Samsung Electronics Co. LTD. (Petitioner)
v.
Ward Participations B.V. (Patent Owner)

Petitioner Demonstratives

Case Nos. PGR2022-00007, IPR2022-00113, and IPR2022-00114
U.S. Patent Nos. 10,992,480 and 11,063,766
Before Hon. Thu A. Dang, Georgianna W. Braden, and James J. Mayberry

FISH.

Table of Contents

Overview of the Proceedings

FISH.

Overview of the Proceedings

- US Patent No. 10,992,480 ("the 480 Patent")
  - PGR2022-00007 and IPR2022-00113
  - 112 Grounds – Lack of Written Description Support
  - 103 Grounds – Obviousness (Ellison, Muir, Al-Salqan, Searle)
- US Patent No. 11,063,766 ("the 766 Patent")
  - IPR2022-00114
  - 103 Grounds – Obviousness (Ellison, Muir, Al-Salqan, Searle, Epstein)
- Grounds
  - 112 Grounds
    - Claim 1 – Four features lack written description support
    - Claims 2, 4, 5, 16, 18, and 19 – Additional features lack written description support
      - Ward did not address support for these additional features—such arguments are waived
  - 103 Prior Art Grounds
    - Combination of Ellison and Muir asserted against the 480 and 766 patent independent claims
    - Ward did not raise arguments against grounds involving Al-Salqan, Searle, and Epstein—such arguments are waived

Instituted Grounds

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
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

480 PGR: Pet., 3-4.

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

480 IPR: Pet., 2.

Ground	Claims	35 U.S.C. § 103
A1	1, 3, 4, 8, 9, 13, 21-33	Ellison in view of Muir
A2	10, 12	Ellison in view of Muir and Al-Salqan
A3	11	Ellison in view of Muir, Al-Salqan, and Searle
A4	5	Ellison in view of Muir and Epstein

766 IPR: Pet., 1.

Issue 1

35 USC § 112: The 480 Patent claims lack written description support

FISH.

General observations on lack written description support

- The claims were amended to diverge further from the original application by replacing “authentication data” with “private key.”
- Only one paragraph describes the private key.
- Corresponding EP and NL patents were found to lack written description support.
- Ward’s expert used the wrong standard (obviousness) to determine whether the claims are supported.

480 PGR: Pet., 11-16, EX1003, ¶¶169-174; PR., 14.

Without regard for support, the 480 patent claims were amended to substitute "authentication data" with "private key" during prosecution

480 Pros. Hist.

1. (Currently Amended) 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, the electronic device having an operating system creating a run-time environment for user applications, the method comprising:

providing a ~~authentication data~~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 ~~authentication data~~private key ~~are~~ is inaccessible to a user of said electronic device, wherein the ~~authentication data~~private key ~~are~~ is encrypted when the ~~authentication data~~private key ~~are~~ is stored in said memory, a decryption key for decrypting the ~~authentication data~~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, wherein said memory is inaccessible to said operating system of said electronic device, thereby rendering the ~~authentication data~~private key inaccessible to said user, wherein the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software;

providing authentication software in said electronic device, the ~~authentication data~~private key being accessible to said authentication software, wherein authentication software is stored in said secure memory inaccessible to said operating system;

activating the authentication software to generate a digital signature from the ~~authentication data~~private key, wherein the authentication software is run in a secure processing environment inaccessible to said operating system;

providing the digital signature to the second transaction party.

480 PGR: EX1002, 91; Pet. 9.

FISH.

Only one paragraph in the 480 Patent describes a private key

480 PGR Pet.

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].

480 PGR: Pet., 15; EX1001, 13:31-44.

Similar EP claims have been found to lack support

EP 099 claim 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, the electronic device having an operating system creating a run-time environment for user applications, the method comprising:

providing authentication data 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 authentication data are inaccessible to a user of said electronic device, wherein the authentication data are encrypted when the authentication data are stored in said memory, a decryption key for decrypting the authentication data being incorporated in the electronic device, said decryption key being inaccessible to said user, to any user-operated software and to said operating system, wherein said memory is inaccessible to said operating system of said electronic device, thereby rendering the authentication data inaccessible to said user;

providing authentication software in said electronic device, the authentication data being accessible to said authentication software, wherein authentication software is stored in said secure memory inaccessible to said operating system;

activating the authentication software to generate a digital signature from the authentication data, wherein the authentication software is run in a secure processing environment inaccessible to said operating system;

providing the digital signature to the second transaction party.

480 PGR: EX1015, 6, Pet., 12.

480 Patent claim 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, the electronic device having an operating system creating a run-time environment for user applications, the method comprising:

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, wherein the private key is encrypted 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, wherein said memory is inaccessible to said operating system of said electronic device, thereby rendering the private key inaccessible to said user, wherein the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software;

providing authentication software in said electronic device, the private key being accessible to said authentication software, wherein authentication software is stored in said secure memory inaccessible to said operating system;

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;

providing the digital signature to the second transaction party.

480 PGR: EX1001, 17:64-18:30.

Ward's expert used the wrong standards for claim interpretation and written description

Dr. Preneel Deposition Trans.

Q. I'm sorry.
So paragraph 37 states, "Patent claims in a PGR are given their broadest reasonable interpretation ('BRI')."
Is that correct?
A. That's correct.
Q. So is it correct that you used the BRI standard to interpret the '480 claims?
A. Yes, I did.

480 PGR: EX1034, 15:11-19; PR, 2-3.

Q. Okay. So in considering the -- like the claims and the written description and the figures, you considered the obviousness standard and then also applied the same standard for the prior art; is that correct?
A. Yes, that's correct.

480 PGR: EX1034, 20:12-17; PR, 2-3.

FISH.

The 480 Patent claims lack written description support

At least the following limitations of claim 1 do not have written description support in the 480 Patent:

- (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 (Feature A)
- (2) private key is inaccessible to a user of said electronic device (Feature B)
- (3) wherein the private key is encrypted when the private key is stored in said memory (Feature C)
- (4) wherein the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software (Feature D)

480 PGR: Pet., 15-16, EX1003, p99.

Similar features are recited in the other independent claims.

The 480 Patent does not describe Feature A

Feature A

[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,

480 PGR: Pet., v; EX1001, 18:4-8.

480 Patent

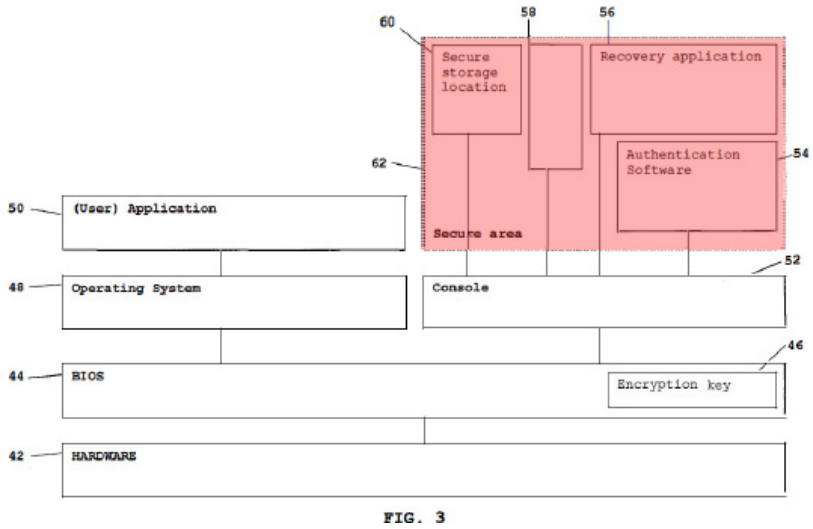


FIG. 3

480 PGR: EX1001, FIG. 3; EX1003, p100; Pet., 17.

Dr. Black's First Dec.

172. 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.

480 PGR: EX1003, ¶172; Pet., 17.

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

480 PGR: EX1003, ¶173; Pet., 18.

There is simply no disclosure that the authentication software stores the private key. (480 PGR: PR, 8; EX1032, ¶¶13-16).

FISH.

The Hague Court also found Feature A as unsupported

Hague Court Judgment (EX1015)

In the passage "a secure storage location (...) is not essential to the BIOS system with respect to the present invention" the average person skilled in the art will read no more than that the *secure location* in the device in which the authentication table or data is stored can also lie outside the BIOS. The average person skilled in the art will not unambiguously read that it is not required that the electronic device is equipped with a BIOS, nor that every storage location in the equipment is a secure storage location.

5.31. In the foregoing, the District Court also took into account the fact that WO 752 does not describe any alternative for shutting off the access of the operating system/user of the electronic device to storage locations other than by means of the BIOS. DTS also did not explain how the authentication data will be safely stored according to the patent if the BIOS is not granted a role in it.

5.32. All of the foregoing makes it clear that the average person skilled in the art will directly and unambiguously deduce from the original application that the security of transactions is achieved by storing the authentication data in a storage location within the BIOS or shielded from the operating system by the BIOS. However, this restriction resulting from the original application is not claimed in feature 1.5. The embodiments with an inextricable link to the BIOS are thus generalised to a more generic embodiment without that link. Thus, in the independent claim 1 that has been granted (i.e. insofar as it expresses that the authentication data can also be stored in 'any other secure location' in the electronic device), impermissible matter has been added.

480 PGR: EX1015, 37-41; Pet., 11-14.

FISH.

