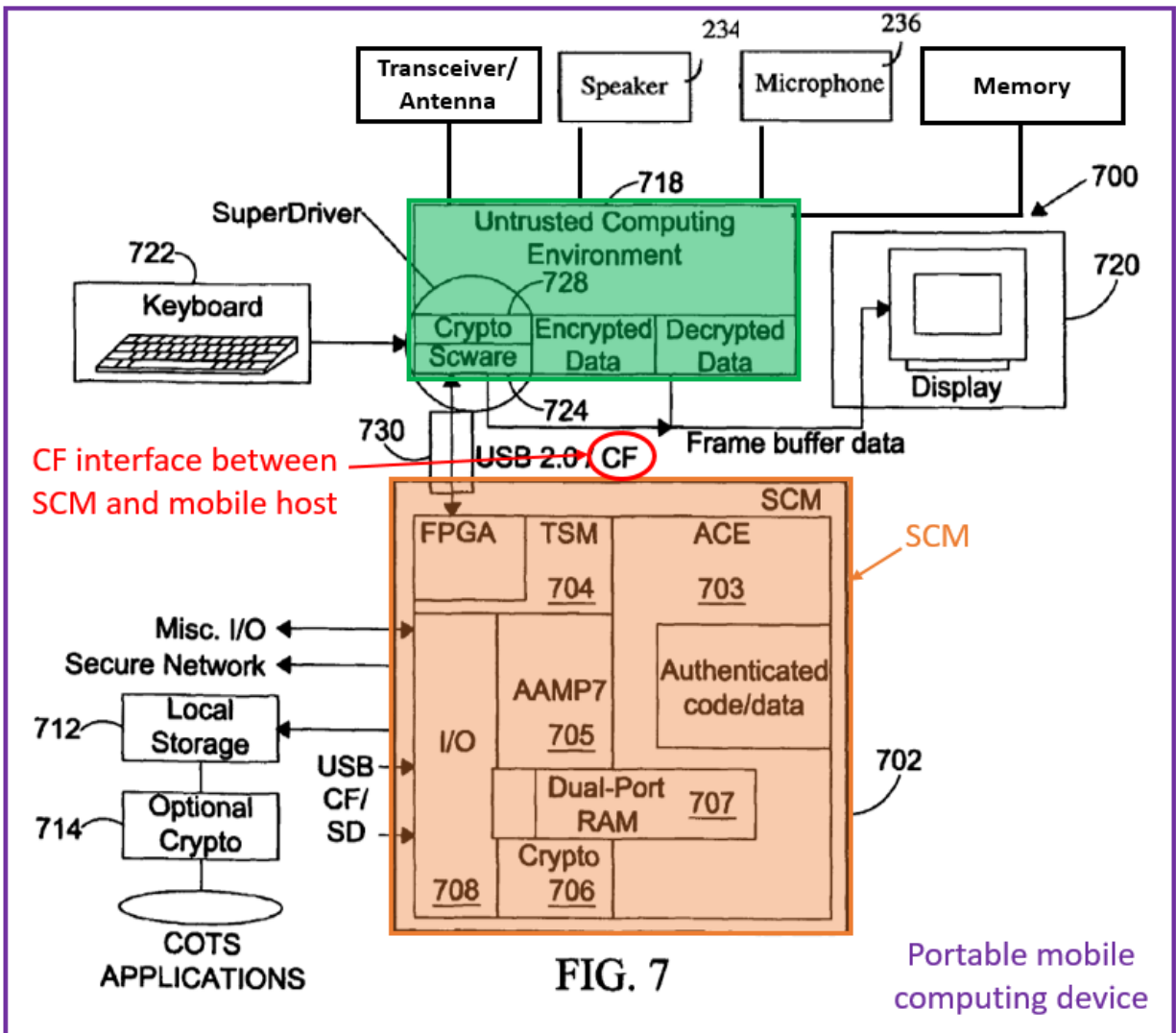


Marek-Skarine Rendering

[1a]

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

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 *infra*) and the SCM 702 (orange), which are each a mobile device as discussed *infra*, together are (or render obvious) a **portable mobile computing device** (outlined in purple). APPLE-1003, ¶57.



Marek-Skarine Rendering

First, Marek's untrusted host (green) is a mobile device, *e.g.*, a PDA or cell phone, and the combination with Skarine does not alter this form factor. APPLE-1003, ¶58; *see* §IV.A.3.

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; APPLE-1003, ¶59.

More specifically, the particular untrusted host 718 of 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; APPLE-1003, ¶60. At least when the SCM employs the illustrated CF interface, the untrusted host is a mobile device. *See* APPLE-1004, 11:45-50; APPLE-1003, ¶60.

Second, Marek’s SCM (orange) is also a mobile device. APPLE-1003, ¶61. 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; APPLE-1003, ¶62.

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]; APPLE-1003, ¶63.

That Marek's SCM has a mobile device form factor, and includes a mobile device processor and operating system, demonstrates that Marek's SCM is a mobile device. APPLE-1003, ¶¶61-63.

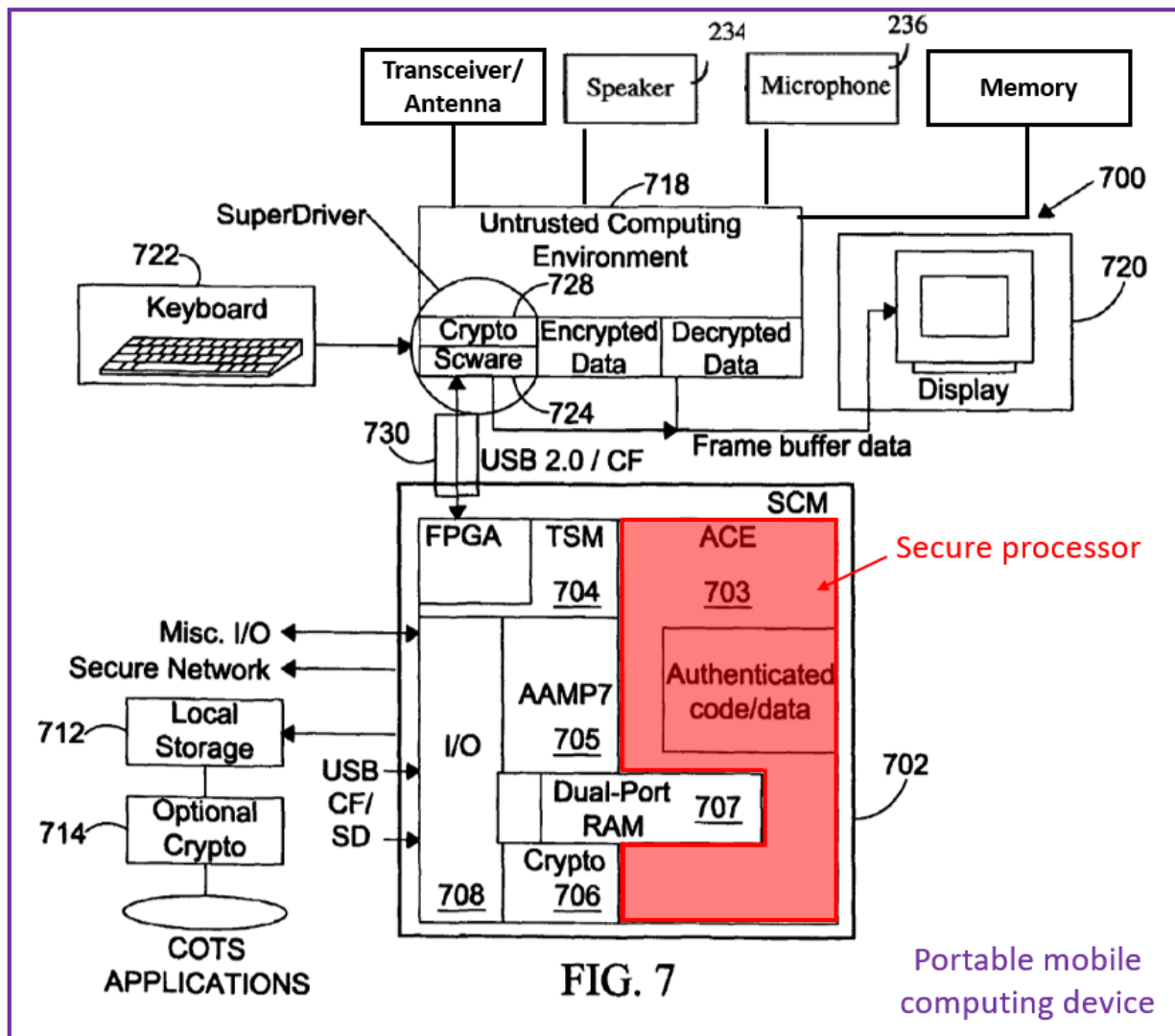
At least because Marek's untrusted host and SCM are both mobile devices, the untrusted mobile device host and the SCM together are, or at least render obvious, **a portable mobile computing device** in the combination. APPLE-1003, ¶64.

The combination device includes a secure user processor

In the Marek-Skarine combination, the SCM includes **a secure user processor**. APPLE-1003, ¶65. 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* [1b]. 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 user processor**.⁵ APPLE-1003, ¶65.

⁵ The '399 Patent describes "a secure processor" including "trusted microprocessor hardware executing trusted operating system software and trusted application software." APPLE-1001, 4:40-43; APPLE-1003, ¶65.



Marek-Skarine Rendering

Alone or combined, it would be obvious for the embedded COTS processor, COTS OS, and software of Marek's ACE to be **secure**, as Marek includes each within its "**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 (“the system including the SCM may provide trusted and portable COTS computing environments against malware”), Figs. 10-11 (showing an ACE in the red domain⁶ of a portable mobile computing device system); APPLE-1003, ¶¶66-68.

The combination device includes a non-secure user processor

In the Marek-Skarine combination, the untrusted host mobile device, green in the figure *infra*, includes **a non-secure user processor**. APPLE-1003, ¶69.

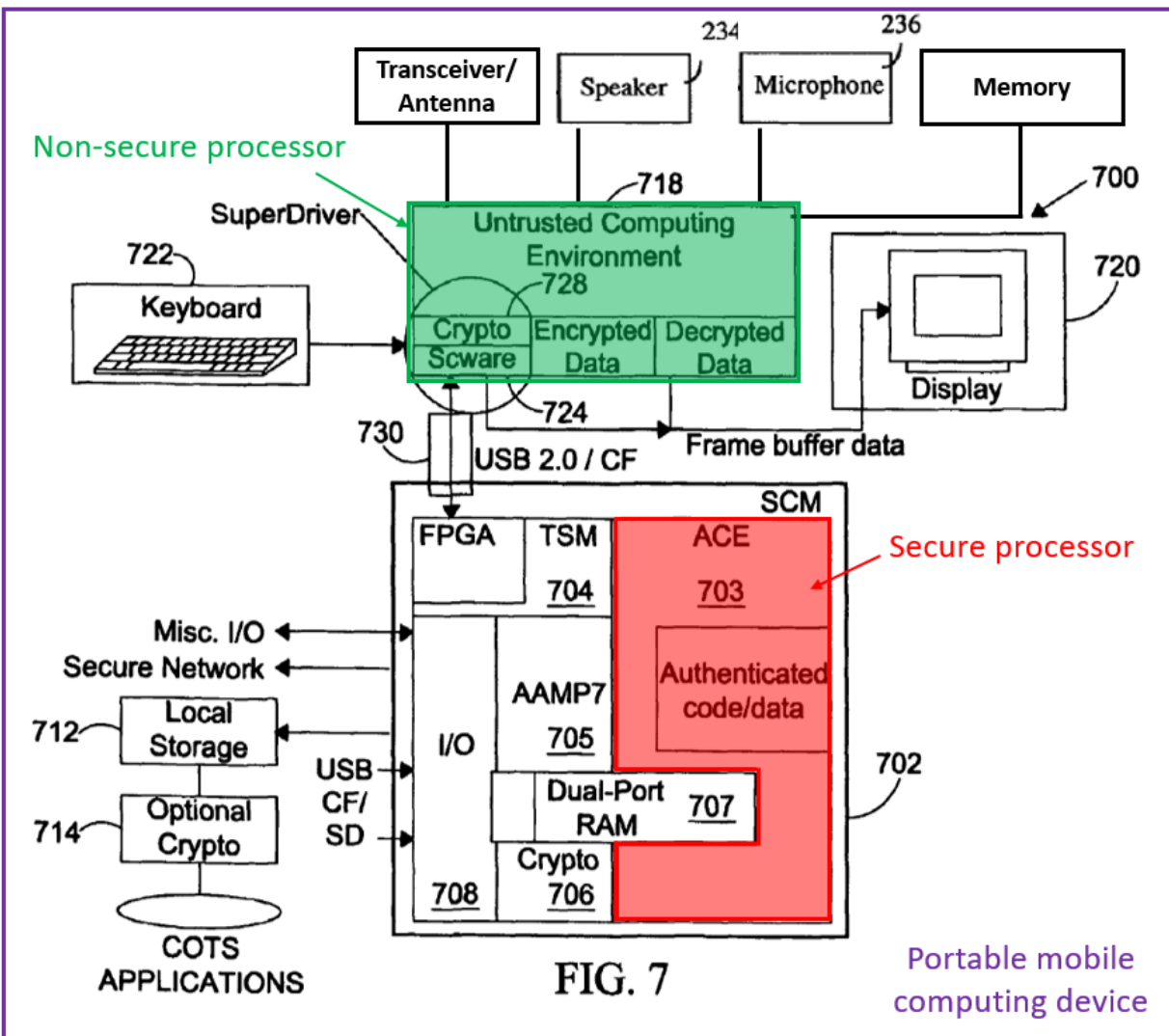
Marek describes that the untrusted host includes COTS processors. *See* APPLE-1004, 8:59-61 (“Conventionally, a host platform employing **COTS processors** is assumed to be untrusted.”). The untrusted host also includes an operating system and application software. *See* APPLE-1004, 7:54-55 (“Windows CE operating system may be utilized as ***an embedded COTS OS on the untrusted host platform***”), 8:40-41 (“***untrusted applications execute 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;

