

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner,

v.

SPEIR TECHNOLOGIES LTD.,

Patent Owner.

Case IPR2023-00542

Patent 7,765,399

PATENT OWNER'S RESPONSE TO THE PETITION

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I. Introduction	1
II. Overview	1
A. The '399 Patent.....	1
B. Claim Construction	3
C. Person of Ordinary Skill in the Art	4
D. Obviousness	4
E. Marek	5
III. The challenged claims are not obvious under grounds 1A, 1B, or 1C	8
A. The Marek-Skarine combination does not disclose or render obvious a secure human/machine interface configured for enabling (or to enable) bi-directional communication of classified information exclusively between a user and a secure user processor	8
1. Marek's Keyboard and Display Are Not Configured for Enabling Communication <u>Exclusively</u> between a User and a Secure User Processor	10
2. Petitioner has Failed to Demonstrate that Marek's Keyboard/Display Interface is <u>Secure</u>	17
B. Petitioner has not shown that at least a portion of the alleged secure human/machine interface is located in a physically secure enclosure.....	19

TABLE OF AUTHORITIES

Cases

<i>In re Magnum Oil Tools Int’l, Ltd.</i> , 829 F.3d 1364 (Fed. Cir. 2016)	5
<i>In re Nuvasive, Inc.</i> , 842 F.3d 1376 (Fed. Cir. 2016)	5
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007)	4
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	3
<i>Unigene Labs., Inc. v. Apotex, Inc.</i> , 655 F.3d 1352 (Fed. Cir. 2011)	5

Regulations

83 Fed. Reg. 51341 (Oct. 11, 2018)	3
--	---

TABLE OF EXHIBITS

Exhibit No.	Description
2001	Plaintiff Speir Technologies Ltd.'s Second Amended Preliminary Disclosure of Asserted Claims and Infringement Contentions to Defendant Apple Inc., <i>Speir Technologies Limited v. Apple Inc.</i> , No. 6:22-cv-00077-ADA (N.D. Cal. Dec. 7, 2022)
2002	Declaration of Anthony DeRosa in Support of Patent Owner's Response to the Petition
2003	October 27, 2023 Dr. Sandeep Chatterjee Deposition Transcript

I. INTRODUCTION

Petitioner has failed to show any of the challenged claims of U.S. Patent Number 7,765,399 is obvious. Petitioner's arguments are based largely on a reference with an inherently unsecure architecture that differs significantly from what is disclosed and claimed in the '399 patent. First, Petitioner's proposed combinations of references do not disclose or render obvious a secure human/machine interface configured to communicate data exclusively between a user and secure processor. Second, the Petition fails to show that the alleged "secure human/machine interface" is a secure interface. And third, Petitioner has not demonstrated that the alleged "secure human/machine interface" is at least partially enclosed in a secure enclosure or that doing so would have been obvious.

II. OVERVIEW

A. The '399 Patent

The '399 patent describes a computer architecture for a mobile device that combines the usability and low-cost benefits of a commercially available mobile device with advanced security measures that also allow the device to be used to transmit and store data requiring a higher level of security. The architecture disclosed in the '399 patent includes a

number of security features that allow secure communication and storage of sensitive data. For example, it includes a cryptographic processor that provides encryption/decryption as well as a data communication pathway between the secure side of the mobile device and the non-secure side of the device. EX1001, 2:57-3:3. The encryption scheme allows the device to communicate sensitive data using the transceiver circuitry of the non-secure processor. *Id.*, 2:41-56. In addition, the '399 patent describes a device having a secure human/machine interface (HMI) that allows classified information to be exchanged exclusively between the user the secure HMI. *Id.*, 7:40-8:13. The secure HMI provides a trusted path to applications executing on the secure processor, and it prevents invasive or unauthorized applications from monitoring user inputs and system outputs. *Id.*, 7:40-47. The device also includes a non-secure HMI suitable for exchanging unclassified information between user and the non-secure processor. *Id.*, 6:43-52.

The '399 patent describes several advantages of the disclosed architecture. Because it includes conventional hardware, operating system, and applications, it can be more familiar to its users and less expensive, offering the expected suite of features such as wired or

wireless communication services, cellular communication services, and so forth. *Id.*, 2:41-56. At the same time, because the device also includes capabilities to process, store, and transmit secure information without risk of that information being compromised by various types of attack, such as viruses, worms, Trojan horses, and others. EX1001, 1:52-55. The secure side of the disclosed device is built on trusted hardware that has been designed and developed using trusted techniques to ensure the integrity of the device and its resistance to penetration. *Id.*, 6:53-66.