Ward's expert admits that the private key may not be a part of the authentication software

Dr. Preneel Deposition Trans.

Q. And paragraph 55, you have no citation to that statement you made; is that correct?

A. That is correct.

Q. So is it correct that the private key can also not be an integral part of the authentication software?

A. That is correct.

Q. So when you make the statement "the private key can be an integral part of the authentication software," is that -- kind of when you're interpreting the '480 patent in view of the obviousness standard, you're saying, "Yeah, it would be obvious that the private key can be an integral part of the authentication software"; is that correct?

A. That is correct, yes.

480 PGR: EX1034, 43:4-17; PR, 7.

15

FISH.

Ward's expert acknowledges that the private key *could possibly be* authentication data and may not be part of authentication software

Dr. Preneel Deposition Trans.

Q. So consistent with your earlier statement, here when you say "a private key can be authentication data," are you saying that it's technically possible for a private key to be authentication data? Is that correct?

A. That is correct.

480 PGR: EX1034, 43:25-44:14* (44:25-45:5); PR, 7.

Q. So is it correct that the private key can also not be an integral part of the authentication software?

A. That is correct.

Q. So when you make the statement "the private key can be an integral part of the authentication software," is that -- kind of when you're interpreting the '480 patent in view of the obviousness standard, you're saying, "Yeah, it would be obvious that the private key can be an integral part of the authentication software"; is that correct?

A. That is correct, yes.

480 PGR: EX1034, 43:7-17; PR, 5.

Ward erroneously relies on disclosure related to "authentication table," "authentication software," and "authentication data" for written description support of claim features related to the private key. Dr. Preneel acknowledges that the terms are not interchangeable and relies on obviousness to bridge the gap. 480 PGR: PR, 3-5.

FISH.

The 480 Patent does not describe Feature B

Feature B

[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,

480 PGR: Pet., v; EX1001, 18:4-8.

Dr. Black's First Dec.

user. In fact, since the private key is described 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. 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 VIII.A.1) 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.

480 PGR: EX1003, ¶176; Pet., 19.

480 Pat.

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.

480 PGR: EX1001, 13:31-44.

Ward incorrectly understands the paragraph above as supporting feature B, which, at best, teaches that the authentication software uses a private key to sign a digital signature. 480 PGR: PR, 7-8.

Contrary to Ward's arguments, the 480 Patent also fails to disclose the private key that is stored in a secure part of a BIOS or any other secure location. 480 PGR: PR, 9-10.

FISH.

The 480 Patent does not describe Feature C

Feature C

[1b]	wherein the private key is encrypted when the private key is stored in said memory,

480 PGR: Pet., v; EX1001, 18:4-8.

Dr. Black's First Dec.

178. 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 Section VIII.A.1.

179. The '480 Patent does disclose a "private encryption key." SAMSUNG-1001, 5:39-40. However, a private encryption key is not the same as an encrypted private key. As I noted above, a private encryption key would have been understood by a POSITA as an encryption key that is kept private. 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

480 PGR: EX1003, ¶¶178-179; Pet., 20-21.

480 Patent

The BIOS **44** may comprise an encryption key **46**. Such an encryption key **46** may be used to encrypt data and only

480 PGR: EX1001, 8:29-30.

The authentication software preferably has its own unique serial number, software ID and/or private encryption key.

480 PGR: EX1001, 5:39-40.

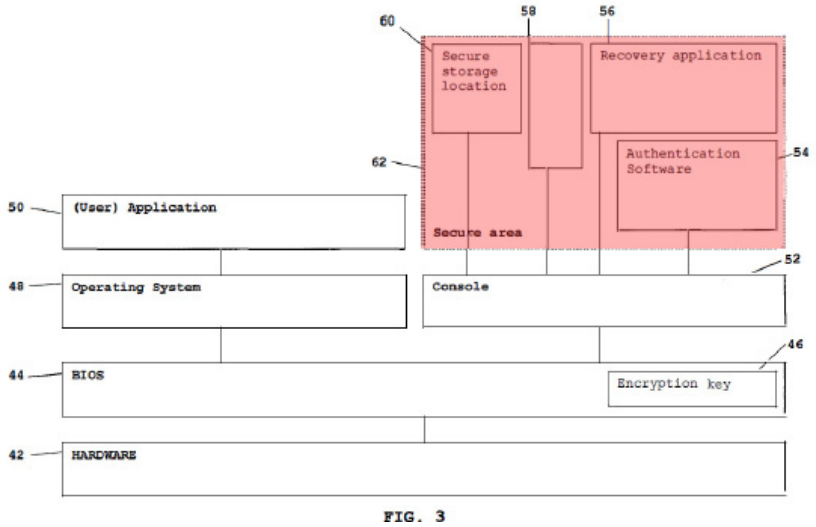


FIG. 3

480 PGR: EX1001, FIG. 3; EX1003, p100; Pet., 17.

FISH.

Ward incorrectly mixes embodiments to conjure support for Feature D

Feature D

[1f]	wherein the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software;

480 PGR: Pet., v; EX1001, 18:15-18.

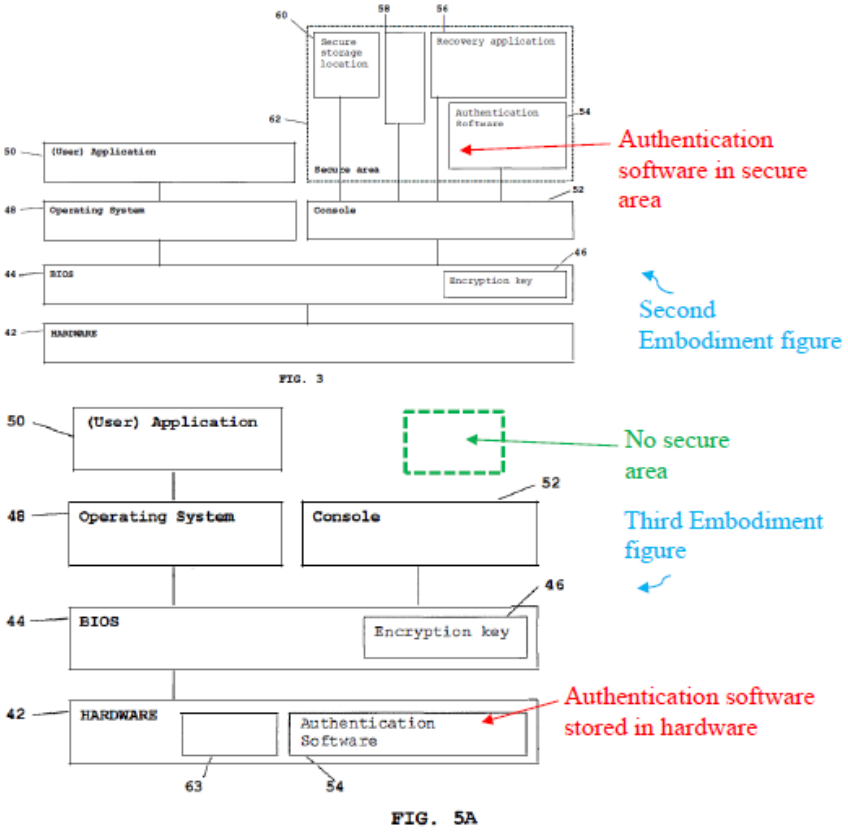
Dr. Black's First Dec.

181. 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.

183. 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.

480 PGR: EX1003, ¶¶181, 183; Pet., 21-24.

480 Pat.



480 PGR: EX1001, FIGS. 3, 5A; EX1003, p107; Pet., 23.

FISH.

The Hague Court also recognized that the 480 Patent's embodiments cannot be combined

Hague Court Judgment (EX1015)

of WO 752 relating to the third embodiment and figures belonging to that embodiment. This concerns in particular figures 5A and 5B, in which a storage location for the authentication data and software is disclosed that is not located in the BIOS. However, the third embodiment is an embodiment in which the authentication data and authentication software are stored in a memory accessible by the operating system of the electronic device (see page 15, l. 11 to 14, and page 18, l. 29 to 31). As considered above, that embodiment is not covered by the claims as granted. Indeed, the core of the granted claims is, as argued by DTS itself, that the memory in which the authentication data and authentication software are stored is not accessible to the operating system (and therefore to the user). In this respect, the Court refers to the following passage from the writ of summons: *'The essence of the patent is (...) that data is stored and processed in a secure area that is not accessible to the operating system and the user of the mobile device and to which unauthorized third parties cannot gain access'*[9] In the passages referred to by DTS in this context, it is also not mentioned that the features of the third embodiment can also be applied in the first embodiment (installation of the invention in a new electronic device) and the second embodiment (installation of the invention in an existing electronic device). This cannot be deduced from the above figures either.

480 PGR: EX1015, 38, 41; Pet., 12, 24-25.

FISH.

Issue 2

Construction of “storage …”

FISH.

Construction of "stored …"

Term	Board Construction	Patent Owner Construction	Petitioner Construction
480: *"wherein authentication software is stored in said secure memory inaccessible to said operating system" (claims 1, 16)* **; *766:* ""stored in said secure memory inaccessible to said operating system" (claims 1, 29, 33)	"encompasses being held in any secure location that is inaccessible to the operating system for an undefined amount of time."	"data (or software) remains stored in the original location (permanent memory);" ("[n]o formal claim constructions are necessary").	Agreed with the Board's construction for the purposes of these proceedings.

