IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Scott MacDonald Ward
U.S. Patent No.:	10,992,480 Attorney Docket No.: 39843-0109PS1
Issue Date:	April 27, 2021
Appl. Serial No.:	16/597,773
Filing Date:	October 9, 2019
Title:	METHOD AND SYSTEM FOR PERFORMING A TRANSACTION AND FOR PERFORMING A VERIFICATION OF LEGITIMATE ACCESS TO, OR USE OF DIGITAL DATA

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 POST-GRANT REVIEW OF UNITED STATES PATENT NO. 10,992,480 PURSUANT TO 37 C.F.R. §42.200 *et seq.*

TABLE OF CONTENTS

EXHIBITS

SAMSUNG-1001 U.S. Patent No. 10,992,480 to Ward et al. ("the '480 Patent")

SAMSUNG-1002 Excerpts from the Prosecution History of the '480 Patent ("the Prosecution History")

SAMSUNG-1003 Declaration and Curriculum Vitae of Dr. Black

SAMSUNG-1004 Complaint, *Ward Participations B.V v. Samsung Electronics Co. Ltd. et al.*, 6:21-cv-00806, W.D. Tex., Aug. 4, 2021

SAMSUNG-1005 Stipulation by Petitioner

SAMSUNG-1006 U.S. Patent No. 7,082,615 ("Ellison")

SAMSUNG-1007 U.S. Patent No. 6,549,626 ("Al-Salqan")

SAMSUNG-1008 PCT Publication No. WO 01/93212 ("Muir")

SAMSUNG-1009 U.S. Patent No. 6,683,954 ("Searle")

SAMSUNG-1010 EP Patent Application Pub. No. EP 1465092 ("Shen")

SAMSUNG-1011 EP Patent Application Pub. No. EP 1240568 ("Ansell")

SAMSUNG-1012 U.S. Patent No. 11,063,766 ("the '766 Patent")

SAMSUNG-1013 PCT application PCT/NL2003/000436 (PCT Publication No. WO 2004/111751)

SAMSUNG-1014 PCT application PCT/NL2004/000422 (PCT Publication No. WO 2004/111752)

SAMSUNG-1015 Certified English Translation of the Hague Court Judgement, *DTS International B.V., v Samsung Electronics Benelux B.V.*, et al., C/09/577703 / HA ZA 19-793, May 13, 2020

SAMSUNG-1016 European Patent Office Preliminary Opinion for EP 1634140, May 25, 2020

SAMSUNG-1017 European Patent Office Preliminary Opinion for EP 3229099, May 27, 2020

SAMSUNG-1018 European Patent Office Decision to Revoke EP 1634140, September 14, 2021

SAMSUNG-1019 U.S. Patent No. 5,872,917 ("Hellman")

SAMSUNG-1020 U.S. Patent No. 7,801,775 ("Roseman")

SAMSUNG-1021 U.S. Patent No. 6,898,288 ("Chui")

SAMSUNG-1022 Excerpts from the Dictionary of Electrical & Computer Engineering, McGraw-Hill, 2004

SAMSUNG-1023 Stipulation for Extension of Time to respond to Complaint, *Ward Participations B.V v. Samsung Electronics Co. Ltd. et al.*, 6:21-cv-00806, W.D. Tex., Aug. 23, 2021

SAMSUNG-1024 [RESERVED]

SAMSUNG-1025 [RESERVED]

SAMSUNG-1026 [RESERVED]

SAMSUNG-1027 "2021 Discretionary Denials Have Passed 100, But Are Slowing," Dani Kass, Law360, July 15, 2021

SAMSUNG-1028 "Leahy And Cornyn Introduce Bipartisan Bill To Support American Innovation And Reduce Litigation", Sep. 29, 2021, available at: https://www.leahy.senate.gov/press/leahy-and-cornyn-introduce-bipartisan-bill-to-support-american-innovation-and-reduce-litigation

SAMSUNG-1029 Restoring the America Invents Act, S. 2891, 117th Cong. (2021).

LISTING OF CHALLENGED CLAIMS

Claim 1	
[1pre-1]	A method for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party,
[1pre-2]	the electronic device having an operating system creating a run-time environment for user applications, the method comprising:
[1a]	providing a private key in a memory of said electronic device, said memory being a secure part of a Basic In Out System or any other secure location in said electronic device, which private key is inaccessible to a user of said electronic device,
[1b]	wherein the private key is encrypted when the private key is stored in said memory,
[1c]	a decryption key for decrypting the private key being incorporated in the electronic device,
[1d]	said decryption key being inaccessible to said user, to any user-operated software and to said operating system,
[1e]	wherein said memory is inaccessible to said operating system of said electronic device, thereby rendering the private key inaccessible to said user,
[1f]	wherein the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software;
[1g]	providing authentication software in said electronic device,
[1h]	the private key being accessible to said authentication software,
[1i]	wherein authentication software is stored in said secure memory inaccessible to said operating system;

[1j]	activating the authentication software to generate a digital signature from the private key,
[1k]	wherein the authentication software is run in a secure processing environment inaccessible to said operating system;
[1l]	providing the digital signature to the second transaction party.
Claim 2	
[2]	The method according to claim 1, wherein the private key is provided by the second transaction party, which stores the private key together with data identifying the first transaction party.
Claim 3	
[3]	The method according to claim 1, wherein the authentication software has its own unique serial number, software ID or encryption key.
Claim 4	
[4]	The method according to claim 1, wherein the private key is encrypted by the second transaction party using an encryption key before the private key is provided to the first transaction party.
Claim 5	
[5]	The method according to claim 4, wherein the authentication software retrieves a decryption key associated with the encryption key and decrypts the private key at its first use.
Claim 6	
[6]	The method according to claim 1, wherein the authentication software is installed in an application environment in the secure area such that it may obtain the private key without passing through an unsecured part of said electronic device.

Claim 7	
[7]	The method according to claim 1, wherein the private key is encrypted using at least two encryption layers.
Claim 8	
[8]	The method according to claim 1, wherein the private key is encrypted using an encryption key which is associated with a hardware device serial number.
Claim 9	
[9]	The method according to claim 1, wherein the private key is encrypted using an encryption key which is associated with a user identifying number, in particular a personal identifying number, PIN, or a number or a template associated with a fingerprint of the user.
Claim 10	
[10]	The method according to claim 1, wherein the decryption key is associated with one or more serial numbers of hardware components of said electronic device.
Claim 11	
[11]	The method according to claim 1, wherein the private key is decrypted by the authentication software.
Claim 12	
[12]	The method according to claim 1, wherein the private key is decrypted by an application stored in the electronic device using a device specific encryption key.
Claim 13	
[13]	The method according to claim 1, wherein the private key is decrypted using a decryption key associated with any identifying characteristic, in particular a serial number, a personal identification number, PIN, or a fingerprint of a user.

Claim 14	
[14]	The method according to claim 1, further comprising identifying the user of the electronic device before activating the authentication software.
Claim 15	
[15]	The method according to claim 1, wherein the authentication software has an encryption key for encrypting digital data.
Claim 16	
[16pre]	An electronic device comprising
[16a]	a network interface configured for an electronic transaction between a first transaction party, and a second transaction party, wherein the electronic device is operated by the first transaction party;
[16b]	a processor configured for an operating system creating a run-time environment for user applications;
[16c]	a memory storing a private key, said memory being a secure part of a Basic In Out System or any other secure location in said electronic device, which private key is inaccessible to a user of the electronic device,
[16d]	wherein the private key is encrypted when the private key is stored in said memory,
[16e]	a decryption key for decrypting the private key being incorporated in the electronic device, said decryption key being inaccessible to said user, to any user-operated software and to said operating system;
[16f]	wherein said memory is inaccessible to said operating system of said electronic device, thereby rendering the private key inaccessible to said user,
[16g]	wherein the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software; and

[16h]	a memory storing authentication software, the private key being accessible to said authentication software, wherein the authentication software is stored in secure memory location inaccessible to said operating system;
[16i]	wherein the processor is configured for activating the authentication software to generate a digital signature from the private key,
[16j]	wherein the authentication software is run in a secure processing environment inaccessible to said operating system, for providing the digital signature to the second transaction party.
Claim 17	
[17pre-1]	Method for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party,
[17pre-2]	the electronic device having an operating system creating a run-time environment for user applications, the method comprising:
[17a]	providing a private key in a memory of said electronic device, wherein the private key is encrypted,
[17b]	when the private key is stored in said memory, a decryption key for decrypting the private key being incorporated in the electronic device, said decryption key being inaccessible to said user, to any user-operated software and to said operating system,
[17c]	wherein the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software;
[17d]	providing authentication software in said electronic device, the private key being accessible to said authentication software;
[17e]	activating the authentication software to generate a digital signature from the private key, wherein the authentication software is run in a secure processing environment inaccessible to said operating system;
[17f]	providing the digital signature to the second transaction party.

Claim 18	
[18pre]	An electronic device comprising:
[18a]	a network interface configured for an electronic transaction between a first transaction party, and a second transaction party, wherein the electronic device is operated by the first transaction party;
[18b]	a processor configured for an operating system creating a run-time environment for user applications;
[18c]	a memory storing a private key, wherein the private key is encrypted, when the private key is stored in said memory,
[18d]	a decryption key for decrypting the private key being incorporated in the electronic device said decryption key being inaccessible to said user, to any user-operated software, and to said operating system,
[18e]	wherein the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software; and
[18f]	a memory storing authentication software, the private key being accessible to said authentication software;
[18g]	wherein the processor is configured for activating the authentication software to generate a digital signature from the private key, wherein the authentication software is run in a secure processing environment inaccessible to said operating system, for providing the digital signature to the second transaction party.
Claim 19	
[19]	The electronic device according to claim 18, wherein the electronic device is a personal computer, a cellular phone, a hand-held personal digital assistant with wireless communication capabilities, or a device containing a BIOS.

Samsung Electronics Co., Ltd. ("**Petitioner**" or "**Samsung**") petitions for Post-Grant Review ("PGR") of claims 1-19 ("**the Challenged Claims**") of U.S. Patent No. 10,992,480 ("**the '480 Patent**"). For the reasons explained below, the challenged '480 patent claims are unpatentable.

I. REQUIREMENTS FOR PGR

A. Grounds for Standing and PGR Eligibility

To the extent that the priority claim of the '480 Patent is not valid, Petitioner certifies that the '480 Patent is available for PGR.[1] Petitioner is also submitting an IPR petition (IPR2022-00113, *see* Section VII.B) challenging the '480 Patent claims, and requests institution of both petitions for the reasons explained in Petitioner's Ranking Paper. Petitioner is not barred or estopped from requesting review. Petitioner was first served with a complaint of infringement of the '480 Patent less than one year prior to the filing of this Petition. SAMSUNG-1004.

"A petition for a post-grant review may only be filed not later than the date

[1] The priority date of the '480 Patent is at issue in Petitioner's invalidity challenges to the '480 Patent. *See* Petitioner's Ranking Paper at 1-5. PGR eligibility hinges on the validity of this priority claim. If the '480 Patent is not entitled to its priority claim to application no. 10/560,579, the '480 Patent is available for PGR.

that is 9 months after the date of the grant of the patent." 35 U.S.C. § 321(c); 37 C.F.R. § 42.202(a). The '480 patent was issued on April 27, 2021, which is less than nine months prior to the filing date of this Petition. Therefore, the '480 patent is eligible for PGR.

The '480 Patent purports to be a transition application because it was filed after March 16, 2013 and claims priority to applications filed before March 16, 2013. In particular, the '480 Patent issued from US Patent Application No. 16/597,773, filed on October 9, 2019, which claims priority from and is a continuation of U.S. Patent Application No. 10/560,579, filed on June 14, 2004, which further claims priority from Dutch Application PCT/NL03/00436, filed on June 13, 2003.

The Board has previously held that a transition application is eligible for PGR when it contains at least one claim that did not have written-description or enablement support in an application filed before March 16, 2013. *See, e.g., Arkema Inc. v. Honeywell Int'l Inc.*, PGR2016-00011, Paper 54 at 22 (Aug. 31, 2017); *US Endodontics, LLC v. Gold Standard Instruments, LLC*, PGR2015-00019, Paper 54 at 11-12 (Dec. 28, 2016); *Intex Recreation Corp. v. Team Worldwide Corp.*, PGR2019-00015, Paper 41 at 65, 71 (Apr. 29, 2020). Specifically, PGR provisions apply only to a patent that contains at least one claim with an effective filing date on or after March 16, 2013. *See* Leahy-Smith America

Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284 (2011), §§3(n)(1), 6(f)(2)(A). An application is not entitled to the priority date of an earlier application, if the earlier application does not disclose the claimed invention "in the manner provided by section 112(a) (other than the requirement to disclose the best mode)." *Id*., §§ 119(e), 120. If a later-filed application is unable to claim priority to an earlier application, then its effective filing date is the actual filing date of the later-filed application. *Id*., § 100(i)(1)(A). Here, and as explained in more detail in Section III below, at least one claim of the '480 Patent does not have written-description support in an application filed before March 16, 2013. The '480 Patent therefore is not entitled to claim priority to an earlier application and has an effective filing date of Oct. 9, 2019 (its actual filing date), thereby making the '480 Patent PGR eligible.

B. Challenge and Relief Requested

Petitioner requests PGR of the Challenged Claims for lacking written description support and on the obviousness grounds noted below. Dr. Black provides supporting explanations in his Declaration cited throughout this petition. SAMSUNG-1003, ¶¶[1]-[199].

Ground	Claims	Invalidity Basis
A1	**1-19**	35 U.S.C. § 112(a)
B1	**1, 3, 6, 11, and 14-19**	35 U.S.C. § 103: Ellison in view of Muir

Ground	Claims	Invalidity Basis
B2	**7, 9, 13**	35 U.S.C. § 103: Ellison in view of Muir and Al-Salqan
B3	**8, 10, 12**	35 U.S.C. § 103: Ellison in view of Muir and Searle

As shown below, each reference predates the effective filing date (Oct. 9, 2019) of the '480 Patent and qualifies as prior art under post-AIA 35 U.S.C. §§ 102(a)(1) and 102(a)(2). Even if the earliest possible priority date of June 13, 2003 is used for any claim, these references remain prior art under post-AIA 35 U.S.C. §§ 102(a)(1) and 102(a)(2) and additionally qualify as prior art under pre-AIA 35 U.S.C. §§ 102(b)/102(e).

Reference	Filing Date	Publication Date	Prior Art Under
Ellison (USPN 7,082,615)	Sept. 22, 2000	Jul. 25, 2006	102(a)(1) 102(a)(2) 102(e)
Muir (PCT Pub. No. WO 01/93212)	May 30, 2001	Dec. 6, 2001	102(a)(1) 102(b)
Al-Salqan (USPN 6,549,626)	Oct. 20, 1997	Apr. 15, 2003	102(a)(1) 102(a)(2) 102(e)
Searle	Oct. 23, 1999	Jan. 27, 2004	102(a)(1)

Reference	Filing Date	Publication Date	Prior Art Under
(USPN 6,683,954)			102(a)(2) 102(e)

C. Claim Construction

No formal claim constructions are necessary because "claim terms need only be construed to the extent necessary to resolve the controversy." *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011).

D. Level of Ordinary Skill in the Art

A person of ordinary skill in the art at the time of the '480 Patent (a "POSITA") would have had a Bachelor's degree in an academic discipline emphasizing the design of electrical, computer, or software technologies, in combination with at least two years of related work experience with software security technologies, such as cryptography or encryption/decryption systems, or in the development of hardware and software for carrying out secure electronic transactions. Alternatively, the person could also hold a Masters or Doctor of Philosophy degree in a relevant academic discipline with less than a year of related work experience in the same discipline. SAMSUNG-1003, ¶¶[15]-[16].

II. THE '480 PATENT

A. Brief Description

Digital data is regularly exchanged to perform various transactions, e.g., financial transactions, in which the need to verify the identity of each party can be important. SAMSUNG-1001, 1:1-35. PINs and passwords known to one of the parties can be used, but sending this information over digital networks can be a security risk. SAMSUNG-1001, 1:19-35. Methods involving the use of a third party transaction server have been developed to enhance security. However, these methods may undesirably require providing additional hardware, such as tokens and token readers. SAMSUNG-1001, 1:36-52. The '480 Patent proposes a solution to this problem without requiring additional hardware. SAMSUNG-1001, 1:52-56; SAMSUNG-1003, ¶[36].

The '480 Patent is directed to "providing authentication data and authentication software to an electronic device" that is "preferably stored in a secure storage location or other location inaccessible to the user or the operating system of the device." SAMSUNG-1001, Abstract. FIG. 3 (reproduced below) illustrates an embodiment to which the '480 Patent claims are directed. SAMSUNG-1003, ¶[37].

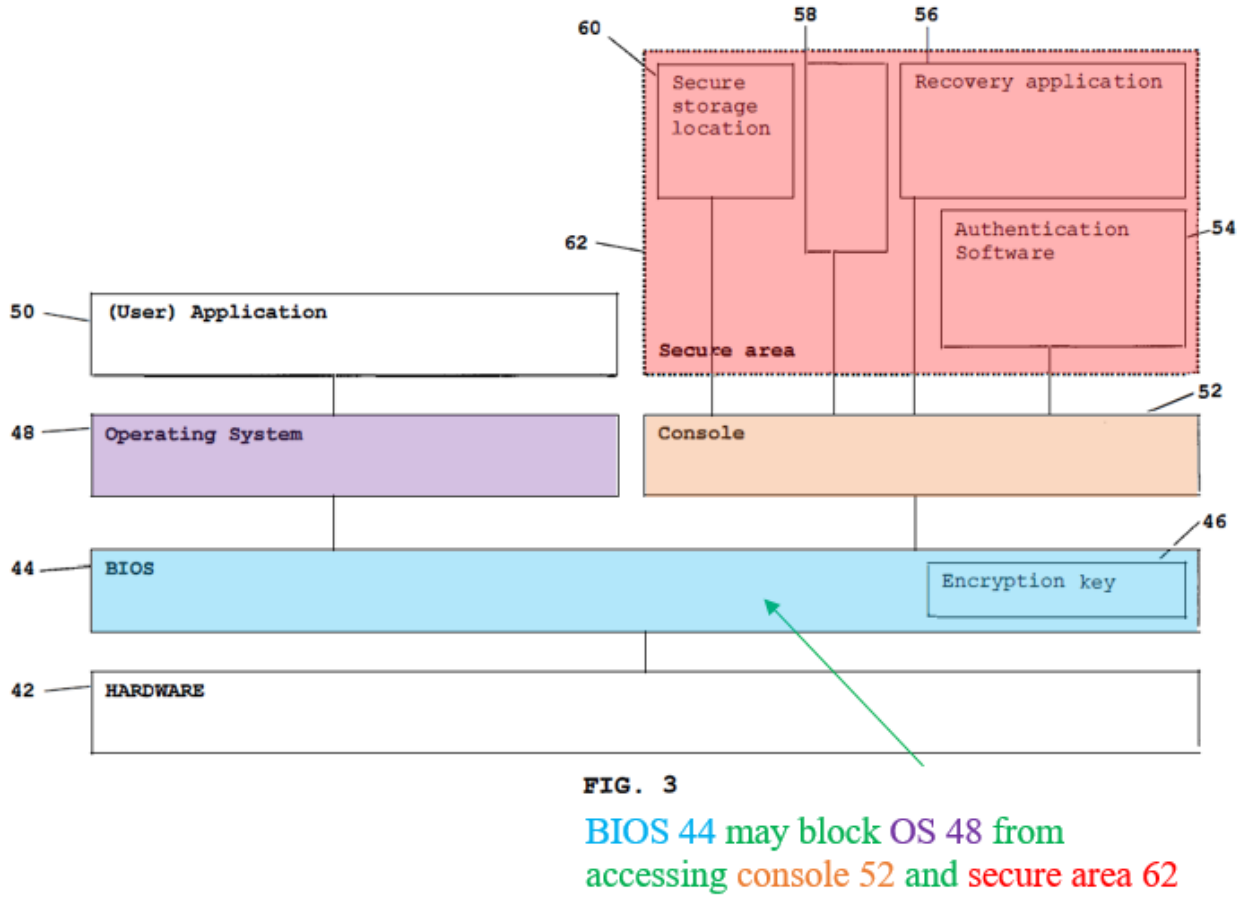


FIG. 3

SAMSUNG-1001, FIG. 3[2]

In FIG. 3, "[t]he BIOS 44 controls most of the instructions and data flowing from one component to another. Data or instructions coming from one component and addressed to another need to pass through the BIOS 44. The BIOS 44 may check whether the instructions to the other component are allowed or not." SAMSUNG-1001, 8:22-27. "All the hardware devices are controlled by the BIOS 44." *Id.*, 8:15-20. "The BIOS 44 may comprise an encryption key 46." *Id.*, 8:29-

[2] Annotations to the figures throughout this petition are shown in color.

30; SAMSUNG-1003, ¶[38].

"The operating system 48 creates a run-time environment for any user applications" and "is an interface between a user and the hardware 42." SAMSUNG-1001, 8:33-47. The operating system 48 may be prohibited by the BIOS 44 "to access certain parts of a hard drive or start certain applications." *Id*.; SAMSUNG-1003, ¶[39].

Console 52 instructs "the hardware devices 42 via the BIOS 44 to start and report their status." SAMSUNG-1001, 8:49-61. "A user may not interrupt or influence the console 52. Any instructions coming from the operating system 48 intended for the console 52 may therefore be blocked by the BIOS 44." *Id*.; SAMSUNG-1003, ¶[40].

"In or behind the console 52, there is a secure area 62 only accessible to the BIOS." SAMSUNG-1001, 8:62-9:6. "[T]he operating system 48 does not know that the applications and data in the storage locations [in the secure area 62] are present and maybe even running in a separate environment." *Id*. "An authentication table may be securely stored in the secure storage location 60. In such a part of the computer, commonly seen as a part of the BIOS 44, the authentication table is unreachable for the operating system 48 and thus for a user." *Id.*, 9:7-11. The "authentication software 54 may be installed in an application environment in the secure area 62 such that it may obtain the authentication table

without passing through an unsecured part of the device." *Id.*, 9:16-19. "By locking the authentication table and the authentication software 54 including the digital signing algorithm in the secure area 62 they are secured." *Id.*, 9:30-35; SAMSUNG-1003, ¶[41].

B. Prosecution History of the '480 Patent

The '480 Patent issued from U.S. Patent Application No. 16/597,773 ("**the '773 Application**"). SAMSUNG-1001, cover. After failing to get an allowance in response to two office actions, Patent Owner amended the claims by replacing "authentication data" with "private key." SAMSUNG-1002, 91-96. 1001. In recognition of the narrowing effect of this amendment and with an additional Examiner's amendment to claims 27 and 28, the '773 Application was allowed. SAMSUNG-1002, 29-31. 1001. In particular, the Examiner indicated that by replacing "authentication data" with "private key" the rejections were overcome purportedly because the art cited by the Examiner did not teach "encrypting the private key for storage by another inaccessible key." SAMSUNG-1002, 80, 111. ***Remarkably, no such language is recited in the claims.*** The issued claims recite that "the private key is encrypted when the private key is stored in said memory," not "encrypting the private key for storage by another inaccessible key." *See, e.g.,* SAMSUNG-1001, 17:63-18:29 ('480 Patent's claim 1). Thus, the rationale and language relied upon by the Examiner to allow the claims are untethered to the

actual claim language. As shown in this petition, the '480 Patent claims are obvious and invalid for failing to satisfy the requirements set forth by 35 U.S.C §§ 112 and 103. SAMSUNG-1003, ¶¶[42]-[43].

III. THE CHALLENGED CLAIMS ARE UNPATENTABLE UNDER 35 U.S.C § 112

A. GROUND A1: Claims 1-19 are unpatentable under the 35 U.S.C. § 112(a) Written Description Requirement

To satisfy the written description requirement under 35 U.S.C. § 112(a), an application must "reasonably convey[] to those skilled in the art that the inventor had possession of" and "actually invented" the claimed subject matter. *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (en banc). This requirement is in place to ensure that the claims do "not overreach the scope of the inventor's contribution to the field of art as described in the patent specification." *Reiffin v. Microsoft Corp.*, 214 F.3d 1342, 1345. The test for adequate written description support "requires an objective inquiry into the four corners of the specification from the perspective of a person of ordinary skill in the art. Based on that inquiry, the specification must describe an invention understandable to that skilled artisan and show that the inventor actually invented the invention claimed." *Ariad*, 598 F.3d at 1351. As explained below, the '480 Patent claims fail to satisfy these requirements and are invalid under 35 U.S.C. § 112(a). SAMSUNG-1003, ¶¶[13], [14], [43]. Specifically, as discussed below, the

'480 Patent specification fails to provide written description support for independent claims 1 and 16-18 and, thus, these claims are unpatentable. Their dependent claims 2-15 and 19 are also unpatentable by virtue of their dependency and for the additional reasons associated with claims 2, 4, and 5 provided below.

1. Claims in corresponding European patents were held invalid for a similar lack of support

The '480 Patent is part of a family of applications that include corresponding European patents, which have been invalidated because the issued claims were not supported by written disclosure. As explained below, the same or similar limitations are recited in the claims of the '480 Patent and do not have written description support for similar reasons. Also, the US Examiner that allowed the '480 Patent was not informed by the Patent Owner of the invalidity of corresponding European claims, thereby rendering the Examiner's patentability analysis for the '480 Patent insufficient and incomplete.

In more detail, the '480 Patent claims priority from PCT application PCT/NL2004/000422, filed on June 14, 2004 and published as WO 2004/111752 ("WO 752" or SAMSUNG-1014). SAMSUNG-1001, cover. European patents EP 1634140 ("EP 140") and EP 3229099 ("EP 099") were granted on the basis of WO 752. SAMSUNG-1015, 3-4. EP 099 was a divisional application of EP 140, which recites claims corresponding to U.S. Patent No. 11,063,766 ("the '766 Patent")—a parent of the '480 Patent. *Id.*; SAMSUNG-1012, 18:10-21:26. EP

140 and EP 099 invoked priority of the same PCT application PCT/NL03/00436, which was filed on 13 June 2003. SAMSUNG-1015, 3-4.

EP 099 recites claims similar to the '480 Patent. SAMSUNG-1001, 17:64-20:47; SAMSUNG-1015, 6-8. Indeed, the only differences between claim 1 of EP 099 and claim 1 of the '480 Patent are that the '480 Patent replaces "authentication data" with "private key" and additionally recites that "the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software."

In the European proceedings, the Hague Court held that claim features "said memory being a secure part of a Basic In Out System ***or any other secure location in said electronic device***," and "the authentication data being accessible to said authentication software, ***wherein authentication software is stored in said secure memory inaccessible to said operating system***" were not supported by the description in the respective patent disclosure. SAMSUNG-1015, 6, 37-45. The '480 Patent recites these same features and similarly lacks written description support for them.

The Hague Court also repeatedly noted that ***DTS's arguments incorrectly relied upon mixing embodiments that could not be combined***. SAMSUNG-1015, 37-41. For example (and as discussed in more detail below in Section III.A.2), the Hague Court explained that Embodiment 3 in EP 140 and EP 099 (which is the

same as Embodiment 3 in the '480 Patent) cannot be combined with other described embodiments (e.g., the first two embodiments of EP 140, EP 099, and the '480 Patent). SAMSUNG-1015, 39 ("'In a third preferred installation method (...) the authentication data, (...) is stored in a memory that is accessible to an operating system of the device (...)'. However, … it is precisely this embodiment that ***does not fall within the scope of protection of the claims as granted***."); SAMSUNG-1015, 38. The '480 Patent suffers from these same deficiencies.

Further, in related European proceedings, the European Patent Office issued additional opinions that similarly held "that the subject-matter of the patent [EP 140 and EP 099] appears to extend beyond the content of the earlier application as filed." SAMSUNG-1017, 76; SAMSUNG-1016, 16, 47, 76; SAMSUNG-1018, 1, 4, 14, 21, 14-21. In spite of multiple proceedings finding claims of corresponding European patents with similar disclosure and claim scope to the '480 and '766 Patents invalid due to written description deficiencies, the Patent Owner never brought these decisions and opinions to the USPTO Examiner's attention. For instance, Patent Owner filed a response to an Office Action on July 13, 2020 and an IDS on August 11, 2020—months after the courts in Europe had found the European claims invalid—but never informed the US Examiner of the invalidity determinations. SAMSUNG-1002, 178-194. Thus, Patent Owner withheld information material to the patentability of the claims of the '480 Patent and

prevented examiner consideration of arguments that demonstrate how the claims of the ’480 Patent lack written description support.

Because the claims of the ’480 Patent include the same limitations found as lacking support in the corresponding European patents, all claims of the ’480 Patent are unpatentable under 35 U.S.C. § 112 for similar reasons. In fact, the ’480 Patent includes additional limitations that cause the claims of the ’480 Patent to diverge even further from the specification than the claims of the European patents. Specifically, during prosecution, the claims were amended to recite “private key” in place of “authentication data” and to add a limitation that “the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software.” As explained below, these “private key” features are missing from the ’480 Patent and create additional written description issues above and beyond those found to invalidate the European claims.

2. The ’480 Patent does not describe a private key in the manner recited in the claims

As noted above in Section II.B, to get the application allowed, Patent Owner amended the claims to replace “authentication data” with “private key.” SAMSUNG-1002, 91-96. However, the ’480 Patent’s specification does not describe the “private key” in the manner that it is claimed. SAMSUNG-1003, ¶[169]. The ’480 Patent teaches that the authentication software may have its own private encryption key. SAMSUNG-1001, 5:39-40. In addition to this sentence,

only one paragraph (13:31-44, reproduced below) in the '480 Patent mentions a "private key."