B. Claim Construction

For purposes of *inter partes* review, disputed claim terms are construed to give them “the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention.” *See* 83 Fed. Reg. 51341 (Oct. 11, 2018) (adopting the standard of *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-13 (Fed. Cir. 2005)). The proper construction is considered in the context of, and must be consistent with, the specification—and the claim language should be read in light of the specification as it would be interpreted by one of ordinary skill in the art. *See, e.g., Phillips*, 415 F.3d at 1313. Petitioner has not proposed any claim terms for construction, and Patent Owner does

contend that any terms require construction to find that all grounds in Petitioner's challenge fail.

C. Person of Ordinary Skill in the Art

The field of technology for the '399 patent is secure mobile computing systems. A person of ordinary skill in the art of the subject matter of the '399 patent would have the equivalent of an undergraduate degree in electrical and computer engineering (or a related field) and approximately two years of work experience in the field of embedded systems. Additional education in the field could be substituted for industry experience, and vice versa.

D. Obviousness

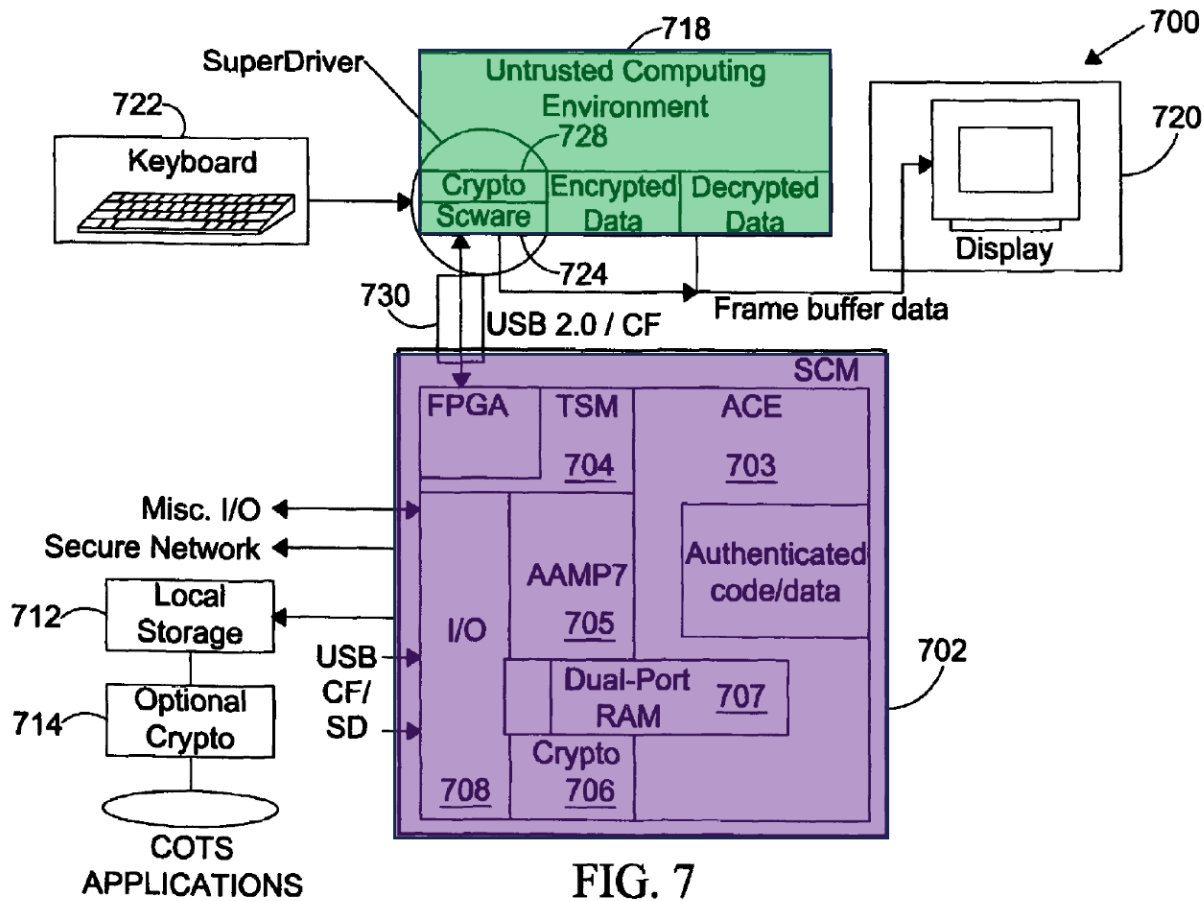
Whether a patent claiming a combination of prior art elements would have been obvious is determined by whether the improvement is more than the predictable use of prior art elements according to their established functions. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007). To reach this conclusion, however, requires more than a mere showing that the prior art includes separate references covering each separate limitation in a claim under examination. *Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1360 (Fed. Cir. 2011). Rather, obviousness

requires the additional showing that a person of ordinary skill at the time of the invention would have selected and combined those prior art elements in the normal course of research and development to yield the claimed invention. *Id.* “To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016); *see In re NuVasive, Inc.*, 842 F.3d at 1383 (stating that “conclusory statements” amount to an “insufficient articulation[] of motivation to combine”; “instead, the finding must be supported by a ‘reasoned explanation’”).