*** similar "storage" limitations recited in claims 17 and 18*

480 PGR: Paper 4 (ID), 24-26; POR, 58-61; PR, 14-16; 480 IPR: Paper 8 (ID), 11-14 ; POR, 57-61; PR, 1-3..
766 IPR: Paper 7 (ID), 8-11 ; POR, 46-50; PR, 2-3.

Institution Decisions (IDs)

"In fact, nothing in the Specification or the general knowledge in the art limits the 'storage' to any amount of time in the secure memory. "

480 PGR: Paper 4 (Institution Decision (ID)), 25.
480 IPR: Paper 8 (ID), 13; 766 IPR: Paper 7 ID), 10; .

FISH.

Construction of "stored …"

Petitioner Reply

First, Ward's arguments rely on a "permanent memory" or storage, which is not required by the claims. Thus, Ward's argument is untethered to the claim language and relies on elements not recited in the claims. SAMSUNG-1032, ¶26.

Second, whether data remains at an original memory location is not relevant to whether that data can then be "stored in said secure memory inaccessible to said operating system." Thus, Ward's second argument is not relevant to the claim language. Moreover, Dr. Black also explains that known principles in the art, such as the Kerckhoffs's Principle, do not support the underlying assumptions in Ward's arguments. SAMSUNG-1032, ¶¶27-30.

480 PGR: PR, 15.
480 IPR: PR, 2.
766 IPR: PR, 2-3.

Dr. Preneel Deposition Trans.

16 Q. So is it correct that buffering -- when you're
17 reading and writing to a memory, where you're reading
18 data from one place and writing it to another place, due
19 to the relative differences of speed, read/write
20 operations, you would store the data on a buffer at
21 least temporarily until you could write it to the
22 destination allocated memory location; is that correct?
23 A. That's correct.
24 Q. And how long does the buffering normally take?

480 PGR: EX1033, 84:16-24; EX1032, ¶¶27-31.
480 IPR: EX1033, 84:16-24; EX1032, ¶¶11-12.
766 IPR: EX1033, 84:16-24; EX1032, ¶¶11-12.

Dr. Preneel acknowledged that storage can involve buffering even if temporarily.

23

Issue 3

EMC renders obvious the Challenged Claims

FISH.

Ellison (USPN 7,082,615)

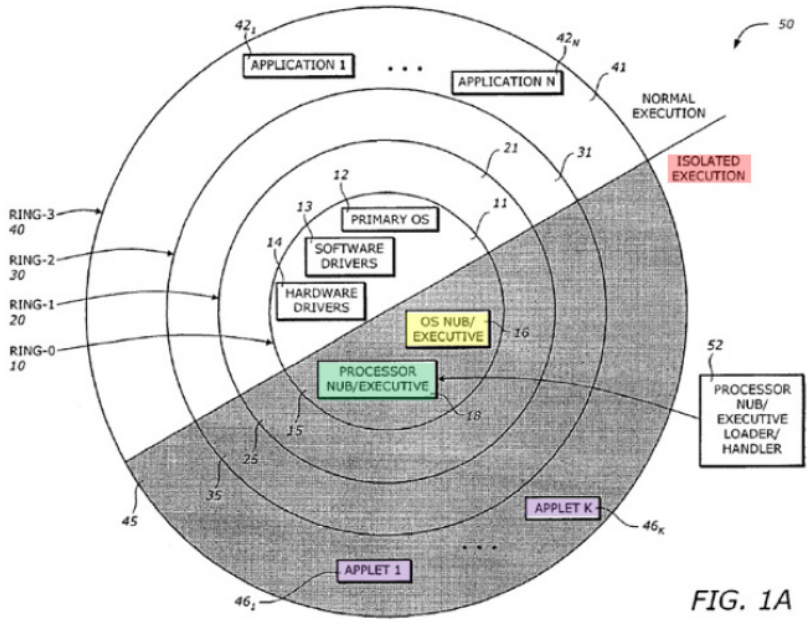


FIG. 1A

480 PGR: EX1006, FIG. 1A; EX1003, p24; Pet., 36.
480 IPR: EX1006, FIG. 1A; EX1003, p24; Pet., 12.
766 IPR: EX1006, FIG. 1A; EX1003, p24; Pet., 9.

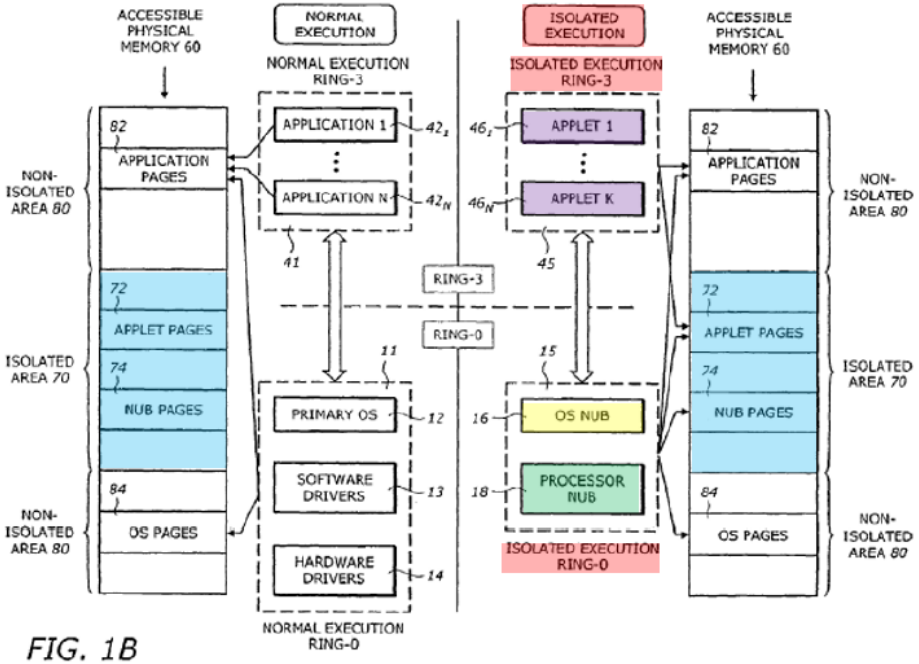


FIG. 1B

480 PGR: EX1006, FIG. 1B; EX1003, p25; Pet., 37.
480 IPR: EX1006, FIG. 1B; EX1003, p25; Pet., 13.
766 IPR: EX1006, FIG. 1B; EX1003, p25; Pet., 10.

page. The isolated mode applets 46_1 to 46_K 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.

480 PGR/480 IPR/766 IPR: EX1006, 4:1-7.

FISH.

Ellison

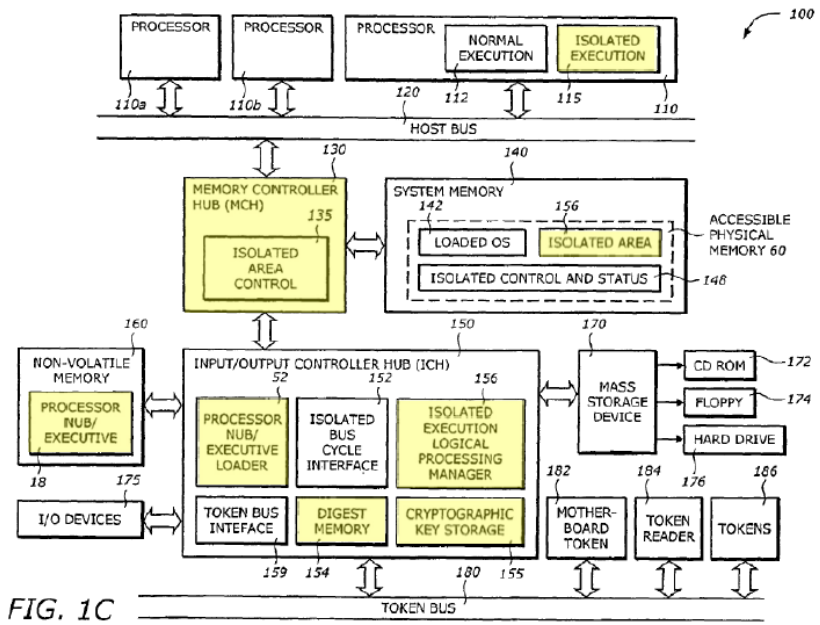


FIG. 1C

480 PGR: EX1006, FIG. 1C; EX1003, p 26; Pet., 38.
480 IPR: EX1006, FIG. 1C; EX1003, p 26; Pet., 14.
766 IPR: EX1006, FIG. 1C; EX1003, p 26; Pet., 11.

features provided by the isolated execution mode. The isolated execution circuit **115** provides a mechanism to allow the processor **110** to operate in an isolated execution mode. The isolated execution circuit **115** provides hardware and software support for the isolated execution mode. This

480 PGR/480 IPR/766 IPR: EX1006, 5:1-5.

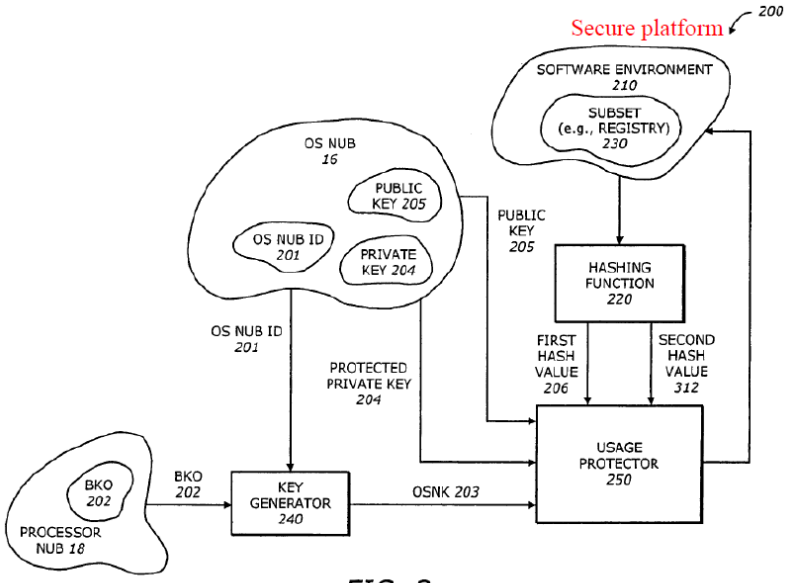


FIG. 2

480 PGR: EX1006, FIG. 2; EX1003, p 29; Pet., 41.
480 IPR: EX1006, FIG. 2; EX1003, p 29; Pet., 17.
766 IPR: EX1006, FIG. 2; EX1003, p 29; Pet., 14.