> In a further embodiment, the authentication software may be provided with a system for signing a digital signature according to the present invention using at least a part of a software identification number (software ID) or any other application identifying character string, hereinafter referred to as a private key. The private key is registered at a third party, for example the authentication software provider which supplied said private key. The private key may be used to uniquely sign the digital signature and append the signed digital signature to the digital signature, which is sent to the second transaction party. The second transaction party is not capable of generating the signed digital signature without the private key. The second transaction party only stores the signed digital signature.

In contrast to this description of a private key, the claims recite numerous features that are not supported by the paragraph above or the four corners of the '480 Patent's specification. Examples of the private key features recited in claim 1 that are not supported by the specification are noted below and discussed in subsequent sections. SAMSUNG-1001, 18:3-18; SAMSUNG-1003, ¶[170].

Unsupported limitations:

(1) providing a private key in a memory of said electronic device, said memory being a secure part of a Basic In Out System or any other secure location in said electronic device,

(2) which private key is inaccessible to a user of said electronic

device,

(3) wherein the private key is encrypted when the private key is stored in said memory,

(4) wherein the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software.

2A. The ’480 Patent does not describe providing a private key in a memory that is a secure part of the BIOS or any other secure location in the electronic device operated by the first transaction party (independent claims 1, 16-18)

The ’480 Patent discloses a secure area 62 that includes a secure storage location 60, authentication software 54, an authentication table, and a memory location 58 that stores a log file of all actions performed by the BIOS 44. SAMSUNG-1001, 8:62-9:34, FIG. 3 (reproduced below). SAMSUNG-1003, ¶[171].

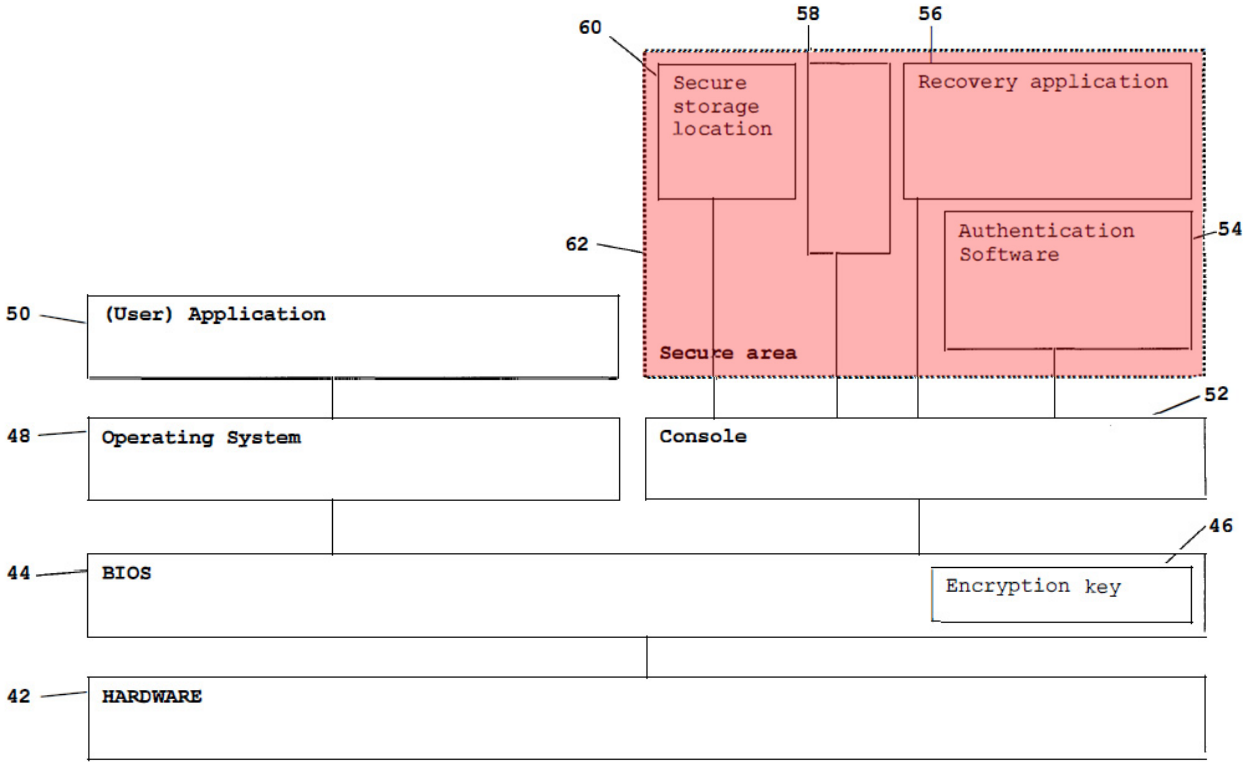


FIG. 3

SAMSUNG-1001, FIG. 3

Although the ’480 Patent explains that the secure area 62 is “[i]n or behind the console 52” and is “only accessible to the BIOS” 44, the ’480 Patent fails to describe where the private key is stored in the electronic device and certainly does not teach that the secure area 62 stores the private key. Claim 1 also recites that the private key is provided in a memory of the electronic device ***that is a secure part of the BIOS or any other secure location*** in the electronic device. Nothing in the ’480 Patent describes providing the private key in a memory that is “a secure part of the BIOS or any other secure location” in the electronic device described. SAMSUNG-1003, ¶[172]; *see also* Section III.A.1 (noting that the Hague Court

and EPO found this claim limitation without support in the specification even with the broader language of authentication data, instead of private key).

The '480 Patent teaches that authentication software for signing a digital signature uses a private key and that "the digital signing algorithm is preferably stored in a secure part of the BIOS 44" and is "protected like the authentication table in the secure storage location 60." SAMSUNG-1001, 9:27-34, 13:31-44. However, this disclosure describes the storage of the ***digital signing algorithm*** and ***not of the private key***, which even if used by the digital signing algorithm to generate a digital signature could be obtained from another storage location. SAMSUNG-1003, ¶[173]. The '480 Patent does not teach that the private key is stored in a secure location when running the digital signing algorithm or that the private key can be stored in "any other secure location in said electronic device." In fact, the '480 Patent only reveals that the private key is "***registered at a third party***, for example the authentication software provider ***which supplied said private key***." SAMSUNG-1001, 13:31-44. Accordingly, the '480 Patent does not provide written description to support "providing a private key in a memory of said electronic device, said memory being a secure part of a Basic In Out System or any other secure location in said electronic device," as recited in claim 1 and similarly in independent claim 16. SAMSUNG-1003, ¶[173].

Claim 17 recites "providing a private key in a memory of said electronic

device," and claim 18 recites "[a]n electronic device comprising: … a memory storing a private key,"—features that are not described by the '480 Patent for the same reasons noted above. SAMSUNG-1003, ¶[174].

2B. The '480 Patent does not describe the private key being inaccessible to the user (independent claims 1 and 16)

The parts of the '480 Patent that describe a "private key" do not describe the private key being inaccessible to the user. SAMSUNG-1001, 5:39-40, 13:31-44. In fact, since the '480 Patent describes the private key as being part of a software ID or an application identifying character string, it could have been accessible to the user because the '480 Patent does not teach that the software ID or application identifying character string are inaccessible to the user. *Id*. Moreover, since there is no teaching in the '480 Patent of where the private key is stored or maintained in user's electronic device (*see supra* Section III.A.2.2A) or how the private key may be protected from the user when provided by the third party, the '480 Patent fails to provide written description in support of the private key being inaccessible to a user of the electronic device. SAMSUNG-1003, ¶¶[175]-[176].

The description of the authentication software having its own "private encryption key" (*see* SAMSUNG-1001, 5:39-40) also does not cure the lack of written description support at least because the '480 Patent does not provide any explanation that such a key is used to perform the operations related to the private

key in claim 1, such as being used to generate a digital signature. At best, based on its name, the private encryption key would be understood by a POSITA as an encryption key that is kept private, but not necessarily inaccessible to the user. SAMSUNG-1003, ¶[177].

2C. The '480 Patent does not describe the private key being encrypted when the private key is stored in the memory (claims 1, 16-18)

The '480 Patent explains that the encryption key 46 in BIOS 44 may be used to encrypt data, but the encrypted data is not a private key. SAMSUNG-1001, 8:29-30. The '480 Patent does not teach "the private key is encrypted when the private key is stored in said memory" because it does not disclose 1) ***a temporal element*** that the private key is encrypted ***when*** it is stored in the memory, and 2) that the private key is stored in the secure memory, as explained above in Sections III.A.2 and III.A.2.2A. SAMSUNG-1003, ¶[178].

The '480 Patent discloses a "private encryption key." SAMSUNG-1001, 5:39-40. However, a private encryption key is not the same as an ***encrypted*** private key. SAMSUNG-1003, ¶[179]. As noted above, a private encryption key would have been understood by a POSITA as an encryption key that is kept private. *Id*. In contrast, an encrypted private key is a private key that has been encrypted—a limitation that is not required by a private encryption key, which may not be encrypted. Rather, the private encryption key is used to encrypt other data,

not itself. *Id*. Thus, the '480 Patent's disclosure of a "private encryption key" does not provide written description support for the features related to encryption of the "private key" in the claims. *Id*.

2D. The '480 Patent does not describe the private key being decrypted in a secure processing environment inaccessible to said user, to any user-operated software, and to said operating system (claims 1, 16-18)

First, the '480 Patent, as a whole, including the paragraph at 13:31-44 and the sentence at 5:39-40 noted above in Section III.A.2 that describe a private key, does not provide any disclosure related to decryption of the private key. SAMSUNG-1003, ¶[180].

Second, to the extent that the '480 Patent describes a secure processing environment that is inaccessible to said user, to any user-operated software, and to said operating system, such a description is provided with respect to the third embodiment disclosed in the '480 Patent, which is not combinable with the embodiment describing the '480 Patent's second method. SAMSUNG-1001, 9:47-53; SAMSUNG-1003, ¶[181].

For example, the '480 Patent discloses that, "[i]n a third preferred installation method …, the authentication data, e.g. authentication table, ***is stored in a memory that is accessible to an operating system*** of the device and possibly to a user of said device." SAMSUNG-1001, 9:35-51. For this third embodiment,

the ’480 Patent teaches that “such a secure processing environment may only be accessible to selected software applications, preferably not to user-operated software applications. Further, a decryption algorithm and/or a decryption key should not be obtainable to any user.” *Id*.; SAMSUNG-1003, ¶[182].

In contrast, the ’480 Patent claims recite “said ***memory is inaccessible to said operating system*** of said electronic device” which is described with respect to the embodiment illustrated in FIG. 3 and in 8:12-10:2. A comparison of FIG. 3 (second embodiment) and FIG. 5A (third embodiment) immediately reveals to those skilled in the art that the system architecture of these two embodiments are not combinable. SAMSUNG-1003, ¶[183].

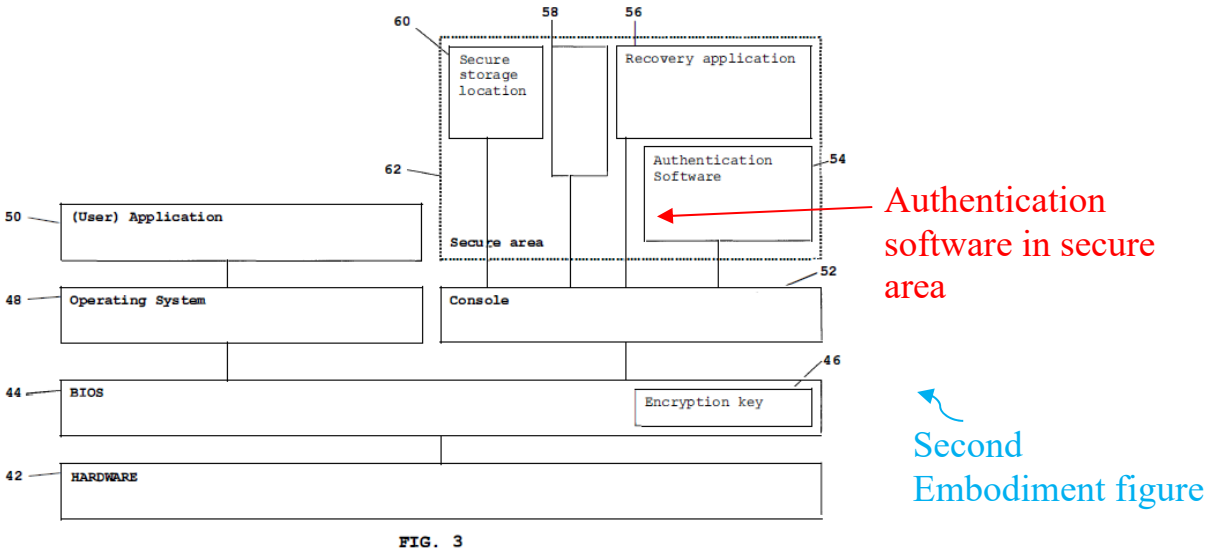


FIG. 3

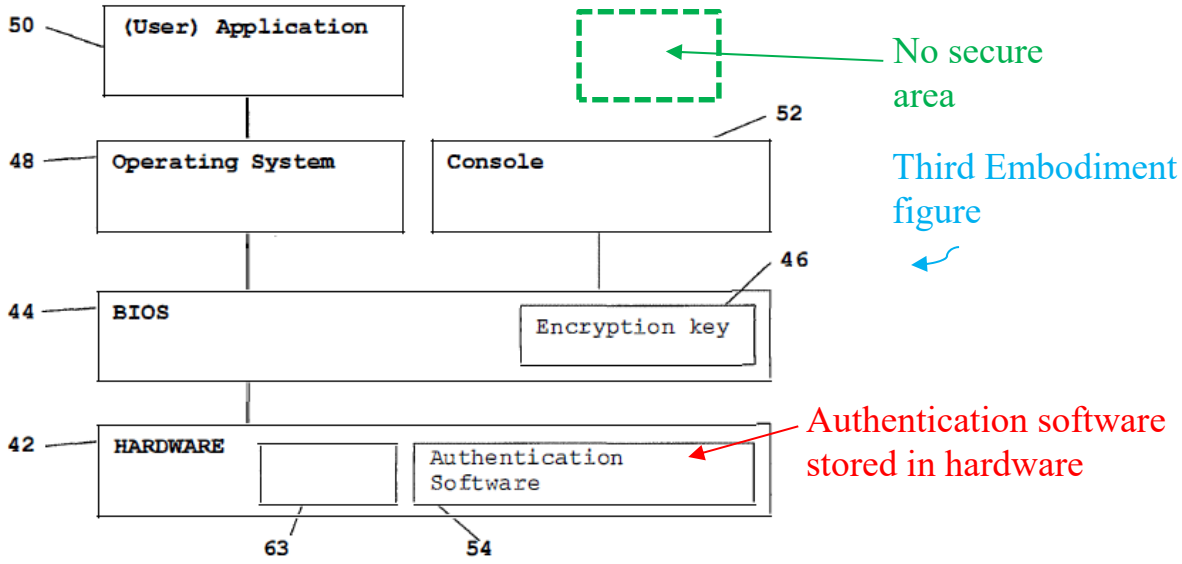


FIG. 5A

SAMSUNG 1001, FIGS 3 (top), 5A (bottom)

For example, the second method embodiment (FIG. 3) has a secure area behind the console 52 which the third method embodiment (FIG. 5A) lacks. In the third method embodiment, the authentication software 54 is stored in hardware 42 and accessible to the operating system and the user. In contrast, in the second method embodiment, the authentication software 54 is stored in a secure area—a

key part of all of the '480 Patent independent claims. Thus, Patent Owner cannot rely on support for features in the third embodiment, which directly contradicts features recited in all the '480 Patent independent claims. And, even if Patent Owner argues that combining the embodiments to arrive at the claimed features would have been obvious, such obviousness cannot be used to cure a lack of written description. S*ee Lockwood v. American Airlines, Inc.,* 107 F.3d 1565, 1571-72 (Fed. Cir. 1997) (confirming the written description must provide more than that which "would lead one to speculate as to modifications that the inventor might have envisioned, but failed to disclose"); *Intuitive Surgical, Inc. v Ethicon LLC*, IPR2019-01110, Paper 30 at 11-15 (Nov. 20, 2020) (explaining that embodiments cannot be mixed to satisfy the written description requirement even if obvious to do so and that "the disclosure must convey with reasonable clarity to one skilled in the art that the inventors possessed the invention claimed.") Moreover, as noted above in Section III.A.1, the Hague Court and the European Patent Office explicitly noted that the disclosure related to the third embodiment "is not covered by the claims as granted." SAMSUNG-1015, 41; SAMSUNG-1018, 14. In short, the result of multiple reviews by multiple courts/offices has confirmed that the '480 Patent specification (which is similar to the specification in EP 099 and EP 140) has no description of an embodiment where a key is stored in a secure memory in encrypted format and decrypted in a secure environment. *Id.*

3. The '480 Patent does not describe claim 2

Claim 2 recites, in part, "the private key is provided by the second transaction party, which stores the private key together with data identifying the first transaction party." SAMSUNG-1001, 18:30-34; SAMSUNG-1003, ¶[185].

The '480 Patent discloses that "[t]he private key is registered ***at a third party***" and that "[t]he second transaction party is not capable of generating the signed digital signature without the private key. ***The second transaction party only stores the signed digital signature***" and is forced to communicate with the third party to verify the digital signature because it does not have the private key. SAMSUNG-1001, 13:31-56. Because the second transaction party is not the third party and does not store the private key (and must therefore communicate with the third party), the '480 Patent clearly fails to provide written description support of claim 2's requirement that the private key be provided by the second transaction party, much less stored by the second transaction party together with data identifying the first transaction party. SAMSUNG-1003, ¶[186].

Moreover, one skilled in the art would have understood that storing the private key at both the first transaction party (claim 1) and the second transaction party (claim 2 which depends from claim 1) would not make sense because then both parties of a transaction would have the private key. As Dr. Black explains, providing the private key to both parties defeats the purpose of having a "private"

key and can prevent the first transaction party from being able to perform its encryption and decryption securely. SAMSUNG-1003, ¶[187]; SAMSUNG-1021, 1:41-45. Thus, the features of dependent claim 2 are inconsistent with the features of claim 1 and are not described in the specification of the '480 Patent. *Id.*

4. The '480 Patent does not describe claims 4 and 5

Claim 4 recites, in part, "wherein the private key is encrypted by the second transaction party using an encryption key before the private key is provided to the first transaction party." SAMSUNG-1001, 18:37-40; SAMSUNG-1003, ¶[188].

As noted above in Section III.A.3, in the '480 Patent, the second transaction party is forced to communicate with the third party to verify the digital signature because it does not have the private key. SAMSUNG-1001, 13:31-56. Accordingly, claim 4 fails the written description requirement because the second transaction party does not encrypt the private key or provide it to the first transaction party. SAMSUNG-1003, ¶[189].

Moreover, as Dr. Black explains, having two parties of a transaction that have knowledge of a private key would run contrary to the goals of a secure exchange. SAMSUNG-1003, ¶[190]. If both parties have possession of a private key, the party for whom the private key is not associated with, could use the private key in an unauthorized manner—which is why private keys are not provided from one party to another in the manner claimed by the '480 Patent. *Id.*;

SAMSUNG-1021, 1:41-45.

Claim 5 also fails the written description requirement because it depends on claim 4 and its features do not cure the deficiencies in claim 4. SAMSUNG-1003, ¶[191].

5. The '480 Patent does not describe claims 16, 18, and 19

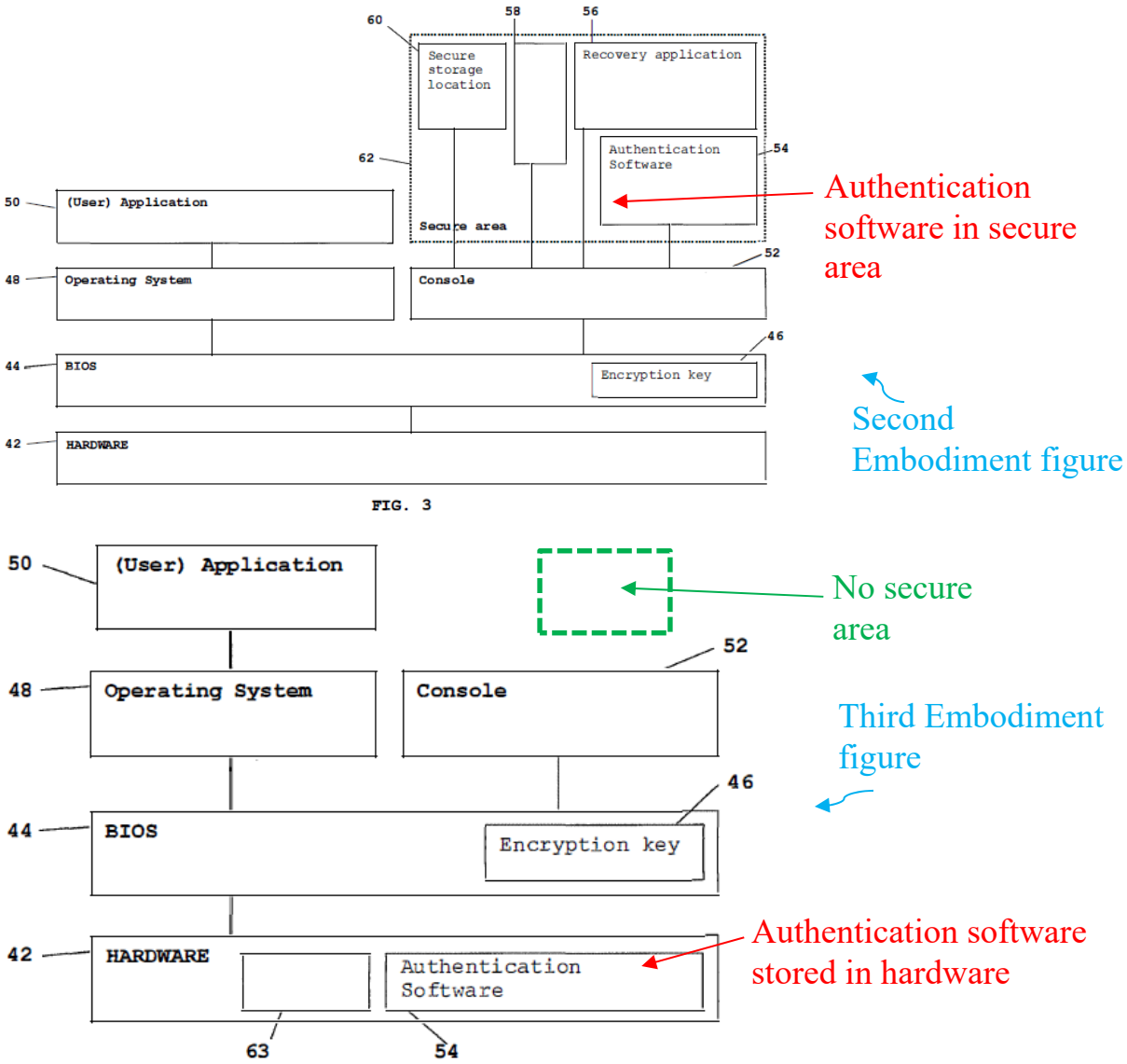
In addition to the reasons noted above in Section III.A.1, the '480 Patent fails to provide written description support for claims 16, 18, and 19 (by virtue of its dependency on claim 18) for the follow reasons. SAMSUNG-1003, ¶[192].

Claim 16 recites, in part:

> a processor configured for an operating system creating a run-time environment for user applications;
>
> …
>
> wherein the processor is configured for activating the authentication software to generate a digital signature from the private key, wherein the authentication software is run in a secure processing environment inaccessible to said operating system, for providing the digital signature to the second transaction party.

However, the '480 Patent does not disclose a processor that is configured for an operation system **and** for activating the authentication software … wherein the authentication software is run in a secure processing environment inaccessible to said operating system. Recall from Section III.A.2.2D and as shown in FIGS. 3 and 5A below, the authentication software is in a secure processing environment in

the second method embodiment shown in FIG. 3, not in the third method embodiment. However, in the second method embodiment, the processor (e.g., hardware 42) is ***not*** configured for activating the authentication software. SAMSUNG-1001, FIG. 3, 8:12-9:34. The processor is configured for activating the authentication software in the third method embodiment, but that embodiment is ***not*** compatible with the second method embodiment for the reasons noted above in Section III.A.2.2D. SAMSUNG-1003, ¶¶[193]-[194].



SAMSUNG 1001, FIGS 3 (top), 5A (bottom)

Thus, claim 16 (and similarly claim 18 which recites similar features) are not supported by the '480 Patent because these claims attempt to capture features from two different embodiments, which are not combinable in the manner claimed by the '480 Patent. *Lockwood v. American Airlines, Inc.,* 107 F.3d 1565, 1571-72 (Fed. Cir. 1997); *Intuitive Surgical, Inc. v Ethicon LLC*, IPR2019-01110, Paper 30

at 11-15 (Nov. 20, 2020). For instance, a processor/hardware 42 that is forbidden from accessing the secure area 62 or contents therein such as the authentication software 54 cannot be combined with a processor/hardware 42 that can access an authentication software with no secure area. SAMSUNG-1003, ¶¶[194]-[195]. Indeed, the same processor is claimed as being configured for both the operating system and the authentication software. *Id*. Yet, the authentication software is "stored in a secure memory ***inaccessible to said operating system***" and "run in a secure processing environment ***inaccessible to said operating system***." *Id*. As Dr. Black explains, a POSITA would have found it unusual and perhaps inoperative to use of the same processor to handle operating system functionality and functionality of authentication software that is ***inaccessible*** to the operating system, and such a processor is certainly not described in the '480 Patent. *Id*.

6. The priority applications and original claims do not cure the written description deficiencies in the '480 Patent

The '480 Patent is a continuation of U.S. Patent Application No. 10/560,579, filed as PCT application No. PCT/NL2004/000422 ("SAMSUNG-1014") on June 14, 2004, and now issued as the '766 Patent. SAMSUNG-1001, cover; SAMSUNG-1012, cover. As explained above in Section III.A.1, the PCT/NL2004/000422 disclosure (which supports EP 140, EP 099, and the '480 Patent) fails to provide support for the claimed features that are similarly recited

across all three patents. SAMSUNG-1003, ¶[195].

PCT/NL2004/000422 also claims priority to PCT application PCT/NL2003/000436 ("SAMSUNG-1013"), filed on June 13, 2003. *Id*. The parent PCT/NL2003/000436 application has a more limited disclosure, e.g., it does not include FIGS. 4, 5, and 10 of the '480 Patent. SAMSUNG-1013. A table showing the relationship between the figures of the PCT/NL2003/000436 application and the '480 Patent is provided below. SAMSUNG-1003, ¶[196].

PCT/NL2003/000436	**US**
FIGS. 1-3	FIGS. 1-3
FIG. 4	FIG. 6
FIG. 5	FIG. 7
FIG. 6	FIG. 8
FIG. 7	FIG. 9
---	FIGS. 4, 5, 10

The parent PCT/NL2003/000436 application lacks the description of FIGS. 4, 5, and 10 and also does not include the sole paragraph included in the '480 Patent that discloses a private key (as explained above in Section III.A.2, claim features related to the "private key" are not supported by the '480 Patent disclosure). Because disclosure in the parent PCT/NL2003/000436 application is a subset of the disclosure in the '480 Patent and does not provide any additional description related to the claimed features found to lack written support in European patents (EP 140, EP 099), PCT/NL2003/000436 also fails to cure the written description deficiencies in the '480 Patent. SAMSUNG-1003, ¶[197].

The original claims submitted during prosecution of the application corresponding to '480 Patent do not recite private key. SAMSUNG-1002, 743-748. The claims were amended by replacing "authentication data" with "private key" in order to reach allowance. *See supra* Section II.B. And, as explained above in Section III.A.2, several features related to the "private key" do not have support in the '480 Patent specification. Thus, the original claims do not provide the required written description support for the issued claims. SAMSUNG-1003, ¶[198].

IV. THE CHALLENGED CLAIMS ARE UNPATENTABLE UNDER 35 U.S.C § 103

A. GROUND B1: Claims 1, 3, 6, 11, and 14-19 are obvious over Ellison and Muir

1. Ellison[3]

Ellison discloses a computer system with "an isolated execution architecture" to prevent attacks and vulnerabilities in electronic and software systems. SAMSUNG-1006, 1:17-51, 2:40-61. An example illustration of Ellison's "isolated execution architecture" is shown in Ellison's FIG. 1A

[3] General descriptions provided for the references and combinations discussed in Section III are incorporated into each subsection addressing/applying those references, as are the discussions of combinations.

(reproduced below). SAMSUNG-1003, ¶[44].