E. Marek

Each of Petitioner’s three ground relies primarily on a reference presented as Exhibit 1004 (“Marek”), which describes a system that combines an untrusted computing environment with an add-on module that Marek describes as a secure computing module (SCM). EX1004, 8:35-41. Marek describes that “the untrusted host environment may include commercial software environments and applications, having . . . no assurance of isolation between tasks.” Marek acknowledges that “most

COTS network components do not meet the level of security to meet information assurance requirements for the secure communication system including military-level applications.” EX1004, 1:20-24. Because Marek’s SCM is designed as an add-on module to a conventional non-secure device, the system utilizes user interface devices (e.g., a keyboard and display) of the untrusted host.



EX1004 (Marek), Fig. 7

For example, Figure 7 of Marek illustrates the SCM (purple) being connected via a USB 2.0/CF interface to an untrusted computing environment (green) whereby the SCM could utilize the keyboard and display of the untrusted computing environment. EX1004, 12:39-41. Marek describes that the SCM may utilize the input and output devices of the untrusted host (i.e., keyboard 722 and display 720) as virtual input and output devices for the secure module. EX1004, 2:42-55. This is achieved, according to Marek, by loading software called Scware 724 onto the untrusted host to create a data path to the SCM using input and output devices of the untrusted host. EX1004, 2:46-53. I/O paths 730 between the untrusted host and the SCM 702 are managed by a low power Field-Programmable Gate Array (FPGA) and a dedicated TSM partition. EX1004, 10:35-39.

Marek states that Scware 724 can implement several modes of operation. H-mode is described as offering a “higher level of security” and M-mode a “lower level of security.” EX1004, 10:55-57. In H-mode, “Scware 724 operates as a dedicated input/output device driver (e.g., keyboard/display driver).” *Id.*, 10:63-65. When H-mode is finished, the

Scware 724 software “zeroizes the appropriate memory regions of the host platform, including the output device’s frame buffer.” *Id.*, 11:7-9.