FIG. **2** is a diagram illustrating a secure platform **200** according to one embodiment of the invention. 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 either inside or outside the isolated execution environment.

480 PGR/480 IPR/766 IPR: EX1006, 8:25-32.

FISH.

Muir (PCT Pub. No. WO 01/93212)

In one embodiment, computing devices coupled to communication medium 255 may include virtual smart card 151 emulating a smart card without using a smart card reader for a smart card. For example, a user of personal data assistant 256 may use virtual smart card 151 to log on to the networking environment 250. Furthermore, 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.

480 PGR/480 IPR/766 IPR: EX1008, p12- ¶1.

Figure 5 is an illustration of an exemplary networking environment 250 for using virtual smart cards 151. Referring to **Figure 5**, networking environment 250 includes communication medium 255 coupling a plurality of computing devices with virtual smart cards 151. For example, a server 258, laptop computer 259, personal computer 257, and personal data assistant 256 each having a virtual smart card 151, may be coupled to communication medium 255. Alternatively, other types of devices having virtual smart card 151 may be coupled to communication medium 255. For example, an electronic token, cellular phone, and other electronic portable devices having a virtual smart card 151 may be coupled with communication medium 255.

480 PGR/480 IPR/766 IPR: EX1008, p33-¶3.

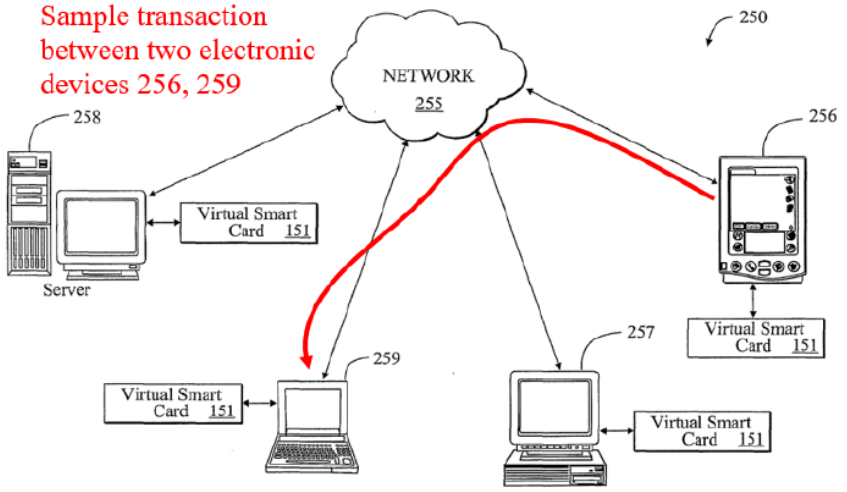


Fig. 5

480 PGR: EX1008, FIG. 5, EX1003, p32; Pet., 44.
480 IPR: EX1008, FIG. 5, EX1003, p32; Pet., 20.
766 IPR: EX1008, FIG. 5, EX1003, p32; Pet., 17.

FISH.

Muir

Computing system 110 includes application 120, device operating system 125, smart card interface 150, and virtual smart card 151. Virtual smart card 151 includes virtual smart card driver 155 and memory 140. Memory 140 is 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 and applications Virtual smart card 151 provides software code, which upon execution, emulates a physical smart card for device operating system 150.

480 PGR/480 IPR/766 IPR: EX1008, p7-¶4.

Virtual smart card driver 155 uses such restricted memory 170 to store private keys 167. Virtual smart card driver 155 may further use restricted memory space 170 to store encrypted and decrypted data. In one embodiment, the restricted memory space 170 is on the hard drive. In another embodiment, restricted memory space 170 may be any type storage media, i.e. random access memory (RAM), read-only memory (ROM), electrically erasable programmable ROM (EEPROM), flash memory, compact disc (CD), CDROM, floppy, etc.

Private key 167 is data that is unique to a specific user. Private key 167 may be used in a public-key (PK) infrastructure. Alternatively, private key 167 may be used in a secret key infrastructure. Private key 167 may be used for a number of security functions such as providing digital signatures that are unique to private key(s) 167.

480 PGR/480 IPR/766 IPR: EX1008, p9-¶4- p10-¶2.

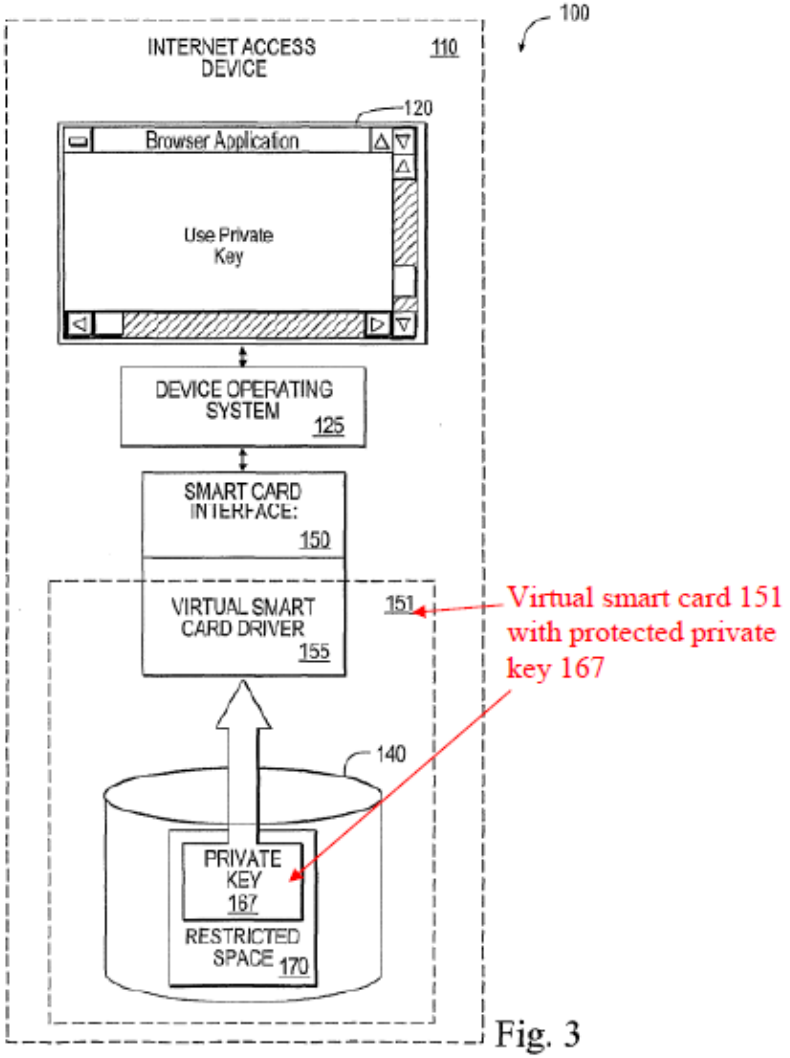


Fig. 3

480 PGR: EX1008, FIG. 3; EX1003, p34; Pet., 46.
480 IPR: EX1008, FIG. 3; EX1003, p34; Pet., 22.
480 PGR: EX1008, FIG. 3; EX1003, p34; Pet., 19.

FISH.

A POSITA would have combined Ellison and Muir

Dr. Black's 1st Dec.

- To implement Ellison's system in e-commerce and B2B transactions (as alluded to in Epstein and disclosed by Muir)

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. However, Ellison does not reveal details of such a system or transaction between multiple parties. Muir does.

480 PGR: EX1003, ¶¶64, 66, Pet., 47-48.
480 IPR: EX1003, ¶¶64, 66, Pet., 23-24.
766 IPR: EX1003, ¶¶65, 67, Pet., 20-21.

- To improve speed performance, flexibility, and reduced costs

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,

480 PGR: EX1003, ¶¶67, Pet., 49-50.
480 IPR: EX1003, ¶67, Pet., 25-26.
766 IPR: EX1003, ¶68, Pet., 23.

- To implement Ellison's system in multi-party system

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. 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

480 PGR: EX1003, ¶69, Pet., 49-50; 480 IPR: EX1003, ¶69, Pet., 25-26.
766 IPR: EX1003, ¶70, Pet., 23.

FISH.