⁶ 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]; APPLE-1003, ¶67.

see [1c]; APPLE-1003, ¶69. Alone or in combination, the COTS processor(s) of the untrusted host, together with the COTS OS and the applications executing on the untrusted host, are or render obvious **a non-secure user processor**.⁷ APPLE-1003, ¶69.

To the extent Marek does not explicitly state that the COTS OS is on the processor of the specific untrusted host 718, a POSITA would have understood this to be the case, or otherwise found this to be obvious, given that it was well-known for mobile devices to have operating systems. *See* APPLE-1005, [0022]-[0023], [0038]; APPLE-1009, 1:64-2:3; APPLE-1010, 3:17-21; APPLE-1011, 4:54-61; APPLE-1003, ¶70.

⁷ The '399 Patent describes a “[n]on-secure processor” including “untrusted microprocessor hardware executing an untrusted operating system and untrusted application software.” APPLE-1001, 4:49-51; APPLE-1003, ¶69.



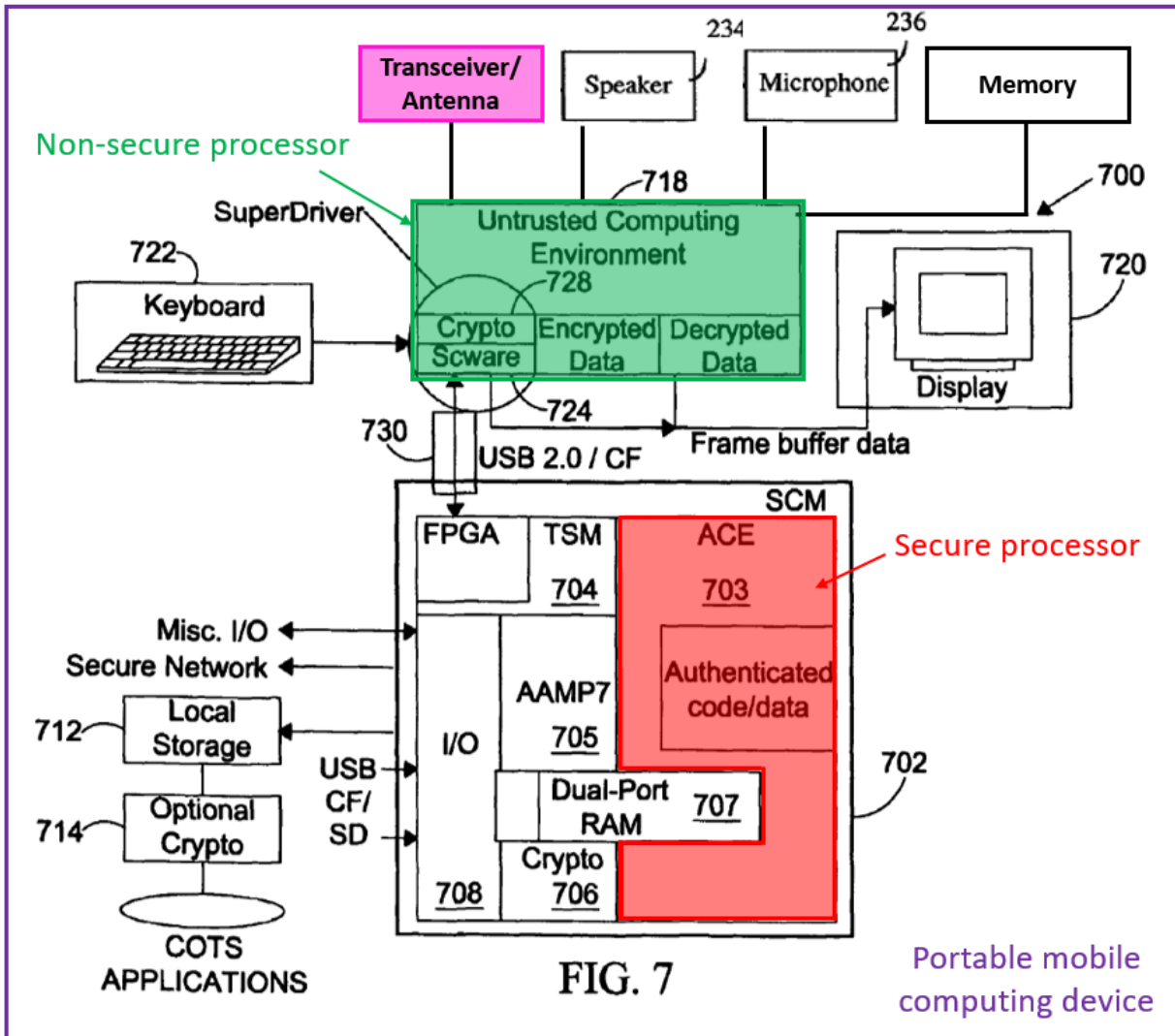
Marek-Skarine Rendering

Alone or combined, it would be obvious for the COTS processor(s), COTS OS, and applications of the untrusted host to be a **non-secure** processor, as Marek includes each within its “untrusted host environment.” APPLE-1004, 8:40-41; *see* 8:56-59 (“a host platform employing COTS processors is assumed to be **untrusted**”), 12:16-18, 2:1-4, 2:36-38, Figs. 10-11 (showing the PDA in the black domain); APPLE-1003, ¶71.

The combination device includes a communications transceiver

Marek's "SCM is added on *wireless devices* such as PDAs, cell phones, and other mobile devices," *e.g.*, the untrusted host mobile device in the combination is a wireless device. APPLE-1004, 11:53-56. A POSITA would have understood—or at least found it obvious—that the untrusted host wireless device of the combination includes **a communications transceiver**, *e.g.*, RF transceiver circuitry and an antenna, pink in the figure *infra*, coupled to the non-secure user processor of the untrusted host (green). As discussed in §IV.A.3, it was conventional for wireless mobile devices to have communications transceivers to enable wireless communication, as evidenced, *e.g.*, by Skarine. *See* APPLE-1005, [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. ... **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"), [0027]-[0029], [0036]-[0038], Figs.

1-2; see APPLE-1011, 5:11-13, 4:46-59; APPLE-1015, 3:11-17; APPLE-1017, 10:14-18; APPLE-1018, 6:33-45, 7:11-29; APPLE-1003, ¶¶72-74.



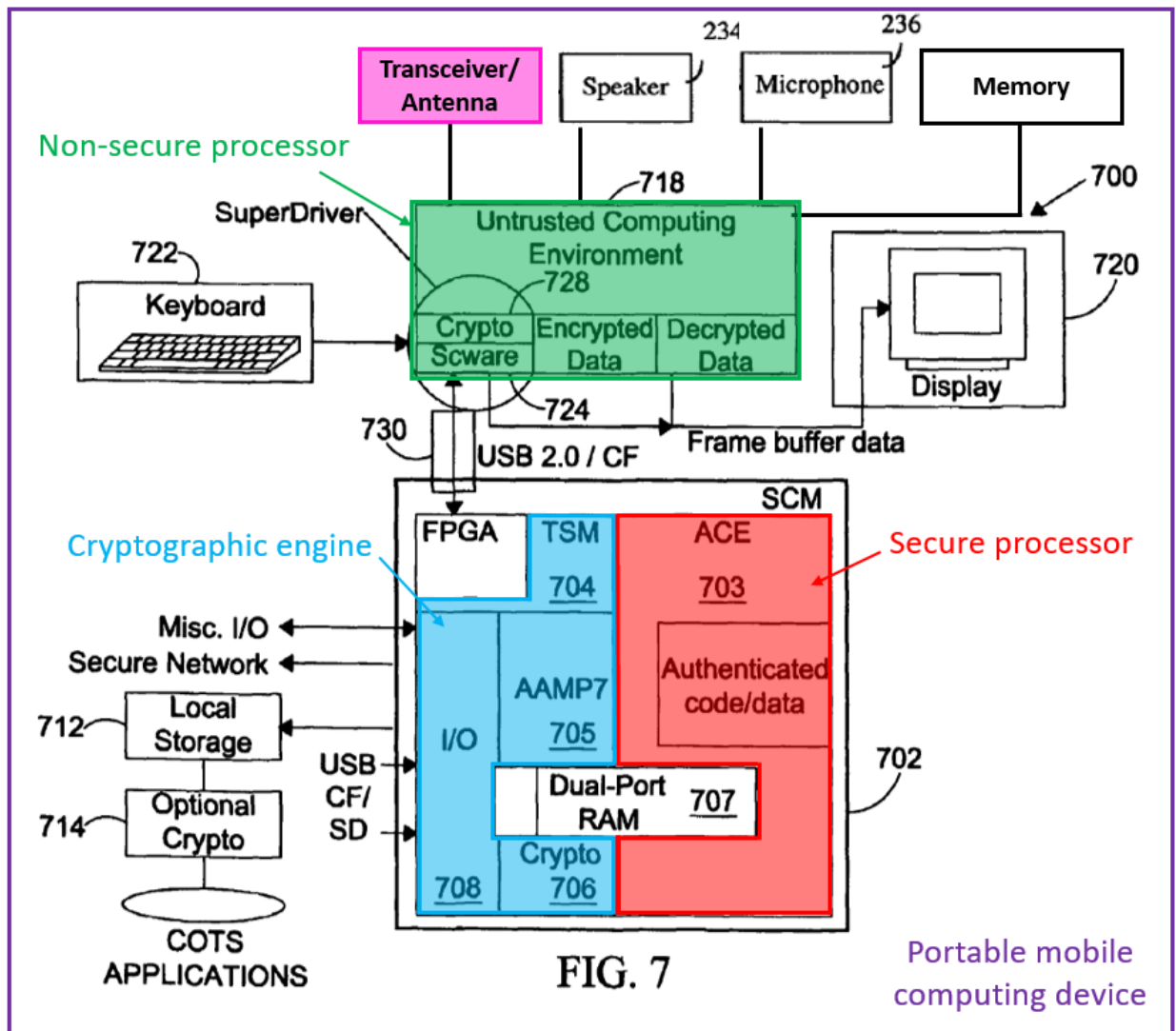
Marek-Skarine Rendering

The combination device includes a cryptographic engine

In the Marek-Skarine combination, the SCM of the portable mobile computing device includes a **cryptographic engine**. APPLE-1003, ¶75.