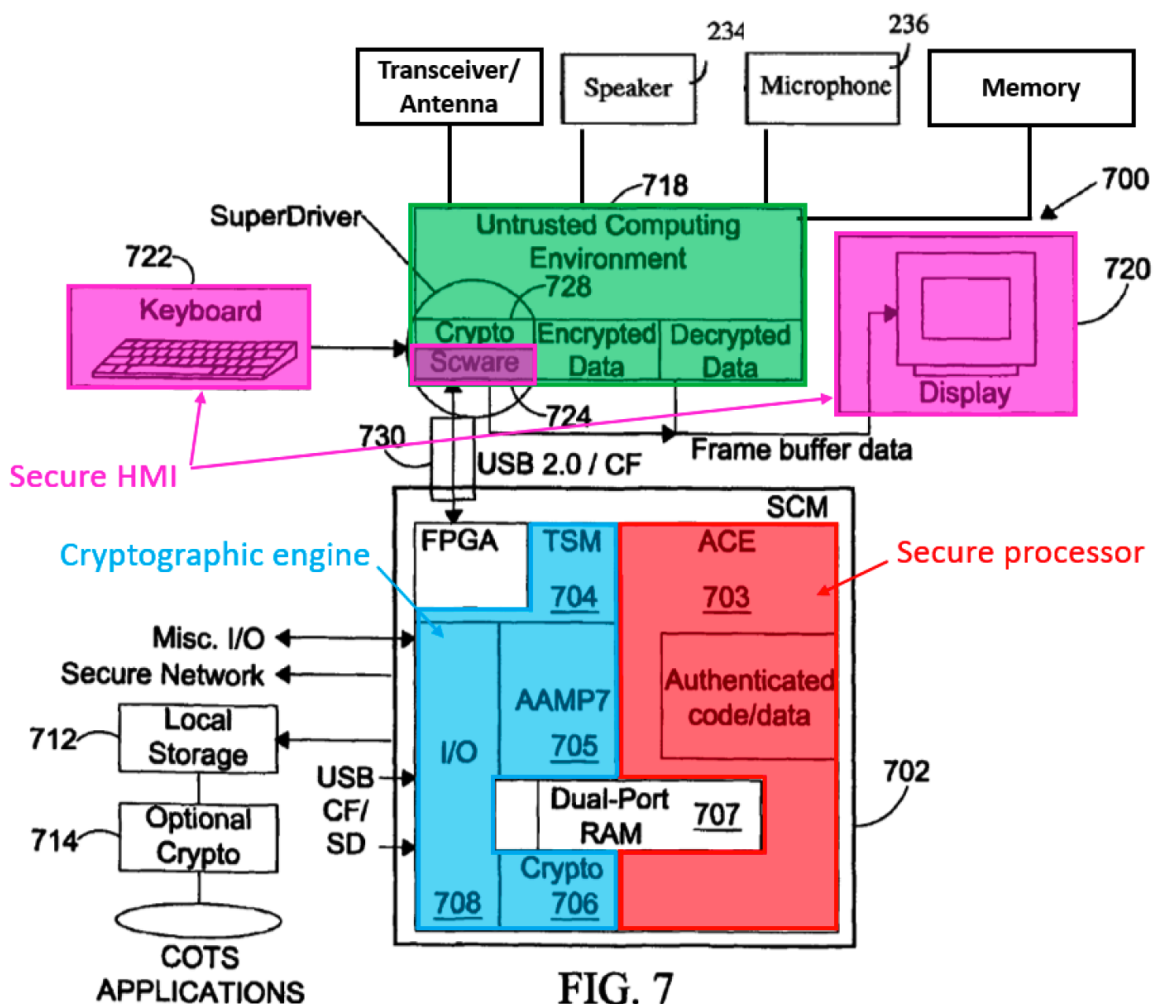
III. THE CHALLENGED CLAIMS ARE NOT OBVIOUS UNDER GROUNDS 1A, 1B, OR 1C

A. The Marek-Skarine combination does not disclose or render obvious a secure human/machine interface configured for enabling (or to enable) bi-directional communication of classified information exclusively between a user and a secure user processor

Every challenged claim requires a secure human/machine interface configured for enabling (or to enable) bi-directional communication of classified information exclusively between a user and a secure user processor. The Petition fails to show that any of the alleged prior art combinations disclose or render obvious a “secure human/machine interface configured for enabling [to enable] bi-directional communication of classified information exclusively between a user and said secure user processor” as recited in claims 1 and 9 of the ’399 patent. The alleged “secure human/machine interface” is neither secure nor is it configured to enable communication exclusively between a user and a secure user processor.

Petitioner alleges that input and output devices 722 and 720 are “a secure human/machine interface.” Pet. 51. These two elements are illustrated as keyboard (722) and display (720) in Petitioner’s rendering of the Marek-Skarine combination.¹

¹ Ground 1A is based on the Marek-Skarine combination, but Petitioner relies on the same arguments for Grounds 1B and 1C as to the “secure human/machine interface” limitation. *See* Pet. 78 (Ground 1B), 84 (Ground 1C). Accordingly, Petitioner’s arguments for those Grounds fail for the same reasons identified here.



Marek-Skarine Rendering

Pet., 52.

1. Marek's Keyboard and Display Are Not Configured for Enabling Communication Exclusively between a User and a Secure User Processor

Petitioner alleges that a POSITA would have understood or found obvious that the communication of information enabled by Marek's

keyboard 722 and display 720 (i.e., the alleged secure human/machine interface) is exclusively between the user and Marek's ACE 703 (i.e., the alleged secure user processor). Pet., 55, 73. Petitioner also says that "at least because the functionality of the untrusted host 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." *Id.* (citing EX1003, ¶114). This is incorrect. As explained below, the Marek system does not enable communication exclusively between the user and the alleged secure processor. Instead, Marek routes communications through the untrusted host first.

Petitioner has not shown any communication of information exclusively between Marek's keyboard 722 or display 720 and the ACE. EX2002, ¶¶64-66. Instead, user information that is entered onto the keyboard is first transferred to the untrusted host device (i.e., Untrusted Computing Environment 718) and then routed, using Scware, through I/O path 730, to the SCM. EX2002, ¶¶54-63.