EMC renders obvious securely generating and transmitting a digital signature

Ellison

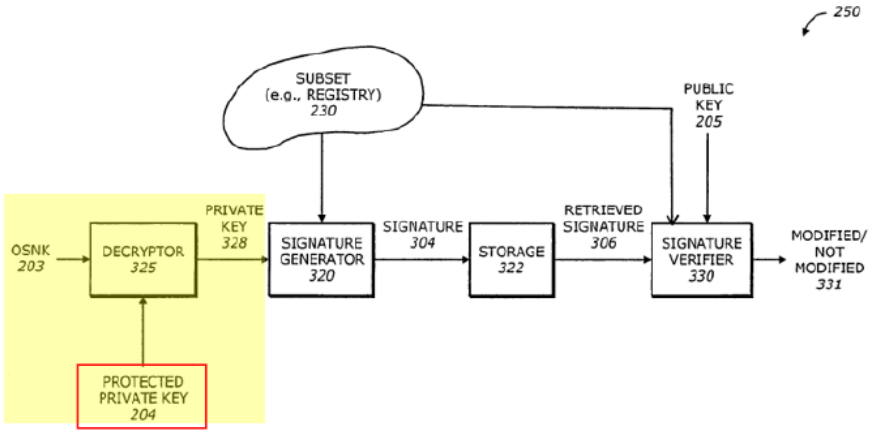


FIG. 3C

480 PGR: EX1006, FIG. 3C; EX1003, p64; Pet., 62.
480 IPR: EX1006, FIG. 3C; EX1003, p64; Pet., 38.
766 IPR: EX1006, FIG. 3C; EX1003, p64; Pet., 62.

FIG. **3C** is a diagram illustrating the usage protector **250** shown in FIG. **2** according to one embodiment of the invention. The usage protector **250** includes a decryptor **325**, a signature generator **320**, a storage medium **322**, and a signature verifier **330**.

480 PGR/480 IPR/766 IPR: EX1006, 10:63-67.

an external random number generator. In one embodiment, the protected private key **204** is generated by the platform **200** itself the first time the platform **200** is powered up. The platform **200** includes a random number generator to create random numbers. When the platform **200** is first powered up, a random number is generated upon which the protected private key **204** is based. The protected private key **204** can then be stored in the multiple key storage **164** of the non-volatile flash memory **160**. The feature of the protected private key **204** is that it cannot be calculated from its associated public key **205**. 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.

480 PGR/480 IPR/766 IPR: EX1006, 8:49-65.

Ward's contention contradicts Ellison's teachings

Ellison

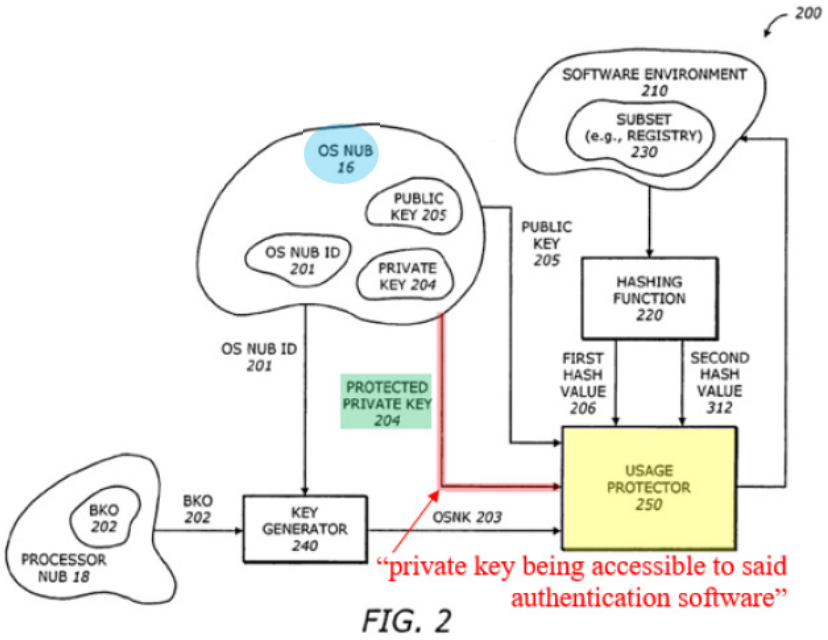


FIG. 2

480 PGR: EX1006, FIG. 2; EX1003, p71; Pet., 69.

associated public key **205**. 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.

480 PGR/480 IPR/766 IPR: EX1006, 8:61-65.

drivers **14**. The isolated execution Ring-0 **15** includes an operating system (OS) nub **16** and a processor nub **18**. The 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. The processor nub

480 PGR/480 IPR/766 IPR: EX1006, 3:15-21.

Ward incorrectly argues that "combining Muir with Ellison would nullify the purpose of Ellison because any request to create a digital signature would come through the primary OS 12 operating with the driver 155 without even touching the isolated execution environment of Ellison." 480 PGR: PO, 29; EX1032, ¶48.

Issue 4

Ellison's OS 12 corresponds to the claimed operating system

[1d]	said decryption key being inaccessible to said user, to any user-operated software and to said operating system,
[1pre-2]	the electronic device having an operating system creating a run-time environment for user applications and authentication software running in a separate operating environment, independent from and inaccessible to the operating system,
[1f]	wherein the authentication software is run in a secure processing environment inaccessible to the operating system; and

480 PGR/480 IPR: Pet., v; EX1001, 18:10-12.

766 IPR: Pet., v; EX1001, 18:13-17.

766 IPR: Pet., vi; EX1001, 18:41-43.

FISH.

Ellison's OS 12 corresponds to the claimed "operating system"

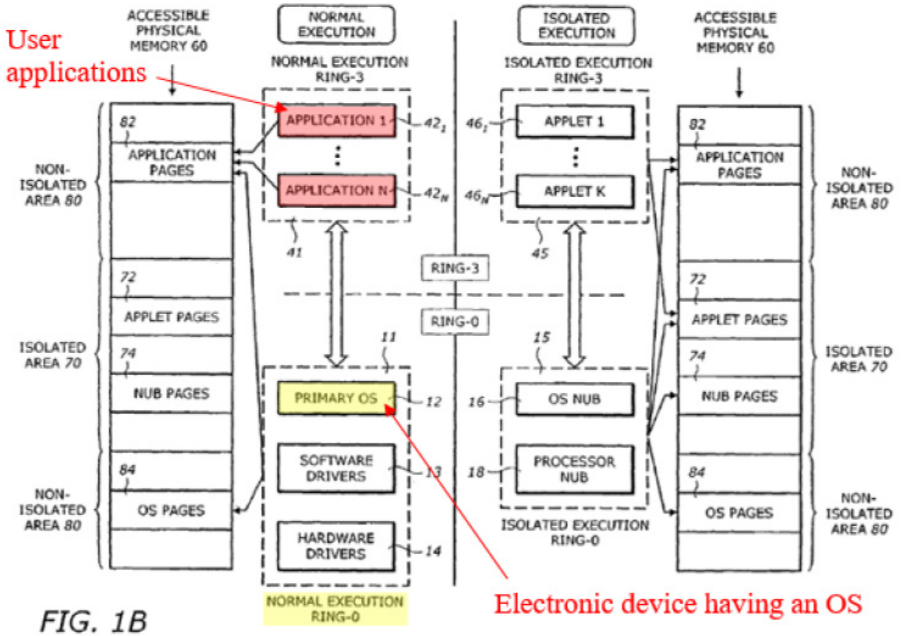
[1d]	said decryption key being inaccessible to said user, to any user-operated software and to said operating system,

480 PGR/480 IPR: Pet., v; EX1001, 18:10-12.

- There is no reason Ellison's OS 12 cannot be the only OS mapped to the claimed OS.
- Ellison's FIG. 1B depicts primary OS 12 in the normal execution region.

480 PGR: PR, 18-19; EX1032, ¶¶35-36; EX1003, ¶¶46-47; EX1006, 2:57-4:29.
480 IPR: PR, 5-9; EX1003, ¶101; EX1032, ¶¶15-16; EX1006, 2:57-4:29.
766 IPR: PR, 9-10; EX1003, ¶¶125-126; EX1032, ¶15;

Ellison's FIG. 1B



480 PGR: EX1006, FIG. 1B; EX1003, p56; Pet., 84.
480 IPR: EX1006, FIG. 1B; EX1003, p56; Pet., 60.
766 IPR: EX1006, FIG. 1B; EX1003, p61; Pet., 28.

FISH.

The OSNK 203 "decryption key" is not accessible to OS 12

[1pre-2]	the electronic device having an operating system creating a run-time environment for user applications and authentication software running in a separate operating environment, independent from and inaccessible to the operating system,

766 IPR: Pet., v; EX1001, 18:13-17.

- 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.***" EX1006, 9:1-6.

- The OS nub 16 and the processor nub 18 operate within an isolated execution environment, and the OSNK 203 is generated and used in the same isolated execution environment of secure platform 200.

480 PGR: PR, 19; EX1032, ¶37; Pet., 40-42.
480 IPR: PR, 7; EX1032, ¶18; Pet., 16-20.
766 IPR: PR 16-18; EX1032, ¶¶13-20; Pet., 14-17.