Specifically, the SCM includes a “Trusted Security Manager subsystem (TSM)

704,” as taught by Marek. APPLE-1004, 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, 9:31-47. In the combination, the TSM subsystem 704, including the trusted processor 705 and cryptographic engine 706, work together as (and render obvious) **a cryptographic engine**, blue in the figure *infra*. APPLE-1003, ¶75.



Marek-Skarine Rendering

The TSM 704 is a cryptographic engine at least because it “provide[s] a robust security interface” (APPLE-1004, 9:40-41; *see* 10:33-35) using

cryptography.⁸ *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.”), 9:31-37; APPLE-1003, ¶76.

[1b]

The **secure user processor** of the Marek-Skarine combination (contained in the ACE of the SCM; *see* [1a]) **includes a trusted microprocessor**, *e.g.*, the hardware of the embedded COTS processor of Marek’s ACE. *See* APPLE-1004, 9:1-5 (“The ACE 703 includes an embedded COTS OS running on a compatible

⁸ 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”); APPLE-1003, ¶76.

embedded COTS processor”), 8:61-62 (“The trusted environment may include *trusted hardware* and software”), 9:7-13, Fig. 7; APPLE-1003, ¶77.

The secure user processor of the combination also includes **a trusted operating system executing on the trusted microprocessor**, *e.g.*, the embedded COTS operating system (OS) of Marek’s ACE. *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; APPLE-1003, ¶78.

The secure user processor of the combination further includes **trusted application software executing on said trusted microprocessor**, *e.g.*, the applications included in Marek’s ACE. *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; APPLE-1003, ¶79.

A POSITA would have understood or found obvious that the trusted microprocessor, trusted operating system, and trusted application software are

trusted 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); APPLE-1003, ¶80.

Alternatively or additionally, a POSITA would have understood or found obvious that the trusted operating system and application software are **trusted** 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; APPLE-1003, ¶81.

[1c]

The **non-secure user processor** of the Marek-Skarine combination (included in the untrusted host mobile device; *see* [1a]) **includes an untrusted microprocessor**, *e.g.*, the hardware of the COTS processor of the untrusted host

PDA. *See* APPLE-1004, 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.”); APPLE-1003, ¶82.

The non-secure user processor of the combination also includes **an untrusted operating system executing on the untrusted microprocessor**, *e.g.*, the operating system of the untrusted host. For instance, 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, 7:54-55; APPLE-1003, ¶83.

Alternatively or additionally, to the extent that Marek does not explicitly state that an operating system such as Windows CE is executed on the microprocessor of the specific untrusted mobile device host 718, a POSITA nevertheless would have understood this to be the case based on Marek’s disclosure of operating systems executing on untrusted host platforms. *See* APPLE-1004, 7:54-55; APPLE-1003, ¶84. Indeed, it was standard that operating systems execute on the microprocessors of mobile devices such as a PDAs or cell phones, *e.g.*, to control execution of applications and for resource allocation. *See* APPLE-1005, [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]; 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-1009, 1:64-2:3; APPLE-1011, 4:54-61; APPLE-1018, 3:58-64; APPLE-1003, ¶84. Thus, given the ubiquity of operating systems in mobile devices, 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, 7:54-55; APPLE-1003, ¶84.

Furthermore, the non-secure user processor of the combination includes **untrusted application software executing on the untrusted microprocessor**, *e.g.*, the applications that execute on Marek’s untrusted host. *See* APPLE-1004, 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, 2:1-4, 2:36-38; APPLE-1003, ¶85.

A POSITA would have understood or found obvious that the untrusted microprocessor, untrusted operating system, and untrusted application software are

untrusted at least because they are part of, or execute on, “the *untrusted* host environment” rather than the secure environment of the SCM. APPLE-1004, 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); APPLE-1003, ¶86. Moreover, a POSITA would have understood or found obvious that the untrusted application software is **untrusted** 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, 8:56-59; APPLE-1003, ¶86.

[1d]

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

In the combination, Marek’s TSM is the **cryptographic engine**. *See* [1a]. Marek describes that **any data communicated from the secure user processor** (red in the figure *infra*) **to the non-secure user processor** (green) passes through the cryptographic engine (blue), *e.g.*, through Marek’s TSM. APPLE-1003, ¶87. 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 user processor and the SCM (which contains the secure user 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 user processor also pass through the cryptographic engine. *Id.*, 9:63-66. Thus, any I/O path between the untrusted host and ACE of the SCM goes through the TSM— *e.g.*, any data communicated between the secure user processor and the non-secure user processor passes through 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; APPLE-1003, ¶88.

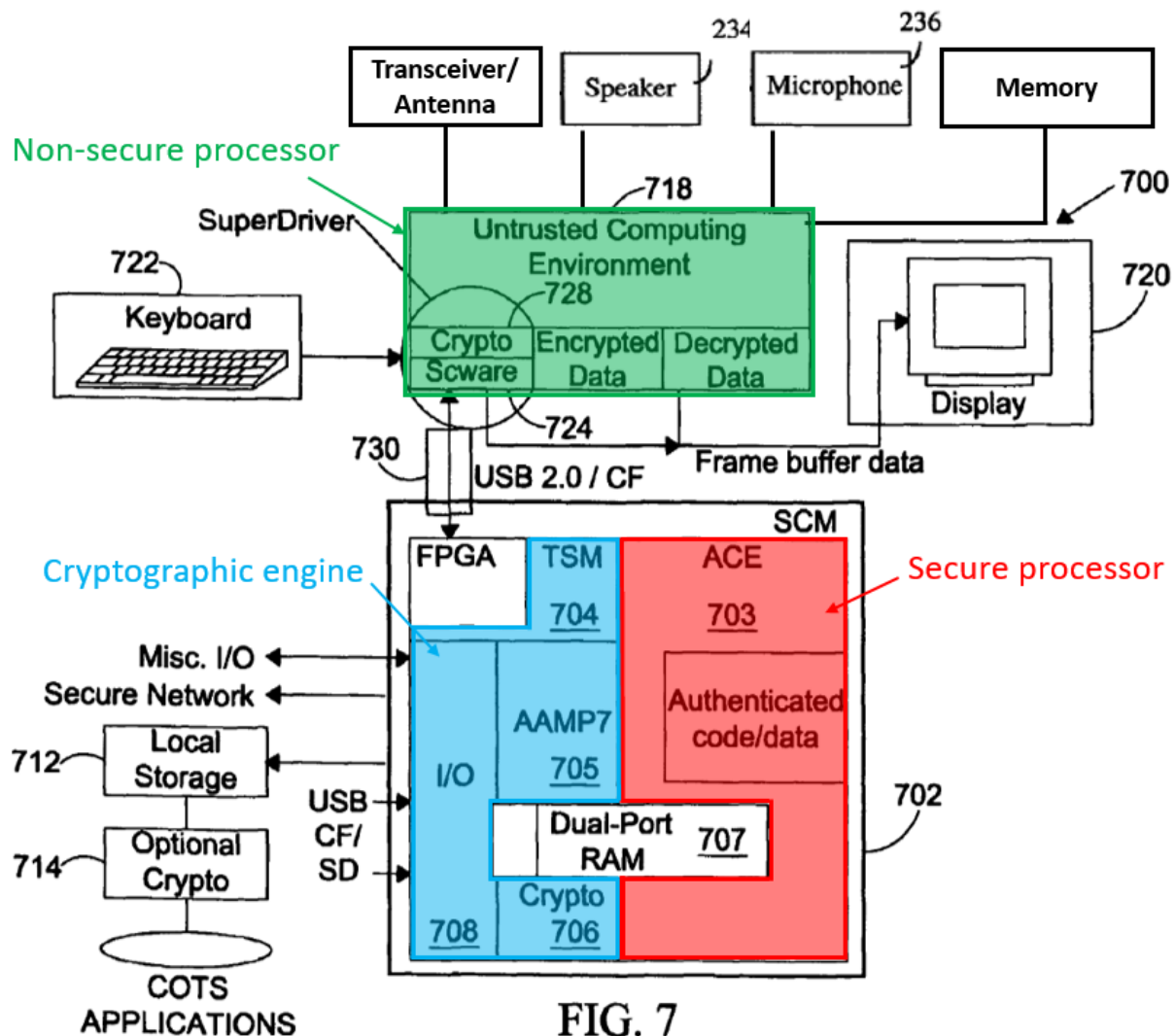


FIG. 7

Marek-Skarine Rendering

Also in the combination, **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 discussed in the following paragraphs.** APPLE-1003, ¶89.

In the cryptographic engine of the combination (*e.g.*, in Marek's TSM), Marek's trusted processor "provides ... partitioning" and "enforc[es] predetermined security policies," *e.g.*, such that "[e]ach I/O path ... [is] secured and authenticated." APPLE-1004, 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 and non-secure user processors) is "***secured and authenticated***" by Marek's TSM, *e.g.*, by the cryptographic engine of the combination. APPLE-1004, 9:52; *see* 10:35-39 ("I/O paths 730 between the untrusted host and the SCM 702 are managed by ... a dedicated TSM partition, allowing for any number of strict ***authentication protocols***"); APPLE-1003, ¶90.

Also in Marek's TSM, *e.g.*, in the cryptographic engine of the combination, Marek's cryptographic engine "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, 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***"). A cryptographic engine encrypts data. *See* APPLE-1016, [0008] ("a hardware based cryptographic engine for encrypting and/or decrypting data as it passes through the secure controller"); APPLE-1017, 8:23-26 ("an SMS

message cryptographic engine capable of encrypting/decrypting the SMS messages to be sent/received”); APPLE-1003, ¶¶91-92. A POSITA would have understood or at least found it obvious in light of the prior art 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, 9:40-52) by encrypting data communicated along those I/O paths. APPLE-1003, ¶93.

Because these I/O paths include I/O paths between the secure and non-secure user processors, as discussed *supra*, a POSITA would have understood or found obvious that the cryptographic engine of the combination (*e.g.*, Marek’s TSM) **is configured for encrypting any data communicated from the secure user processor to the non-secure user processor.** APPLE-1003, ¶94.

Alternatively or additionally, 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.** APPLE-1003, ¶95. For instance, 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, 9:48-52). APPLE-1003, ¶95. Indeed, a cryptographic engine generally capable of encrypting data performs the same function as a

cryptographic engine encrypting any data, with no unexpected results. *Id.*; *see In re Kuhle*, 526 F.2d 553, 555 (CCPA 1975) (use of claimed feature solves no stated problem and presents no unexpected result and “would be an obvious matter of design choice within the skill of the art”); *In re Chu*, 66 F.3d 292, 298-99 (Fed. Cir. 1995) (“design choice” is appropriate where the applicant fails to set forth any reasons why the differences between the claimed invention and the prior art would result in a different function).

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

In the combination, the cryptographic engine (*e.g.*, Marek’s TSM) includes **a trusted cryptographic processor**. Specifically, Marek’s TSM includes “***a trusted processor 705***” and “***a cryptographic engine 706***.” APPLE-1004, 9:31-41; *see* 10:12-14 (“the trusted processor 705 may include ***ROCKWELL COLLINS AAMP7™ microprocessor***”), 10:31-35 (“The cryptographic engine 706 of the SCM 702 may include ***ROCKWELL COLLINS Janus Crypto Engine***.”). 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**. APPLE-1003, ¶96.

Also in the combination, 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 discussed in the following paragraphs. APPLE-1003, ¶97.

First, a POSITA would have understood or found obvious that there is **an operating system executing on the cryptographic processor** (e.g., Marek’s trusted processor 705) given the functionality of Marek’s trusted processor. Marek’s trusted processor “provid[es] a brick-wall partitioning of memory, time, and device resources, and enforcing predetermined security policies.” APPLE-1004, 9:31-34; *see* 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—relating to controlling the operation and/or resources of the trusted processor—are functions that a POSITA would have understood to be provided by an operating system executing on the trusted processor 705. *See, e.g.*, APPLE-1009, 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, 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.”); APPLE-1020,

1:23-26 (“The operating system of a mobile device provides an application programming interface (API) that provides *access to data* ... and *a task manager for controlling application execution.*”); APPLE-1021, 13:35-37; APPLE-1003, ¶98.