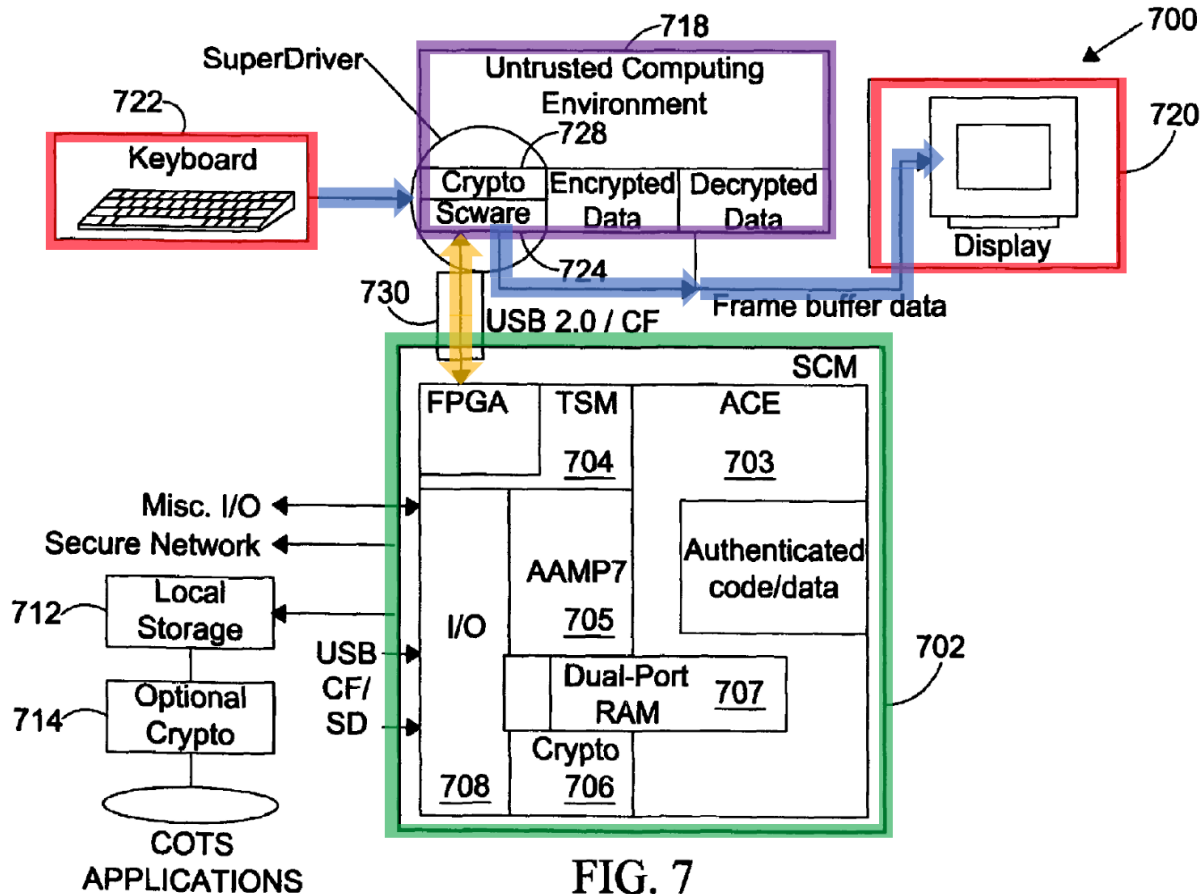


FIG. 7

EX1004, Fig. 7 (color annotations added). For example, user information entered on a keyboard is sent first to the untrusted host environment, and then software running on the untrusted host (i.e., Scware) transfers that user information over I/O lines 730 to the TSM. EX2002, ¶54, ¶57; EX2003, 66:17-24 (“So the keyboard stroke would – the electrical signal would be received by the – within the PDA, the host environment. The Scware would take that data, transfer it over the I/O lines 730, which would go to the TSM, and that’s essentially the flow that would happen.”).

Similarly, user information originating at, for example, SCM 702, proceeds first to the untrusted host and then display 720, as illustrated below.



Illustration of Information Flow in Marek

EX2002, ¶57. Petitioner ignores the actual path of user information in Marek and instead relies on Marek’s description of “H-mode.” Pet., 55. Petitioner argues that the “host OS is completely bypassed” in H-mode, and that therefore the communication between the user and the SCM must be “exclusive.” Pet., 53, 55. But the host OS is irrelevant here. The claims recite communication that is exclusively between the user and the secure user processor. The claims make no mention of whether the untrusted operating system is active, inactive, or in any other state.

Marek’s description of what happens after Scware has completed the transfer of information from keyboard to TSM (or from TSM to display) confirms that the user information is not communicated

exclusively between the user and the alleged secure processor, but instead is stored (at least temporarily) in memory regions within the untrusted host. EX2002, ¶56-58. Marek describes that “[w]hen H-mode is finished, the Scware 724 zeroizes the appropriate memory regions of the host platform, including the output device’s frame buffer.” EX1004, 11:7-12. In other words, Scware attempts to erase the memory regions of the untrusted host that were used during the information transfer process to temporarily store the user information on the untrusted host. EX2002, ¶56. As a POSITA would readily recognize, if user information weren’t stored in memory on the untrusted host environment, there would be no practical reason for zeroizing those memory regions after the data transfer is finished. *Id.* Even Petitioner’s expert acknowledged that it would be important to zeroize the appropriate memory regions of the host platform “so that there’s no remnants of Scware running or having been run when, for example, the operating system is rebooted.” EX2003, 78:12-17. Dr. Chatterjee also acknowledged that these “remnants” could include either the information that came from the keyboard or information that was sent to the display and are stored in a frame buffer. *Id.*, 78:18-79:5.