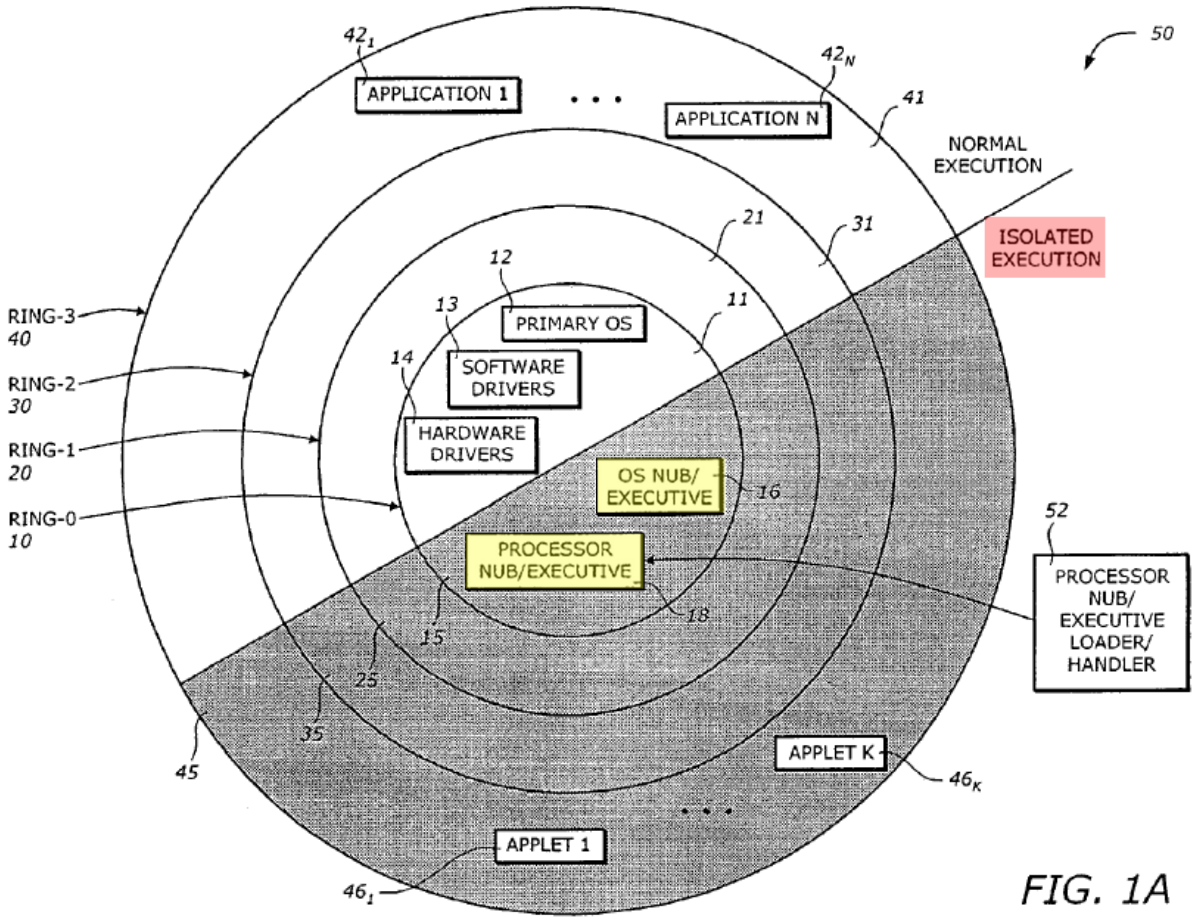


FIG. 1A

SAMSUNG-1006, FIG. 1A

The logical operating architecture 50 shown in FIG. 1A "includes ring-0 10, ring-1 20, ring-2 30, ring-3 40, and a processor nub loader 52." SAMSUNG-1006, 2:62-3:1. The different ring levels are associated with different privilege levels. SAMSUNG-1006, 2:41-61. Ellison explains that:

> A ring is a logical division of hardware and software components that are designed to perform dedicated tasks within the operating system.

> The division is typically based on the degree or level of privilege, namely, the ability to make changes to the platform. For example, a ring-0 is the innermost ring, being at the highest level of the hierarchy. Ring-0 encompasses the most critical, privileged components. In addition, modules in Ring-0 can also access to lesser privileged data, but not vice versa. Ring-3 is the outermost ring, being at the lowest level of the hierarchy. Ring-3 typically encompasses users or applications level and has the least privilege. Ring-1 and ring-2 represent the intermediate rings with decreasing levels of privilege.

SAMSUNG-1006, 2:41-61. "The logical operating architecture 50 has two modes of operation: normal execution mode and isolated execution mode. Each ring in the logical operating architecture 50 can operate in both modes. The processor nub loader 52 operates only in the isolated execution mode." SAMSUNG-1006, 3:4-8. "Ring-0 10 includes two portions: a normal execution Ring-0 11 and an isolated execution Ring-0 15." SAMSUNG-1006, 3:8-10. "The isolated execution Ring-0 15 includes an operating system (OS) nub 16 and a processor nub 18." SAMSUNG-1006, 3:15-16; SAMSUNG-1003, ¶¶[45]-[46].

The operating system (OS) nub 16 and the processor nub 18 are "instances of an OS executive (OSE) and processor executive (PE), respectively. The OSE and the PE are part of executive entities that operate in a secure environment associated with the isolated area 70 and the isolated execution mode." SAMSUNG-1006, 3:9-25; SAMSUNG-1003, ¶[47].

Ellison's isolated execution architecture includes "an isolated region in the system memory" (*see* isolated area 70 in physical memory 60 shown in FIG. 1B (reproduced below)) and "is protected by both the processor and chipset in the computer system." SAMSUNG-1006, 3:32-36, FIGS. 1A, 1B. "The isolated area 70 is accessible only to elements of the operating system and processor operating in isolated execution mode." SAMSUNG-1006, 4:8-22. "The operating system nub 16 provides links to services in the primary OS 12 (e.g., the unprotected segments of the operating system), provides page management within the isolated area [70], and has the responsibility for loading ring-3 application modules 45, including applets 46 to 46, into protected pages allocated in the isolated area [70]." SAMSUNG-1006, 3:32-36, 4:30-37. "[T]he operating system nub 16 is also responsible for encrypting and hashing the isolated area pages before evicting the page to the ordinary memory, and for checking the page contents upon restoration of the page." SAMSUNG-1006, 3:64-4:7; SAMSUNG-1003, ¶[48].

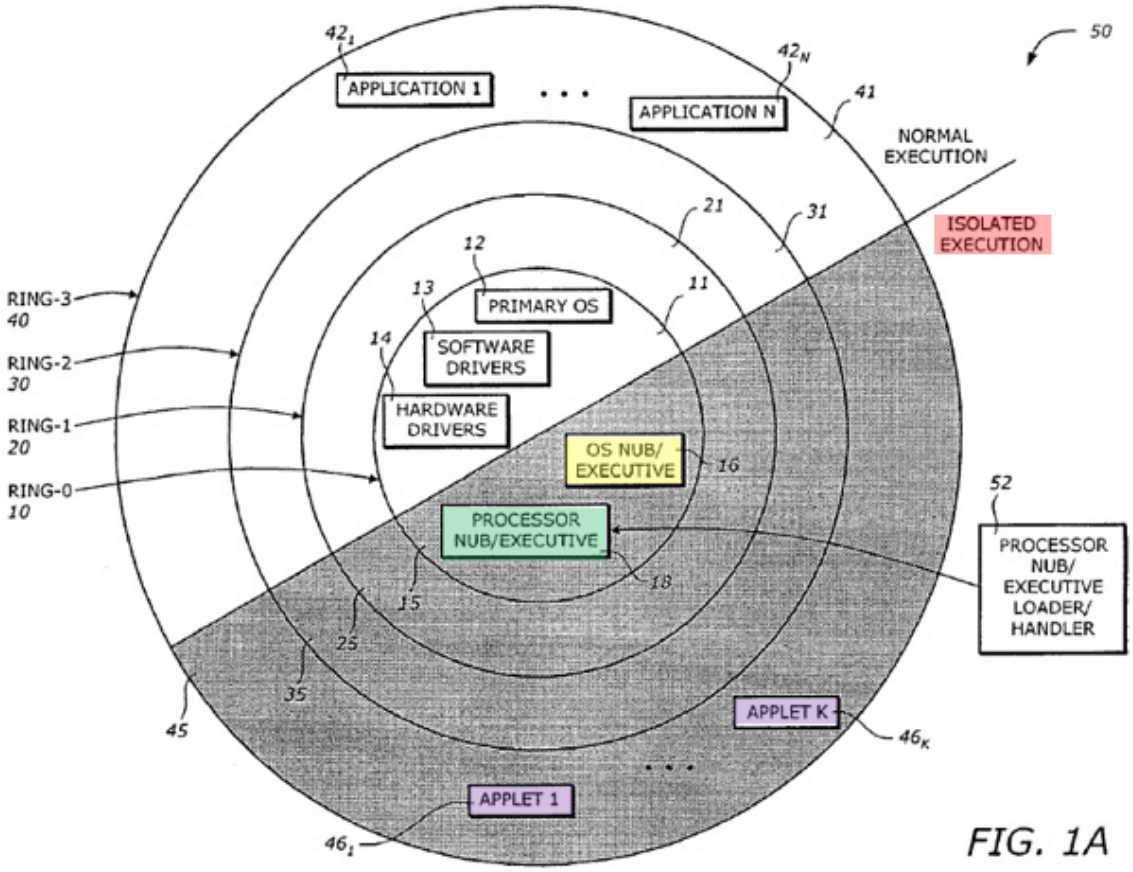


FIG. 1A

SAMSUNG-1006, FIG. 1A

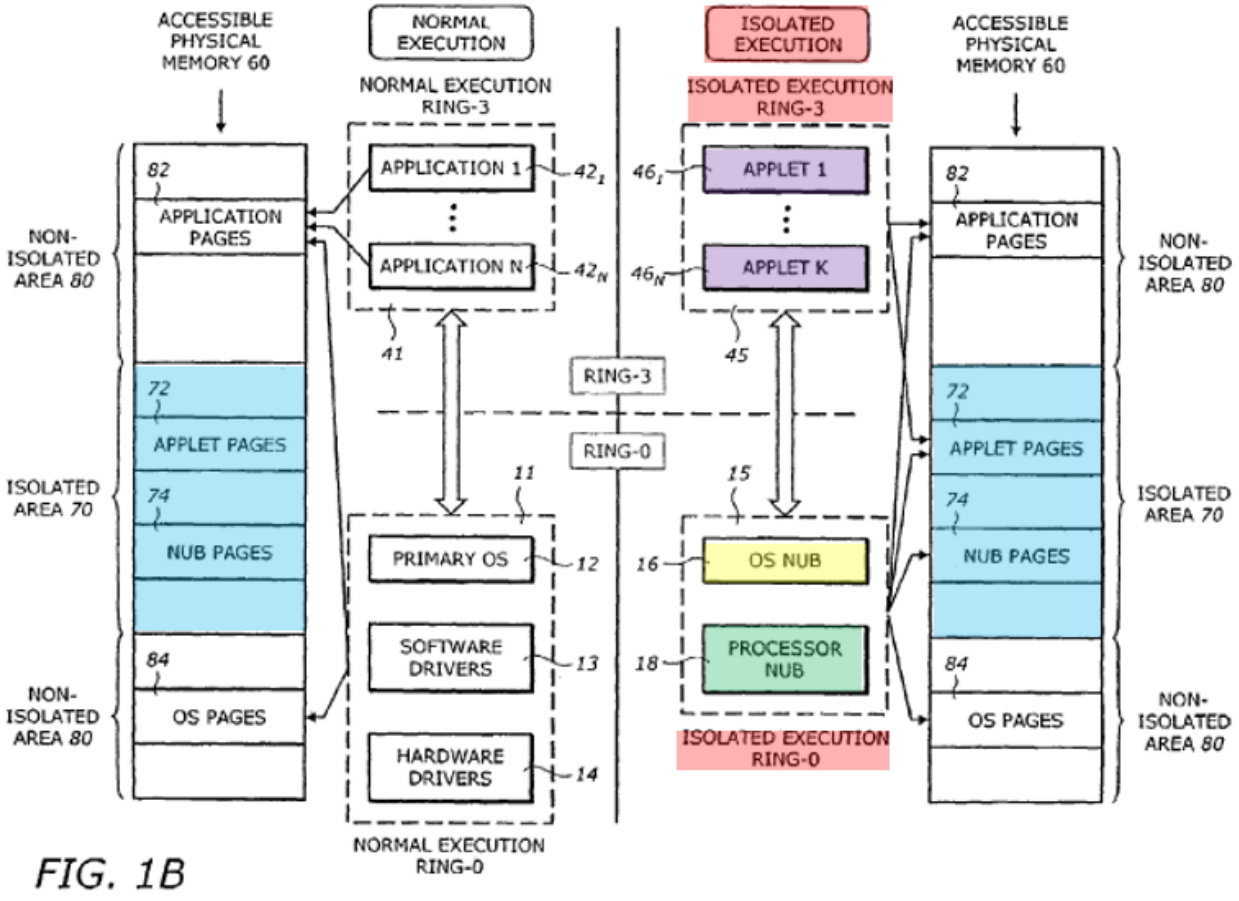


FIG. 1B

SAMSUNG-1006, FIG. 1B

"The isolated mode applets 46_1 to 46_N and their data ***are tamper-resistant and monitor-resistant from all software attacks from other applets, as well as from non-isolated space applications*** (e.g., 42_1 to 42_N), dynamic link libraries (DLLs), ***drivers and even the primary operating system 12***. ***Only the processor nub 18 or the operating system nub 16 can interfere with or monitor the applet's execution***." SAMSUNG-1006, 4:1-7; SAMSUNG-1003, ¶[49].

A computer system 100 design that implements Ellison's isolated execution architecture is shown in Ellison's FIG. 1C (reproduced below). "The computer

system 100 includes a processor 110, a host bus 120, a memory controller hub (MCH) 130, a system memory 140, an input/output controller hub (ICH) 150, a non-volatile memory, or system flash, 160, a mass storage device 170," and other components. SAMSUNG-1006, 4:38-56; SAMSUNG-1003, ¶[50].

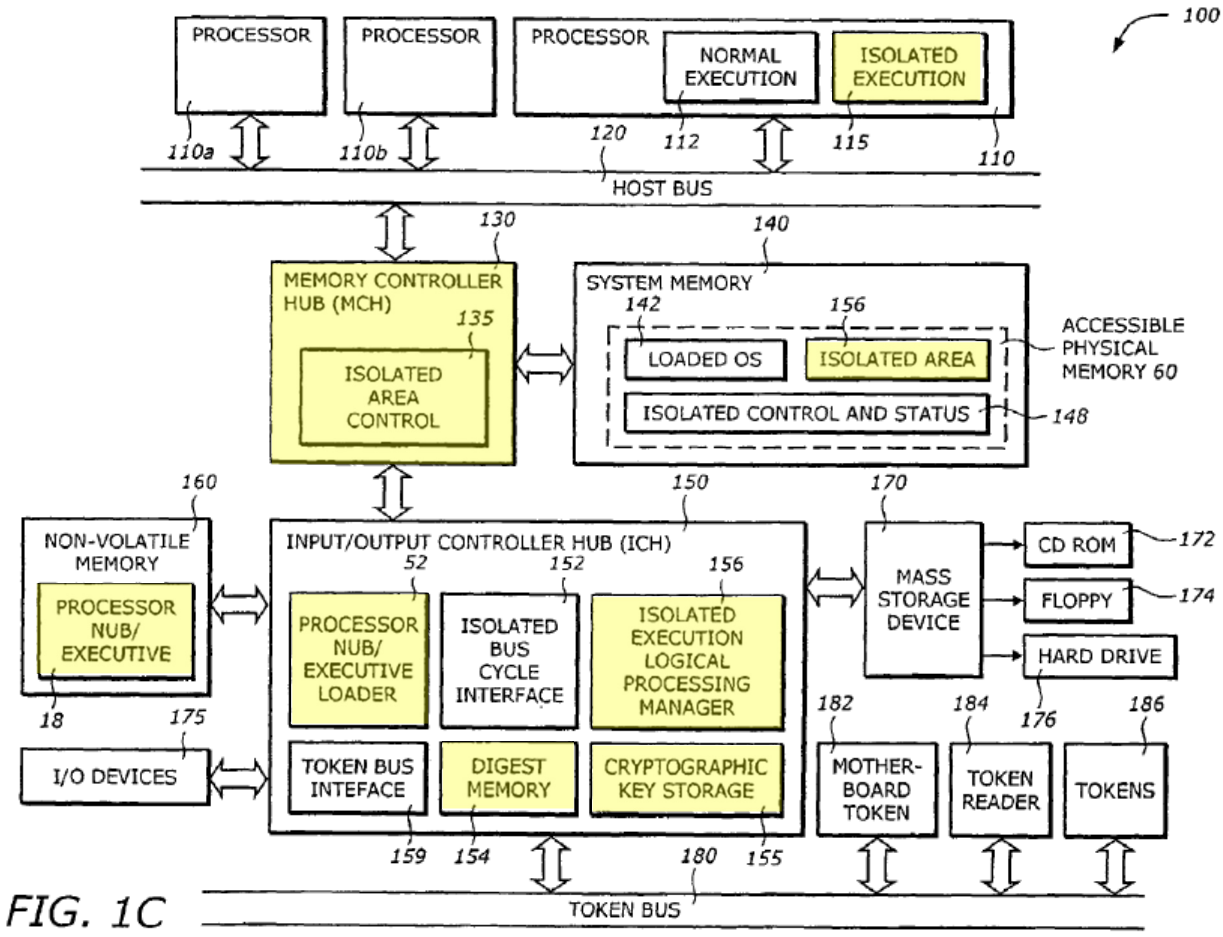


FIG. 1C

SAMSUNG-1006, FIG. 1C

"The processor 110 includes a normal execution mode 112 and an isolated execution circuit 115." SAMSUNG-1006, 4:63-65. "The isolated execution circuit 115 provides a mechanism to allow the processor 110 to operate in an

isolated execution mode" and "provides hardware and software support for the isolated execution mode." SAMSUNG-1006, 5:1-5. "[T]he MCH 130 has memory range registers (e.g., base and length registers) to represent the isolated area in the system memory 140. Once configured, the MCH 130 aborts any access to the isolated area that does not have the isolated access bus mode asserted." SAMSUNG-1006, 5:62-67. "Access to the isolated area 70 [shown in FIG. 1B] is restricted and is enforced by the processor 110 and/or the MCH 130." SAMSUNG-1006, 6:15-17; SAMSUNG-1003, ¶[51].

The computer system 100 also includes a processor nub loader 52 (part of the I/C Controller Hub (ICH) 150) that "copies the processor nub 18 from the system flash memory (e.g., the processor nub code 18 in non-volatile memory 160) into the isolated area 70, verifies and logs its integrity, and manages a symmetric key used to protect the processor nub's secrets." SAMSUNG-1006, 6:52-56. "For security purposes, the processor nub loader 52 is unchanging, tamper-resistant and non-substitutable." SAMSUNG-1006, 6:57-61; SAMSUNG-1003, ¶[52].

The ICH 150 "represents a known single point in the system having the isolated execution functionality" and includes a digest memory 154 and a cryptographic key storage 155. SAMSUNG-1006, 6:27-67. "The digest memory 154, typically implemented in RAM, stores the digest (e.g., hash) values of the loaded processor nub 18, the operating system nub 16, and any other critical

modules (e.g., ring-0 modules) loaded into the isolated execution space. The cryptographic key storage 155 holds a symmetric encryption/decryption key that is unique for the platform of the system 100." SAMSUNG-1006, 6:60-67; SAMSUNG-1003, ¶[53].

A non-volatile memory 160 is coupled to the ICH 150 and includes the processor nub 18 (*see* FIGS. 1A, 1B, 1C). SAMSUNG-1006, 7:19-22. "The processor nub 18 provides the initial set-up and low-level management of the isolated area 70 (in the system memory 140), including verification, loading, and logging of the operating system nub 16, and the management of the symmetric key used to protect the operating system nub's secrets." SAMSUNG-1006, 7:22-27; SAMSUNG-1003, ¶[54].

Ellison's FIG. 2 (reproduced below) illustrates a secure platform 200 for performing isolated execution. The secure platform 200 includes "the OS nub 16, the processor nub 18, a key generator 240, a hashing function 220, and a usage protector 250, all operating within the isolated execution environment, as well as a software environment 210" that may exist inside the isolated execution environment. SAMSUNG-1006, 8:12-32. Unauthorized attempts at accessing the software environment (including the usage protector 250) are blocked and terminated. SAMSUNG-1006, 13:4-14:5, FIGS. 4-7; SAMSUNG-1003, ¶[55].

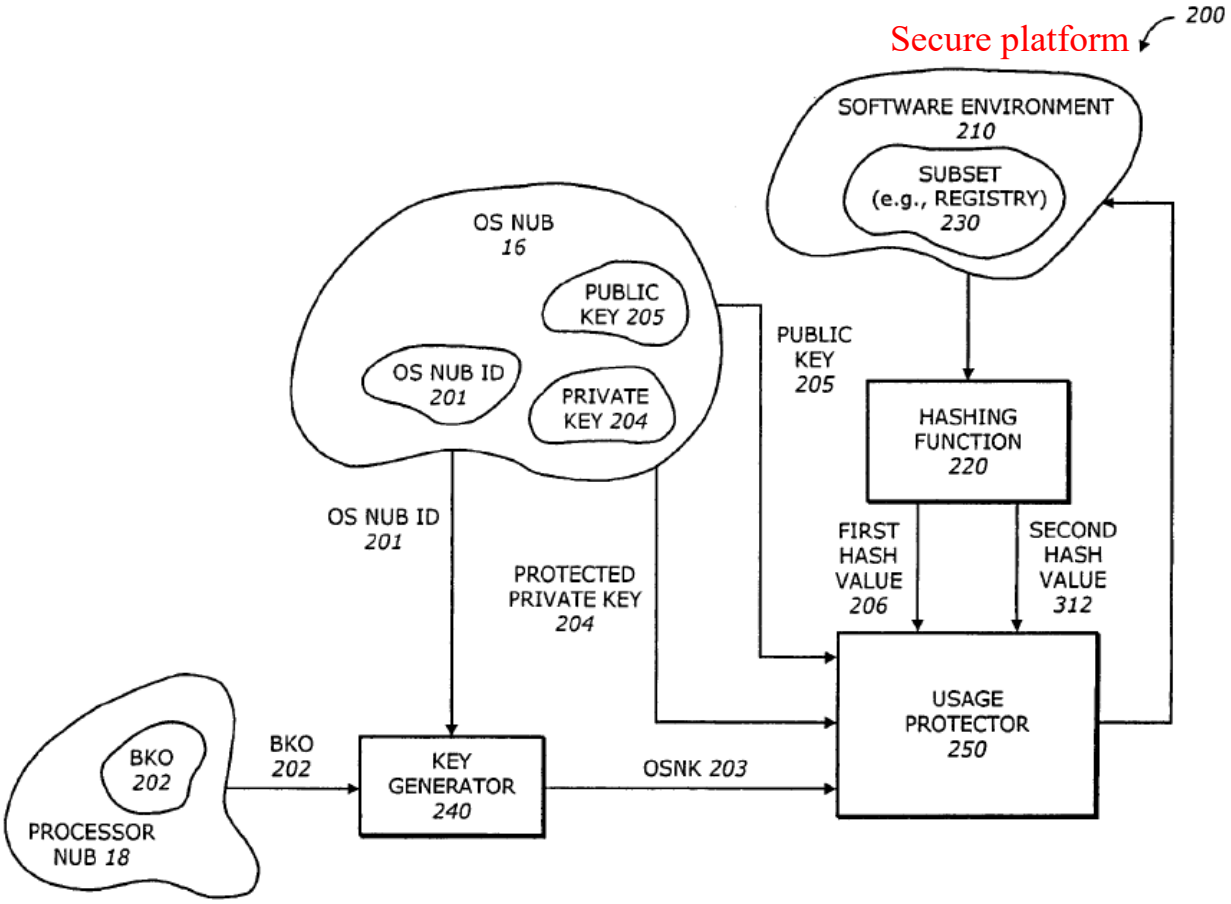


FIG. 2

SAMSUNG-1006, FIG. 2

"The OS nub or OS executive (OSE) 16 is part of the operating system running on the secure platform 200" and includes a protected private key 204 and a public key, as shown in FIG. 2. SAMSUNG-1006, 8:33-65. "The protected private key 204 may be programmed into the fuses of a cryptographic key storage 155 of the input/output control hub (ICH) 150 or elsewhere in persistent storage within the platform 200." SAMSUNG-1006, 8:44-47. "Only the OS nub 16 can retrieve and decrypt the encrypted private key for subsequent use. In the digital

signature generation process, the protected private key 204 is used as an encryption key to encrypt a digest of a message producing a signature, and the public key 205 is used as a decryption key to decrypt the signature, revealing the digest value." SAMSUNG-1006, 8:57-65; SAMSUNG-1003, ¶[56].

A "key generator 240 generates a key operating system nub key (OSNK) 203" "by combining [a master binding key] BK0 202 and [an] OS Nub ID 201 using a cryptographic hash function." SAMSUNG-1006, 8:66-9:40. "The OS nub 16 may supply the OSNK 203 to ***trusted agents, such as the usage protector 250***." *Id.*; SAMSUNG-1003, ¶[57].

"The usage of the software environment 210 or the usage of [a] subset 230 [(e.g., a registry)] is protected by the usage protector 250," which "uses the OSNK 203 to protect the usage of the subset 230." SAMSUNG-1006, 9:28-35. "The usage protector 250 is coupled to the key generator 240 to protect usage of the software environment 210 or the subset 230, using the OSNK 203. The usage protection includes protection against unauthorized reads, and detection of intrusion, tampering or unauthorized modification." SAMSUNG-1006, 9:48-52. "The[re] are several different embodiments of the usage protector 250. In one embodiment, the usage protector 250 decrypts the subset using the OSNK 203." SAMSUNG-1006, 9:63-65. In "other embodiments, the usage protector uses the

OSNK 203, the protected private key 204 and the pubic key 205." SAMSUNG-1006, 10:1-3; SAMSUNG-1003, ¶[58].

FIG. 3C illustrates one embodiment of the usage protector 250. SAMSUNG-1006, 10:63-67. "The usage protector 250 includes a decryptor 325, a signature generator 320, a storage medium 322, and a signature verifier 330." SAMSUNG-1006, 10:63-67; SAMSUNG-1003, ¶[59].

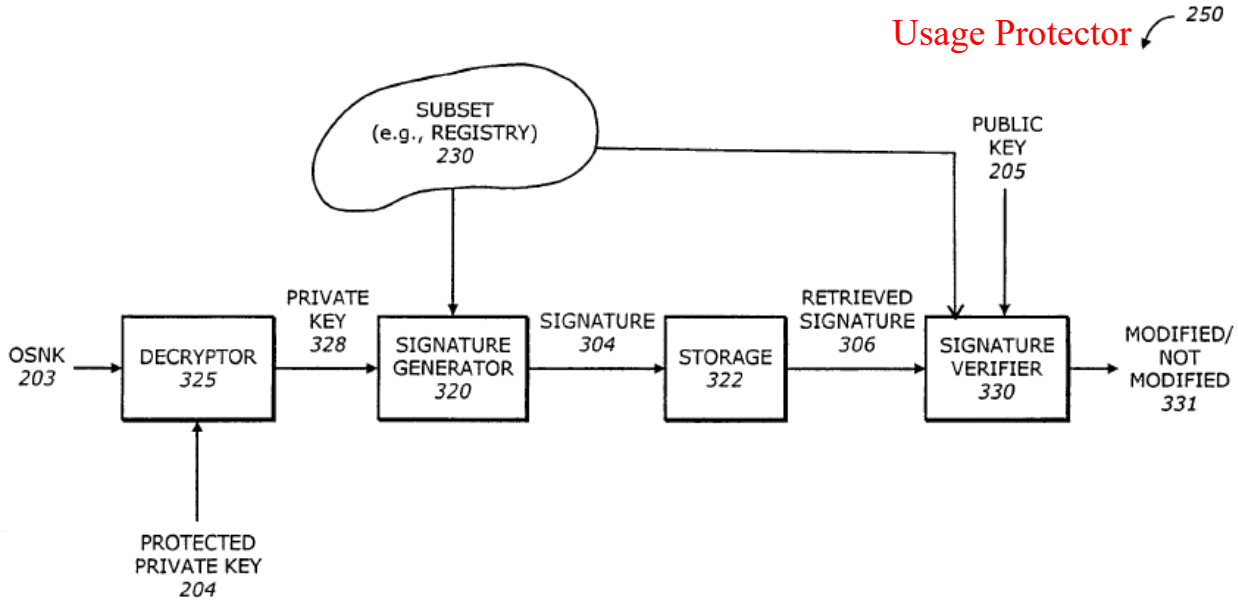


FIG. 3C

SAMSUNG-1006, FIG. 3C

"The decryptor 325 accepts the OS nub's encrypted private key (i.e., protected) 204, and decrypts it using the OSNK 203, exposing the private key 328 for use in the isolated environment. The signature generator 320 generates a signature 304 for the subset 230 using the private key 328." SAMSUNG-1006,

11:1-30. "The signature algorithm used by the signature generator 320 may be public-key digital signature algorithm which makes use of a secret private key to generate the signature, and a public key to verify the signature." SAMSUNG-1006, 11:1-30; SAMSUNG-1003, ¶[60].

2. Muir

Muir is directed to providing data security in computer systems and electronic devices. SAMSUNG-1008, pg. 1-¶1. As shown in Muir's FIG. 5 (reproduced below), Muir discloses an example computer system and network in which a transaction, e.g., a financial transaction for e-commerce, can be performed between different electronic devices. SAMSUNG-1008, pp. 9-¶2, 11-¶3, 1-¶2; SAMSUNG-1003, ¶[61].