Moreover, it was standard for mobile device processors to have operating systems. *See* APPLE-1005, [0038]; APPLE-1009, 1:64-2:3; APPLE-1010, 3:17-19; APPLE-1011, 4:59-61; APPLE-1018, 3:58-64; APPLE-1003, ¶99.

Thus, given the overlap between the functionality of Marek’s trusted processor 705 and the conventional functionality of an operating system, and given that mobile device processors were well-known to have operating systems, 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**. APPLE-1003, ¶100.

Alternatively or additionally, 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, 9:40-47. This is a function that a POSITA would have understood to be provided by an operating system executing 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”); 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”); APPLE-1003, ¶101.

Moreover, it was standard for mobile device processors to have operating systems, as discussed *supra*, and specifically for cryptographic engines in mobile devices to have operating systems. *See* APPLE-1006, 17:32-48 (“the cryptographic engine 220 comprises an operating system 605”); APPLE-1003, ¶102.

Thus, given the overlap between the functionality of Marek’s cryptographic engine 706 and the conventional functionality of an operating system, and given that cryptographic engines were well-known to have operating systems, 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**. APPLE-1003, ¶103.

A POSITA would have understood or found obvious that the processor and operating system of the combination's cryptographic engine are **trusted** at least because they are part of the "Secure COTS computing environment" provided by the SCM. APPLE-1004, 8:37-39; *see* 8:39-45, 1:66-2:4, 2:31-38, 11:60-65, Figs. 10-11; APPLE-1003, ¶104.

[1e]

In the combination, 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 (containing the secure processor; red in the figure *infra*) and the TSM (the cryptographic engine; blue). APPLE-1004, 9:63-66. Given that data is communicated between the secure processor and the cryptographic engine, a POSITA would have understood there to be **a first data communication link (purple) communicating data between the secure processor and the cryptographic engine**, *e.g.*, to enable the disclosed I/O between the ACE and the TSM to occur. *See* APPLE-1004, 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"); APPLE-1003, ¶105.

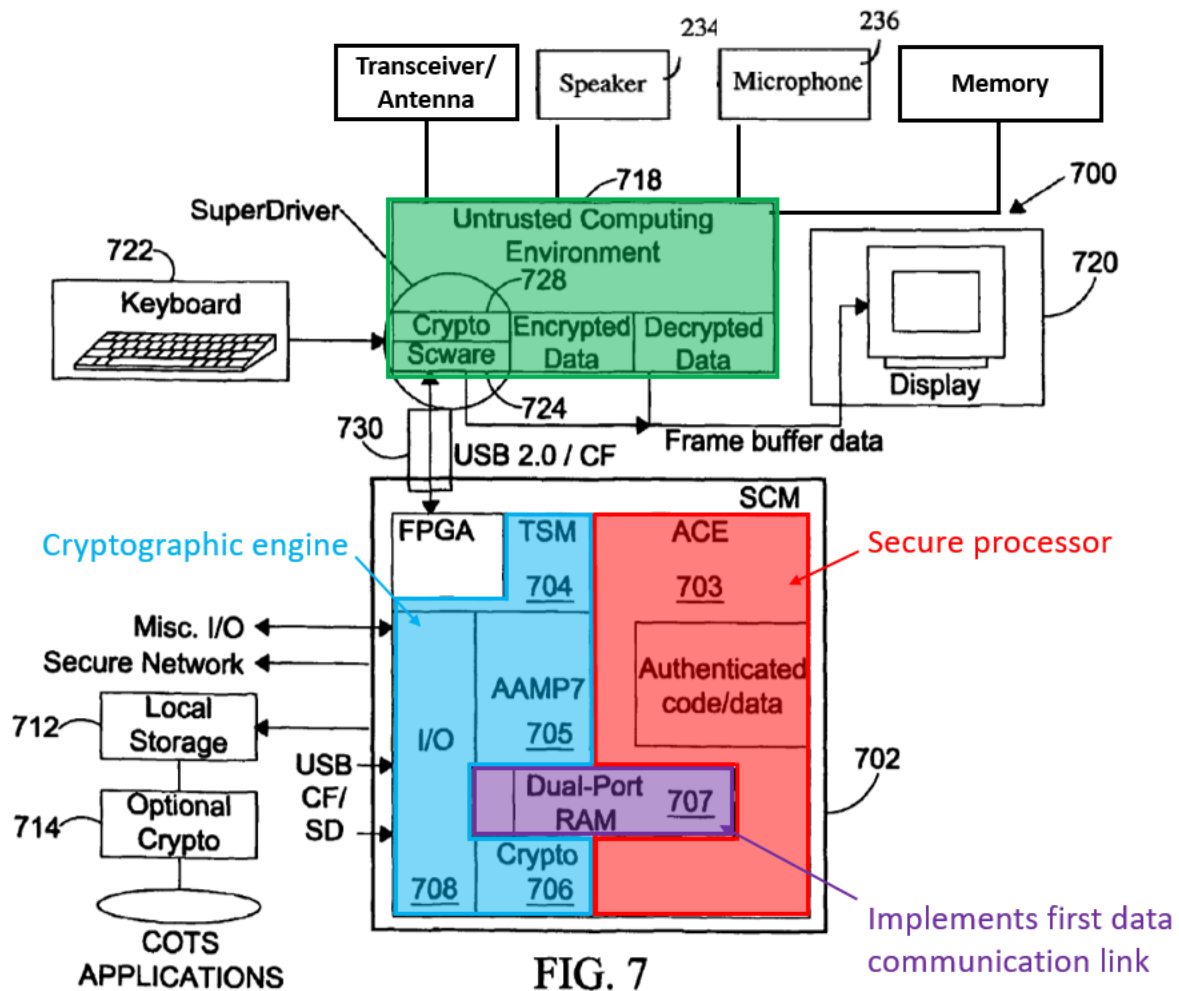


FIG. 7

Marek-Skarine Rendering

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, 9:66-67. These virtual I/O paths are a **first data communication link communicating data between the secure processor** (contained in the ACE) **and the cryptographic engine** (the TSM). APPLE-1003, ¶106. 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,” purple, “with each I/O path and a

memory-mapped resource being controlled by a dedicated TSM partition.”

APPLE-1004, 9:67-10:4. That is, in one implementation of the combination, **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.

APPLE-1003, ¶106.

[1f]

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, 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, 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, 9:48-64. These I/O paths 730, purple in the figure *infra*, are **a second data communication link communicating data between the non-secure processor and the cryptographic engine**. APPLE-1003, ¶107.

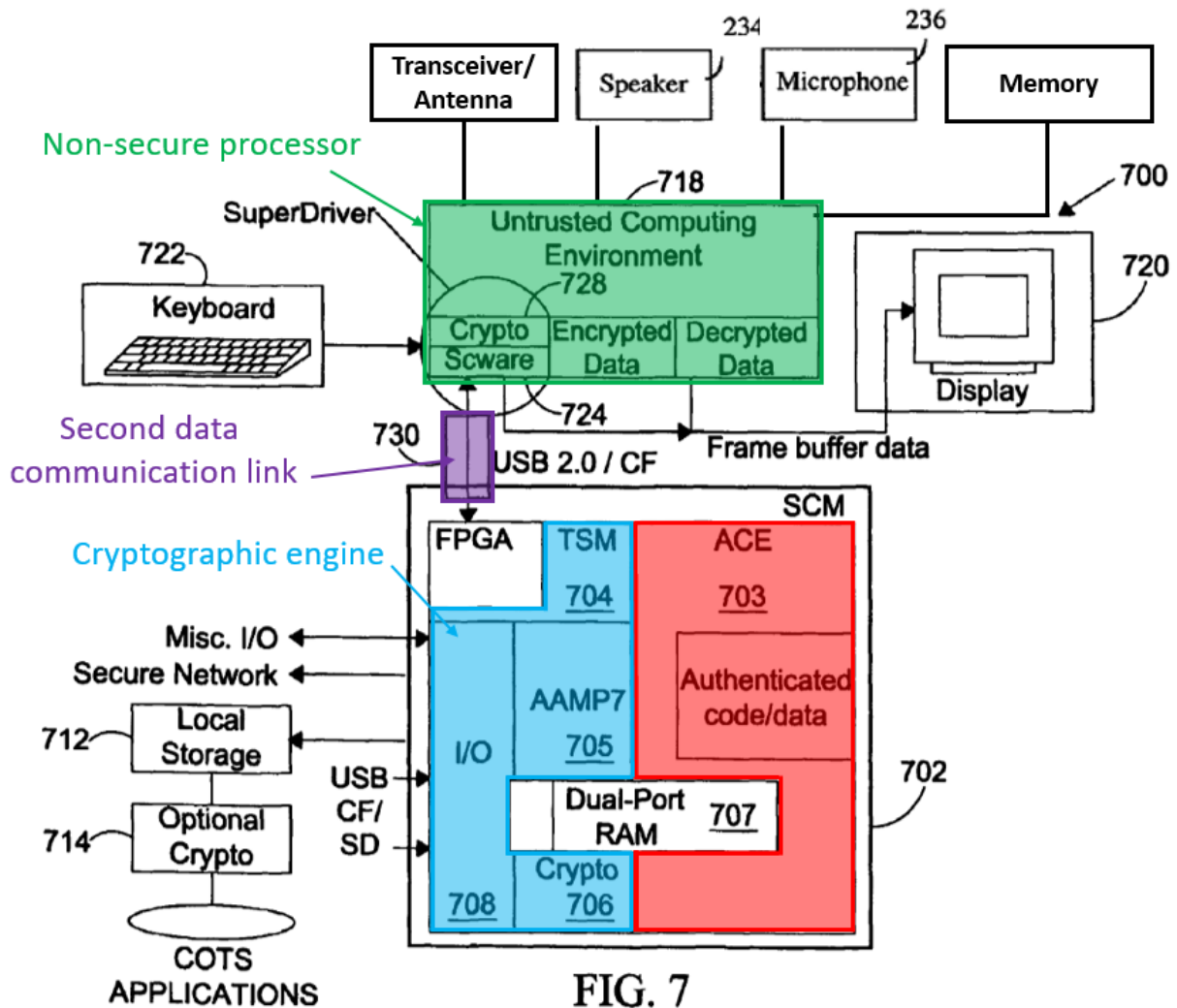


FIG. 7

Marek-Skarine Rendering

[1g]

Marek's untrusted host mobile device includes "*input and output devices* 722, 720," such as a keypad and display. APPLE-1004, 10:50-51. In the combination, these input and output devices, pink in the figure *infra*, are a **secure human/machine interface**, as discussed in the following paragraphs. APPLE-1003, ¶108.