As Mr. DeRosa explains in detail, bypassing the host OS or disabling the functionality of the untrusted host does not mean that any data stored on memory locations within the untrusted host is safe from interception or attack. EX2002, ¶74. Indeed, such an architecture is vulnerable to attack and compromise of the non-secure processor, because the classified data coming from the user (via the keyboard) or being presented to the user (via the display) is not protected by encryption. *Id.* If malware is present on the untrusted computing environment, then the user information passing unencrypted through the untrusted host could be intercepted, even if Scware attempts to ensure that the host OS is bypassed. *Id.*

Marek's technique for routing communications through the untrusted host is markedly different from what the '399 patent describes. In the '399 patent, the untrusted host is not an intermediate recipient of classified information. Instead, classified information passes exclusively between the user and the secure user processor.

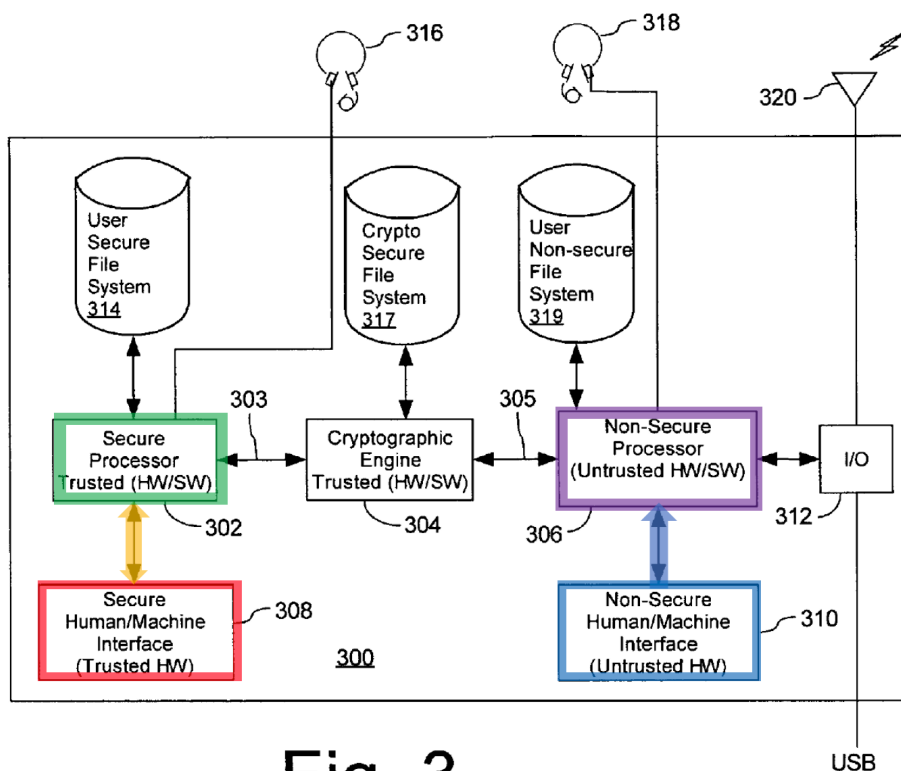


Fig. 3

Ex. 1001, Fig. 3 (annotated). As illustrated here, communication from the secure HMI (red) to the secure processor (green) is direct and does not pass through the untrusted hardware (purple).

Thus, Petitioner has failed to prove that the Marek-Skarine combination discloses communication of classified information exclusively between a user and a secure user processor. Petitioner also hasn't demonstrated why this limitation is obvious. Indeed, Petitioner provides no explanation as to any alternative techniques or configurations that would include exclusive communication between a

user and a secure user processor. Nor has Petitioner provided any basis to conclude that a POSITA would have been motivated to change the architecture disclosed in Marek or any reason that a POSITA would have expected such a change to be successful.

2. Petitioner has Failed to Demonstrate that Marek’s Keyboard/Display Interface is Secure

Petitioner alleges that a POSITA would have understood or found obvious that the identified interface (i.e., keyboard 722 and display 720) is secure “at least because it is an interface to the ‘Secure COTS computing environment’ provided by the SCM 702 of the combination” and because “they are an interface by which a user inputs information to and receives information from the SCM.” Pet. 53, 55-56. In other words, Petitioner appears to argue that the Marek’s keyboard and display are secure because they are an interface to the SCM, which is itself secure. This kind of inferential reasoning is not evidence, and Petitioner points to nothing in Marek showing that the alleged “secure human/machine interface” (i.e., Marek’s keyboard 722 and display 720) is itself secure.