Ellison's FIG. 2

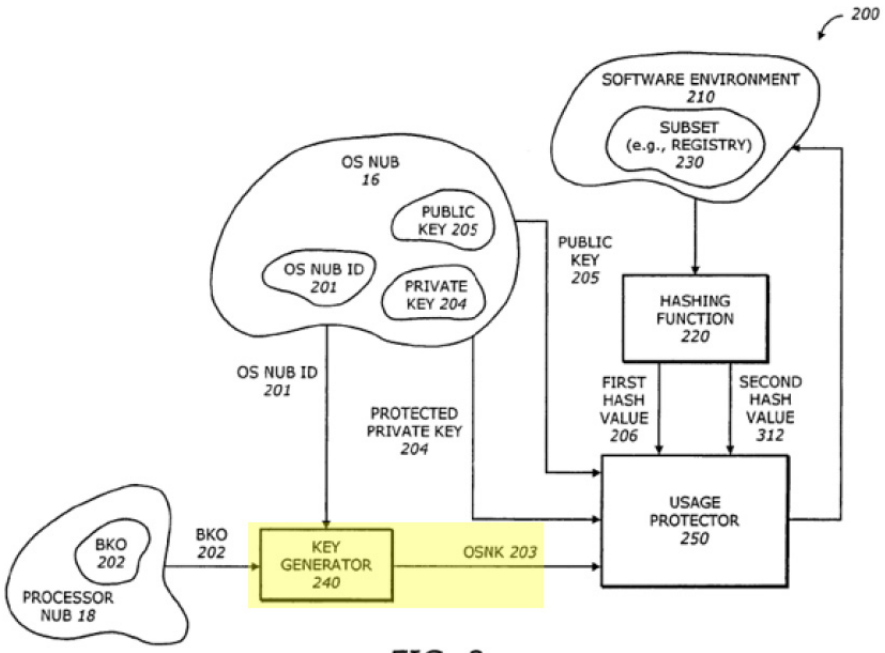


FIG. 2

480 PGR: EX1006, FIG. 2; EX1003, p66; Pet., 64.
480 IPR: EX1006, FIG. 2; EX1003, p66; Pet., 40.
766 IPR: EX 1006, FIG. 2; EX1003, p29; Pet., 40.

FISH.

OS nub 16 is part of the isolated region or "secure platform 200"

[1f]	wherein the authentication software is run in a secure processing environment inaccessible to the operating system; and

766 IPR: Pet., vi; EX1001, 18:41-43.

Dr. Black's 2nd Dec.

- OS nub 16 and other components of Ellison's system that are part of ***an isolated execution region***, which cannot be attacked in the manner Ward claims.

- Ward provides no citations or support for its conclusory assertions.

480 PGR: EX1032, ¶¶35-38.
480 IPR: EX1032, ¶¶16-19.
766 IPR: EX1032, ¶¶16-19.

Ellison

FIG. **2** is a diagram illustrating a secure platform **200** according to one embodiment of the invention. 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 either inside or outside the isolated execution environment.

480 PGR/480 IPR/766 IPR: EX1006, 8:25-32.

Ellison

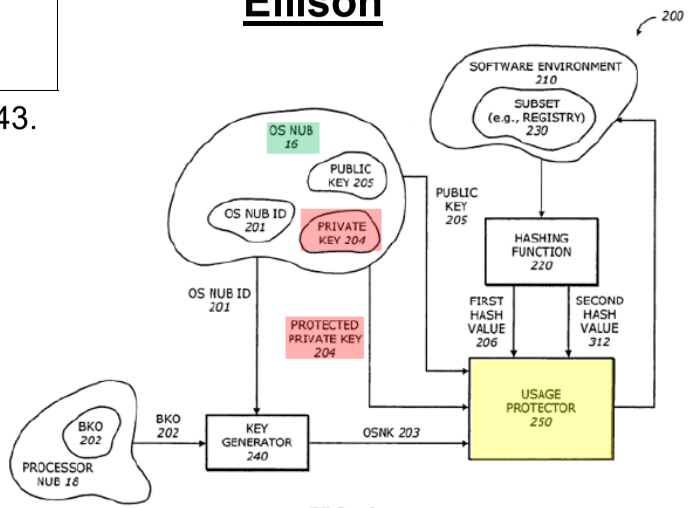


FIG. 2

480 PGR: EX1006, FIG. 2; EX1003, p79; Pet., 77.
480 IPR: EX1006, FIG. 2; EX1003, p79;Pet., 53.

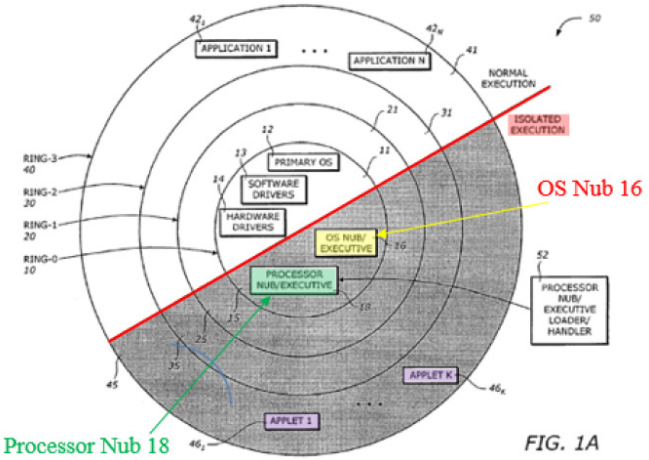


FIG. 1A

766 IPR: EX1006, FIG. 1A; EX1003, p74; Pet., 40.

FISH.

Issue 5

EMC renders obvious an authentication software being stored in a secure memory and being inaccessible to an operating system, as recited in 480 feature [1i] & 766 feature [1d]

[1i]	wherein authentication software is stored in said secure memory inaccessible to said operating system;

480 PGR/480 IPR: Pet., v; EX1001, 18:21-23.

[1d]	wherein the authentication software is stored in the secure area inaccessible to the operating system;

766 IPR: Pet., v; EX1001, 18:38-39.

FISH.

Ellison's usage protector corresponds to the "authentication software"

[1i]	wherein authentication software is stored in said secure memory inaccessible to said operating system;

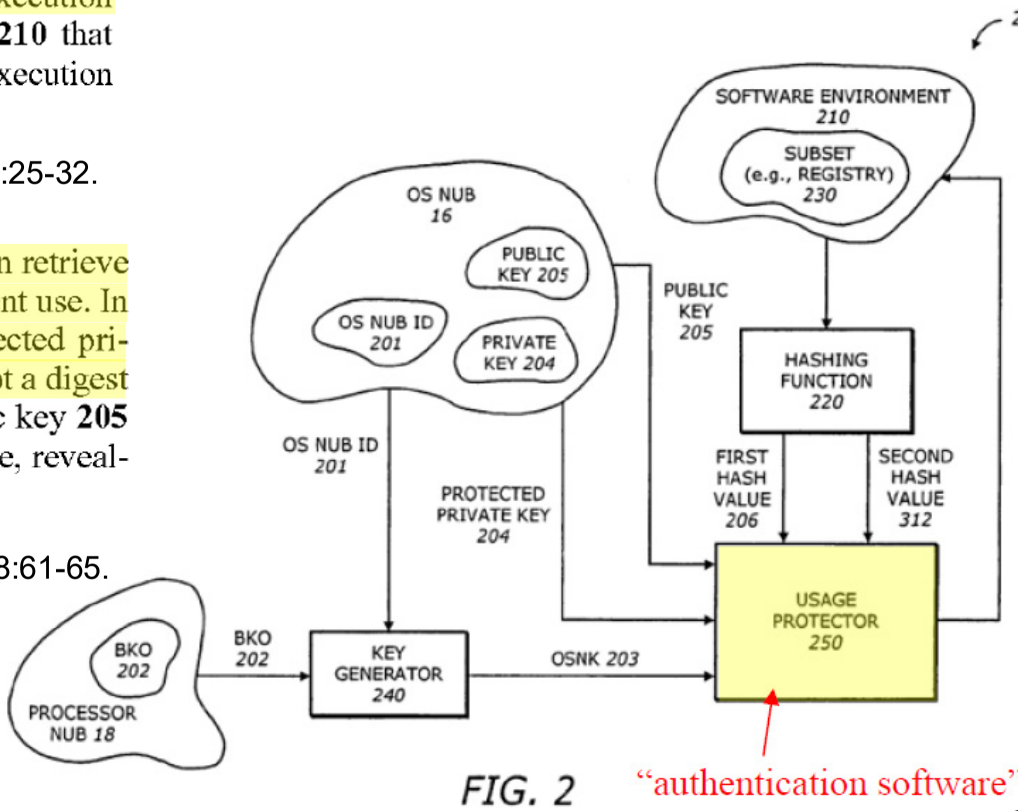
480 PGR/480 IPR: Pet., v; EX1001, 18:21-23.

FIG. **2** is a diagram illustrating a secure platform **200** according to one embodiment of the invention. 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 either inside or outside the isolated execution environment.

480 PGR/480 IPR/766 IPR: EX1006, 8:25-32.

associated public key **205**. 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.

480 PGR/480 IPR/766 IPR: EX1006, 8:61-65.



480 PGR: EX1006, FIG. 2; EX1003, p70; Pet., 68.
480 IPR: EX1006, FIG. 2; EX1003, p70; Pet., 44.
766 IPR: EX1006, FIG. 2; EX1003, p80; Pet., 46.