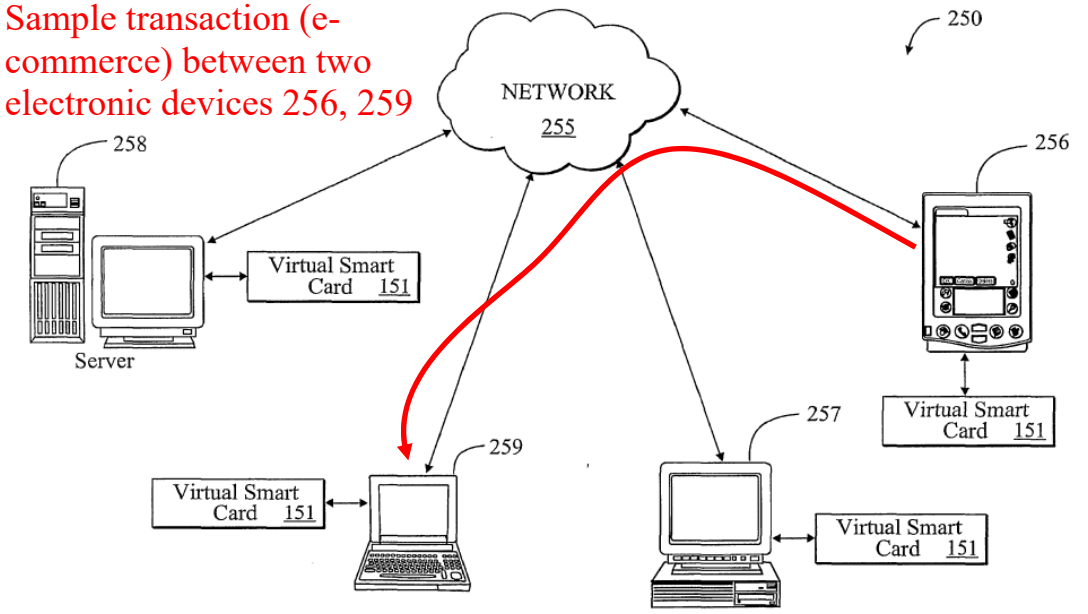


Fig. 5

SAMSUNG-1008, FIG. 5

Communication medium 255 connects computing devices (e.g., server 258, laptop computer 259, personal computer 257, [ ] personal data assistant 256, cellular phone) with virtual smart cards 151. SAMSUNG-1008, pp. 11-¶3, 8-¶1. "[A] user of personal data assistant 256 may send a user of laptop computer 259 a digital signature using private key 167 stored in virtual smart card 151 of personal data assistant 256. Similarly, other devices may use the virtual smart card 151 for similar functions." SAMSUNG-1008, pg. 12-¶1; SAMSUNG-1003, ¶[62].

The *virtual* smart card 151 in the computing devices "provides software code, which upon execution, emulates a physical smart card for device operating system 150." SAMSUNG-1008, pg. 7-¶4. The *virtual* smart card 151 includes a "restricted memory space 170 used for storing private keys 167. Restricted memory space 170 and private key 167 are normally inaccessible to operating system 125." SAMSUNG-1008, FIG. 3, pg. 7-¶4. The private key 167 is stored in a restricted memory space 170 to avoid the private key 167 from being exposed to the operating system 125 or an unauthorized user, which was a problem in earlier systems. SAMSUNG-1008, pp. 3-¶3, 7-¶1. The private key 167 may be used to generate a digital signature and sent to another device. SAMSUNG-1008, pp. 9-¶5-10-¶2, 11-¶1; SAMSUNG-1003, ¶[63].

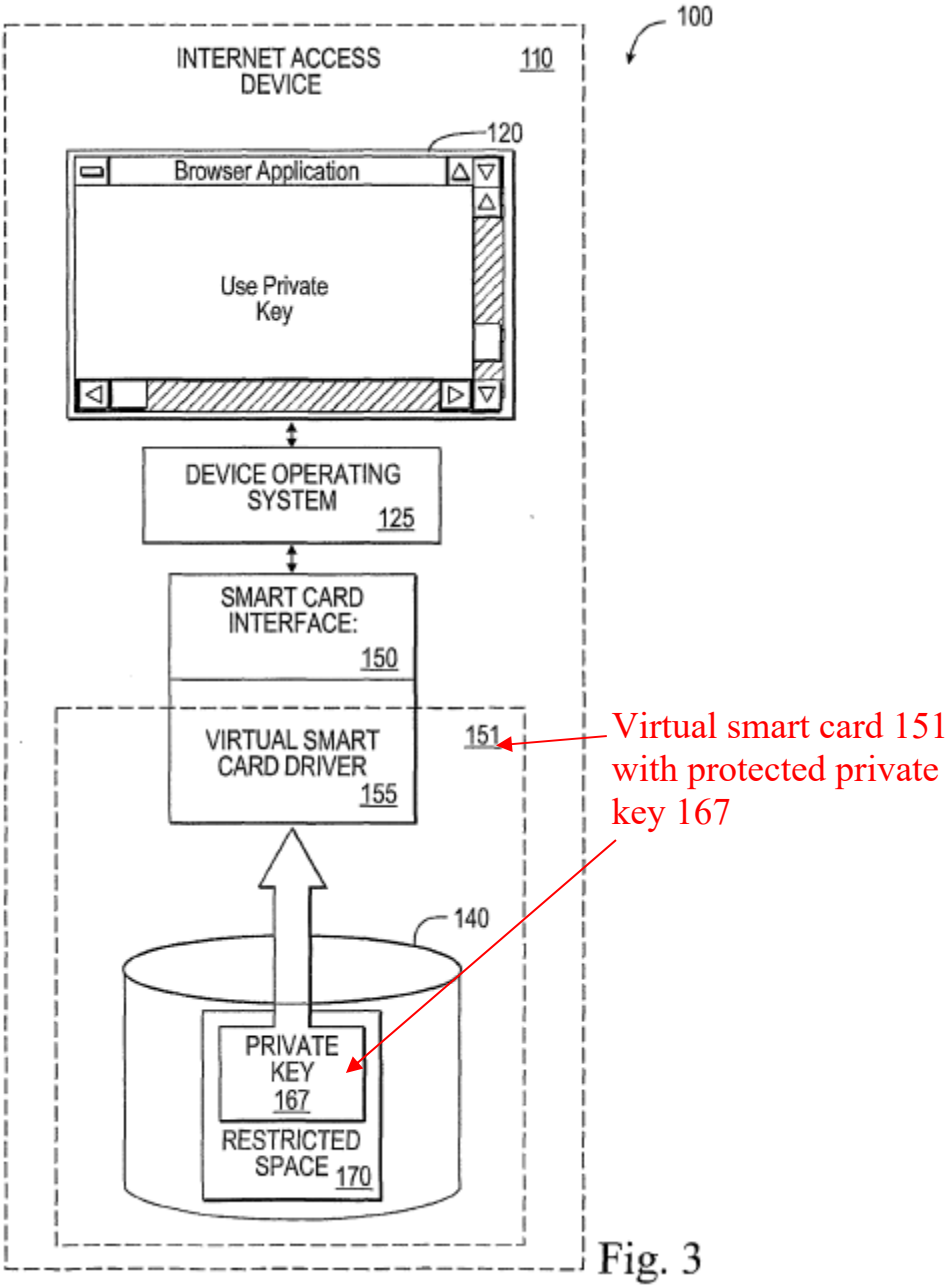


Fig. 3

SAMSUNG-1008, FIG. 3

3. Combination of Ellison and Muir

Ellison discloses an isolated execution architecture that improves security in a computer system or platform by implementing several levels of hierarchy and

normal and isolation execution modes for the operating system and processor. SAMSUNG-1006, 1:12-15, 2:40-61, Abstract, FIG. 1. Ellison's isolated execution architecture can be applied to systems involving "[e]lectronic commerce (E-commerce) and business-to-business (B2B) transactions," which were previously "[v]ulnerable to unscrupulous attacks" such as "intrusion, security breach, and tampering." SAMSUNG-1006, 1:17-30. Earlier systems and work environments, such as systems involving security co-processors or smart cards using cryptographic or other security techniques, had limitations and drawbacks "in speed performance, memory capacity, and flexibility." SAMSUNG-1006, 1:38-51. Because Ellison's isolated execution architecture provides a solution to such limitations and drawbacks, a POSITA would have applied Ellison's isolated execution architecture to such systems, e.g., systems involved in e-commerce or B2B transactions or smart cards using cryptography. SAMSUNG-1003, ¶[64]. However, Ellison does not reveal details of such a system or transaction between multiple parties. Muir does.

As noted above in Section IV.A.2, Muir discloses a computer network with multiple devices involved in electronic transactions, e.g., e-commerce. SAMSUNG-1008, pp. 9-¶2, 11-¶3, 1-¶2. In Muir's computer network, devices (e.g., server 258, laptop computer 259, personal computer 257, PDA 256, or cellular phone) are configured to perform secure transactions. SAMSUNG-1008,

pp. 11-¶3, 8-¶1. Muir's virtual smart cards 151 include a restricted memory space 170 to store a private key 167 and for performing operations such as encryption of data or generation of a digital signature using the private key. SAMSUNG-1008, pp. 9-¶3, 2-¶1, 3-¶¶1-2, 6-¶3, 10-¶¶1-2, 12-¶1, 18-¶6, FIG. 3; SAMSUNG-1003, ¶[65].

A POSITA looking to implement Ellison's isolated execution architecture in a computer system with multiple devices would have looked to Muir's teachings to implement a secure electronic transaction between two parties. SAMSUNG-1003, ¶[66]. The combination would have been obvious, predictable, and a POSITA would have had a reasonable expectation of success in implementing the combination because both Ellison and Muir are related to providing improved security for transactions involving keys using cryptographic techniques. SAMSUNG-1006, 1:38-51; SAMSUNG-1008, pp. 11-¶3, 8-¶1, 7-¶4; SAMSUNG-1003, ¶[66].

In the combination of Ellison and Muir (hereinafter "**EMC**"), each device involved in a transaction would have been connected through a computer network, such as Muir's network shown in FIG. 5. The individual devices would have included Ellison's isolated execution architecture and one or more parts of Muir's system (e.g., a restricted memory space for storing the private key and performing cryptographic operations such as encryption). When utilized in a transaction

involving smart cards, such a combination would also have improved speed performance, flexibility, and reduced costs by eliminating the need for additional hardware, such as physical smart cards coupled to the computing devices and use Muir's *virtual* smart card instead. SAMSUNG-1006, 1:38-51; SAMSUNG-1008, pp. 4-¶¶3-4, 6-¶5; SAMSUNG-1003, ¶[67].

To complete the transaction between the two devices, a digital signature generated using a private key associated with one (transmitting) party and optionally along with encrypted data would have been sent to the other (receiving) party in a transaction to securely transmit data and allow the receiving party to decrypt the data and verify the identity of the transmitting party. SAMSUNG-1008, pp. 9-¶3, 2-¶1, 3-¶¶1-2, 6-¶3, 10-¶¶1-2, 12-¶1, 18-¶6; SAMSUNG-1003, ¶[68].

As Dr. Black explains, a POSITA would have viewed extension of Ellison's system to include the multi-party transactions described by Muir to have been a natural and obvious extension. Indeed, Muir itself describes the benefits of secure multi-party transactions (*see*, *e.g.*, SAMSUNG-1008, pp. 4-¶¶3-4, 6-¶5) and a POSITA would have been motivated to enable such multi-party transactions (e.g., e-commerce transactions) in Ellison's system to increase the functionality and usefulness of Ellison's system. SAMSUNG-1003, ¶[69]. In extending Ellison's functionality to include secure multi-party transactions, as described in Muir, a

POSITA would have retained the benefits of Ellison's security functionality (e.g., the isolated execution environment and key-based encryption) because such functionality remains valuable to secure operation of Ellison's system and complements the security of the multi-party transactions described by Muir. SAMSUNG-1003, ¶[69].

In fact, Ellison itself alludes to use of its system in e-commerce and B2B transactions. *See* SAMSUNG-1006, 1:17-30. From this description, a POSITA would have envisioned use of Ellison's system in multi-party e-commerce or business transactions, although Ellison does not explicitly describe details of multi-party transactions. SAMSUNG-1003, ¶[70]. Given the lack of details in Ellison, a POSITA would have been motivated to look to other references that describe e-commerce and business transactions, such as Muir, and would have found it obvious to apply the details of those transactions (e.g., Muir's multi-party transactions) to Ellison. *Id*. Indeed, as Dr. Black explains, a POSITA would have seen addition of multi-party transactions to Ellison's system as use of a known technique (e.g., as disclosed by Muir) to improve similar devices (the Ellison and Muir secure processing systems) in the same way. *Id*.

For at least the foregoing reasons, a POSITA would have combined the teachings of Ellison and Muir and would have had a reasonable expectation of success. SAMSUNG-1003, ¶[71]. Indeed, the combination would have simply

involved combining prior art elements (Muir's computer system with restricted memory space and secure cryptographic operations) according to known methods (Ellison's isolated execution architecture) to yield the predictable result of performing electronic transactions securely between two parties. *Id*.

4. Manner in which the Prior Art Renders Claims 1, 3, 6, 11, and 14-19 Obvious

[1pre-1]

To the extent the preamble is limiting, EMC renders [1pre-1] obvious. SAMSUNG-1003, ¶[87]. As explained above in Sections IV.A.1-IV.A.3, EMC discloses a method to perform an electronic transaction (e.g., e-commerce) between two portable electronic devices associated with two transaction parties. SAMSUNG-1008, pp. 1-¶¶2-3, 11-¶3, 12-¶1, FIG. 5. EMC teaches that cryptographic systems and methods can be used to protect sensitive electronic data used in an e-commerce transaction ("***method for performing an electronic transaction***"). SAMSUNG-1008, pp. 9-¶2, 1-¶¶2-3, FIG. 5; SAMSUNG-1006, FIGS. 1A-1C, 2, 3C-3D, 3:9-4:56, 8:13-13:3. As shown below in Muir's FIG. 5, the transaction can be conducted ***between the electronic devices of two transaction parties*** (e.g., first and second transaction parties). SAMSUNG-1008, pp. 11-¶3, 12-¶1; SAMSUNG-1003, ¶[88]. The electronic devices may include, for example, cellular phones, personal data assistants, and smart cards. SAMSUNG-1008, pp. 11-¶3, 8-¶1, 1-¶¶2-3. Although two devices in FIG. 5 below have been labeled as

the transaction parties, other devices in FIG. 5 may also correspond to the transaction parties if involved in a transaction with each other. SAMSUNG-1003, ¶[88].

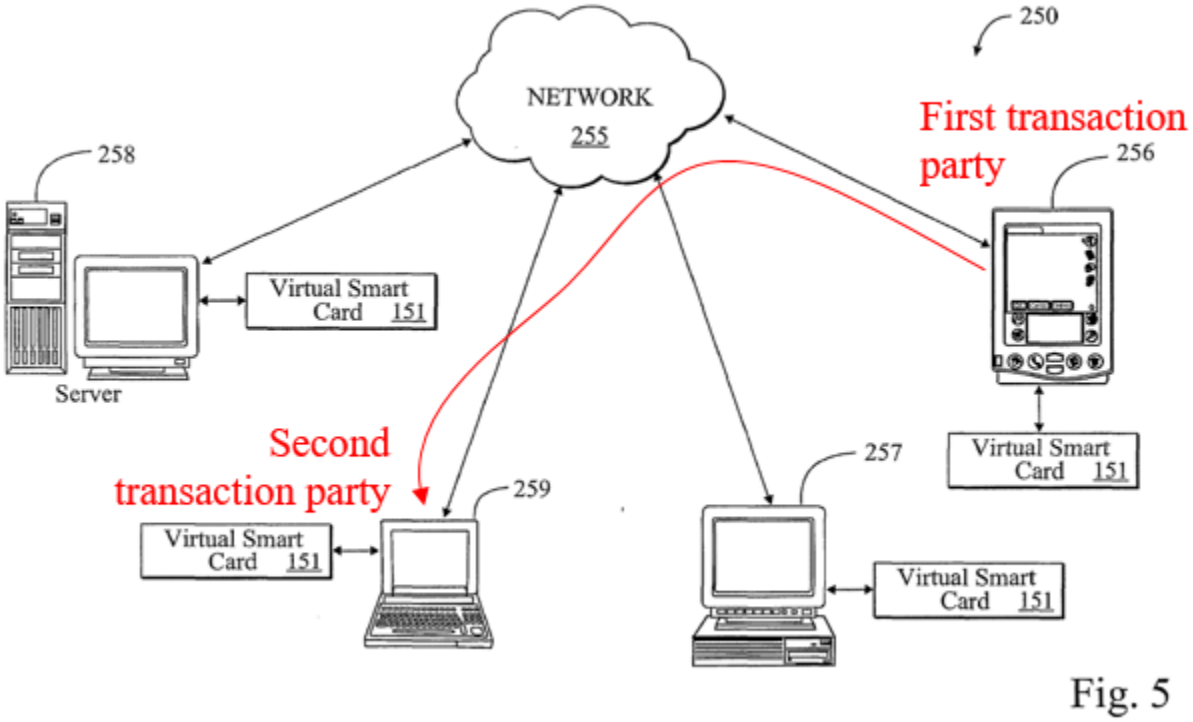


Fig. 5

SAMSUNG-1008, FIG. 5

[1pre-2]

As noted above in Section IV.A.3, in EMC, Ellison's "isolated execution architecture" would have been implemented in Muir's electronic devices including the electronic device of the first transaction party. Thus, an architecture similar to the one shown in Ellison's 615's FIGS. 1A-1C (reproduced below) would have been implemented in Muir's electronic device of the first transaction party.

SAMSUNG-1003, ¶[89].

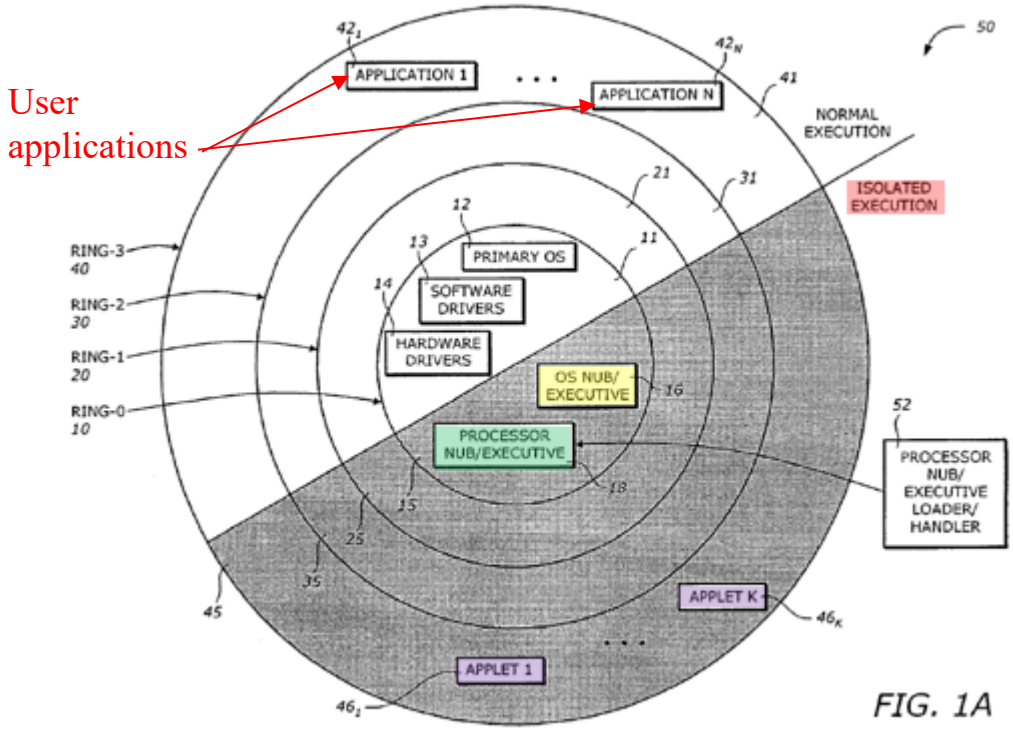


FIG. 1A

SAMSUNG-1006, FIG. 1A

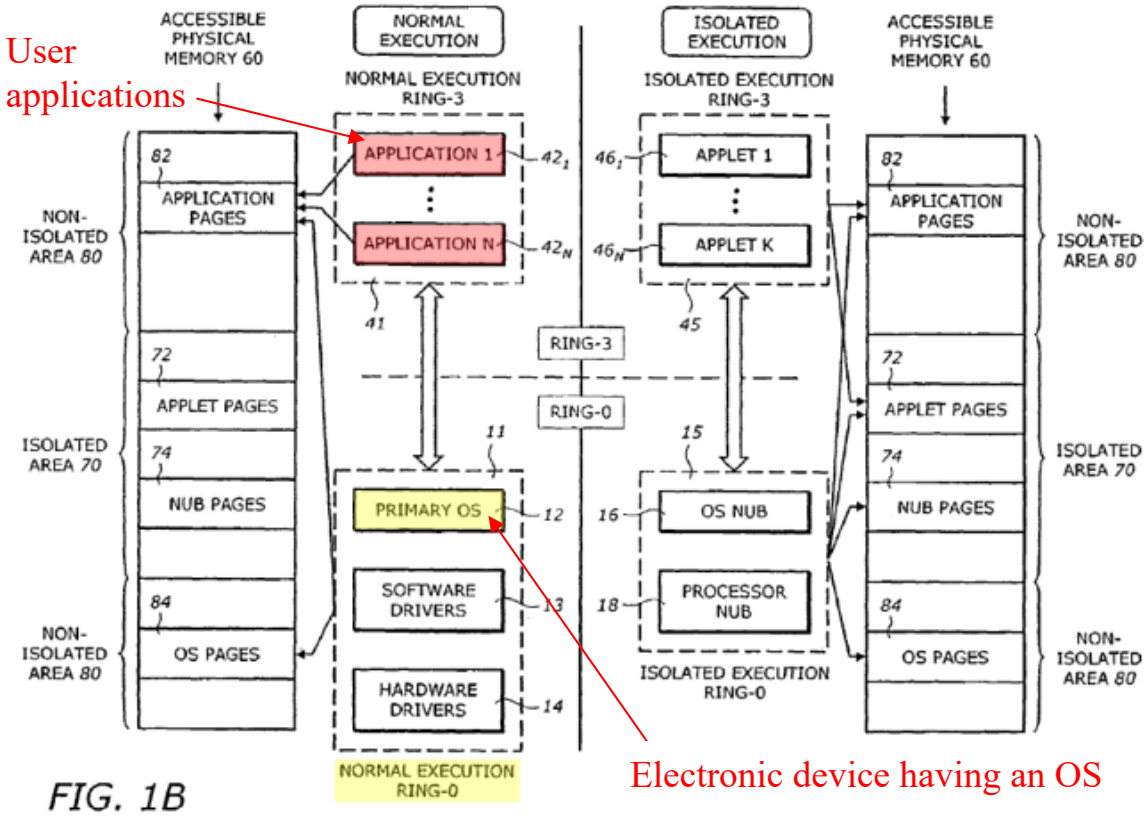


FIG. 1B

SAMSUNG-1006, FIG. 1B

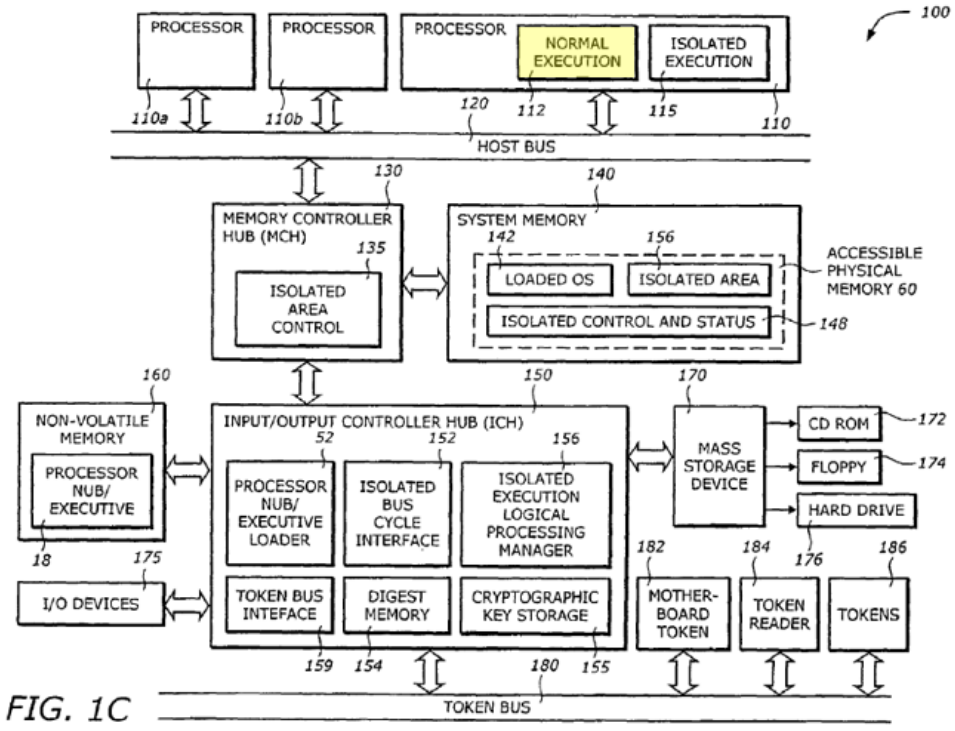


FIG. 1C

SAMSUNG-1006, FIG. 1C

FIGS. 1A and 1B depict ***a primary operating system (OS) 12 that creates a run-time environment for user applications, such as applications 42_1-42_N*** which can be executed in the normal execution mode and are isolated from components of the isolated execution rings. SAMSUNG-1006, 3:9-61, 4:1-29, 2:57-61. Applications 42_1-42_N are configured to operate in Ring-3, which "typically encompasses users or applications level and has the least privilege," and would therefore be understood by a POSITA as encompassing user applications. SAMSUNG-1006, 2:57-61; SAMSUNG-1003, ¶[90]. OS 12 operates in the normal execution mode 112 and may be executed by processor 110. SAMSUNG-1006, 4:23-29, 4:57-5:27, FIGS. 1A, 1C. Thus, in EMC, an electronic device associated with the first transaction party would have an OS 12 that creates a run-time environment for applications 42_1-42_N. SAMSUNG-1003, ¶[90].

[1a]

As explained above in Section IV.A.1, Ellison's isolation execution architecture includes an isolated execution region (*see* FIG. 1A below) in which entities such as OS nub 16 and processor nub 18 operate in a secure environment in an isolated execution mode. SAMSUNG-1006, 3:9-25, 2:41-61, FIG. 1B; SAMSUNG-1003, ¶[91].

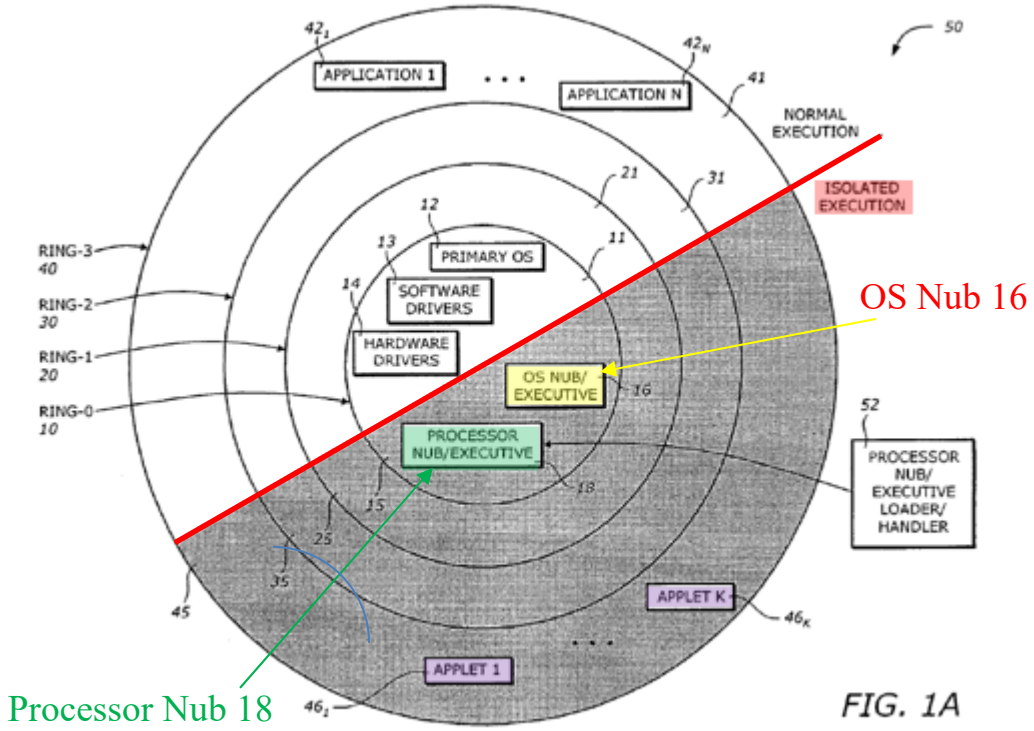


FIG. 1A

SAMSUNG-1006, FIG. 1A

Ellison explains that the isolated execution region "is ***accessible only to elements of the operating system and processor operating in isolated execution mode***" and that isolated mode applets 46_1 to 46_K and their data are tamper-resistant and monitor-resistant from all software attacks from other applets and OS 12. SAMSUNG-1006, 4:1-22. ***A user*** is not an element of the operating system and processor operating in isolated execution mode, and therefore ***cannot access elements within the isolated execution region***. SAMSUNG-1003, ¶[92]. The

isolated execution region is protected by the processor and chipset in the computer system, and access to the isolated region is possible only through isolated read and write cycles which are issued by a processor executing in an isolated execution mode. SAMSUNG-1006, 3:32-49. Effectively, the isolated execution mode and region are protected from user tampering and software outside of the isolated execution region. SAMSUNG-1003, ¶[92].