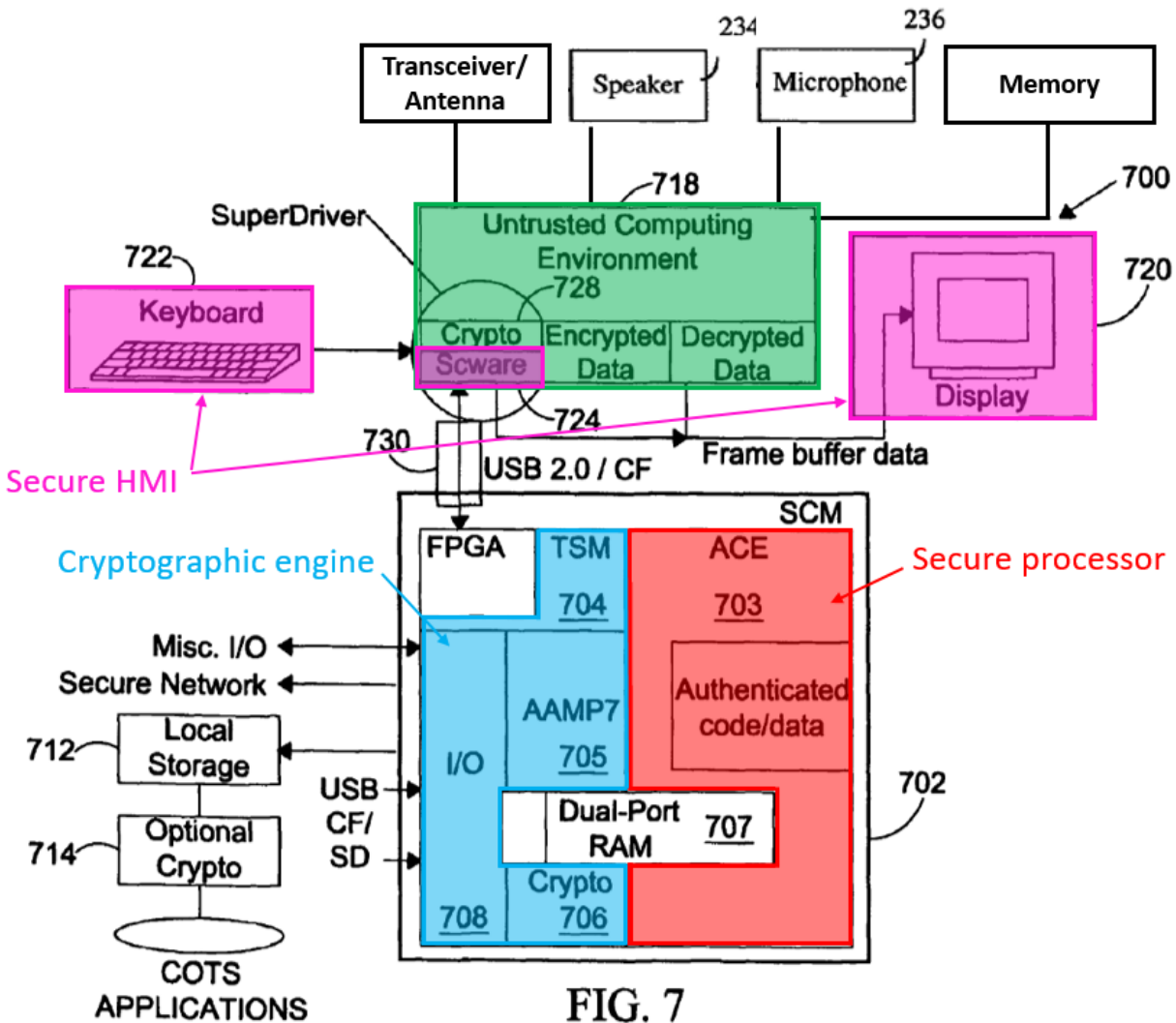


FIG. 7

Marek-Skarine Rendering

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. 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. When SCM is in operation, information input into input device 722 (*e.g.*, by a user) bypasses untrusted host and instead is provided to the SCM along secure I/O path 730; similarly, information from the SCM is provided to output device 720 (and thus to a user) via secure I/O path 730, again bypassing the untrusted host. APPLE-1003, ¶109.

In the combination, Marek’s input and output devices 722, 720 are **a secure human/machine interface** at least because they are an interface by which a user inputs information to and receives information from the SCM (via the input and output devices 720, 722, respectively). *See* APPLE-1004, 10:42-62, APPLE-1003, ¶110. 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* APPLE-1004, 10:42-62, APPLE-1003, ¶110.

In the combination, the secure human/machine interface enables bi-directional communication of information **between a user and the secure user processor**, *e.g.*, the processor of the ACE 703 (red in the figure *supra*), as discussed in the following paragraphs. APPLE-1003, ¶111.

First, Marek generally describes that the input and output devices 722, 720, *e.g.*, the secure human/machine interface, enables communication between a user and the SCM, which contains the ACE. *See* APPLE-1004, 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***”), 10:49-51, Figs. 7 and 8; APPLE-1003, ¶112.

Second, 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. APPLE-1003, ¶113. For instance, such communication would occur, *e.g.*, to enable a user to provide 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 output to a user. APPLE-1004, 9:13-14; APPLE-1003, ¶113. Additionally, 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, 9:50-51, 9:63-64; *see* 10:49-51; APPLE-1003, ¶113.

Moreover, a POSITA would have understood or found obvious that the communication of information enabled by the secure human/machine interface is **exclusively** between the user and the secure user processor. 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. Thus, at least because the functionality of the untrusted host device is disabled when the SCM is operational, 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. APPLE-1003, ¶114.

A POSITA would have understood or found obvious that the secure human/machine interface is **secure** at least because it is an interface to the “*Secure COTS computing environment*” provided by the SCM of the combination.

APPLE-1004, 8:37-39; *see* 8:39-45, 1:66-2:4, 2:13-20, 2:31-38; APPLE-1003, ¶115.

The secure human/machine interface enables communication of **classified information**⁹: the information is encrypted and communicated along “secured and authenticated” I/O paths. APPLE-1004, 9:50-52; *see* 9:37-44; APPLE-1003, ¶116. 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. APPLE-1004, 10:33-36. Information communicated between a user and the red domain (Marek’s SCM) can be **classified information**. APPLE-1003, ¶116.

⁹ In the co-pending litigation, Apple Inc. has argued that the term “classified” is indefinite. *See* APPLE-1034, 20-25. Because indefiniteness issues cannot be raised in an IPR proceeding, Petitioner addresses this term here and elsewhere in this Petition as best understood, and without conceding that the term is not indefinite.

[1h]

In the combination, the untrusted host mobile device 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; APPLE-1003, ¶117. *See* §IV.A.3. 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]; APPLE-1003, ¶118.

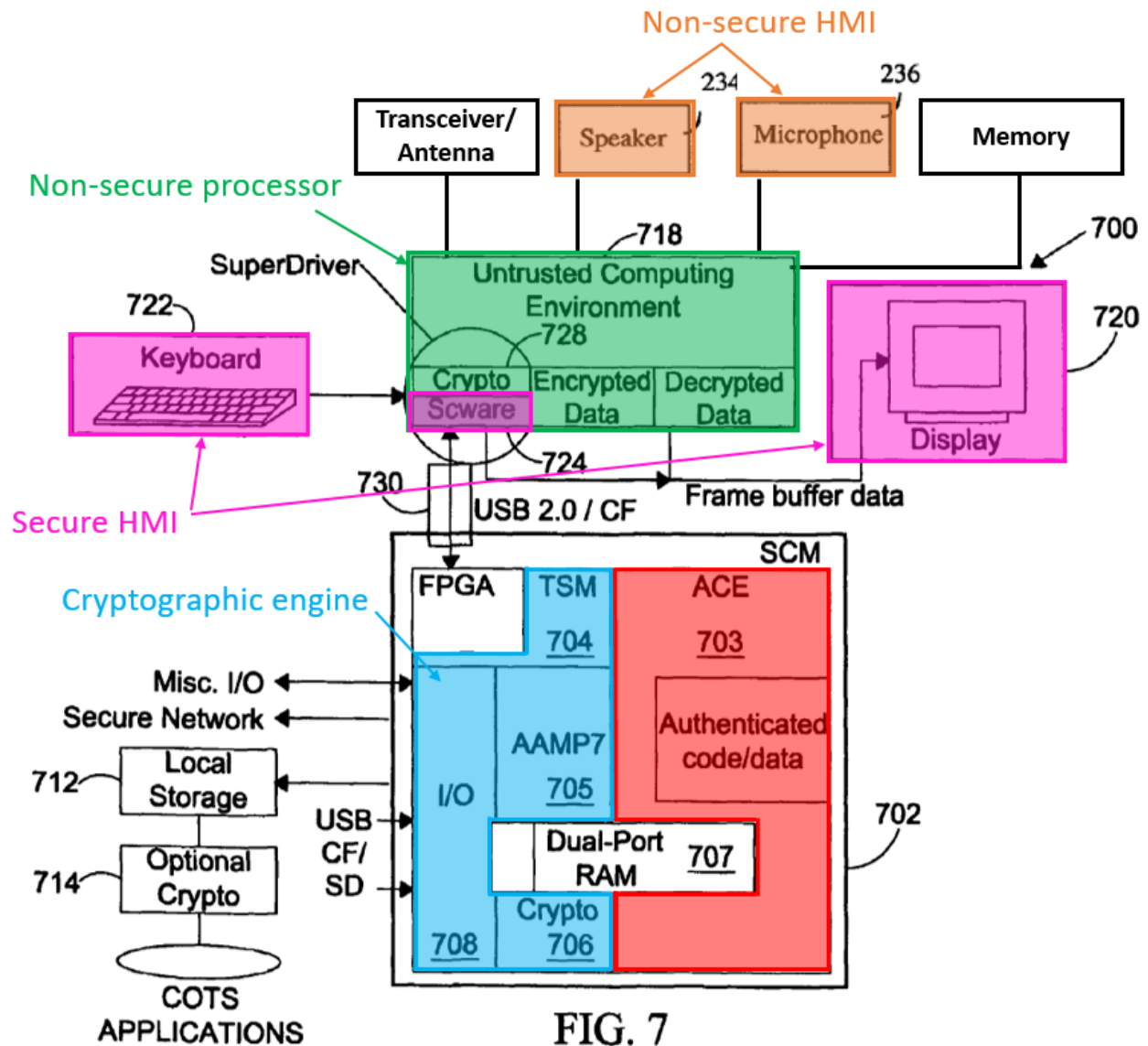


FIG. 7

Marek-Skarine Rendering

The non-secure human/machine interface is **distinct from the secure human/machine interface**: 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* [1g]), as illustrated *supra*. APPLE-1003, ¶119.

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 combination, based on 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, [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; APPLE-1003, ¶120. Also based on Skarine, signals from the speaker are communicated to a user, and audio input from a user are received by the microphone. *See* APPLE-1005, [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”); APPLE-1003, ¶120. 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, green).

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, 9:50-51. Based on Skarine, the microphone and speaker are connected to the non-secure user processor of the untrusted host mobile device; these connections do not go through 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**. APPLE-1003, ¶121.

A POSITA would have understood or found obvious that the non-secure human/machine interface is **non-secure** at least because it is part of “the untrusted host environment” of the combination. APPLE-1004, 8:40-41; *see* 8:56-59, 12:16-18, 2:1-4, 2:36-38, Figs. 10-11; APPLE-1003, ¶122.

The non-secure human/machine enables communication of **unclassified information**¹⁰ because the information communicated between the