Ellison's usage protector corresponds to the "authentication software"

[1i]	wherein authentication software is stored in said secure memory inaccessible to said operating system;

480 PGR/480 IPR: Pet., v; EX1001, 18:21-23.

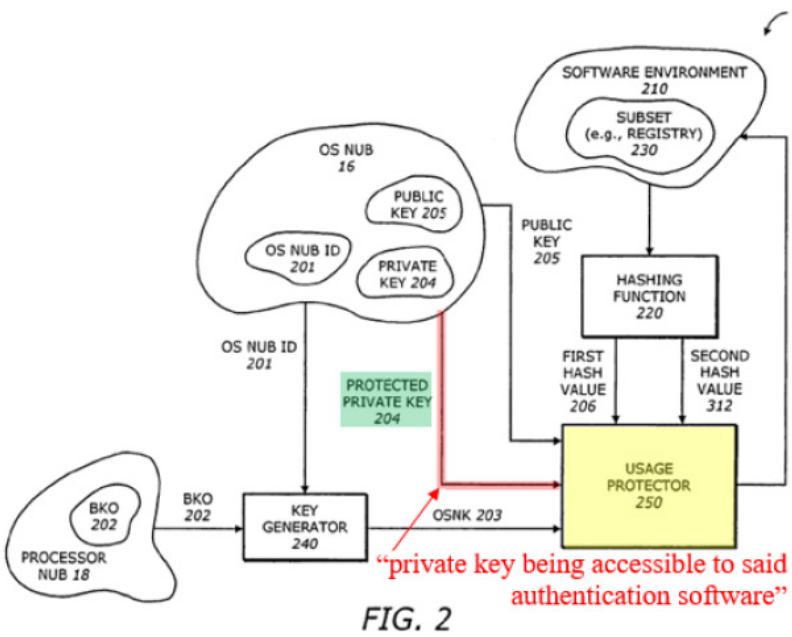


FIG. 2

480 PGR: EX1006, FIG. 2; EX1003, p71; Pet., 69.
480 IPR: EX1006, FIG. 2; EX1003, p71; Pet., 45.
766 IPR: EX1006, FIG. 2; EX1003, p81; Pet., 47.

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**. It

480 PGR/480 IPR/766 IPR: EX1006, 11:1-5.

FIG. **3C** is a diagram illustrating the usage protector **250** shown in FIG. **2** according to one embodiment of the invention. The usage protector **250** includes a decryptor **325**, a signature generator **320**, a storage medium **322**, and a signature verifier **330**.

480 PGR/480 IPR/766 IPR: EX1006, 10:63-67.

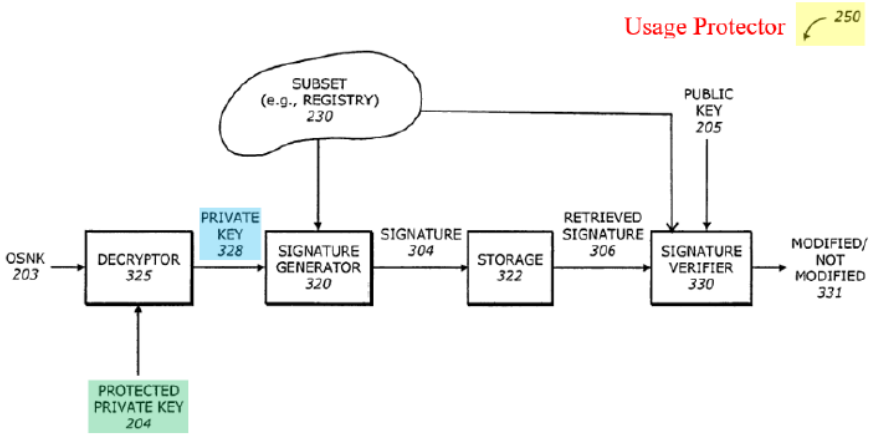


FIG. 3C

480 PGR: EX1006, FIG. 3C; EX1003, p72; Pet., 70.
480 IPR: EX1006, FIG. 3C; EX1003, p72; Pet., 46.
766 IPR: EX1006, FIG. 3C; EX1003, p82; Pet., 48.

The Board's construction and even Dr. Preneel's understanding of storage/buffering confirms that feature [1i] is obvious

[1d]	wherein the authentication software is stored in the secure area inaccessible to the operating system;

766 IPR: Pet., v; EX1001, 18:38-39.

Institution Decision

In view of the Specification and the general knowledge in the art, we determine that the term "stored in the secure memory inaccessible to the operating system" encompasses being held in any secure location that is inaccessible to the operating system for an undefined amount of time. The parties are invited to address this claim construction issue during trial, if so desired.

480 PGR: ID, 25-26.
480 IPR: ID, 14.
766 IPR: ID, 11.

Dr. Preneel Deposition Trans.

Q. So is it correct that buffering -- when you're reading and writing to a memory, where you're reading data from one place and writing it to another place, due to the relative differences of speed, read/write operations, you would store the data on a buffer at least temporarily until you could write it to the destination allocated memory location; is that correct?

A. That's correct.

480 PGR: EX1033, 84:16-24; EX1032, ¶¶27-31.
480 IPR: EX1033, 84:16-24; EX1032, ¶¶11-12.
766 IPR: EX1033, 84:16-24; EX1032, ¶¶11-12.

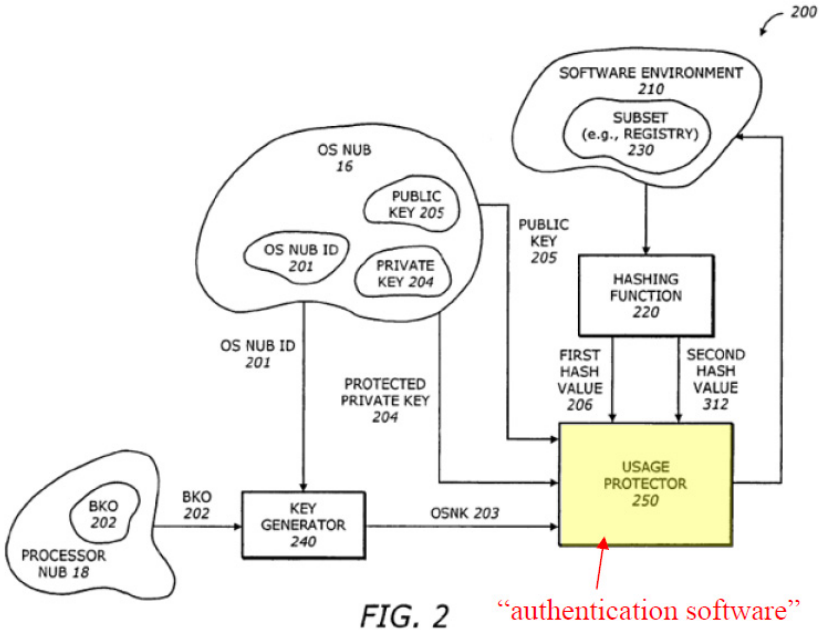
Ward's arguments rely on limitations not recited

[1d]	wherein the authentication software is stored in the secure area inaccessible to the operating system;

766 IPR: Pet., v; EX1001, 18:38-39.

- Ward argues that "Ellison does not teach or suggest authentication software *for securing user transactions*."
- But neither [1i]/[1d] nor the 480 and 766's claim 1, considered as a whole, recite storing authentication software *for securing transactions.*
- Ward also makes arguments similar to the ones noted in previous slides with respect to the "operating system" for 480's [1i] and 766's [1d]. These arguments fail for the same reasons noted above.

480 PGR: EX1032, ¶¶40-41.
480 IPR: EX1032, ¶¶21-22.
766 IPR: EX1032, ¶¶22-23.



480 PGR: EX1006, FIG. 2; EX1003, p63; Pet., 29.
480 IPR: EX1006, FIG. 2; EX1003, p70; Pet., 44.
766 IPR: EX1006, FIG. 2; EX1003, p63; Pet., 29.

FISH.

EMC does not bodily incorporate all aspects of Muir's virtual smart card, as Ward represents

- Ward argues that EMC fails because Muir's *virtual smart card driver 155* is not stored in a secure memory.
  - *Not relevant.* Petitioner did not argue that Muir's *virtual smart card driver 155* is stored in a secure memory (nor is it required by the claim).
  - EMC does not bodily incorporate all aspects of Muir's virtual smart card driver 155 or device 110, as Ward represents.
- The Ellison and Muir combination would have been obvious at least because Muir discloses a restricted space 170 that stores a private key 167 (similar to the manner in which Ellison handles its private key).