"One task of [a] processor nub 18 is to verify and load the ring-0 OS nub 16 into the isolated area, and to generate the root of a key hierarchy unique to a combination of the platform, the processor nub 18, and the operating system nub 16." SAMSUNG-1006, 3:46-55. "***The isolated area 70 is accessible only to elements of the operating system and processor operating in isolated execution mode***." SAMSUNG-1006, 4:19-23. Thus, processors and OSs not operating in the isolated execution mode (e.g., OSs that can be interfered with by users) cannot interfere or access elements operating in the isolated execution mode, such as OS nub 68 and processor nub 18. SAMSUNG-1003, ¶[93].

The OS nub 16 has access to a ***protected private key 204*** that "can be stored in the multiple key storage … ***of the non-volatile flash memory 160***" and can be "programmed into the fuses of a ***cryptographic key storage 155*** of the ICH 150 or elsewhere in persistent storage within platform 200." SAMSUNG-1006, 8:33-65, FIG. 1C (reproduced below); SAMSUNG-1003, ¶[94].

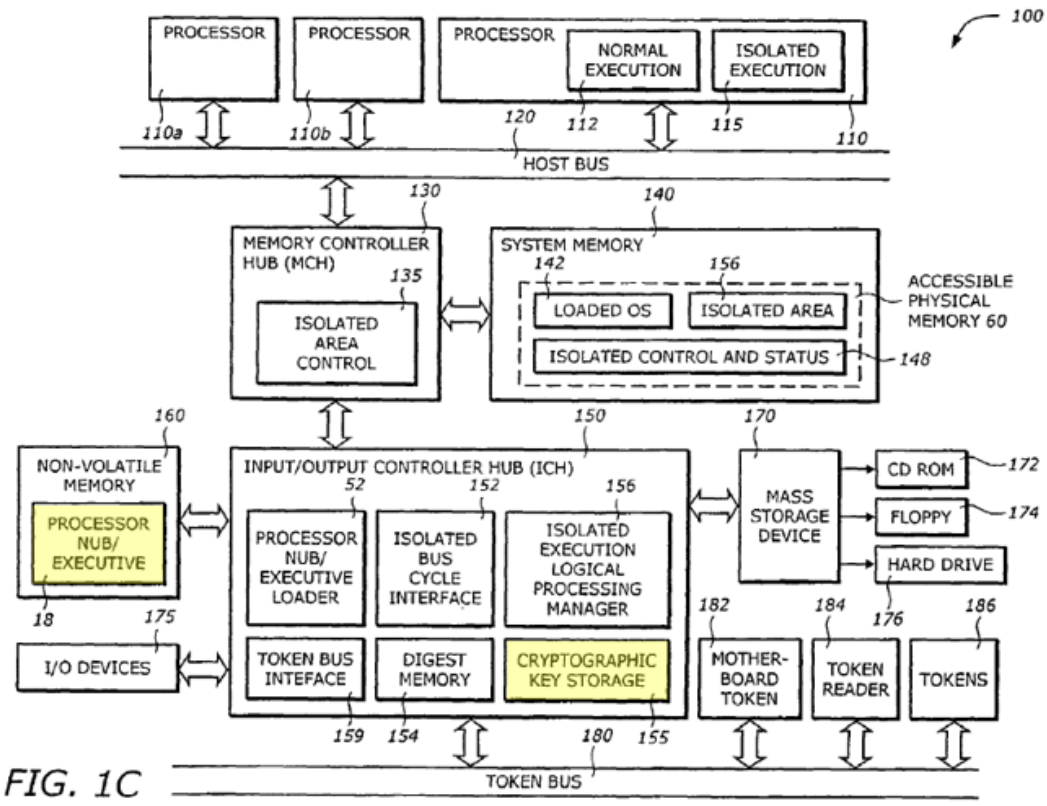


FIG. 1C

SAMSUNG-1006, FIG. 1C

Platform 200 is depicted in FIG. 2 below and is described as a ***secure platform*** 200 that "includes the OS nub 16, the processor nub 18, a key generator 240, a hashing function 220, and a usage protector 250, ***all operating within the isolated execution environment***." SAMSUNG-1006, 8:25-32; SAMSUNG-1003, ¶[95].

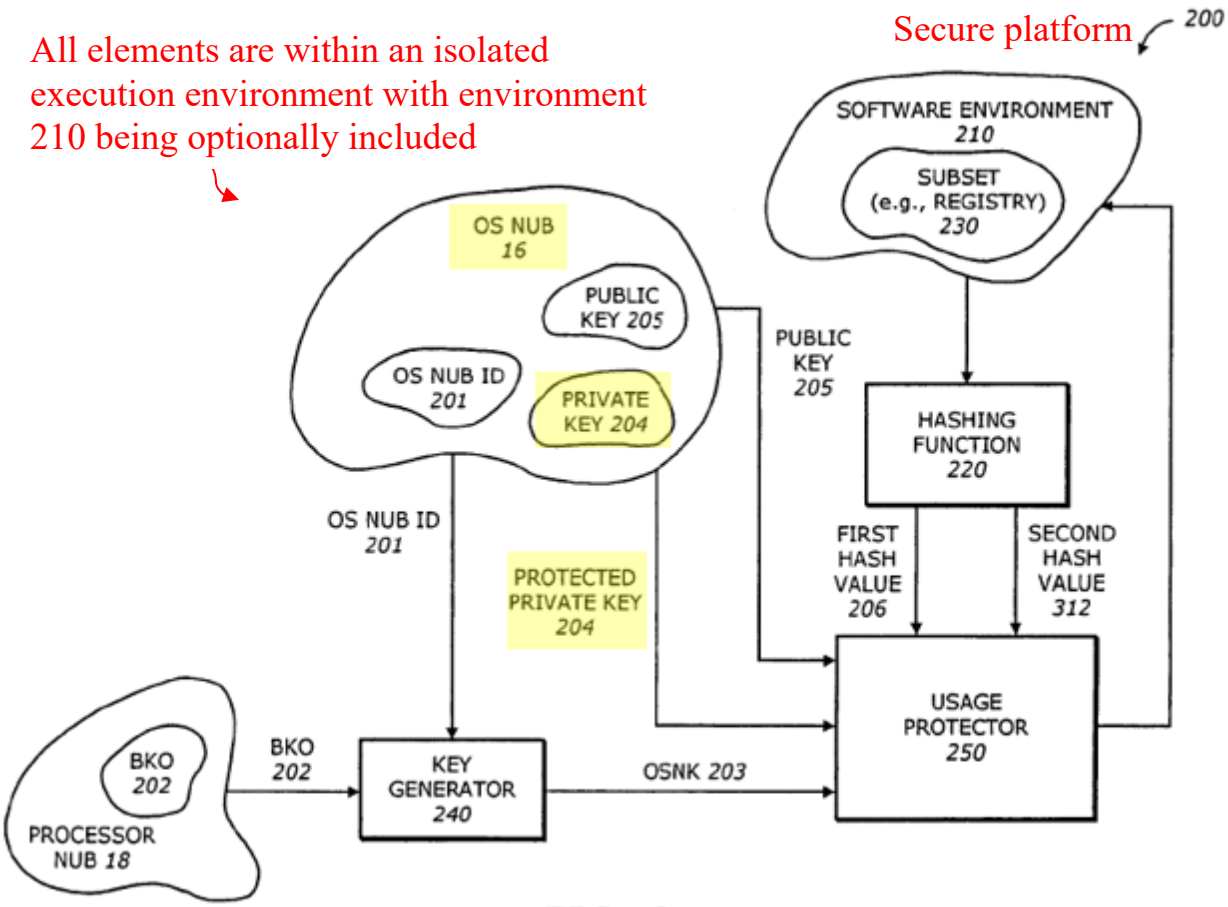


FIG. 2

SAMSUNG-1006, FIG. 2

As noted above, the private key 204 can be stored in the cryptographic key storage 155 and in a multiple key storage of the non-volatile flash memory 160. SAMSUNG-1006, 8:33-65. Moreover, "***[o]nly the OS nub 16 can retrieve and decrypt the encrypted private key*** for subsequent use." *Id*. Because only the OS nub 16 can retrieve the private key and the OS nub 16 is within the secure platform and isolated environment, it would have been obvious to a POSITA that the cryptographic key storage 155 and the non-volatile flash memory 160 are secure

storage locations so that the private key 204 can be accessed securely by OS nub 16 at an area within non-volatile memory 160 that is inaccessible by the normal OS or the user of the device. SAMSUNG-1003, ¶[96]; *see also infra* [1e]. Ellison explicitly teaches that the OS nub 16 and private key 204 shown in platform 200 all ***operate within the isolated execution environment***, which would indicate to a POSITA that private key 204 is stored in a secure memory and is inaccessible to a user of said electronic device. SAMSUNG-1003, ¶[96]. Indeed, since a private key is an important element for maintaining security in a cryptographic process or more generally a secure electronic transaction, it would have been obvious to a POSITA to store the ***private key 204 in a secure memory location that is inaccessible to a user***. *Id*. This obviousness is reinforced by the OS nub 16 and processor nub 18 being located in isolated execution Ring-0 15, which encompasses the most critical and highest degree of privilege—in contrast to Ring-3 which ***provides user level*** privilege. SAMSUNG-1006, 3:9-4:22, 2:45-61; *see supra* Section IV.A.1; SAMSUNG-1003, ¶[96].

To the extent Patent Owner contends that Ellison does not store the private key 204 in a secure memory location, EMC also renders this feature obvious in view of Muir's disclosure, which explicitly teaches ***a private key 167 being stored in a restricted memory space 170 which is inaccessible to the operating system***. SAMSUNG-1008, pp. 7-¶1, 8-¶4, 9-¶3, 3-¶3. Since Muir's restricted memory

space 170 can store a plurality of private keys and is not accessible to the operating system to maintain security of the private keys, it would have been obvious to a POSITA that the restricted memory space 170 is not accessible to the user. SAMSUNG-1003, ¶[97]. Moreover, given the use of private key 204 by an OS nub 16 that operates within the isolated execution environment in the EMC system, it would have been obvious to a POSITA to provide Ellison's private key 204 in a secure memory location (as revealed by Muir) and that the private key would have been inaccessible to a user of the electronic device. *Id*.

[1b]

As noted above in [1a], ***the encrypted/protected private key 204 is stored at a secure location in multiple key storage*** of non-volatile flash memory 160, programmed into the cryptographic key storage 155, or another secure storage within secure platform 200 (e.g., Muir's restricted memory space 170). SAMSUNG-1006, 8:33-65; SAMSUNG-1008, pp. 7-¶1, 8-¶4, 9-¶3. OS nub 16 retrieves the encrypted private key 204 and decrypts it for use in the isolated environment. SAMSUNG-1006, 8:33-65, 11:1-12:26. An example of this decryption is shown in Ellison's FIGS. 3C and 3D (reproduced below), which show decryptor 325 decrypting an encrypted private key 204 using an operating system nub key (OSNK) 203, and thereby yielding an unencrypted private key

328. *Id.*; SAMSUNG-1003, ¶[98].

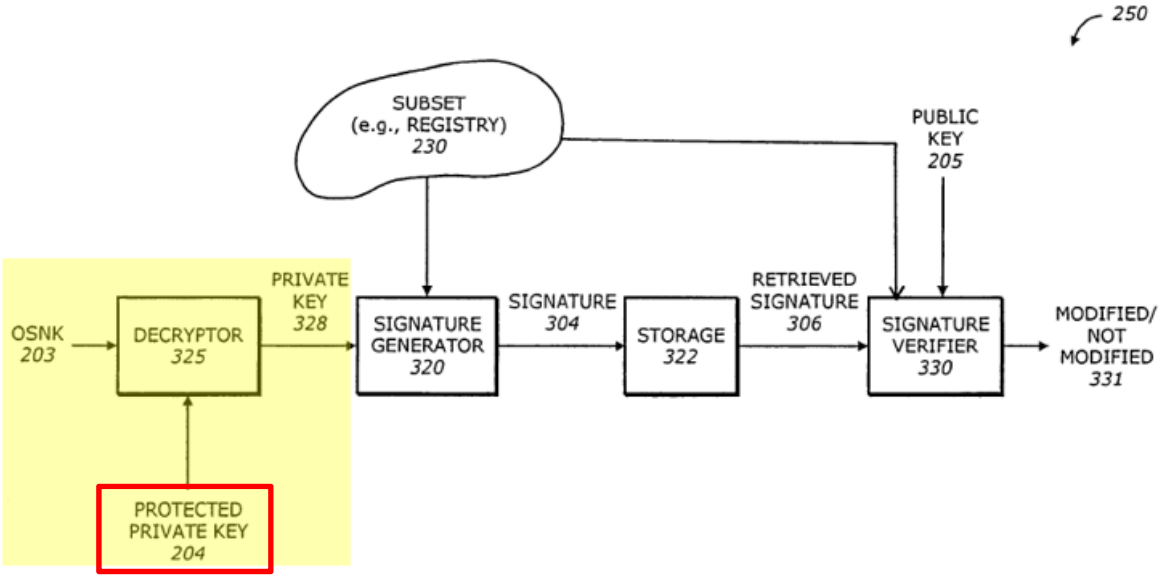


FIG. 3C

SAMSUNG-1006, FIG. 3C

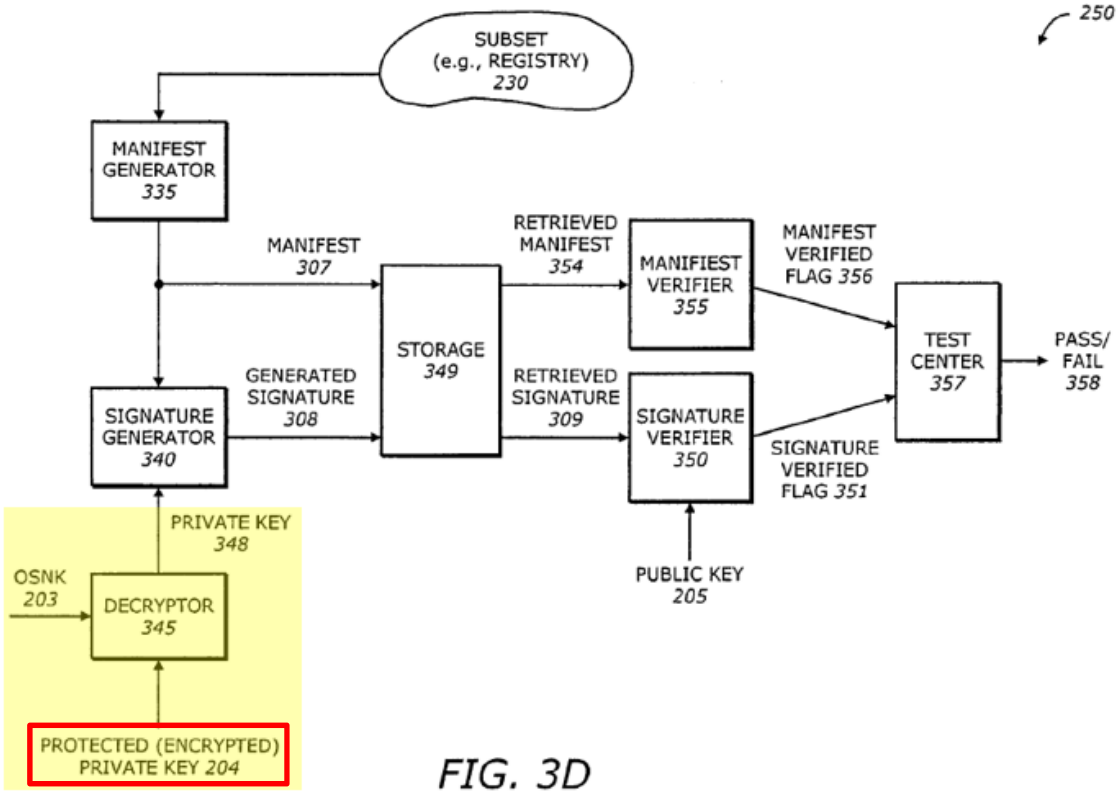


FIG. 3D

SAMSUNG-1006, FIG. 3D

Accordingly, Ellison and Muir render obvious ***the private key 204 being encrypted when stored in a secure memory (e.g., memory 160 or Muir's restricted memory space 170)*** and obtained therefrom by OS nub 16. SAMSUNG-1003, ¶[99]; *see also supra* [1a].

[1c]

As noted above in [1b], the ***OSNK 203 is used as a decryption key for decrypting the private key 204***. SAMSUNG-1006, 8:33-65, 11:1-30, FIG. 3C. The ***OSNK 203 is incorporated in the electronic device of the first transaction party***. For example, the OSNK 203 is generated by the key generator 240, which is part of the isolated execution environment in the electronic device of the first transaction party. SAMSUNG-1006, 8:25-32, 9:1-14, FIG. 2 (reproduced below). As explained above in [1a], the private key also is incorporated in the electronic device. SAMSUNG-1003, ¶[100].

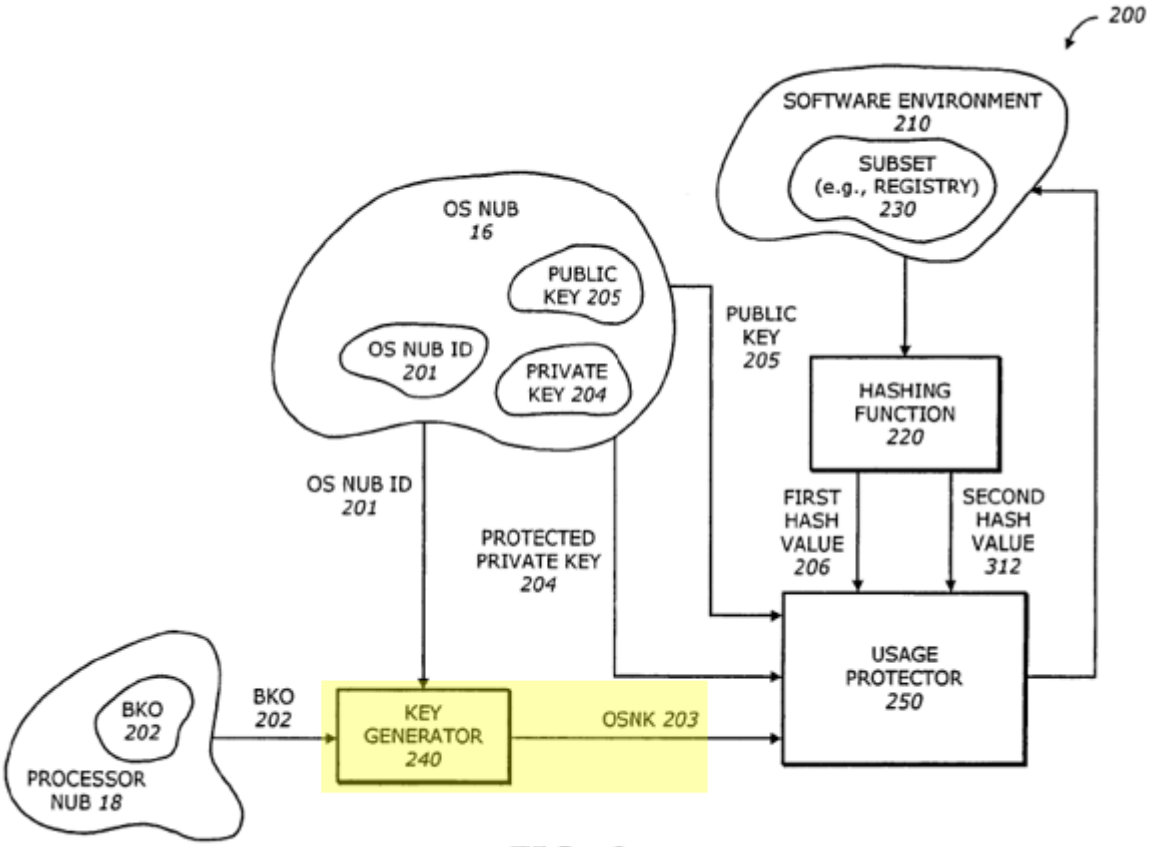


FIG. 2

SAMSUNG-1006, FIG. 2

[1d]

As described above in [1a]-[1c], the OSNK 203 ("***decryption key***") is generated and used within the ***isolated environment region, which is not accessible to a user, any user-operated software, and the operating system (OS) 12*** of the electronic device in the normal execution mode. SAMSUNG-1006, 8:25-65, 11:1-12:26, 9:1-14, FIGS. 2, 3C, 3D. As Dr. Black explains, to prevent a user or malicious software controlling one or more operations of the operating system

from corrupting sensitive or personal data that needs to be protected, such as the OSNK 203 or private key, Ellison's system architecture provides the isolated environment region in which the usage protector 250, key generator 240, and nubs 16 and 18 can execute their operations in a secure environment that is free from interference and access of the user, user-operated software, or OS 12. SAMSUNG-1003, ¶[101]. Ellison explicitly discloses that OSNK 203 "is provided only to the OS Nub 16," which may further "supply the OSNK 203 ***to trusted agents, such as the usage protector 250***." SAMSUNG-1006, 9:1-14. Ellison teaches that the OS nub 16 and the processor nub 18 operate in a secure environment associated with the isolated area 70 and the isolated execution mode" and are present in Ring-0 10 of the isolated execution environment, which has the least amount of privileges. SAMSUNG-1006, 3:9-25, 4:8-22, FIG. 1A. Moreover, the key generator 240 and usage protector 250, which generate and use the OSNK 203, are each described as being part of the isolated execution environment in secure platform 200. SAMSUNG-1006, 8:12-32. Accordingly, and as explained above in [1a], a POSITA would have understood that the isolated execution region is inaccessible to the user, any user-operated software, and OS 12. SAMSUNG-1003, ¶[101]. Indeed, as shown in Ellison's FIG. 1A, the isolated execution portion of the operating architecture 50 contrasts with the normal execution portion in which OS 12 resides as an unprotected OS, and supports user-accessible

applications 42_1-42_N. SAMSUNG-1006, 3:55-56, 3:9-31. SAMSUNG-1003, ¶[101].

[1e]

See supra [1a], [1pre-2]. For example, OS 12 is in Ring-0 11 of the normal execution region of architecture 50 and does not access components of the isolated execution region, as explained above in [1a] and [1d]. SAMSUNG-1006, 3:9-4:29, FIG. 1A. The cryptographic key storage 155 is configured to store cryptographic keys, and is part of the ICH 150, which operates in the isolated execution mode. SAMSUNG-1006, 6:64-67, 6:27-43, 4:8-37. Non-volatile flash memory 160 is coupled to the ICH 150 and includes the processor nub 18, which also operates in the isolated execution mode (*see* FIGS. 1A, 1B, 1C). SAMSUNG-1006, 7:19-22. Accordingly, because cryptographic key storage 155 and memory 160 operate in the isolated execution mode, it would have been obvious to a POSITA that the cryptographic key storage 155 and the non-volatile flash memory 160 are secure storage locations that are inaccessible to the OS 12 and thereby the user. SAMSUNG-1003, ¶[102]. As explained above, the protected private key 204 "can be stored in the multiple key storage … of the non-volatile flash memory 160" and can be "programmed into the fuses of a cryptographic key storage 155 of the ICH 150 or elsewhere in persistent storage within platform 200." SAMSUNG-1006,

8:33-65, FIG. 1C. Therefore, a POSITA would also have found it obvious that the private key is inaccessible to the user. SAMSUNG-1003, ¶[102].

[1f]

As noted in [1a]-[1d], Ellison's private key 204 is decrypted using the decryption key, OSNK 203, in the isolated execution environment of secure platform 200 that is inaccessible to a user or user-operated software. SAMSUNG-1006, 8:33-65, 11:1-30, FIG. 3C; SAMSUNG-1003, ¶[103].

[1g]

Ellison's isolation execution architecture ***provides authentication software in the electronic device in the form of the usage protector 250***, which is part of the secure platform 200 in the electronic device (e.g., Muir's device 256 in EMC) associated with the first transaction party and operates within the isolated execution environment. SAMSUNG-1006, 8:25-32, FIG. 2 (reproduced below); SAMSUNG-1003, ¶[104].

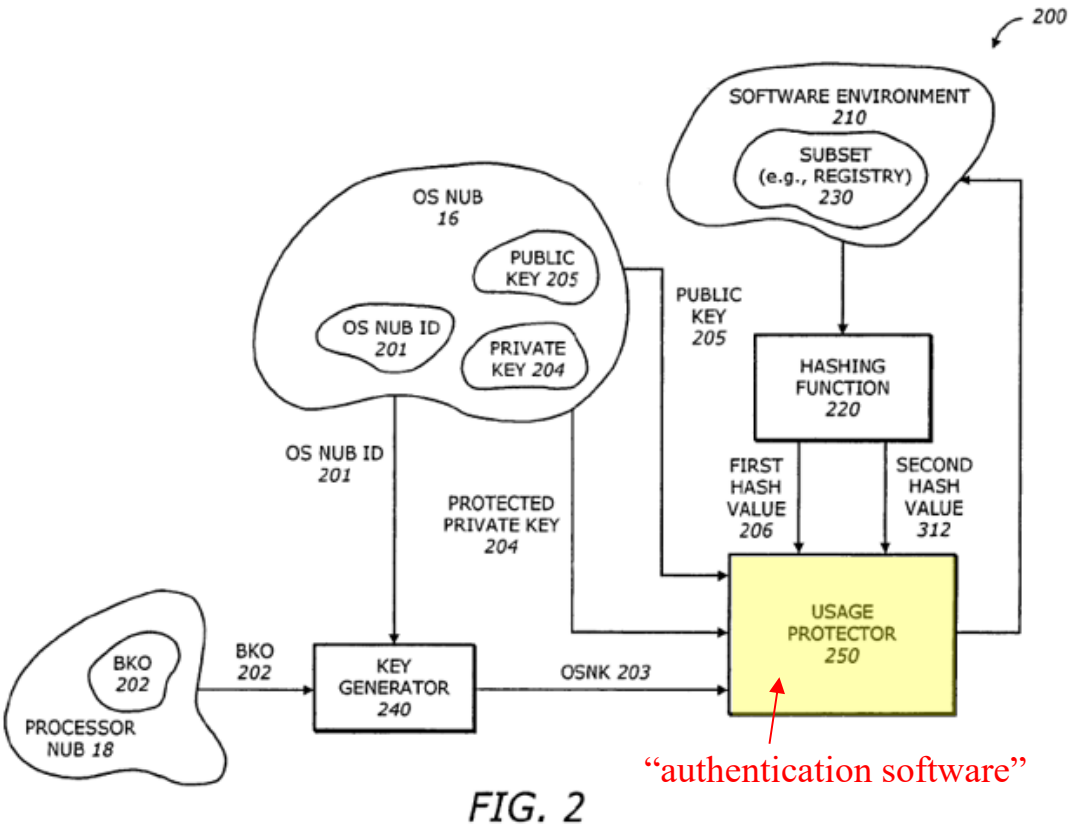


FIG. 2

SAMSUNG-1006, FIG. 2

One example, among several authentication operations of the usage protector 250, is that the usage protector 250 compares a first hash value 206 and a second hash value 312 after a time period to authenticate subset 230 and detect intrusion or modification of the subset 230. SAMSUNG-1006, 9:40-58. FIGS. 3A-3E depict various other implementations of the usage protector 250 and its operations (that also include authentication operations). SAMSUNG-1006, 10:4-13:3; SAMSUNG-1003, ¶[105].

[1h]

As explained above in [1a] and [1b] and shown clearly in Ellison's FIG. 2, private key 204 is accessible to the usage protector 250 ("***authentication software***"). SAMSUNG-1006, 10:1-3, 10:63-12:26, 8:40-65; SAMSUNG-1003, ¶[106].