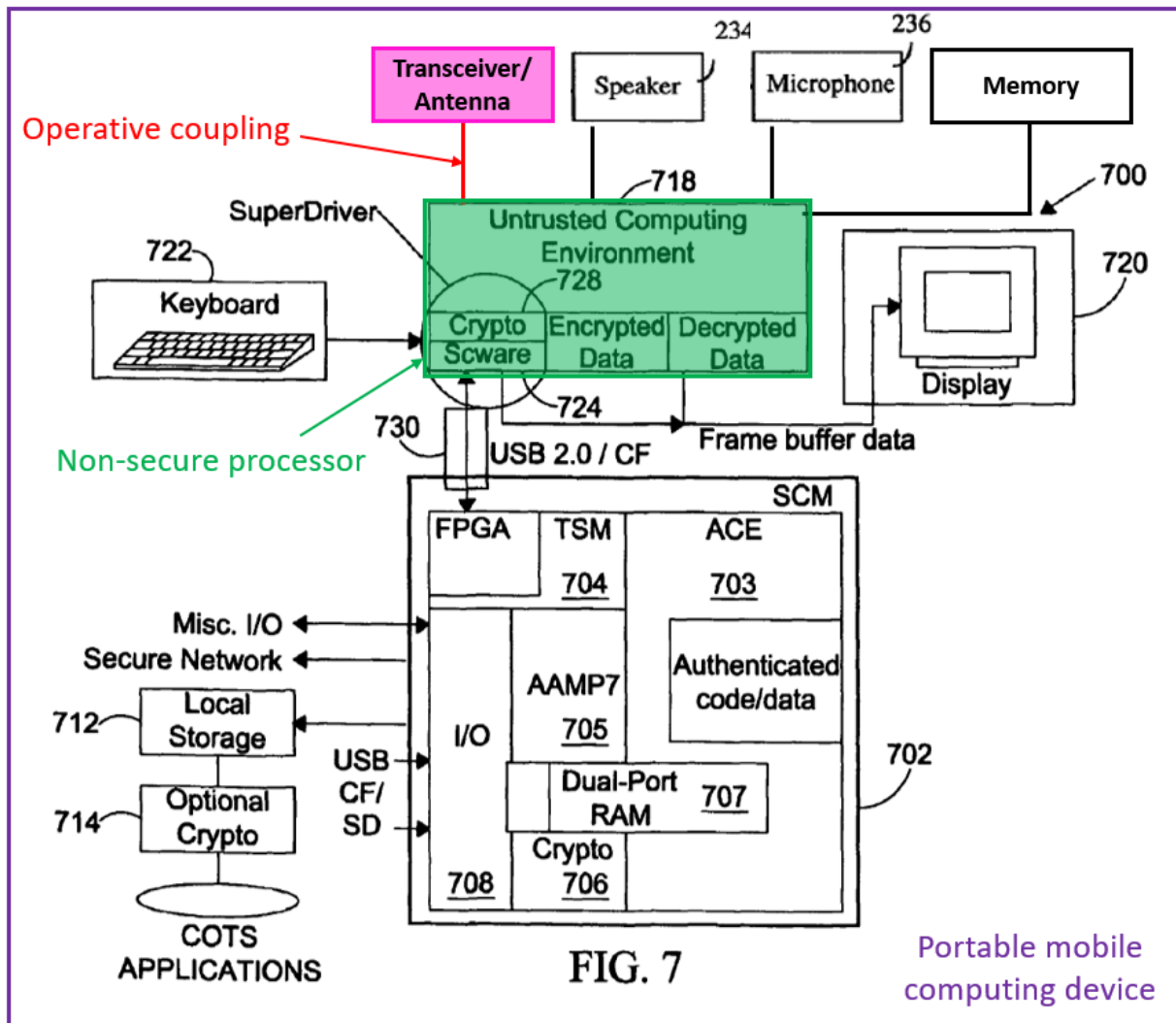
¹⁰ In the co-pending litigation, Apple has argued that the term “unclassified” is indefinite. *See* APPLE-1034, 20-25. Because indefiniteness issues cannot be

speaker/microphone and the non-secure user 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; APPLE-1003, ¶123. Furthermore, 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, 10:33-36, Figs. 10-11. 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**. APPLE-1003, ¶123.

[1i]

In the combination, **the communications transceiver is operatively coupled to the non-secure user processor** based on Skarine, as illustrated in the figure *infra*. *See* APPLE-1005, [0038], Fig. 2 (illustrating a mobile device in which the receiver and transmitter, *e.g.*, a communications transceiver, are coupled to the microprocessor); APPLE-1003, ¶124.

raised in an IPR proceeding, Petitioner addresses this term here and elsewhere in this Petition as best understood, and without conceding that the term is not indefinite.



Marek-Skarine Rendering

A POSITA would have understood or found obvious that the communications transceiver is configured for communicating data external to the portable mobile computing device, *e.g.*, given that this was a standard function of communications transceivers. *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 APPLE-1003, ¶125.

(ii) **Claim 2**

[2]

In the combination, the secure human/machine interface includes the input and output devices 722, 720 (*e.g.*, the keypad and display of the mobile device). *See* [1g]. The input device, *e.g.*, a keypad, is an **input device that allows the user to control the secure processor**. APPLE-1003, ¶126. Input received from a user through the input device is provided to the secure user processor. *See* APPLE-1004, 9:13-14, 9:50-64, 10:49-54, 11:39-41; *see* [1g]. Moreover, “COTS applications [and] manufacturer-supplied software” execute on Marek’s ACE, *e.g.*, on the secure user processor. APPLE-1004, 9:13-15; *see* 2:31-42, 12:18-19; *see* [1b]. 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**. APPLE-1003, ¶126.

(iii) **Claim 3**

[3]

In the combination, information output from the secure user processor is provided to the output device 722 of the secure human/machine interface, *e.g.*, the display (*see* [1g]), for presentation, thereby informing the user of that information. *See* APPLE-1004, 10:42-54. That is, the output device 720 of the secure human/machine interface is **an output device that allows the secure user processor to inform the user**. APPLE-1003, ¶127.

(iv) **Claim 4**

[4]

In the combination, the microphone of the non-secure human/machine interface (*see* [1h]) is **an input device that allows the user to control the non-secure user processor**. APPLE-1003, ¶128.

For instance, 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. 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, [0041]-[0042], Fig. 2. A user inputting an audio signal into the microphone controls Skarine's microprocessor:

the audio signal is received by the microprocessor, which in response provides that signal to the communication subsystem for transmission. APPLE-1003, ¶129. In the combination, based on Skarine, a user inputting an audio signal into the microphone causes the non-secure user processor of the untrusted host mobile device to provide that signal to the communications transceiver of the untrusted host mobile device, thus controlling the non-secure processor. APPLE-1003, ¶130.

Additionally or alternatively, the untrusted host mobile device of the combination includes “a voice message recording subsystem,” *e.g.*, as taught by Skarine. APPLE-1005, [0042]. A microphone is usable in the context of voice message recording, *e.g.*, to record a voicemail greeting, and the microprocessor of the mobile device facilitates capturing and storing data for the voicemail greeting. APPLE-1003, ¶131. Thus, the user controls the microprocessor of the mobile device: the processor coordinates data storage responsive to receiving user input via the microphone, *e.g.*, the user controls the microprocessor using the microphone. APPLE-1003, ¶131. In the combination, a POSITA would have recognized or found obvious that the use of the microphone to record a voicemail greeting thus is user control of the non-secure processor via the microphone. APPLE-1003, ¶131.

(v) **Claim 5**

[5]

In the combination, the speaker the non-secure human/machine interface (*see* [1h]) is **an output device that allows the non-secure user processor to inform the user**. For instance, a POSITA would have understood that audio signals are provided from the non-secure user processor to the speaker for output to the user, thereby allowing the non-secure user processor to inform the user, *e.g.*, as evidenced by Skarine. *See* APPLE-1005, [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]; APPLE-1010, 6:5-32; APPLE-1003, ¶132.

(vi) **Claim 6**

[6]

In the combination, the communications transceiver (*see* [1a]) is **a cellular telephone transceiver**, *e.g.*, based on Skarine. APPLE-1003, ¶133. 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, [0023]; *see* [0035]. 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, [0011], APPLE-1027, Abstract, [0026], [0034]); APPLE-1003, ¶133. In the combination, the communications transceiver is designed for operation in a cellular telephone network, *i.e.*, it is a cellular telephone transceiver.

A POSITA would have been motivated to implement the communications transceiver as a cellular telephone transceiver, *e.g.*, based on Skarine, for at least the following reasons. APPLE-1003, ¶¶134-137.

First, a POSITA would have been motivated to pursue this implementation 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. See APPLE-1005, [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”); APPLE-1003, ¶135. A POSITA would have recognized that providing such communication functionality is desirable: it enables the PDA to be used not only for self-contained computing, but also for two-way mobile communications. APPLE-1003, ¶135.

Second, a POSITA would have been prompted to pursue this implementation because doing so is merely the application of known techniques (*e.g.*, a cellular telephone transceiver) by a known system (*e.g.*, a wireless device)

to yield predictable results (*e.g.*, a wireless device with cellular network communication capability). APPLE-1003, ¶136; *see KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

A POSITA would have expected success in implementing the communications transceiver as a cellular telephone transceiver because Marek specifically indicates that its PDA is capable of wireless communications: “an untrusted host platform communicating with unsecured wireless and/or wired networks.” APPLE-1004, 11:58-59; *see* Fig. 9; APPLE-1003, ¶137. Moreover, a POSITA would have expected success because wireless communication components such as cellular telephone transceivers were standard components in mobile devices. *See* APPLE-1005, [0022]-[0023], [0027]-[0029], [0035], [0038], Figs. 1-2; APPLE-1011, 5:11-13; APPLE-1015, 3:11-17; APPLE-1017, 10:14-18; APPLE-1018, 6:33-45, 7:11-29; APPLE-1003, ¶137.

(vii) **Claim 7**

[7]¹¹

The combination includes a first file system for storing classified data

In the combination, Marek’s SCM includes “a local storage 712” (orange in the figure *infra*), *e.g.*, **a first file system**.¹² APPLE-1004, 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; APPLE-1003, ¶138. To the extent that “classified data” is interpreted to refer

¹¹ Petitioner notes the lack of antecedent basis for “The mobile PDA computer system” as recited in the preamble of claim 7. Because indefiniteness issues cannot be raised in an IPR proceeding, Petitioner addresses this term here as best understood, and without conceding that the term is not indefinite. *See* APPLE-1034, 25-27.

¹² Marek’s SCM is part of both the computer system of the combination (*see* [1pre]) and the portable mobile computing device of the combination (*see* [1a]). Thus, regardless of whether the phrase “The mobile PDA computer system” is interpreted as referring to the computer system or to the portable mobile computing device, that the SCM includes a first file system is sufficient to satisfy this feature.

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, 10:33-36; *see* [1g]; APPLE-1003, ¶138.

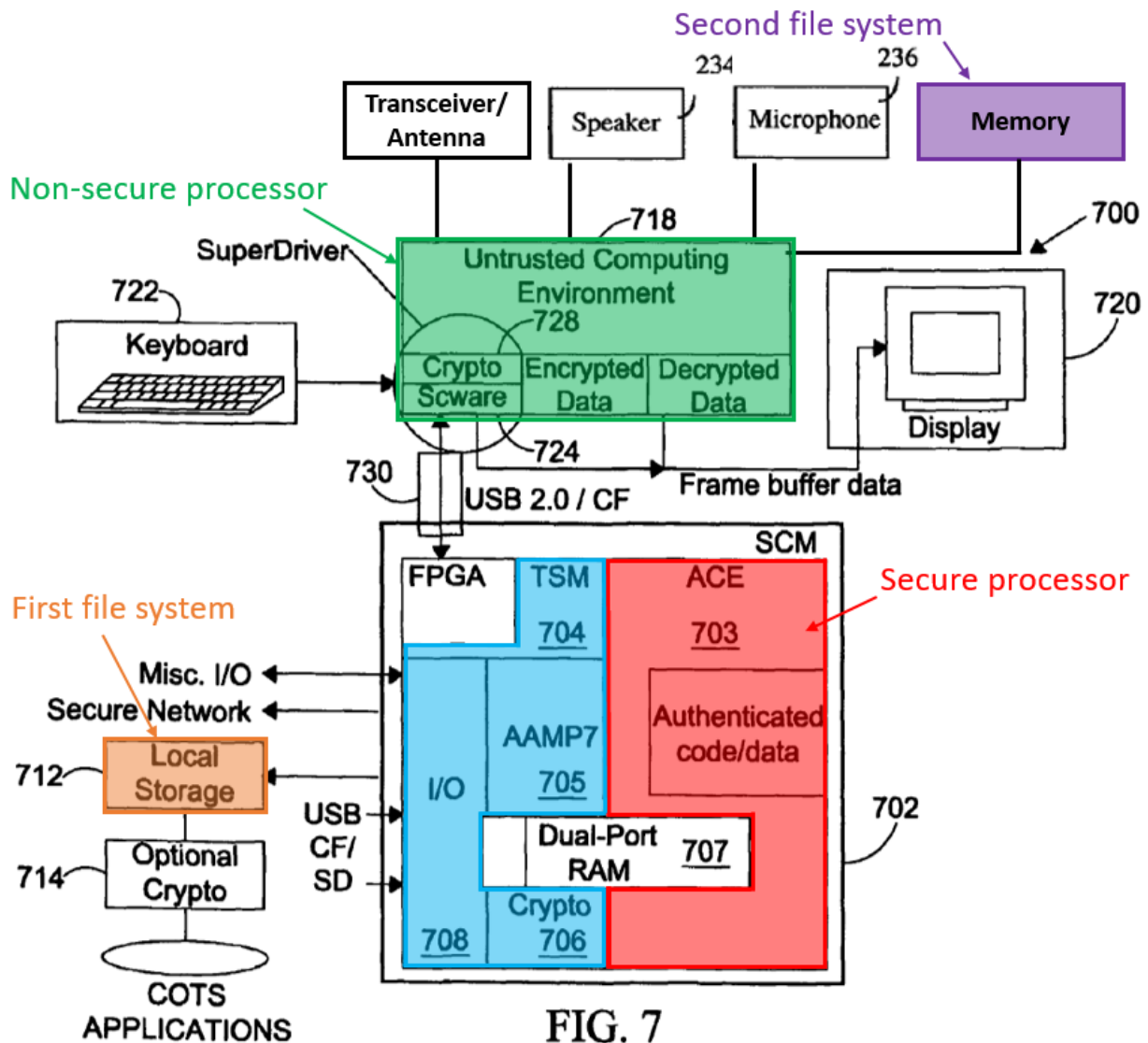


FIG. 7

Marek-Skarine Rendering

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. 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, 2:5-7; *see* 2:40-41. Moreover, Marek describes that the secure processor accesses the local storage: "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; APPLE-1003, ¶139.