Instead of providing evidence relevant to the identified interface, Petitioner merely identifies various statements in Marek that relate

generally to the security of the SCM (i.e., the secure side of the architecture), which is distinct from the keyboard and display on the unsecure side of the architecture. Pet., 56 (citing EX1004, 8:37-39, 8:39-45, 1:66-2:4, 2:13-20, 2:31-38). Petitioner's expert offers no further explanation, as his declaration merely parrot's the words of the Petition. EX1003, ¶115 ("This secure human/machine interface is secure (or at least a POSITA would have found this to be obvious) at least because it is an interface to the 'Secure COTS computing environment' provided by the SCM 702 of the combination.")

Petitioner has also failed to demonstrate that a secure human/machine interface would have been obvious in light of Marek's disclosure. Other than simply stating that a secure interface "would have been obvious," the Petition presents virtually no explanation as to *why* such an interface would have been obvious. Pet., 55-56. At best, Petitioner may have been attempting to argue that a secure human/machine interface would have been advantageous, since it served as an interface to a secure computing environment. But, even if this was Petitioner's intention, Petitioner cannot meet its burden of demonstrating that a claim is obvious simply by describing its potential

advantages. And Petitioner offers no explanation as to why a POSITA would have changed the architecture described in Marek, how the interface disclosed in Marek could have been made secure, whether a POSITA would have known how to make these changes to Marek's architecture, or whether a POSITA would have had a reasonable expectation of success in doing so.

In addition, as described above in Section III.A.1, Marek's architecture that relies on software running on the untrusted host to allegedly secure the data path from the user to the secure processor is inherently insecure. *See supra* Section III.A.1; *see* EX2002, ¶73.

B. Petitioner has not shown that at least a portion of the alleged secure human/machine interface is located in a physically secure enclosure

Claim 9 of the '399 patent recites, in part, "at least a portion of said secure human/machine interface located in a physically secure enclosure." For Ground 1A, the entirety of Petitioner's argument with respect to this limitation is presented in two sentences. Pet., 74 (first paragraph). In the first sentence, Petitioner says "[m]oreover, 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." Pet., 74 (citing EX1011,

5:28-6:7, 1:8-25, Figs. 3-4). Petitioner then alleges that “[i]n 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]).” *Id.* Petitioner’s argument is plainly insufficient. First, Petitioner provides no explanation of which element(s) of the “untrusted host mobile device” Petitioner alleges is a “housing” and cites to no portion of Marek to support its argument. Petitioner’s expert also provides no explanation as to what constitutes a “housing.” EX1003, ¶147. Because Petitioner has not identified any housing, Petitioner has not shown that at least a portion of Marek’s keyboard and display are within any such housing. Second, even if Petitioner had identified a housing in the Marek-Skarine combination and shown that the keyboard and display are within this housing, neither Petitioner nor its expert have offered any basis at all for Ground 1A to conclude that such a housing is a “physically secure enclosure.” Accordingly, Petitioner has failed to show that the Marek-Skarine combination relied on for Ground 1A discloses “at least a portion of said secure human/machine interface located in a physically secure enclosure” or renders claim 9 or 10 obvious.

Petitioner also challenges claim 9 under Ground 1C. There, Petitioner adds the Moon reference to the Marek-Skarine combination. Petitioner says “[i]n the Marek-Skarine-Moon combination, tamper detection and zeroization functionality, as described by Moon, is incorporated into the combination’s untrusted host mobile device,” which Petitioner illustrates as shown below.