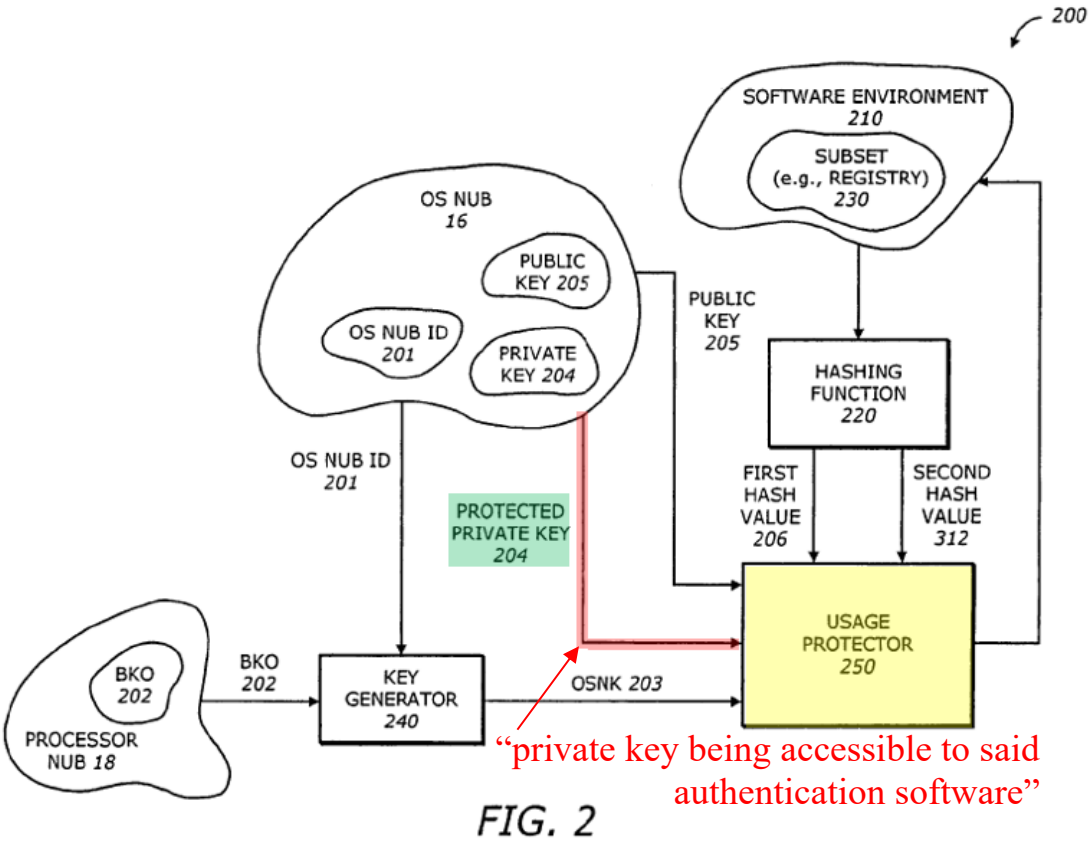


FIG. 2

SAMSUNG-1006, FIG. 2

FIGS. 3C and 3D are two example implementations of the usage protector 250 that show the private key 204 being accessible to the usage protector 250 and used for decryption purposes. SAMSUNG-1006, 10:63-12:26; SAMSUNG-1003, ¶[107].

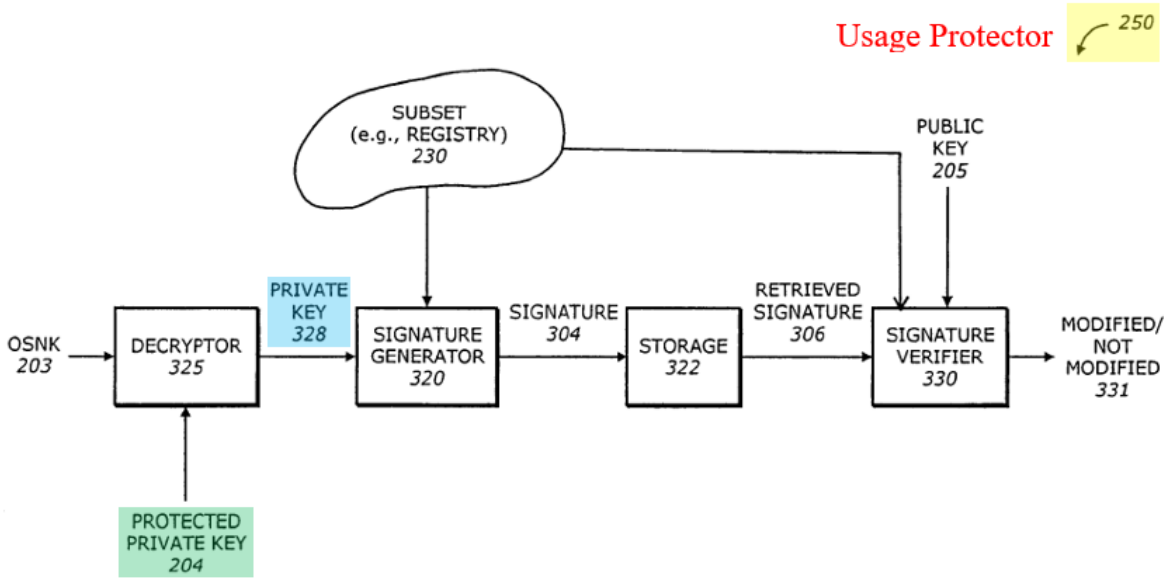


FIG. 3C

SAMSUNG-1006, FIG. 3C

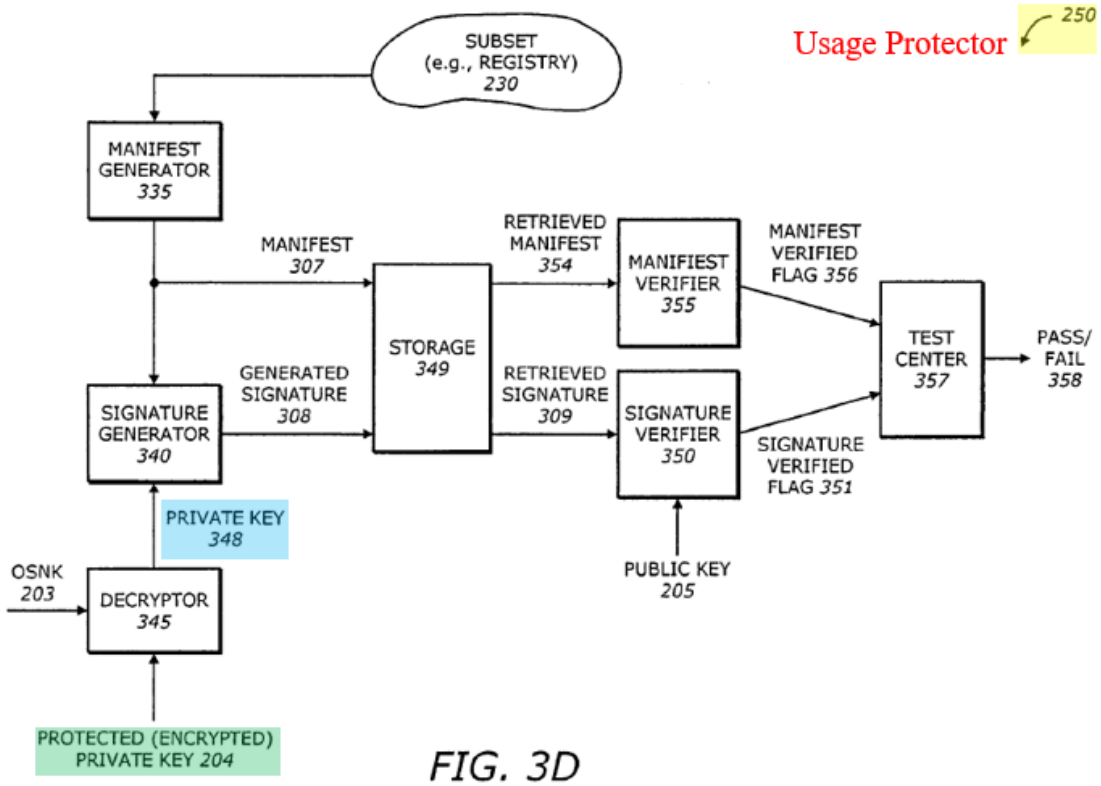


FIG. 3D

SAMSUNG-1006, FIG. 3D

[1i]

As explained above in [1a]-[1d], the ***usage protector 250 ("authentication software")*** is located in a ***secure*** platform 200 and ***operates within the isolated execution environment (****note:* the location of the usage protector 250 can be contrasted with the software environment 200, which Ellison explains can be inside or outside the isolated execution environment). SAMSUNG-1006, 8:25-32. The ***usage protector 250 is a trusted agent***. SAMSUNG-1006, 9:2-8; SAMSUNG-1003, ¶[108]. Furthermore, Ellison explains that the operating system (OS) nub 16 and processor nub 18 are located in Ring-0 15 of the isolated execution environment, and are operated in a secure environment associated with isolated area 70." SAMSUNG-1006, 3:15-25. "The isolated area 70 is accessible only to elements of the operating system and processor operating in isolated execution mode." SAMSUNG-1006, 4:19-22.

Based on the foregoing descriptions of the usage protector 250, the isolated execution mode, and the secure environment, it would have been obvious to a POSITA that the usage protector 250 would have been stored in secure memory (e.g., isolated area) inaccessible to elements outside of the isolated execution environment such as OS 12. SAMSUNG-1003, ¶[109]. And even if the usage protector 250 is loaded from another memory into the isolated execution environment, code for executing the usage protector 250 while in the isolated

execution environment would have been stored in a secure memory so as to prevent unauthorized access of sensitive data. SAMSUNG-1003, ¶[109]. For example, various implementations of the usage protector 250 shown in FIGS. 3A-3E include operations involving encryption and decryption using a private key. SAMSUNG-1006, 10:4-13:3. It would have been obvious to a POSITA that, to perform encryption and decryption using a private key—operations for which a high level of security are vital—all or at least the authentication portion of the usage protector 250 and its operational software/code would have been stored in a secure memory of the isolated execution environment such as isolated area 70. SAMSUNG-1003, ¶[109].

[1j]

Ellison's FIG. 3C (reproduced below) depicts an illustration of the usage protector 250 in which ***the signature generator 320 generates a digital signature*** 304 for the subset 230 ***using private key 328***, which is a decrypted version of encrypted private key 204. SAMSUNG-1006, 10:63-11:30, 8:55-65; SAMSUNG-1003, ¶[110].

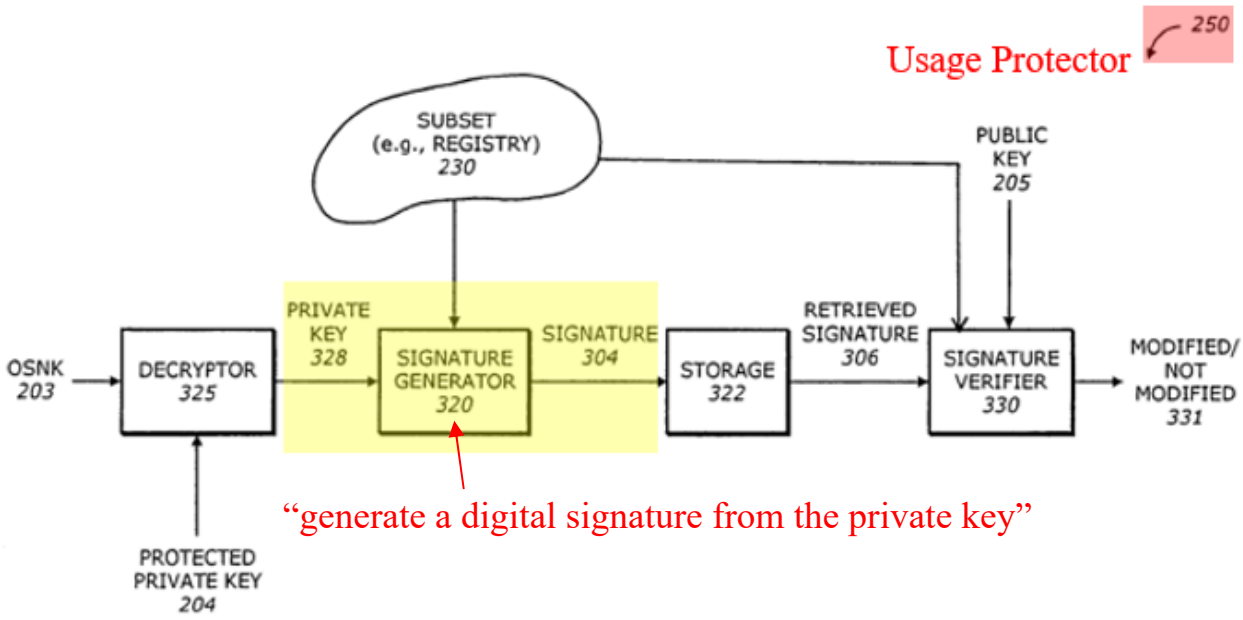


FIG. 3C

SAMSUNG-1006, FIG. 3C

[1k]

As noted above in Sections IV.A.1, [1pre-2], [1a]-[1d], and [1i], the usage protector 250 is run in an isolated environment ("***secure processing environment***") that is not accessible to the OS 12 ("***said operating system***"). SAMSUNG-1006, 3:9-61, 4:1-29, 4:57-5:27, FIGS. 1A, 1B; SAMSUNG-1003, ¶[111].

[1l]

After the digital signature 304 is generated (as described above in [1j]), Muir teaches that the ***generated digital signature is provided to another user ("second transaction party")*** connected in the networking environment to the computer system 20 to allow the other user "to determine the identity" of the first transaction

party. SAMSUNG-1008, pp. 9-¶3, 2-¶1, 3-¶¶1-2, 6-¶3, 10-¶¶1-2, 12-¶1, 18-¶6. As explained in Section IV.A.3, doing so allows data to be securely transmitted, received, and decrypted by second transaction party. SAMSUNG-1003, ¶[112].

[3]

Ellison's ***usage protector 250 has its own encryption key in the form of the operating system nub key (OSNK) 203***. SAMSUNG-1003, ¶¶[113]-[114]. As shown in FIG. 2 below, the "key generator 240 generates the OSNK 203 by combining the BK0 202 and the OS Nub ID 201 using a cryptographic hash function." SAMSUNG-1006, 9:9-11.

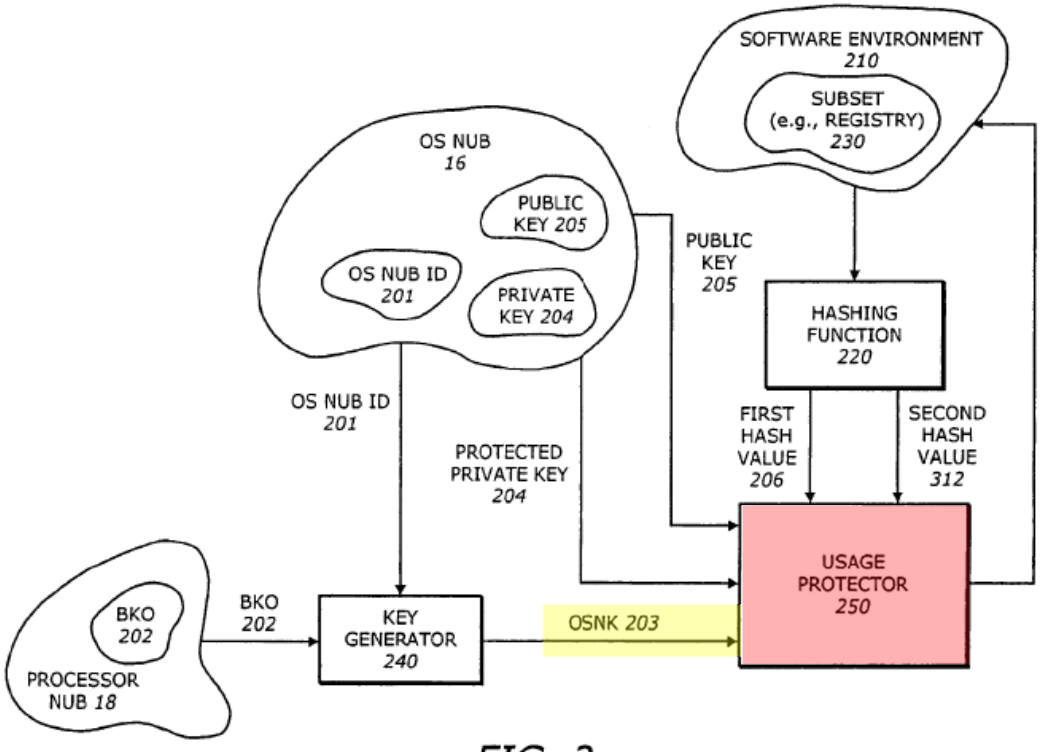


FIG. 2

SAMSUNG-1006, FIG. 2

The "cryptographic hash function is a one-way function, mathematical or otherwise, which takes a variable-length input string, called a pre-image and converts it to a fixed length, generally smaller, output string referred to as a hash value." SAMSUNG-1006, 9:17-22. In one embodiment, "[t]he OS nub ID 201 can be the hash of the OS nub 16, or a hash of a certificate that authenticates the OS nub 16, or an ID value extracted from a certificate that authenticates the OS nub 16." SAMSUNG-1006, 9:11-17. "The usage protector 250 uses the OSNK 203 to protect the usage of the subset 230." SAMSUNG-1006, 9:31-35. For example, the usage protector 250 ***uses the OSNK 203 as an encryption key to encrypt the first hash value 206*** obtained from subset 230. SAMSUNG-1006, FIG. 3B, 9:48-10:3, 10:32-62 ("[t]he encryptor 305 ***encrypts*** the first hash value 206 ***using the OSNK 203*** to generate an encrypted first hash value 302"). SAMSUNG-1003, ¶[115].

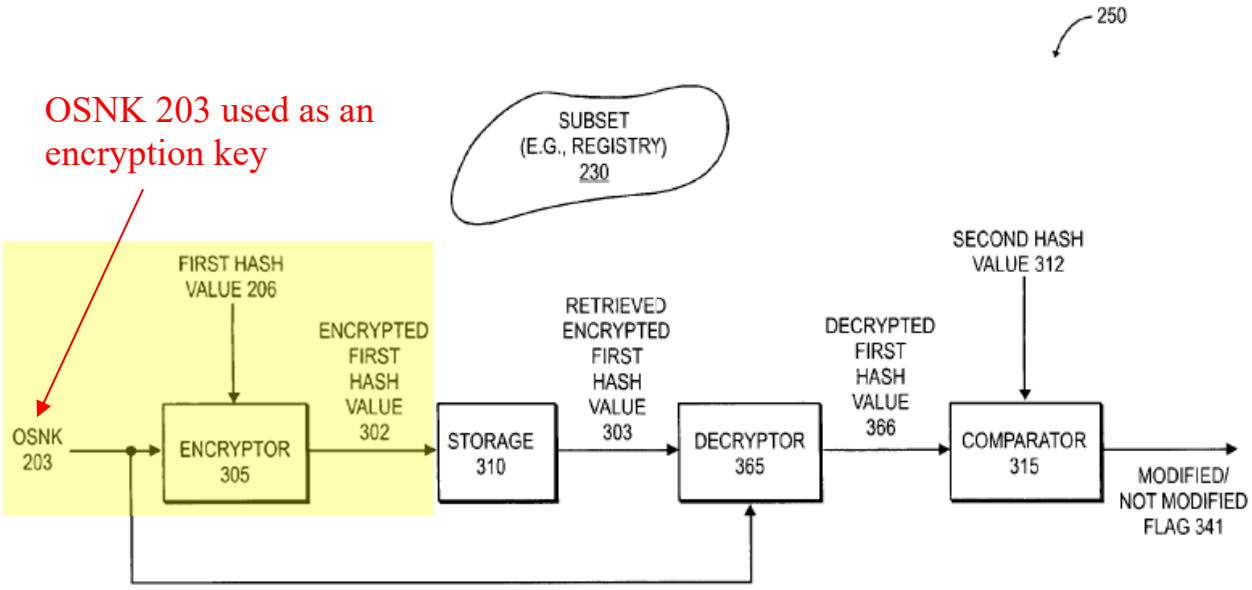


FIG. 3B

SAMSUNG-1006, FIG. 3B

[6]

As explained above in [1a] and [1i], "the OS nub 16, the processor nub 18, a key generator 240, a hashing function 220, and a ***usage protector 250, all operat[e] within the isolated execution environment***" and form part of the ***secure platform 200 ("secure area")***. SAMSUNG-1006, 8:25-32. To operate securely within the isolated execution environment, it would have been obvious to a POSITA that the usage protector 250 (***"authentication software"***) is installed in an application environment in the secure area. SAMSUNG-1003, ¶¶[116]-[117].

As shown in FIG. 2 below, since usage protector 250 and OS nub 16 are

both part of the isolated execution environment, the usage protector 250 may obtain the private key without passing through an unsecured part of said electronic device. SAMSUNG-1003, ¶[118].

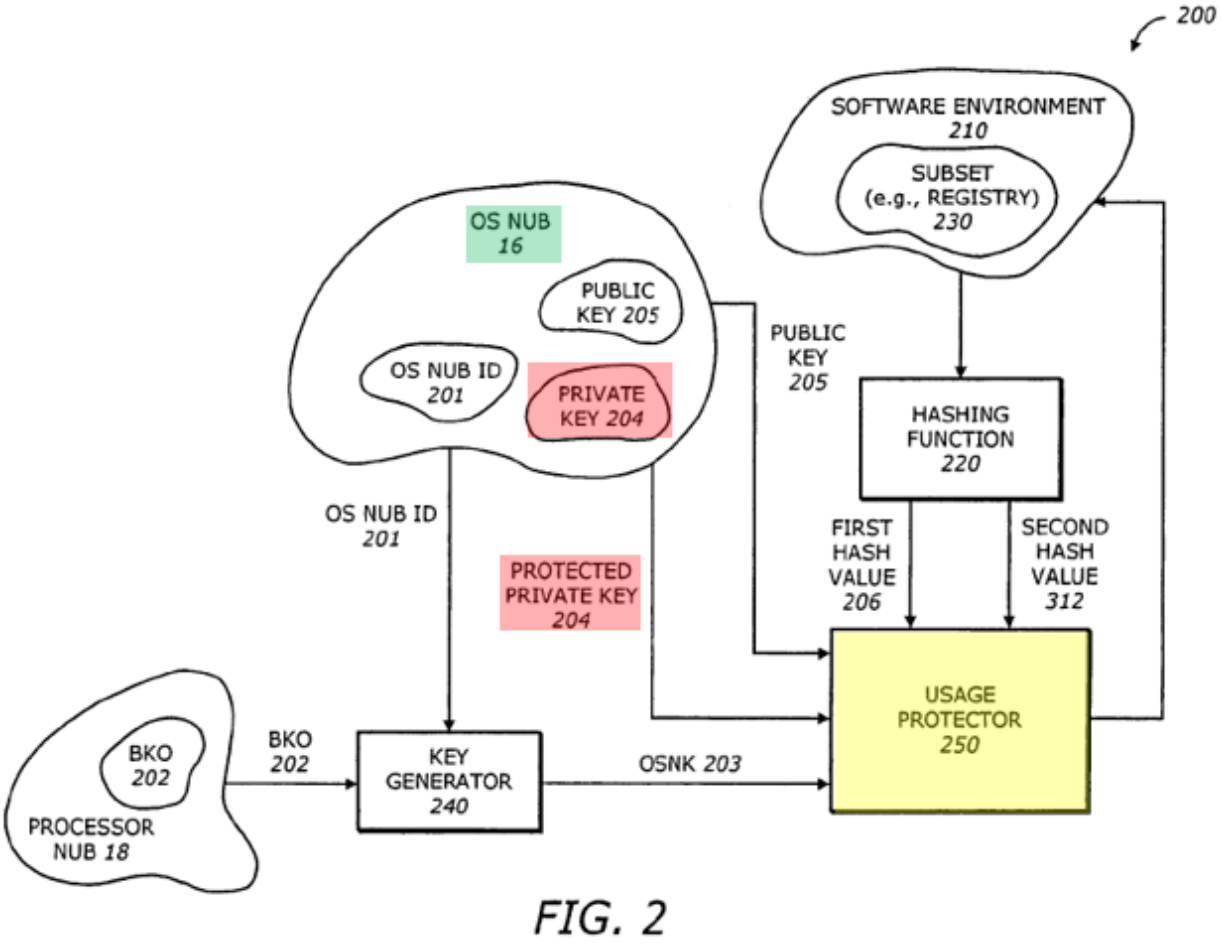


FIG. 2

SAMSUNG-1006, FIG. 2

In particular, Ellison teaches that, "[i]n one embodiment, the protected private key 204 is generated by the platform 200 itself the first time the platform 200 is powered up." SAMSUNG-1006, 8:48-52. "Only the OS nub 16 can retrieve and decrypt the encrypted private key [204] for subsequent use."

SAMSUNG-1006, 8:59-61. The subsequent use involves use by the usage protector 250 to perform operations such as decryption operations, as explained above in [1b]. SAMSUNG-1006, 8:33-65, 11:1-12:26, FIGS. 3C, 3D. At least in such an embodiment, the usage protector 250 "may obtain the private key without passing through an unsecured part of said electronic device" since the usage protector 250, the OS nub 16, and the private key 204 are all within the isolated execution environment. SAMSUNG-1003, ¶[119].

[11]

As explained in [1b], private key 204 is decrypted by decryptor 325, which is part of the usage protector 250 ("***authentication software***"). SAMSUNG-1006, 8:33-65, 11:1-12:26, FIGS. 3C, 3D (reproduced below); SAMSUNG-1003, ¶¶[128]-[129].

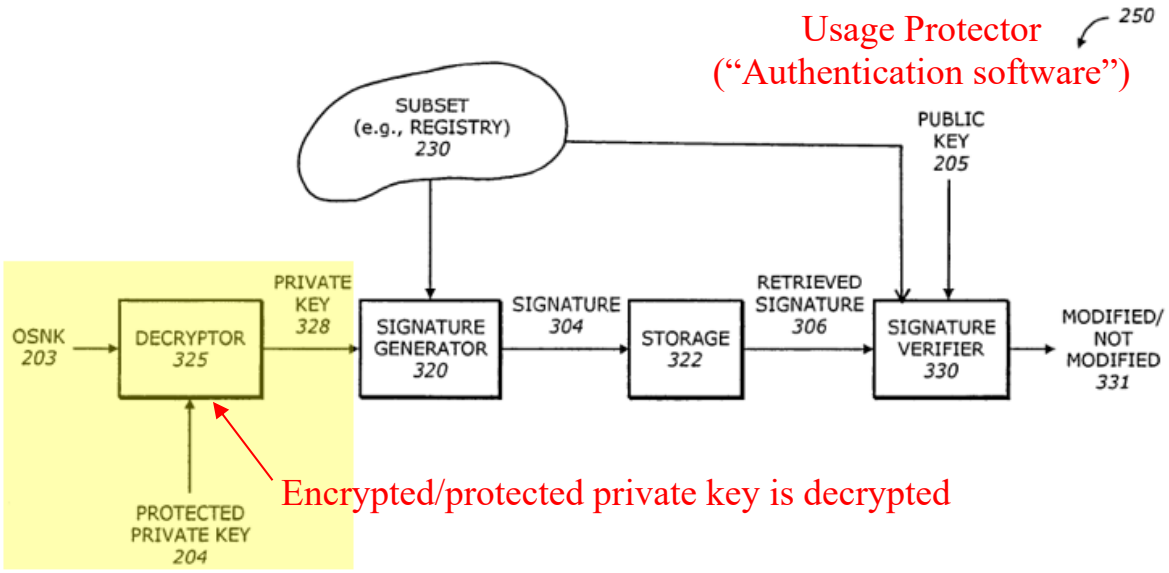


FIG. 3C

SAMSUNG-1006, FIG. 3C

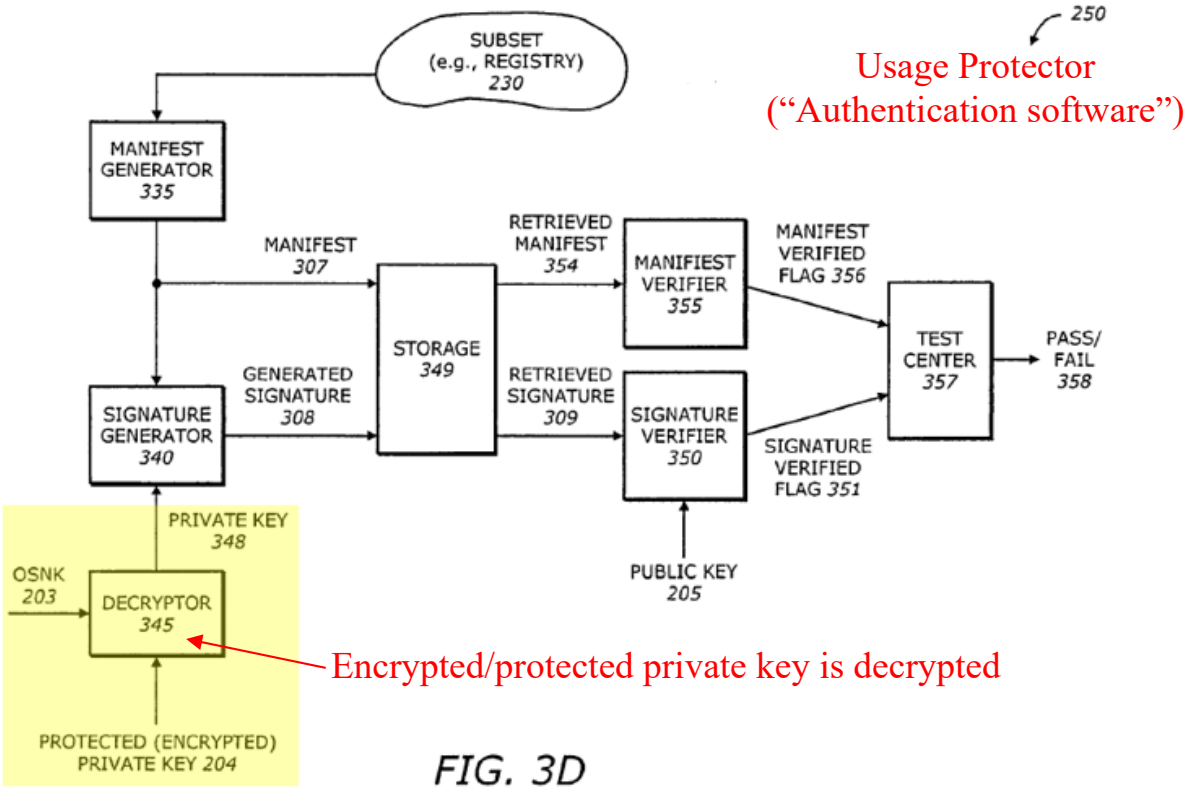


FIG. 3D

SAMSUNG-1006, FIG. 3D

[14]

Ellison discloses using a symmetric key to protect the secrets of the processor nub 18 and the operating system nub 16, but does not provide details of how the symmetric key is generated. SAMSUNG-1006, 6:51-57, 7:19-32. Muir discloses that, before performing encryption and decryption operations, a user provides a user ID/password to confirm an identification of the user. SAMSUNG-1008, 15-¶¶3-5, FIG. 8. It would have been obvious to a POSITA to combine the above-noted teachings of Ellison and Muir so that a user identity can be verified prior to conducting a secure transaction between two transaction parties. SAMSUNG-1003, ¶¶[135]-[136]. Indeed, providing login credentials, such as user ID/password, to identify a user is a well-known user authentication method and would have been obvious to implement in EMC prior to conducting encryption/decryption operations and/or a secure transaction with another party so that the user of the electronic device can be authenticated. SAMSUNG-1019, 1:53-66; SAMSUNG-1020, FIGS. 2, 7, 2:49-65, 7:40-52; SAMSUNG-1003, ¶[136]. An additional benefit here is that the information identifying the user can be used to generate a symmetric key, thereby enabling a user-specific symmetric key to protect electronic device elements such as the processor nub 18 and the operating system nub 16. SAMSUNG-1003, ¶[136]. Combining the teachings of Ellison and Muir would have involved combining prior art elements (Ellison's

system and Muir's user identification mechanism) according to known methods (obtaining user id/password information from a user) to yield predictable results (generation of a user id/password-based symmetric key). SAMSUNG-1003, ¶[136]. Accordingly, EMC renders [14] obvious.