The combination includes a second file system for storing unclassified data

As discussed in [1c], 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. A POSITA would have understood or at least found obvious that the untrusted host mobile device includes **a second file system**, *e.g.*, memory including non-volatile and volatile memory (purple), *e.g.*, for storage of the operating system, applications, and associated data, as was conventional and as evidenced by, *e.g.*, 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; APPLE-1003, ¶¶140-141.

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, [0038] (“Operating system software used by [the] microprocessor” of the untrusted host mobile device is “stored in a persistent store”), [0022]-[0023]; APPLE-1004, 7:54-55; APPLE-1010, 3:17-39; APPLE-1011, 4:54-59; APPLE-1018, 3:58-64; [1c]. Data stored in the untrusted host mobile device, such as the untrusted operating system software, is **unclassified**: it 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. APPLE-1004, 9:40-53; *see* 2:36-37 (“untrusted applications execute on the untrusted host environment”); APPLE-1003, ¶¶142-143. 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—can be **unclassified data**. *See* APPLE-1004, 10:33-36; [1g]; APPLE-1003, ¶143.

The second file system is **distinct from the first file system**, *e.g.*, the persistent storage of the untrusted host mobile device is distinct (*e.g.*, physically separate) from the local storage 712 in the SCM, as illustrated *supra*. APPLE-1003, ¶144. Because the first and second file systems are distinct, 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**. APPLE-1003, ¶144.

(viii) **Claim 9**

[9pre]-[9g]

See [1pre]-[1f], [1i] of Ground 1A.¹³

[9h]

The Marek-Skarine combination 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* [1g]. The secure human/machine interface (Marek's input and output devices 722, 720, *e.g.*, the mobile device's keypad and display) is **communicatively coupled** to the secure user processor (contained in the ACE): they are coupled such that there

¹³ Citations of this form incorporate by reference the text from the cited section.

is communication of information therebetween, *e.g.*, via Marek's TSM. *See* APPLE-1004, 9:13-14, 9:50-64, 10:49-54, 11:39-41; [1g]; APPLE-1003, ¶146.

Moreover, it was well-known that at least a portion of the keypad and display of a mobile device are located in a housing of the mobile device. *See* APPLE-1011, 5:28-6:7, 1:8-25, Figs. 3-4; APPLE-1003, ¶147. In the combination, the housing of the untrusted host mobile device is **a physically secure enclosure** that houses at least a portion of the keypad and the display (the secure human/machine interface; *see* [1g])—*e.g.*, **at least a portion of the secure human/machine interface is located in a physically secure enclosure.** APPLE-1003, ¶147.

[9i]

The Marek-Skarine combination 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* [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): they are coupled such that there is communication of information therebetween. *See* APPLE-1005, [0038], Fig. 2; [1h]; APPLE-1003, ¶148.

(ix) **Claim 10**

[10]

See [1i].

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

The sections below provide a brief introduction to Yoon and its combination with Marek and Skarine.¹⁴

**1. Yoon describes voice command functionality on
conventional mobile devices**

Yoon describes “a mobile communication terminal” “provided with a hands-free function capable of originating a call or receiving a call by a user’s voice command.” APPLE-1007, [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.”

¹⁴ Petitioner incorporates this discussion into Ground 1B.

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” and ultimately “originates a calling with the selected telephone number thus to perform a calling connection.”

Id., [0043]-[0047]; APPLE-1003, ¶225.

2. The combination of Marek, Skarine, and Yoon

In the Marek-Skarine-Yoon combination, the untrusted host mobile device implements voice command functionality based on Yoon. For instance, the non-secure microprocessor of the untrusted host mobile device 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. *See* APPLE-1007, [0032]-[0032], [0043]-[0047]; APPLE-1003, ¶226.

3. Reasons for the combination

A POSITA would have been motivated to implement the Marek-Skarine-Yoon combination for at least the following reasons. APPLE-1003, ¶¶227-232.

First, a POSITA would have been motivated to pursue this implementation because the hands-free calling functionality 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. APPLE-1003, ¶228. For instance,

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, [0005]; APPLE-1003, ¶228.

Second, a POSITA would have been prompted to pursue this implementation because doing so is merely the application of known techniques (*e.g.*, voice commands) by a known system (*e.g.*, the untrusted host mobile device of the combination) to yield predictable results (*e.g.*, a mobile device with voice command capabilities). APPLE-1003, ¶229; *see KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

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 that the relevant hardware components (*e.g.*, microphone and speakers) were included in the Marek-Skarine combination untrusted host mobile device. *See* [1h]; APPLE-1003, ¶230. Moreover, a POSITA would have expected to be successful given the widespread use of voice recognition and voice command technology in mobile devices. *See* APPLE-1040, Abstract; APPLE-1041, Abstract; APPLE-1042, Abstract; APPLE-1043, Abstract; APPLE-1003, ¶231. Furthermore, a POSITA would have expected success because Yoon, like Marek and Skarine, generally pertains to mobile devices. *See* APPLE-1004, 11:44-56, 12:31021, 13:49-51, 2:56-59, 7:53-57, 8:25-

38, Figs. 10 and 11; APPLE-1005, [0001]; APPLE-1007, Abstract; APPLE-1003, ¶232.

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

(i) Claim 4

[4]

In the combination, a user inputs a voice command via the microphone of the untrusted host mobile device, *e.g.*, via the non-secure human/machine interface, based on Yoon. *See* APPLE-1007, [0030]-[0032], [0043]-[0047]; APPLE-1003, ¶233. 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, [0032], [0043]-[0047]; APPLE-1003, ¶233. 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, *e.g.*, the microphone of the non-secure human/machine interface is **an input device to allow the user to control the non-secure user processor**. APPLE-1003, ¶233.

(ii) Claim 5

[5]

See [5] of Ground 1A.

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

The sections below provide a brief introduction to Moon and its combination with Marek and Skarine.¹⁵

**1. Moon describes configuring a conventional mobile device
for tamper-resistance**

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 compromised.” APPLE-1008, Abstract, 2:36-41. Moon’s electronic device “includes a zeroization circuit 302 [and] a monitor 304” (both in blue), “a plurality of sensors 306” (orange) and “storage sub-systems where sensitive information is stored or retained” (purple). *Id.*, 4:23-26; Fig. 3, *infra*. 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; APPLE-1003, ¶235.

¹⁵ Petitioner incorporates this discussion into Ground 1C.

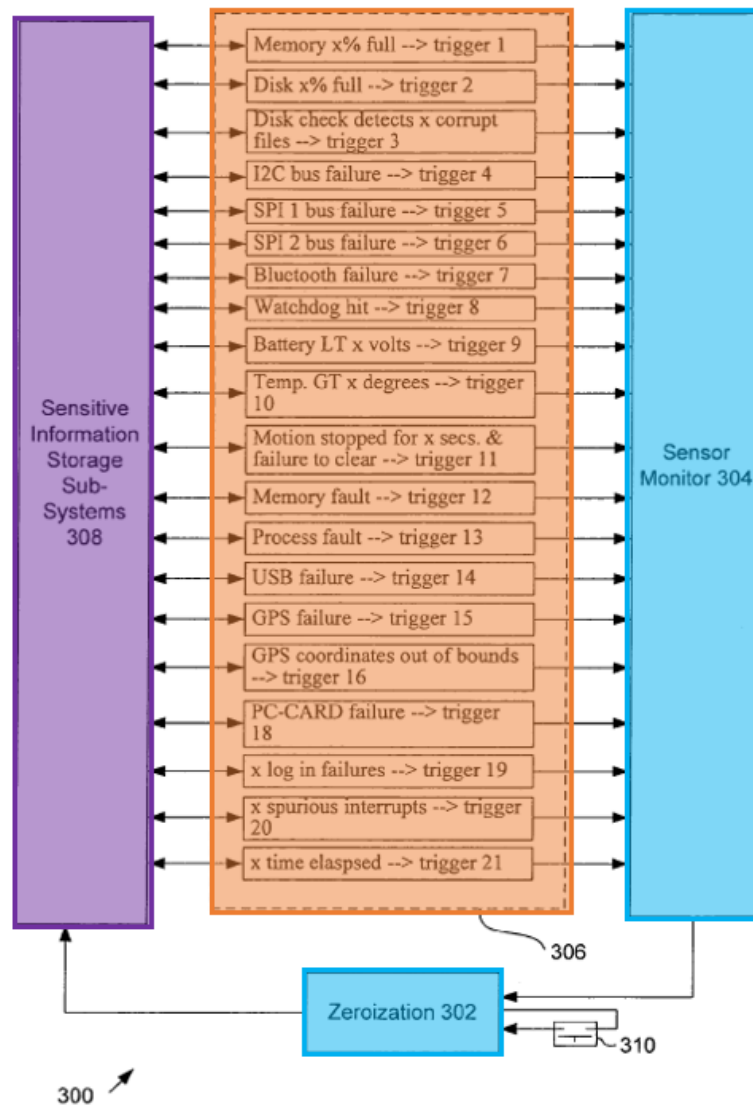


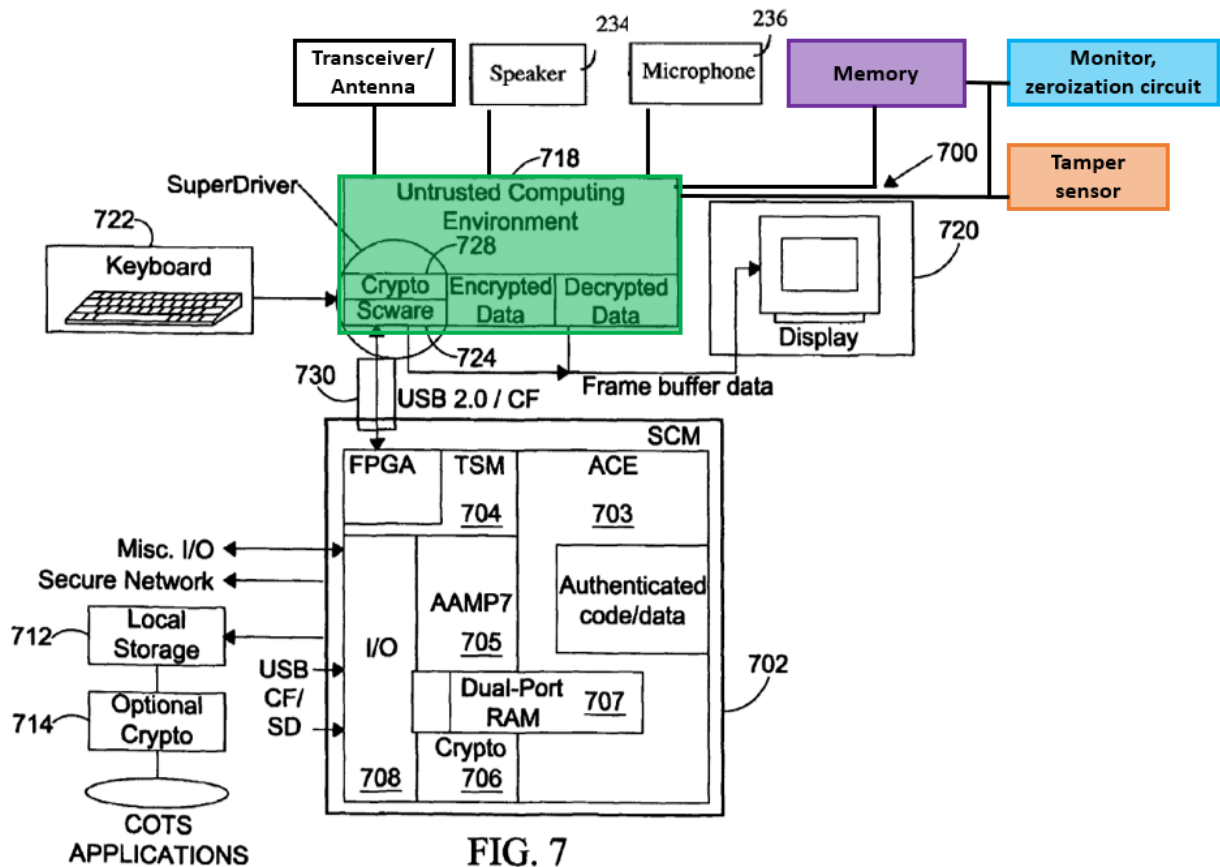
FIGURE 3

Moon, Fig. 3 (annotated)