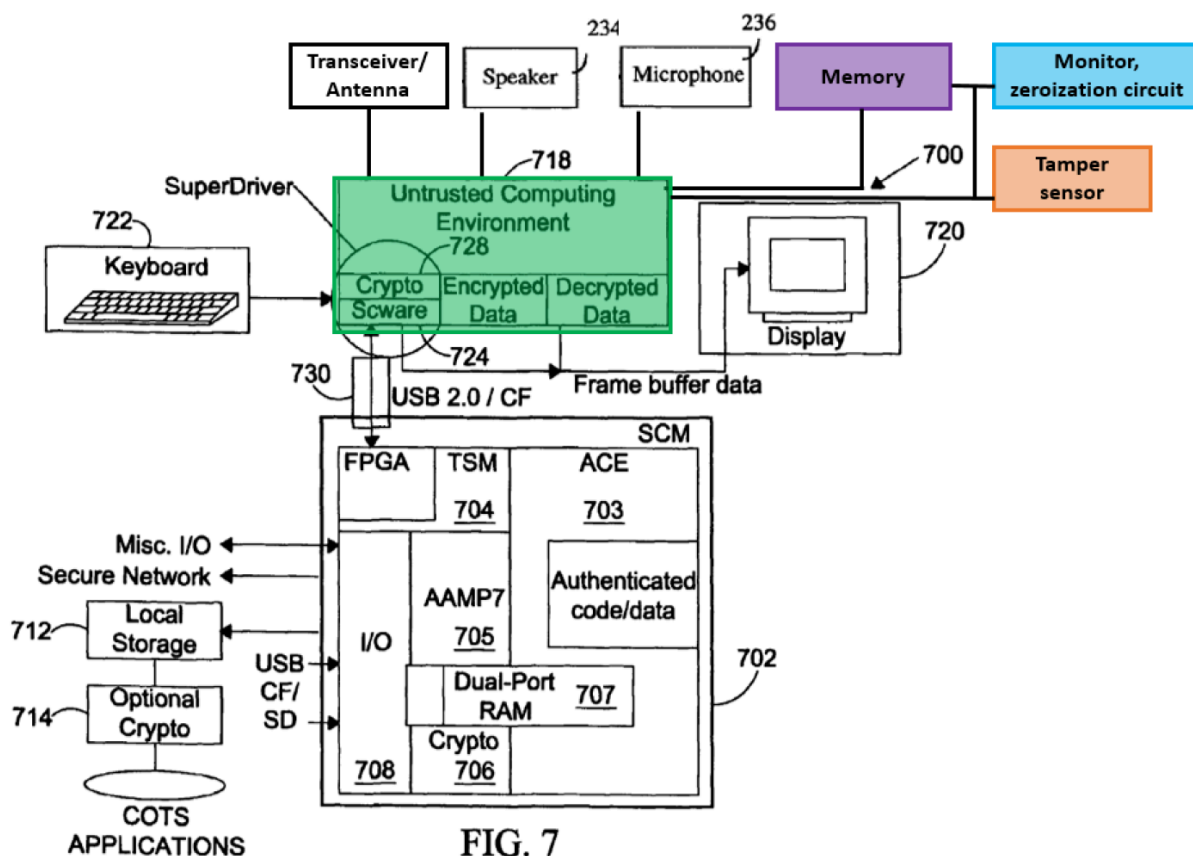


FIG. 7

Marek-Skarine-Moon Rendering

Pet., 80-81. Petitioner then repeats the unsupported assertion it made it Ground 1A, stating “[t]he 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.” Pet. 84. And, just as it did for Ground 1A, Petitioner provides no explanation as to which element(s) in this Marek-Skarine-Moon combination constitute a “housing” and, critically, no basis for its contention that any portion of Marek’s keyboard and display are within this undefined housing. *Id.* Had Petitioner provided any basis for this contention, Patent Owner could have substantively responded. But without it, Petitioner’s argument must fail because it has not satisfied its burden. Accordingly, Petitioner has not demonstrated that the Marek-Skarine-Moon combination, as proposed for Ground 1C, discloses “at least a portion of said secure human/machine interface located in a physically secure enclosure” or renders claim 9 or 10 obvious.

Date: November 14, 2023

Respectfully submitted,

/Brett Cooper/

Brett Cooper, Reg. No. 55,085

Lead counsel for Patent Owner

CERTIFICATION REGARDING WORD COUNT

Pursuant to 37 C.F.R. § 42.24(d), Patent Owner certifies that there are 3,357 words in the paper excluding the portions exempted under 37 C.F.R. § 42.24(a)(1).

Dated: November 14, 2023

/s/ Brett Cooper
Brett Cooper, Reg. No. 55,085
BC Law Group, P.C.
200 Madison Avenue, 24th Floor
New York, NY 10016
Phone: (212) 951-0100
bcooper@bc-lawgroup.com

CERTIFICATE OF SERVICE (37 C.F.R. § 42.6(e))

The undersigned hereby certifies that the above document was served on November 14, 2023, by filing this document through the Patent Trial and Appeal Case Tracking System as well as delivering a copy via electronic mail upon the following attorneys of record for the Petitioner:

W. Karl Renner, Reg. No. 41,265
renner@fr.com
David Holt, Reg. No. 65,161
dth@fr.com
Gretchen A. DeVries, Reg. No. 72,505
devries@fr.com
Fish & Richardson P.C.
3200 RBC Plaza
60 South Sixth Street
Minneapolis, MN 55402
Tel: 612-335-5070
Fax: 612-288-9696
Email: IPR50095-0112IP1@fr.com

Date: November 14, 2023

/Brett Cooper/

BC Law Group, P.C.
200 Madison Avenue, 24th Floor
New York, NY 10016
(212) 951-0100

Brett Cooper, Reg. No. 55,085
Attorney for Patent Owner