[15]

As explained above in [3], the usage protector 250 ("***authentication software***") has an encryption key in the form of OSNK 203. The ***OSNK 203 ("encryption key") is used for encrypting various data*** such as a compressed subset 377 (*see* SAMSUNG-1006, FIG. 3A, 10:4-31), a first hash value 206, and a second hash value 312 (*see* SAMSUNG-1006, FIGS. 3B, 3E, 4, 10:32-62, 12:27-13:20); SAMSUNG-1003, ¶¶[137]-[138].

A POSITA reading Ellison would have understood that Ellison's disclosure relates to encrypting and decrypting digital data. SAMSUNG-1003, ¶[139]. For example, when the usage protector 250 decrypts an encrypted private key 204 by using OSNK 203, a ***digital*** signature algorithm is applied by the signature generator 320 on the resulting private key 204 suggesting to a POSITA that the data being processed is digital. SAMSUNG-1006, 11:1-16; SAMSUNG-1003, ¶[139]. Ellison discloses that the "signature algorithm used by the signature generator 320 may be public-key ***digital*** signature algorithm" and that "[e]xample

algorithms include … ***Digital*** Signature Algorithms [sic] schemes." SAMSUNG-1006, 11:1-16, 8:59-62. Moreover, a POSITA would have understood that, with the inclusion and use of "a compressor 370, an encryptor 375, … a decryptor 385, and a decompressor 390," the usage protector 250 is configured to process ***digital data*** (e.g., encrypt digital data). SAMSUNG-1006, 10:4-8; SAMSUNG-1003, ¶[139]. Thus, a POSITA would have found it obvious that Ellison encrypts digital data. For at least these reasons, EMC renders [15] obvious. *Id*.

[16pre]

See supra [1pre-1]; SAMSUNG-1003, ¶[140].

[16a]

See supra [1pre-1]. In addition, Muir's FIG. 5 shown below discloses the network interface for an electronic transaction between a first transaction party and a second transaction party. SAMSUNG-1008, pp. 9-¶2, 11-¶3, 1-¶2; SAMSUNG-1003, ¶[141].

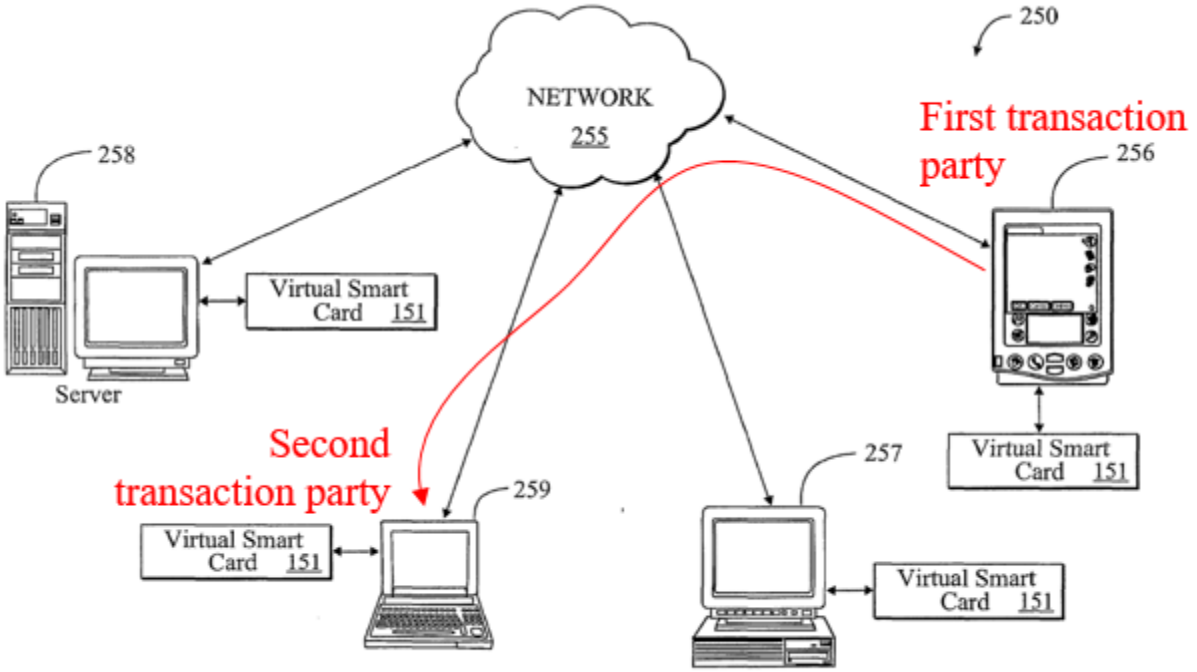


Fig. 5

SAMSUNG-1008, FIG. 5

[16b]

As explained in [1pre-2], Ellison discloses an operating system, OS 12, "creating a run-time environment for user applications." Processor 110 is configured for OS 12 in the normal execution mode 112. SAMSUNG-1006, 4:23-29, 4:57-5:27, FIGS. 1A, 1C; SAMSUNG-1003, ¶[142].

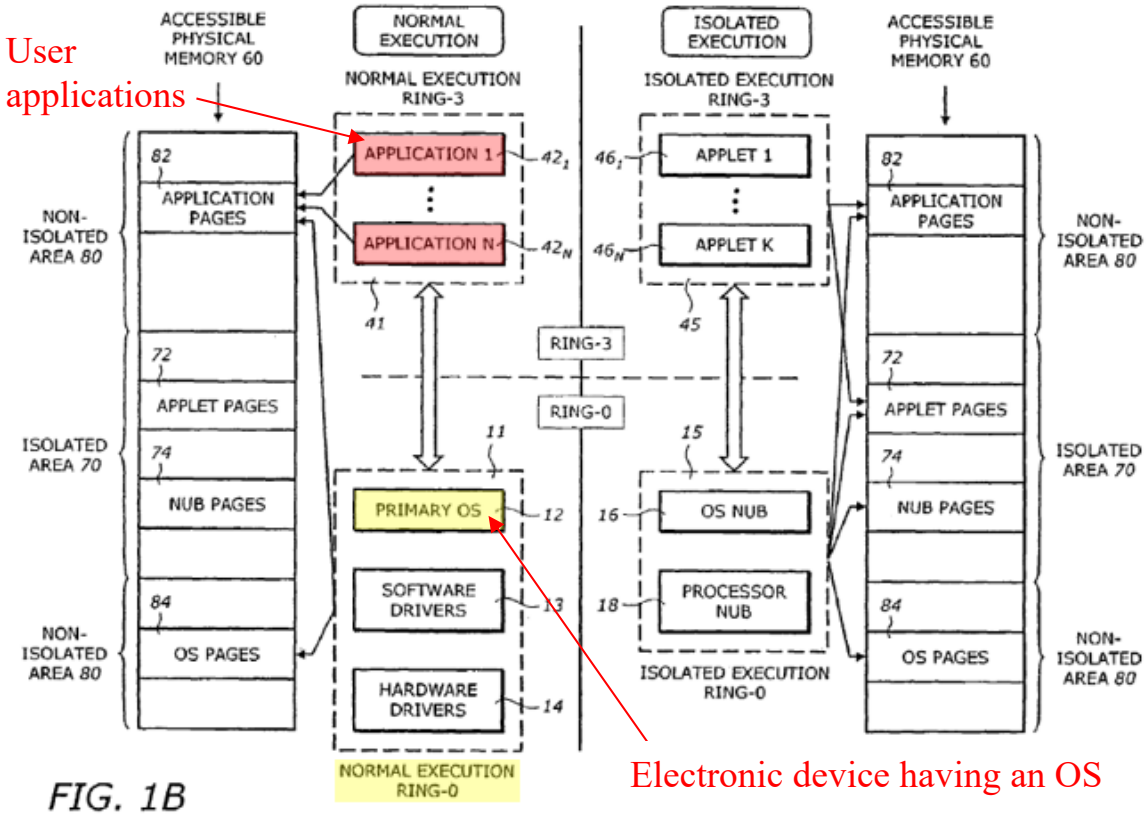


FIG. 1B

SAMSUNG-1006, FIG. 1B

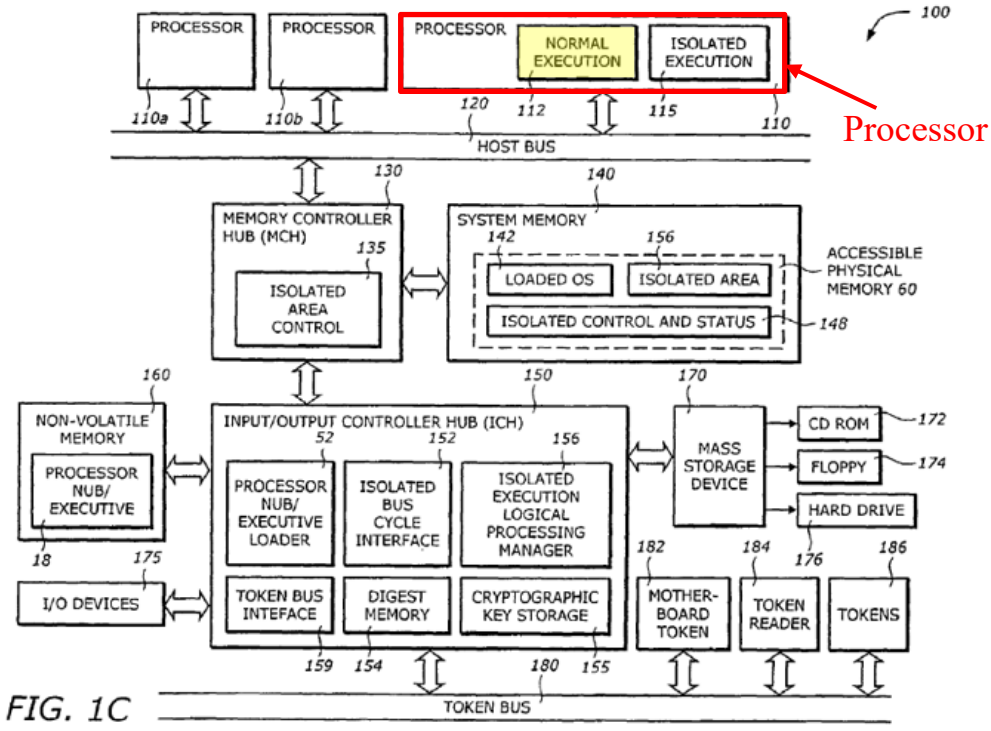


FIG. 1C

SAMSUNG-1006, FIG. 1C

[16c]

See supra [1a]; SAMSUNG-1003, ¶[143].

[16d]

See supra [1b]; SAMSUNG-1003, ¶[144].

[16e]

See supra [1c], [1d]; SAMSUNG-1003, ¶[145].

[16f]

See supra [1e]; SAMSUNG-1003, ¶[146].

[16g]

See supra [1f]; SAMSUNG-1003, ¶[147].

[16h]

See supra [1g], [1h], [1i]; SAMSUNG-1003, ¶[148].

[16i]

As explained in [1j], Ellison discloses "activating the authentication software to generate a digital signature from the private key." Ellison also discloses that the processor 110 is configured for the activating. In particular, Ellison teaches that processor 110 also includes an "isolated execution circuit 115 [that] provides hardware and software support for the isolated execution mode. This support includes configuration for isolated execution, definition of an isolated area, definition (e.g., decoding and execution) of isolated instructions, generation of isolated access bus cycles, and generation of isolated mode interrupts."

SAMSUNG-1006, 5:1-10, FIG. 1C (reproduced below); SAMSUNG-1003, ¶[149].

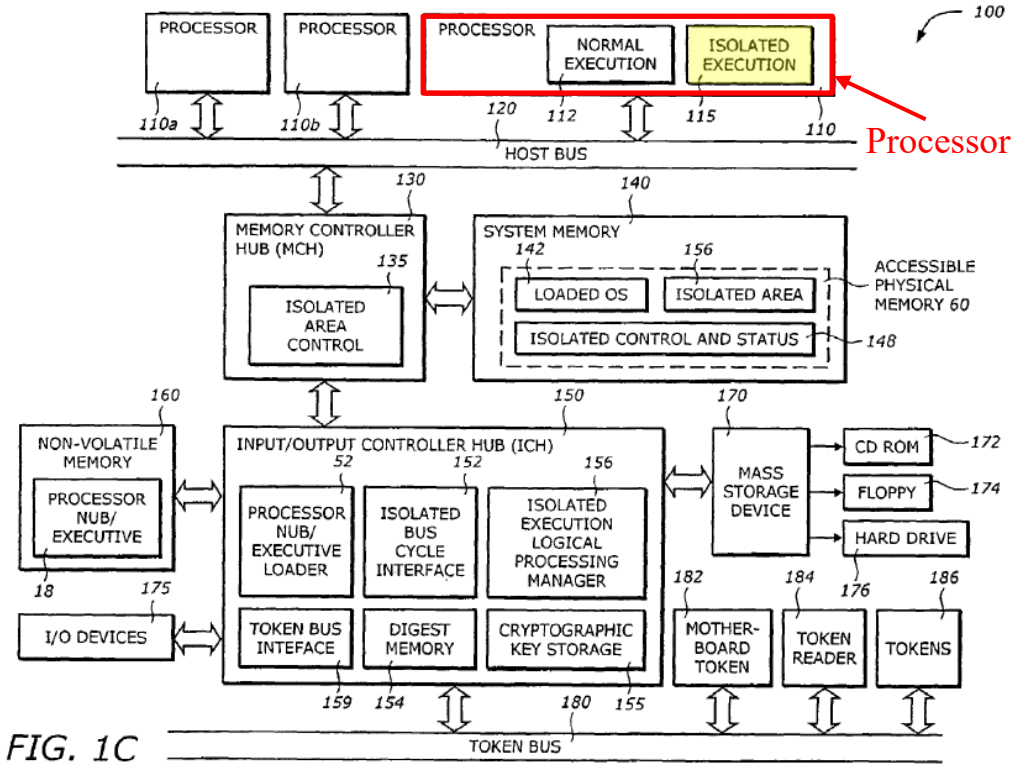


FIG. 1C

SAMSUNG-1006, FIG. 1C

In addition, as explained above in [1i], it would have been obvious to a POSITA that, to perform encryption and decryption using a private key, all or at least a portion of the usage protector 250 and its operational software/code would have been stored in a secure memory of the isolated execution environment such as isolated area 70. SAMSUNG-1003, ¶[150]. Ellison teaches that processor 110 can define and control access to the isolated area 70. SAMSUNG-1006, 6:1-26. It would have been obvious to a POSITA that because (i) processor 110 configures the isolated execution mode and controls access to the isolated area 70, and (ii) the

usage protector 250 operates within the isolated execution environment and is stored in a secure memory such as isolated area 70, the processor 110 would have also been configured to activate the usage protector 250 ("***authentication software***") as part of its control and configuration of the isolated execution mode and/or the isolated area 70. SAMSUNG-1003, ¶[150].

[16j]

See supra [1k], [1l]; SAMSUNG-1003, ¶[151].

[17pre-1]

See supra [1pre-1]; SAMSUNG-1003, ¶[152].

[17pre-2]

See supra [1pre-2]; SAMSUNG-1003, ¶[153].

[17a]

See supra [1a], [1b]; SAMSUNG-1003, ¶[154].

[17b]

See supra [1a]-[1d]; SAMSUNG-1003, ¶[155].

[17c]

See supra [1f]; SAMSUNG-1003, ¶[156].

[17d]

See supra [1g], [1h]; SAMSUNG-1003, ¶[157].

[17e]

See supra [1j], [1k]; SAMSUNG-1003, ¶[158].

[17f]

See supra [1l]; SAMSUNG-1003, ¶[159].

[18pre]

See supra [1pre-1], [16pre]; SAMSUNG-1003, ¶[160].

[18a]

See supra [1pre-1], [16a]; SAMSUNG-1003, ¶[161].

[18b]

See supra [1pre-2]-[16b]; SAMSUNG-1003, ¶[162].

[18c]

See supra [1a], [1b], [16c], [16d]; SAMSUNG-1003, ¶[163].

[18d]

See supra [1c], [1d], [16e]; SAMSUNG-1003, ¶[164].

[18e]

See supra [1f], [16g]; SAMSUNG-1003, ¶[165].

[18f]

See supra [1g], [1h], [1i], [16h]; SAMSUNG-1003, ¶[166].

[18g]

See supra [1j], [1k], [1l], [16i], [16j]; SAMSUNG-1003, ¶[167].

[19]

See supra [1pre-1]. Muir's electronic devices may include, for example, cellular phones, personal data assistants, and smart cards. SAMSUNG-1008, pp. 11-¶3, 8-¶1, 1-¶¶2-3; SAMSUNG-1003, ¶[168].

B. GROUND B2: Claims 7, 9, and 13 are obvious over Ellison, Muir, and Al-Salqan

1. Al-Salqan

Al-Salqan explains that, although private keys can be used in asymmetric encryption techniques, there can be practical limitations that make it difficult to use them. SAMSUNG-1007, 1:21-2:47. For example, a principal (owner of the private key) may "lose or forget his or her private key or private key password," and a principal may be the only one in an organization to know the private key and may leave the organization without anyone having knowledge of the private key. SAMSUNG-1007, 1:55-60, 2:25-41. In addition, an intruder may breach security and steal the private key. *Id*.; SAMSUNG-1003, ¶[72].

To address these concerns, Al-Salqan discloses a method to encrypt and store a key or key password in a secure manner that would allow the principal or members of the principal's organization to recover the key in the scenarios noted above. SAMSUNG-1007, 2:42-63. Al-Salqan's method involves encoding "[p]rivate information of the principal such as mother's maiden name and social security number … for example by hashing. The result of this encoding is used to

symmetrically encrypt the private key or key password. The encrypted private key or key password is again encrypted, for example asymmetrically using the public key of a trusted party such as a certification authority as the encryption key." SAMSUNG-1007, 2:50-60, 4:4-5:9, FIG. 2 (reproduced below); SAMSUNG-1003, ¶[73].

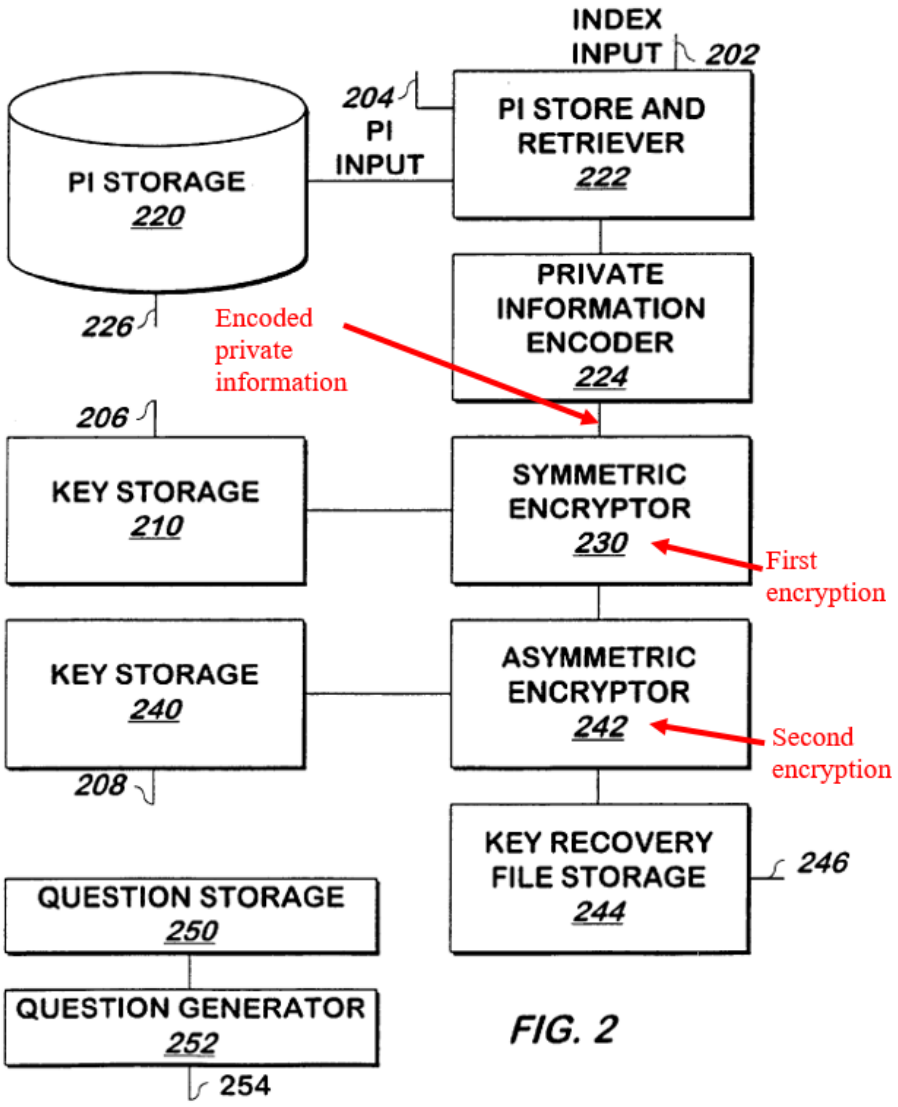


FIG. 2

SAMSUNG-1007, FIG. 2.

As shown in FIG. 2, a key based on the principal's private information is

encrypted twice, first symmetrically and second asymmetrically. SAMSUNG-1003, ¶[74].

To decrypt such keys, Al-Salqan discloses a decryption method that uses an asymmetric decryptor 314 and symmetric decryptor 330 to remove the two layers of encryption. In particular, referring to Al-Salqan's FIG. 3 (reproduced below), "a key that will decrypt the encryption performed by the asymmetric encryptor 242 of FIG. 2 is supplied at input 304 and stored in key storage 312." SAMSUNG-1007, 5:15-25. A "key recovery file is received at input 306 and stored in key recovery file storage 310." *Id*. "Asymmetric decryptor 314 receives the key recovery file from key recovery file storage 310 and receives the certificate authority's private key from key storage 312. Asymmetric decryptor 314 decrypts the key recovery file using the … key stored in key storage 312 as the key." SAMSUNG-1007, 5:25-35. "Symmetric decryptor 330 decrypts the key recovery file decrypted by [a]symmetric decryptor 314 using the encoded private information received from private information encoder 324 as the decryption key." SAMSUNG-1007, 5:25-35, 4:15-5:24; SAMSUNG-1003, ¶[75].

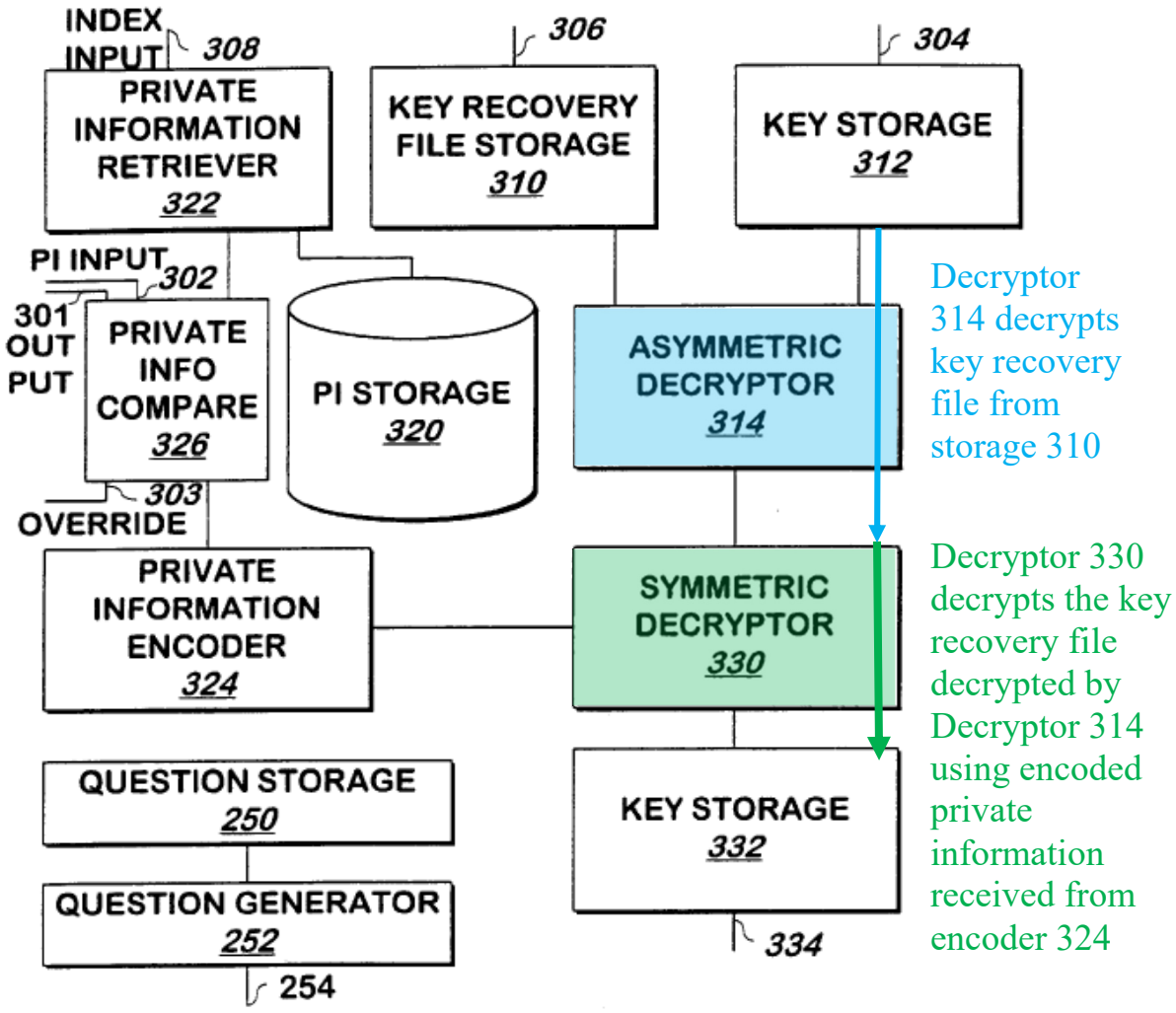


FIG. 3

SAMSUNG-1007, FIG. 3

2. Combination of Ellison, Muir, and Al-Salqan

It would have been obvious for a POSITA to combine the teachings of EMC with the teachings of Al-Salqan because doing so would merely involve combining prior art elements according to known methods to yield predictable results, as

explained in more detail below. SAMSUNG-1003, ¶[76].

Ellison teaches using an encrypted private key 204, but does not provide details of how the private key 204 is encrypted. SAMSUNG-1006, 8:33-65, 11:1-12:26, FIGS. 3C, 3D, 6:60-67, *see supra* [1b]. It would have been obvious to a POSITA that encrypting a private key 204 involves a key to encrypt the private key 204. SAMSUNG-1021, 1:13-2:7; SAMSUNG-1003, ¶[77]. In this regard, and given the lack of details in Ellison, a POSITA would have been motivated to look to other references that describe key encryption, such as Al-Salqan, and would have found it obvious to apply the details of that key encryption to implement the key encryption in Ellison. *Id*. Indeed, as Dr. Black explains, a POSITA would have seen Al-Salqan's key encryption as use of a known technique to improve similar devices (the EMC and Al-Salqan processing systems) in the same way. SAMSUNG-1003, ¶[77].