2. The combination of Marek, Skarine, and Moon

In the Marek-Skarine-Moon combination, tamper detection and zeroization functionality, as described by Moon, is incorporated into the combination's untrusted host mobile device. APPLE-1003, ¶236. As illustrated *infra*, the combination's untrusted host mobile device includes a "[t]amper sensor" (orange)

integrated into its housing, and tamper detection and zeroization elements (blue) such as “a zeroization circuit” and “a monitor,” *e.g.*, based on Moon. APPLE-1008, 6:1, 4:23-26. The tamper sensor “monitors the enclosure” (*e.g.*, the housing) of the untrusted host mobile device. APPLE-1008, 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 (*see* [7]). *Id.*, 4:33-37; *see* 6:12-39; APPLE-1003, ¶236.



Marek-Skarine-Moon Rendering

3. Reasons for the combination

A POSITA would have been motivated to implement the Marek-Skarine-Moon combination for at least the following reasons. APPLE-1003, ¶¶237-242.

First, a POSITA would have been motivated to pursue this implementation because doing so would enhance security by “protect[ing] stored sensitive information from being wrongfully acquired,” consistent with Marek’s security-focused objectives. APPLE-1008, 1:10-12; *see* APPLE-1004, 1:5-37; APPLE-1003, ¶238.

Second, a POSITA would have been motivated to implement tamper detection and zeroization functionality based specifically on Moon 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, 1:57-62; APPLE-1003, ¶239. A POSITA would have recognized the advantages of this approach in terms of rapid response speed. *See* APPLE-1008, 1:48-57; APPLE-1003, ¶239. Moreover, a POSITA would have recognized that this approach advantageously allows for tamper detection and zeroization 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 security. APPLE-1008, 1:29-42; APPLE-1003, ¶239.

Third, a POSITA would have been prompted to incorporate tamper detection and zeroization sensors and circuitry into the mobile device of the combination because doing so is merely the application of known techniques (*e.g.*, tamper detection and zeroization) by a known system (*e.g.*, the untrusted host mobile device of the combination) to yield predictable results (*e.g.*, a mobile device with tamper detection and zeroization functionality). APPLE-1003, ¶240; *see KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

A POSITA would have expected to be successful in pursuing this implementation because zeroization is a well-known feature provided in “mission critical electronic devices.” APPLE-1008, 1:14-23; APPLE-1003, ¶241.

Furthermore, a POSITA would have expected success because Moon, like Marek and Skarine, generally pertains to mobile devices. *See* APPLE-1004, 11:44-56, 12:31021, 13:49-51, 2:56-59, 7:53-57, 8:25-38, Figs. 10 and 11; APPLE-1005, [0001]; APPLE-1008, 2:36-42; APPLE-1003, ¶242.

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

(i) Claim 9

[9pre]-[9g]

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

[9h]

The Marek-Skarine-Moon combination 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* [1g], [9h] of Ground 1A; APPLE-1003, ¶244.

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; *see* [1g]). *See* [9h] of Ground 1A. Moreover, in the Marek-Skarine-Moon combination, the housing incorporates a tamper sensor to “monitor,” the housing. APPLE-1008, 6:1-2; APPLE-1003, ¶245. If the tamper sensor detects a forced entry, storage locations in the untrusted host mobile device are zeroed out. *See* APPLE-1008, 6:1-39, 4:23-37. The housing of the untrusted host mobile device, including the tamper sensor, is **a physically secure enclosure**: it provides physical security by detecting physical tampering or intrusion into the housing. APPLE-1003, ¶245. Thus, **at least a portion of the secure human/machine interface is located in a physically secure enclosure.**

[9i]

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

(ii) **Claim 10**

[10]

See [9b].

V. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION

Institution is consistent with the Director’s recent guidance on applying the *Fintiv* Factors. *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential) (“*Fintiv I*”); *Memorandum: Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation* (June 21, 2022) (“*Director’s Memo*”). First and foremost, the merits of the Petition are “compelling,” and this “alone demonstrates that the PTAB should not discretionarily deny institution under *Fintiv*.” *Director’s Memo*, 3-5. Grounds 1A-1C present independent and distinct theories of obviousness, any of which, “if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.” *Id.*, 4. Regardless, even if the Board were to address the full *Fintiv* framework, a holistic analysis favors institution. *Fintiv I*, 6.

A. The *Fintiv* Factors Favor Institution—§314(a)

Under the Director’s interim guidance, *Fintiv* Factors favor institution. APPLE-1046 (“*Director’s Memo*”). The merits of the Petition are “compelling,” and this “alone demonstrates that the PTAB should not discretionarily deny

institution under *Fintiv*.” APPLE-1046, 3-5. The Ground presents independent and distinct theories of obviousness under both parties’ proposed constructions, either of which, “if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.” *Id.*, 4.

Regardless, even under the full *Fintiv* framework, a holistic analysis of the factors favors institution. *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11, 6 (PTAB Mar. 20, 2020) (precedential) (“*Fintiv I*”).

Factor 1 (possibility of a stay) is neutral because neither party in the Litigation has yet requested a stay. *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 15, p.12 (PTAB May 13, 2020) (“*Fintiv II*”) (declining to “infer” how the district court “would rule should a stay be requested”); *Sand Revolution II, LLC v. Cont’l Intermodal Group–Trucking LLC*, IPR2019-01393, Paper 24 at 7 (PTAB June 16, 2020).

Factor 2 (proximity of trial date to final written decision) favors institution. The Board’s projected Final Written Decision date is July 2024. In contrast, the district court case has recently been transferred from the WDTX to the Northern District of California (NDCA) and has no scheduled trial date. Applying the NDCA’s recent median time from filing to trial of approximately 31 months (APPLE-1036, 5), yields an estimated trial date in August 2024. The trial date could be delayed even further. APPLE-1046, 8. This uncertainty weighs in favor

of institution. And, even if it did not, “the proximity to trial should not alone outweigh” other relevant factors. *Id.*

Factor 3 (investment in parallel proceedings) favors institution. The Litigation is still in its early stages. Aside from exchanging preliminary infringement/invalidity contentions, several document productions, and claim construction briefs in WDTX prior to transfer, the parties have yet to expend significant resources in the Litigation. APPLE-1030. As noted above, the Litigation has been transferred to NDCA and discovery before that court has not yet begun. No claim construction proceedings have occurred in NDCA and no depositions have been taken. In contrast, Petitioner here worked diligently to overcome the challenging circumstances of the Litigation in filing this Petition. Patent Owner added the ’399 patent to the Litigation—alongside three other patents—in an amended complaint filed on March, 22, 2022. APPLE-1032. The PTAB has determined in similar circumstances that this factor does not weigh against institution where parallel litigation is in early stages and the petition is filed proximate to the statutory bar date. *See e.g., Intel Corp. v. PACT XPP Schweiz AG*, IPR2020-00540, Paper 11, 14-15 (PTAB September 10, 2020) (instituting IPR petition filed three days before bar date).

Factor 4 (overlap in issues) is neutral. Petitioner asks the Board to consider the unique challenges raised in the Petition. *See Fintiv I*, 12-13. If instituted,

Petitioner will not pursue in the Litigation invalidity challenges against the '399 Patent that are the same as the Grounds in this Petition, thereby mitigating the risk of duplicated effort and inconsistent decisions.

Factor 5 (overlap in parties) favors institution because Petitioner and Patent Owner are parties to the Litigation and because the Board's earlier projected Final Written Decision will bind Petitioner via the § 315(e)(2) estoppel before a jury trial, and thereby promote judicial efficiency.

Factor 6 (other circumstances, including the merits) favors institution. A determination that evidence "presented at the institution stage presents a compelling unpatentability challenge" favors institution. APPLE-1046, 2-5, 9. Compelling merits shows that it is "highly likely that the petitioner would prevail with respect to at least one challenged claim." *See Opensky Indus., LLC et al. v. VLSI Tech. LLC*, IPR2021-01064, Paper 107, 4-5 (PTAB October 14, 2022). As explained herein and supported by the expert declaration of Dr. Chatterjee, the strength of the Ground strongly favors institution. APPLE-1003, ¶¶1-253.

B. The *Advanced Bionics* Test Favors Institution—§ 325(d)

Marek, Skarine, Yoon, and Moon were not considered or cited in the prosecution of the '399 Patent, and consequently, each is being considered for the first time in this IPR proceeding. Thus, none of the Grounds involve the same or substantially the same prior art or arguments previously presented to the Office.

35 U.S.C. § 325(d).

VI. FEES

Petitioner authorizes the Patent and Trademark Office to charge Deposit Account No. 06-1050 for the fee set in 37 C.F.R. § 42.15(a) for this Petition.

VII. CONCLUSION

Petitioner requests cancellation of all Challenged Claims.

VIII. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1)

A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)

Apple Inc., is the real party-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

Petitioner is not aware of any disclaimers, reexamination certificates or petitions for *inter partes* review for the '399 Patent. The '399 Patent is the subject of the following civil action: *Speir Technologies Ltd. v. Apple Inc.*, Case 6:22-cv-00077-ADA (WDTX), filed on January 20, 2022 and *Speir Technologies Ltd. v. Apple Inc.*, 5:23-cv-00095 (NDCA), filed on January 9, 2023.

This Petition is being filed concurrently with another petition for IPR of the '399 Patent (IPR2023-00543).¹⁶

¹⁶ Pursuant to the Trial Practice Guide, both petitions for IPR of the '399 Patent are being filed with a paper providing a succinct explanation of the differences

C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Petitioner provides the following designation of counsel.

Lead Counsel	Backup Counsel
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email: IPR50095-0112IP1@fr.com	David Holt, Reg. No. 65,161 Gretchen A. DeVries, Reg. No. 72,505 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 IPR50095-0112IP1@fr.com

D. Service Information

Please address all correspondence and service to the address listed above.

Petitioner consents to electronic service by email at IPR50095-0112IP1@fr.com.

Respectfully submitted,

Dated: February 1, 2023

/David L. Holt/
W. Karl Renner, Reg. No. 41,265
David Holt, Reg. No. 65,161
Gretchen A. DeVries, Reg. No. 72,505
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

between the petitions, why the issues addressed by the differences are material, and why the Board should exercise its discretion to institute both petitions.

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 13,948 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated: February 1, 2023

/David L. Holt/
W. Karl Renner, Reg. No. 41,265
David Holt, Reg. No. 65,161
Gretchen A. DeVries, Reg. No. 72,505
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Counsel for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on February 1, 2023, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided, via Federal Express, to the Patent Owner by serving the correspondence address of record as follows:

L3Harris Technologies, Inc.
C/O FOX ROTHSCHILD, LLP
997 Lenox Drive, Building 3
Lawrenceville, NJ 08543-5231

/Crena Pacheco/
Crena Pacheco
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(617) 956-5938