A POSITA interested in using an encrypted private key, such as Ellison's private key 204, also would have turned to Al-Salqan's method for generating the encrypted private key to avoid the practical limitations of using private keys such as a user/principal forgetting the private key or private key password or leaving a place of employment, as explained above. SAMSUNG-1007, 1:55-60, 2:25-41; SAMSUNG-1003, ¶[78]. A POSITA would have incorporated Al-Salqan's method of generating an encrypted private key using private information "such as

[the principal's] social security number, mother's maiden name, and other similar information." SAMSUNG-1007, 4:4-7, Abstract, 2:49-63; SAMSUNG-1003, ¶[78]. Furthermore, by using two encryption layers–a first symmetrical encryption layer and a second asymmetric encryption layer—the private key generated based on Ellison and Al-Salqan's teachings would have additional layers of protection. *Id*.

To combine the teachings of Muir, Ellison, and Al-Salqan, EMC's system would have been modified to be able to obtain principal input, as described by Al-Salqan (e.g., by prompting the principal with questions requesting the principal's private information) and to include the symmetric encryption 230 and asymmetric encryptor 242 for adding two encryption layers to protect the private key. In order to decrypt the private key, EMC's decryptor 325 would have been modified to include Al-Salqan's symmetric decryptor 330 and asymmetric decryptor 314 so that it can decrypt the two layers of encryption (as disclosed by Al-Salqan's FIG. 3) and yield the private key 328 for further use by the usage protector 250. SAMSUNG-1003, ¶[79].

Because encrypting data using symmetric or asymmetric techniques was well-known and implementing user interfaces to query users for information was well-known, such a combination would have been predictable and a POSITA would have had a reasonable expectation of success in implementing the

combination. SAMSUNG-1003, ¶[80]. Moreover, because only a finite number of encryption options exist and Ellison does not describe a specific encryption method, a POSITA would have investigated and found obvious the use of a known option, such as Al-Salqan's. *Id*. A POSITA would have been motivated to choose Al-Salqan's method to achieve the above-noted benefits that Al-Salqan explicitly mentions for using multiple layers of encryption using private information. *Id*. Indeed, the practical limitations of using private keys, as explained in Al-Salqan and noted above, were commonly experienced and would have protected the EMC system from similar deficiencies, thereby making the combination of Ellison and Al-Salqan foreseeable. *Id*.

3. Manner in which the Prior Art Renders Claims 7, 9, and 13 Obvious

[7]

As explained above in Sections IV.B.1-IV.B.2, the combination of Ellison, Muir, and Al-Salqan (EMAS) renders obvious ***a private key that is encrypted using at least two encryption layers***. SAMSUNG-1003, ¶[120]. For instance, a first encryption layer would have been a symmetric encryption layer implemented when Al-Salqan's symmetric encryptor 230 encrypts encoded private information, and a second encryption layer would have been an asymmetric encryption layer implemented when Al-Salqan's asymmetric encryptor 242 encrypts the output from the symmetric encryptor 230. SAMSUNG-1007, 2:50-60, 4:4-5:9, FIG. 2;

SAMSUNG-1003, ¶[121].

[9]

As explained above in Sections IV.B.1-IV.B.2, the EMAS combination renders obvious Ellison's private key 204 being encrypted using an encryption key which is associated with a user identifying number or personal identifying number such as the user's social security number. SAMSUNG-1007, Abstract, 2:49-63, 4:4-7; SAMSUNG-1003, ¶[124]. Accordingly, EMAS renders obvious "wherein ***the private key is encrypted using an encryption key which is associated with a user identifying number***, in particular ***a personal identifying number***, PIN, or a number or a template associated with a fingerprint of the user." SAMSUNG-1003, ¶[125].

[13]

As explained above in Sections IV.B.1-IV.B.2, in the EMAS combination, Al-Salqan's asymmetric decryptor 314 uses the encoded ***private information*** received from private information encoder 324 ***as the decryption key***." SAMSUNG-1007, 5:25-35. The private information includes the "social security number, mother's maiden name, and other similar information." SAMSUNG-1007, 4:4-7, Abstract, 2:49-63. Accordingly, EMAS renders obvious "wherein the

private key is decrypted using ***a decryption key associated with any identifying characteristic***, in particular a serial number, ***a personal identification number***, PIN, or a fingerprint of a user." SAMSUNG-1003, ¶¶[133]-[134].

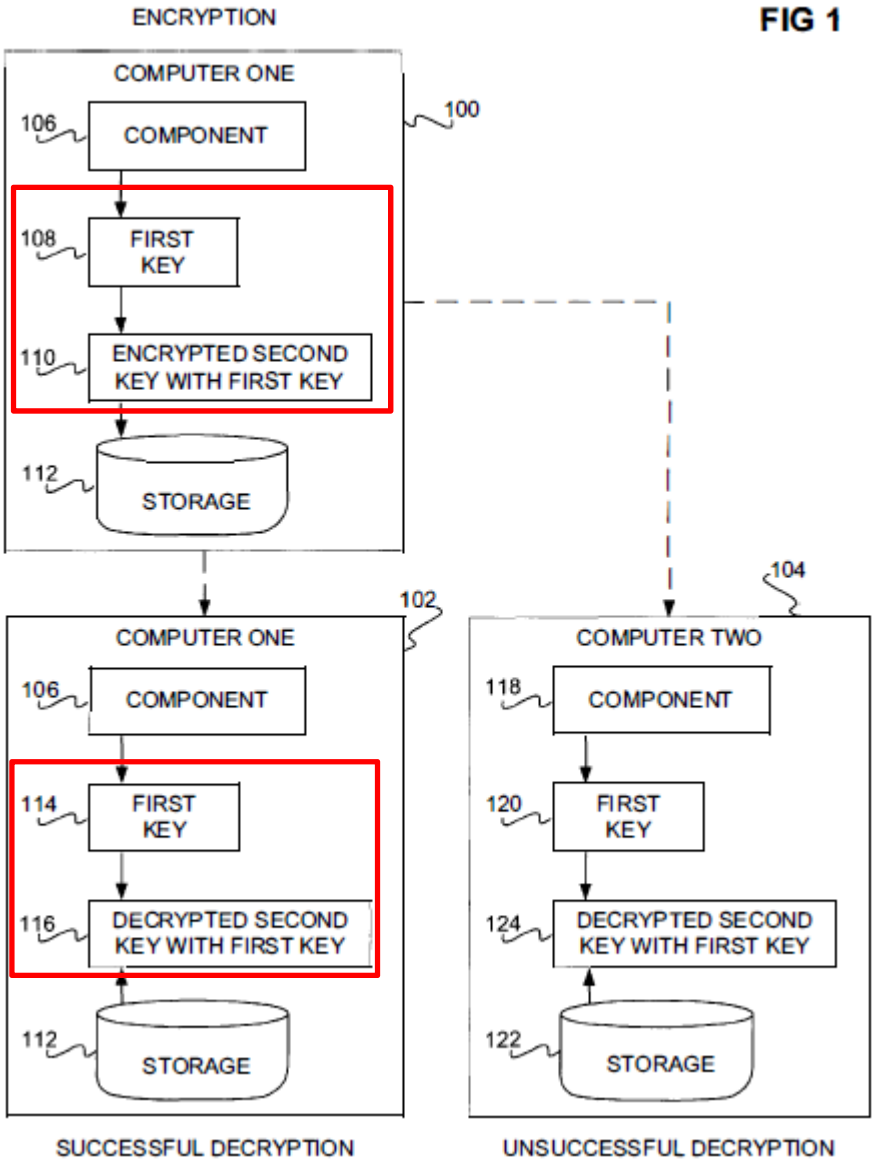
C. GROUND B3: Claims 8, 10, and 12 are obvious over Ellison, Muir, and Searle

1. Searle

Searle discloses encrypting "a key [(second key)] using another key [(first key)] that is unique and particular to a given client, such as a desktop computer, a laptop computer, a portable electronic device, etc., for fraud prevention and other purposes." SAMSUNG-1009, 2:14-18. An identifier of a computer component can be used as the first key. SAMSUNG-1009, 4:48-65. The component can be a processor "that has a unique serial number or other identifier," or a network card "having a unique media access controller (MAC) address." SAMSUNG-1009, 4:48-65. The first key can be "one or more of: a processor identifier, a network card address, … serial numbers and/or the number of cylinders of attached hard disk drives, checksums of the read-only memory (ROM) or other system components, the Internet Protocol (IP) address of the computer or system, and a combination of installed cards." SAMSUNG-1009, 2:13-33, 4:58-5:7; SAMSUNG-1003, ¶[81].

The second key is encrypted using the first key. SAMSUNG-1009, 2:30-33, Abstract, 5:8-28, FIGS. 1, 2 (reproduced below). When decryption is desired, the

second key is decrypted using the first key. SAMSUNG-1009, 2:33-40, FIG. 1, 2, 5:65-6:27. "Because the first key is specific to the underlying computer or device, if the encrypted second key is moved to another computer or device, it will not be decrypted successfully." SAMSUNG-1009, 2:33-40; SAMSUNG-1003, ¶[82].



SAMSUNG-1009, FIG. 1

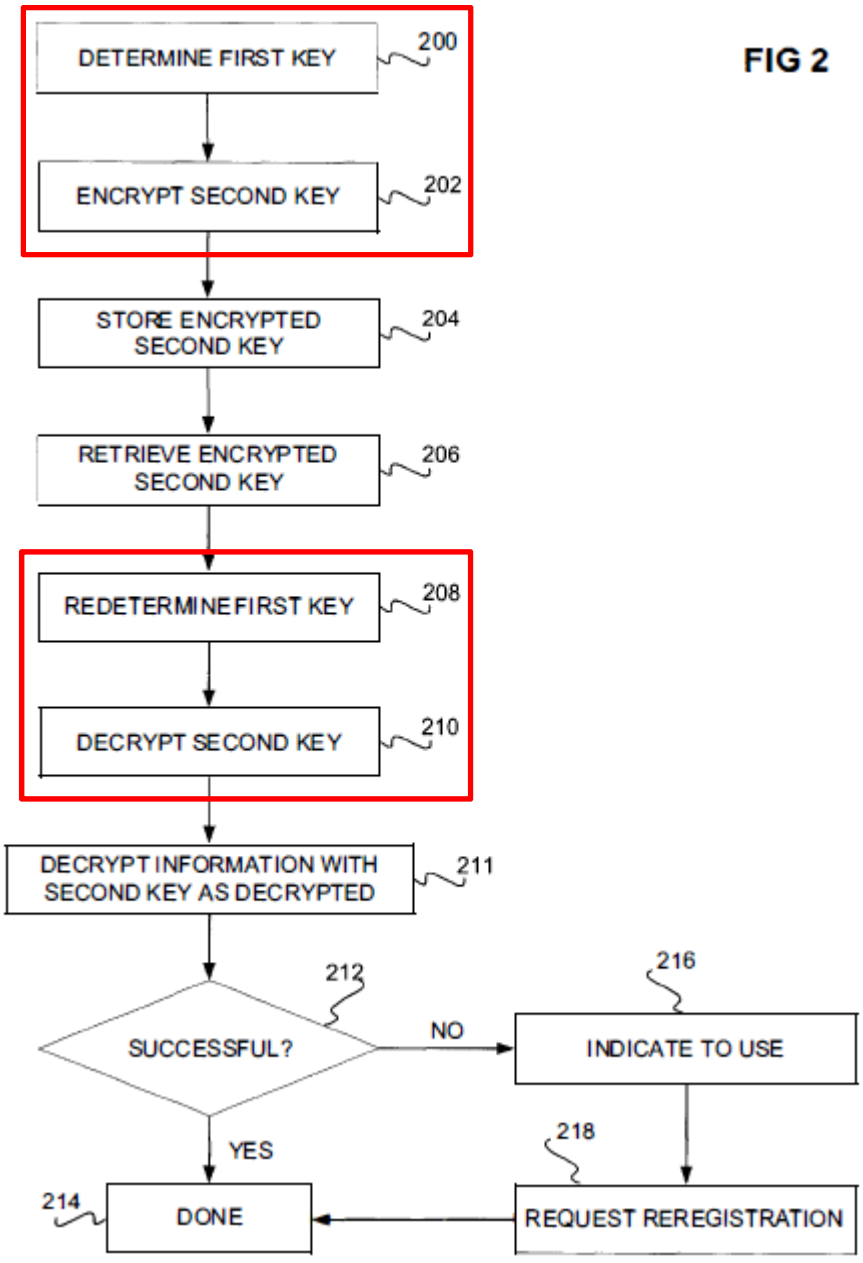


FIG 2

SAMSUNG-1009, FIG. 2

2. Combination of Ellison, Muir, and Searle

Ellison teaches using an encrypted private key 204, but does not provide details of how the private key 204 is encrypted. SAMSUNG-1006, 8:33-65, 11:1-

12:26, FIGS. 3C, 3D, 6:60-67, *see supra* [1b]. It would have been obvious to a POSITA that encrypting a private key 204 involves an encryption key to encrypt the private key 204. SAMSUNG-1021, 1:13-2:7; SAMSUNG-1003, ¶[83]. In this regard, and given the lack of details in Ellison, a POSITA would have been motivated to look to other references that describe key encryption, such as Searle, and would have found it obvious to apply the details of that key encryption to implement the key encryption in Ellison. *Id*. Indeed, as Dr. Black explains, a POSITA would have seen Searle's key encryption as use of a known technique to improve similar devices (the EMC and Searle processing systems) in the same way. *Id*.

A POSITA using Ellison's encrypted private key 204 also would have turned to Searle to perform encryption and decryption of the private key (Searle's second key) using a key associated with a hardware device serial number (Searle's first key) because doing so would have provided an enhanced level of security and protection from intruders. SAMSUNG-1003, ¶[84]. In particular, by encrypting the private key using a hardware device serial number associated with a user's electronic device, only a device with the information on the hardware device serial number would be able to perform the decryption of the private key, which would be helpful in preventing hacking of the private key even if an intruder gets possession of the encrypted private key (and any accompanying public key).

SAMSUNG-1010, Abstract, ¶[0023]; SAMSUNG-1003, ¶[84]. As explained by Shen, when a hardware serial number is used as part of the encryption/decryption technique (like in Searle), data to be protected cannot be encrypted/decrypted by other users whose user end device hav[e] different hardware serial numbers from that of the true user, even if they know the true user's public key and private key." SAMSUNG-1010, ¶[0019]; SAMSUNG-1003, ¶[84].

To incorporate the teachings of Searle in the EMC system, a POSITA would have used or associated a hardware device serial number with the encryption key or decryption key (Searle's first key) when performing encryption/decryption of the private key (Searle's second key). SAMSUNG-1003, ¶[85]. Searle explains that various suitable schemes can be used to perform encryption and decryption. SAMSUNG-1009, 3:66-4:11. For instance, as noted above and described in Searle, when encrypting EMC's private key, a suitable encryption scheme would have been used to configure an encryption key that is associated with a hardware device serial number and subsequently encrypt the private key. When decrypting EMC's encrypted private key, a suitable decryption scheme would have been used to obtain a decryption key that is associated with a hardware device serial number and subsequently decrypt the encrypted private key. SAMSUNG-1003, ¶[85].

Combining the teachings of EMC with the teachings of Searle in this manner would have been obvious to a POSITA because doing so would merely involve

combining prior art elements (e.g., known hardware device serial number encryption) according to known methods (e.g., suitable known encryption/decryption methods) to yield predictable results (private key encrypted or decrypted using a key associated with a hardware device serial number). SAMSUNG-1003, ¶[86]. And, because encrypting a private key or decrypting an encrypted private key using a "hardware identifier of [a] computer system," such as a hardware serial number, was known to a POSITA, such a combination would have been predictable and a POSITA would have had a reasonable expectation of success in implementing the combination. SAMSUNG-1011, ¶[0042]; SAMSUNG-1003, ¶[86]. Moreover, because only a finite number of encryption and decryption options existed and Ellison does not describe a specific encryption method, a POSITA would have investigated and found obvious the use of a known option, such as Searle's. SAMSUNG-1003, ¶[86]. A POSITA would have been motivated to choose Searle's method to achieve the above-noted benefits that Searle explicitly mentions for encrypting a private key or decrypting an encrypted private key using a hardware identifier of a computer system. *Id*. The demand for better computer security and fraud prevention would have further rendered the combination of Ellison, Muir, and Searle predictable and foreseeable. *Id*.

3. Manner in which the Prior Art Renders Claims 8, 10, and 12 Obvious

[8]

As explained above in Sections IV.C.1-IV.C.2, the Ellison-Muir-Searle combination renders obvious [8] at least because Searle teaches encrypting a second key ("***the private key***") using a first key ("***an encryption key***") which is associated with "***a hardware device serial number***" (e.g., "a unique serial number or other identifier" of a processor, a network card address, serial numbers and/or the number of cylinders of attached hard disk drives). SAMSUNG-1009, 2:13-33, 4:58-5:7; SAMSUNG-1003, ¶¶[122]-[123].

[10]

As noted above in Sections IV.C.1-IV.C.2, Searle also teaches decrypting the second key using a first key ("***decryption key***") that is "associated with one or more serial numbers of hardware components of said electronic device," such as a serial number of a processor, network address card, cylinders of hard disk drives. SAMSUNG-1009, 2:13-40, 4:58-5:7, 5:65-6:27, FIG. 1; SAMSUNG-1003, ¶¶[126]-[127].

[12]

For the reasons explained above in [8] and [10], it would have been obvious to a POSITA that, in the Ellison-Muir-Searle combination, "the private key is decrypted … using a device specific encryption key." SAMSUNG-1003, ¶¶[130]-[131].

It would also have been obvious to a POSITA that the decryption is performed "by an application stored in the electronic device." SAMSUNG-1003, ¶[132]. For example, Ellison's FIGS. 3C and 3D depict a decryptor 325/345 that decrypts an encrypted private key 204 using OSNK 203. SAMSUNG-1006, 10:63-11:40. The decryptor 325/345 is part of the usage protector 250, which is described as being "a subset of a software environment." *Id.*, 2:7-12, 10:63-11:40. Since an application would have generally been understood by a POSITA to be a computer program that performs a specific task, and Ellison's decryptor 325/345 is a program in Ellison's software environment tasked with decrypting, it would have been obvious to a POSITA that decryptor 325 is an application stored in the electronic device of the Ellison-Muir-Searle combination. SAMSUNG-1022, 36; SAMSUNG-1003, ¶[132].

V. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION

Patent Owner filed its complaint relating to the '480 Patent on August 4, 2021. SAMSUNG-1004. This petition is being filed well in advance of Samsung's January 18, 2021 deadline to respond to the complaint and before any procedural schedule has been entered. Thus, there are no present deadlines for *Markman* briefing, contentions, or trial. Given Samsung's diligence in filing the present petition before answering the complaint, the *Fintiv* factors, and recent Board decisions applying them, weigh against discretionary denial.[4] IPR2020-00019, Paper 11, 5-6 (Mar. 20, 2020) (precedential)).

1. Factor 1: Either Party May Request Stay

Factor 1 is neutral because neither party in the co-pending litigation has, to date, requested a stay pending the result of PGR. *Apple Inc. v. Fintiv, Inc*., IPR2020-00019, Paper 15 at 12 (PTAB May 13, 2020); *Sand Revolution II, LLC v. Cont'l Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (PTAB June 16, 2020) ("*Sand Revolution*") (informative).

[4] Apart from Samsung's showing that the *Fintiv* factors favor institution, the *Fintiv* framework should not be followed because it is legally invalid. The framework (1) exceeds the Director's authority, (2) is arbitrary and capricious, and (3) was adopted without notice-and-comment rulemaking.

2. Factor 2: The Trial Schedule is Unclear

The trial date has not yet been scheduled. However, because of Petitioner's diligence in filing this petition within three months of being served with a complaint and because the parties agreed to a 135 day extension of time (90 days for extension of time to file response to complaint, and 45 days for waiver of service) for Samsung to file an Answer/Response to the complaint (SAMSUNG-1023), the Final Written Decision ("**FWD**") will likely issue a few months before the trial date.

Moreover, as in *NHK*, district court trial dates shift, even in normal times. *Mylan Pharma. Inc. v. Sanofi-Aventis Deutschland GMBH*, IPR2018-01680, Paper 22 at 17 (PTAB Apr. 3, 2019). Scheduling issues cannot be ruled out, as continued outbreaks of COVID-19 are not unlikely. Indeed, it is not improbable that the trial schedule will incur delays that would increase the difference between the FWD and trial dates. *See e.g.,* SAMSUNG-1027, 3 ("the speed of resolution in patent cases across all districts has risen substantially, even as COVID restrictions have begun to lift; the significant backlog is, rather than dissipating, apparently increasing time to resolution across the country"); *Juniper Networks, Inc. et al. v. Packet Intelligence LLC*, IPR2020-00388, Pap. 22 at 14 (Sept. 9, 2020)("it is more likely that the District Court will incur delays due to the COVID-19 pandemic than the Board").

In contrast, despite the pandemic, the Board has consistently adhered to the one-year statutory deadline for FWDs prescribed by 35 U.S.C. § 316(a)(11) and, in fact, routinely issues decisions before their statutory deadlines. *See Sand Revolution II* at 9 ("even in the extraordinary circumstances under which the entire country is currently operating because of the COVID-19 pandemic, the Board continues to be fully operational").

Notwithstanding uncertainty of the co-pending litigation schedule, even if a FWD date were to be scheduled after the trial date, such FWD date timing should not be dispositive. The Board has previously granted institution in cases in which a FWD was issued months after the scheduled trial date. The Board has relied on various justifications when granting institution, e.g., Petitioners exercised diligence in filing the petition, the petition was accompanied with a stipulation not to pursue the asserted § 103 grounds in litigation, minimal investment had been made in litigation (fact and expert discovery not started, petition was filed even before the serving of preliminary invalidity contentions), and the merits of the invalidity challenge were strong. *Verizon Business Network Services, Inc. v. Huawei Techs. Co.*, IPR2020-01141, Paper 12 (Jan. 14, 2021); *HP Inc. v. Slingshot Printing LLC*, IPR2020-01084, Paper 13 (Jan. 14, 2021). The same factors are present in this case. For instance, Petitioner has exercised diligence and filed this petition not only well in advance of the one-year bar date, but prior to the due date for

Petitioner's response to the complaint in the co-pending litigation. Petitioner is submitting a stipulation (SAMSUNG-1005) not to pursue the asserted § 103 grounds in litigation. *See Sand Revolution at* 11-12. Given that initial pleadings have not even closed in the co-pending litigation, fact and expert discovery have not started, no depositions have occurred, and no *Markman* hearing has been scheduled, much less held. And, in view of the grounds asserted in this petition, the merits of the invalidity challenge are strong.

Therefore, *Fintiv* Factor 2 weighs against discretionary denial.

3. Factor 3: Petitioner's Diligence and Investment in PGR Outweighs the Parties' Minimal Investment in Litigation

This petition was filed almost 9 months before the one-year statutory bar date. *Mylan*, IPR2018-01680, Paper 22 at 18 (finding that petition filed two months before bar date is "well within the timeframe allowed by statute, weighing heavily in [petitioner's] favor").

Moreover, Petitioner filed this petition at a very early stage of the litigation—a fact that "has weighed against exercising the authority to deny institution under *NHK*." *Seven Networks*, IPR2020-00156, Paper 10 at 11-12 (June 15, 2020). Again, Petitioner filed this petition before the deadline for its response to the complaint and thus before a schedule has been issued for litigation. As such,

no substantive orders have been issued by the court, no depositions have been taken, and fact and expert discovery have not begun.

Overall, Factor 3 weighs against discretionary denial.

4. Factor 4: The Petition's Grounds Are Materially Different From Any That Might Be Raised in Litigation

As noted above, the co-pending litigation is in its earliest stage (e.g., no discovery, no depositions, no substantive orders, and no hearings have been held). At present, there is no overlap in issues between the litigation and any PGR resulting from this petition.

Moreover, consistent with *Fintiv*, Petitioner asks the Board alone to consider the unique challenges raised in the Petition. Petitioner has further eliminated any risk of duplicated effort by voluntarily stipulating to counsel for Patent Owner that, if the Board institutes the pending Petition, Petitioner will not pursue district court invalidity challenges based on the asserted § 103 grounds. SAMSUNG-1005; *see Sand Revolution at* 11-12. A lack of overlap between the petition and the district court proceeding "has tended to weigh against exercising discretion to deny institution." *Fintiv*, IPR2020-00019, Paper 11 at 12-14.

For at least these reasons, Factor 4 weighs against discretionary denial. *See*, *e.g.*, *Fintiv* at 12-13; *Snap* at 13-16; *Sand Revolution* at 11-12.

5. Factor 5: Institution Would Promote Judicial Efficiency

Petitioner and Patent Owner are parties to the co-pending litigation. Petitioner has stipulated not to assert instituted § 103 grounds in the co-pending litigation if the PTAB institutes PGR, a fact that favors institution and promotes judicial efficiency. *See Sand Revolution* at 11-12. At worst, where the parties are the same such as in this case, Factor 5 is neutral. *Cisco Sys., Inc. v. Ramot at Tel Aviv Univ. Ltd.*, IPR2020-00122, Paper 15 at *10 (PTAB May 15, 2020) (APJ Crumbley, dissenting).

6. Factor 6: The Merits of this Petition Strongly Favor Institution

As *Fintiv* noted, "the factors...are part of a balanced assessment of all the relevant circumstances in the case," and, "if the merits of a ground raised in the petition seem particularly strong…the institution of a trial may serve the interest of overall system efficiency and integrity…." *Fintiv*, 14-15.

The merits of this Petition are particularly strong. As demonstrated in the Petition with reference to Dr. Black's testimony and additional evidence, institution would result in a finding of unpatentability of the Challenged Claims, which are obvious based on prior art references that materially differ from those considered by the Examiner during prosecution. The strength of the merits alone is enough to outweigh any inefficiencies born of parallel litigation (and as explained

above, institution of this petition would actually *promote* efficiency). *See Fintiv* at 14-15.

Moreover, as noted above, institution would actually *promote* the AIA's objectives of providing an effective and efficient alternative to district court litigation with respect to claims that Patent Owner has serially asserted.[5] *See* Sen. Rep. No. 110-259 (2008)(Leahy, Judiciary Committee Report)("The legislation is designed to…improve patent quality and limit unnecessary and counterproductive litigation costs"), H.R. Rep. No. 112-98, pt. 1, pp. 39-40.

Accordingly, *Fintiv* Factor 6 weighs strongly against discretionary denial. *See Snap* at 16-19.

VI. CONCLUSION

Petitioner respectfully requests institution of the PGR and requests that the

[5] Senators Leahy and Cornyn recently reaffirmed the AIA's objectives through their introduction of "legislation [that] would improve the ability of our system to maintain the quality of American patents…[b]y ensuring there is a less expensive and more transparent option than drawn-out litigation," namely, the PTAB. SAMSUNG-1028, 1; SAMSUNG-1029, 16-17 (addressing the standard for institution under 35 U.S.C. 314(a)).

Board ultimately find the Challenged Claims unpatentable.

VII. PAYMENT OF FEES

Petitioner authorizes charge of fees to Deposit Account 06-1050.

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)

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. are the real parties-in-interest.

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

The '480 Patent is the subject of the following civil actions *Ward Participations B.V. v. Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.,* 6:21-cv-00806, W.D. Tex., August 4, 2021 (SAMSUNG-1004). Petitioner is not aware of any disclaimers, reexamination certificates, other than the IPR petition (IPR2022-00113) filed simultaneously with this petition. An IPR petition (IPR2022-00114) challenging the validity of related parent patent, U.S. Patent No. 11,063,766, are being filed concurrently with this petition.

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. 3200 RBC Plaza 60 South Sixth Street Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email:PGR39843-0109PS1@fr.com	Jeremy J. Monaldo, Reg. No. 58,680 Usman A. Khan, Reg. No. 70,439 3200 RBC Plaza 60 South Sixth Street Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 PTABInbound@fr.com

D. Service Information

Please address all correspondence and service to the address listed above. Petitioner consents to electronic service by email at PGR39843-0109PS1@fr.com (referencing No. 39843-0109PS1 and cc'ing PTABInbound@fr.com, axf-ptab@fr.com, monaldo@fr.com, and khan@fr.com).

Respectfully submitted,

Dated October 29, 2021

/Jeremy J. Monaldo/
W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Usman A. Khan, Reg. No. 70,439
Fish & Richardson P.C.
3200 RBC Plaza, 60 South Sixth Street
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. PGR2022-00007)

Attorneys for Petitioner

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 Post Grant Review totals 17,531 words, which is less than the 18,700 allowed under 37 CFR § 42.24.

Dated October 29, 2021

/Jeremy J. Monaldo/

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Usman A. Khan, Reg. No. 70,439
Fish & Richardson P.C.
3200 RBC Plaza, 60 South Sixth Street
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Attorneys 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 October 29, 2021, a complete and entire copy of this Petition for Post Grant Review and all supporting exhibits were provided via Federal Express, to the Patent Owner by serving the correspondence address of record as follows:

KENEALY VAIDYA LLP
3050 K Street, N.W., Suite 302
Washington DC 20007

/Diana Bradley/

Diana Bradley
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(858) 678-5667