480 PGR: PR, 22; EX1032, ¶42.
480 IPR: PR, 10; EX1032, ¶22.
766 IPR: PR, 15-16; EX1032, ¶¶30-31.

Muir

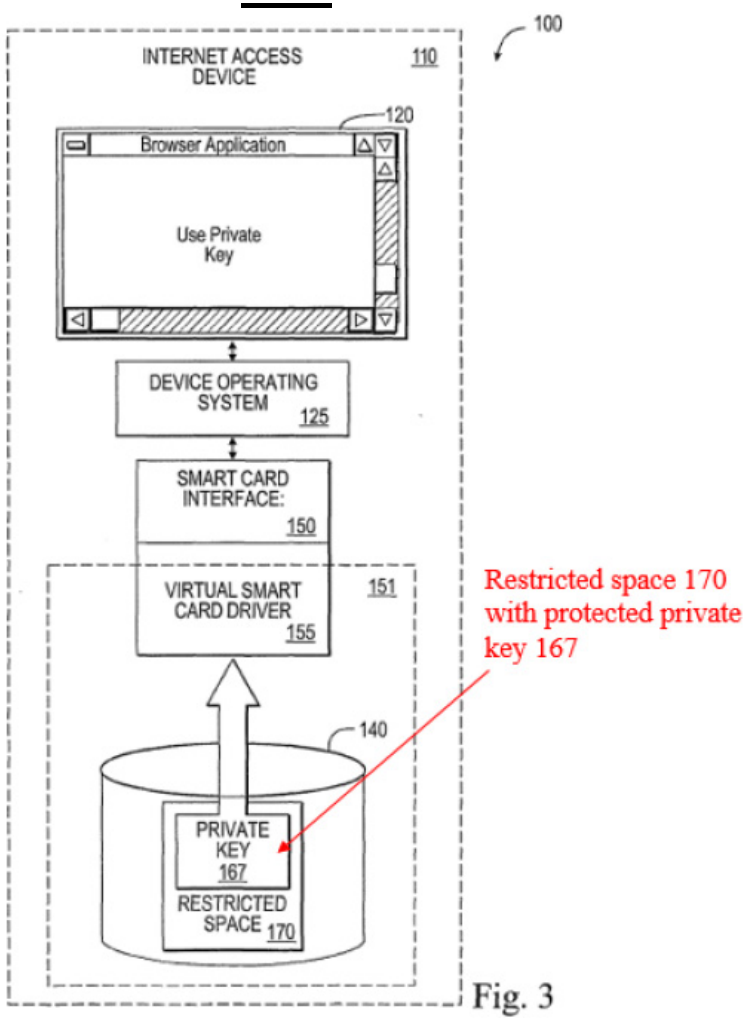


Fig. 3

480 PGR: EX1008, FIG. 3; EX1003, p34; Pet., 46.
480 IPR: EX1008, FIG. 3; EX1003, p34; Pet., 22.
480 PGR: EX1008, FIG. 3; EX1003, p34; Pet., 19.

FISH.

Issue 6

EMC renders obvious a private key in a memory as recited in 480 feature [1a]

[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,

480 PGR/480 IPR: Pet., v; EX1001, 18:3-7.

FISH.

Ward's contention regarding [1a] contradicts Ellison's teachings

Feature [1a]

[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,

480 PGR/480 IPR: Pet., v; EX1001, 18:4-8.

Ward POR

Ward argues that "Ellison discloses a private key 204 for the protection of the isolated environment itself, but not for the protection of digital transactions involving two parties."

480 PGR: POR, 35.
480 IPR: POR, 35.

Ellison

associated public key **205**. 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.

480 PGR/480 IPR: EX1006, 8:61-65.

Petitioner Reply

Next, Ward argues that EMC does not render obvious [1a]. POR, 47. Without any support or citations, Ward argues that "Ellison discloses a private key 204 for the protection of the isolated environment itself, but not for the protection of digital transactions involving two parties." POR, 47. Again, this is false. Ellison teaches that the private key 204 can be used "to encrypt a digest of a message producing a signature." SAMSUNG-1006, 8:59-65. In addition, in EMC, Muir clearly discloses using a digital signature for transactions between two parties. SAMSUNG-1008, pp. 9-¶3, 2-¶1, 3-¶¶1-2, 6-¶3, 10-¶¶1-2, 12-¶1, 18-¶6; Pet., 73-74; SAMSUNG-1032, ¶48.

480 PGR: PR, 25.
480 IPR: PR, 13.

Issue 7

EMC renders obvious “user applications” as recited in 766 feature [1pre-2]

FISH.

Ellison's OS 12 would have been understood to support user applications

[1pre-2]	the electronic device having an operating system creating a run-time environment for user applications and authentication software running in a separate operating environment, independent from and inaccessible to the operating system,

766 IPR: Pet., v; EX1001, 18:13-17.

Petitioner Reply

Second, to the extent the claimed operating system would have been understood to support user programs, as Ward appears to argue, Ellison's OS 12 provides such support. POR, 21 ("According to the ordinary meaning of the 'operating system', in a computer system, the 'operating system' help user programs to manage resource"), 19-22. For instance, Ellison's FIG. 1B clearly depicts primary OS 12 in the normal execution region and Ellison explains that OS 12 interacts with OS pages 84, application pages 82, and applets 42_1-42_K, which are user applications in the non-isolated region. SAMSUNG-1006, 2:57-4:29, FIGS. 1A, 1B. In contrast, applets 46_1-46_K run in the isolated execution area (e.g., isolated execution ring-3) that is a separate operating environment, independent from and inaccessible to, the OS 12. SAMSUNG-1006, 2:57-4:29, FIGS. 1A, 1B; SAMSUNG-1032, ¶16.

766 IPR: PR, 6-7.

Ellison

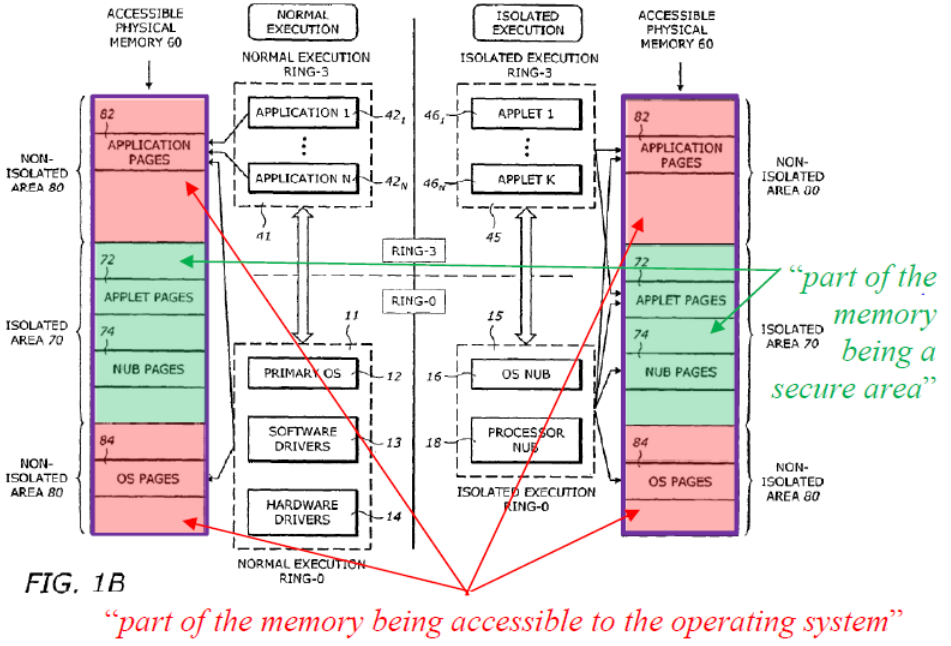


FIG. 1B

766 IPR: EX1006, FIG. 1B; EX1003, p64; Pet., 31.

Claim 1 does not recite limitations that would require all applets to be mapped to "user applications"

[1pre-2]	the electronic device having an operating system creating a run-time environment for user applications and authentication software running in a separate operating environment, independent from and inaccessible to the operating system,

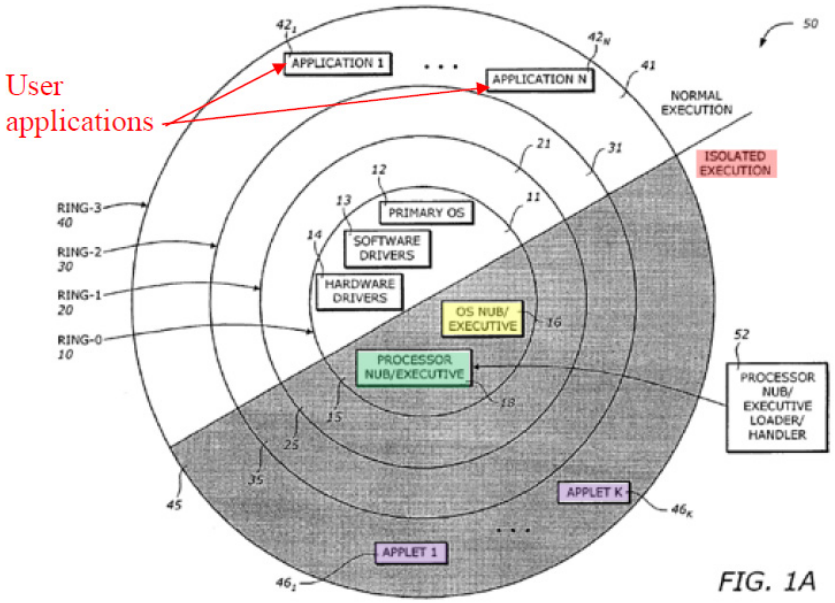
766 IPR: Pet., v; EX1001, 18:13-17.

Petitioner Reply

Third, Ward concedes that Ellison's applets 46_1-46_K 12 are "user applications," but incorrectly argues that Ellison's applets 42_1-42_K and applets 46_1-46_K must both be mapped to the claimed "user applications" (not just applets 46_1-46_K). POR, 23-24. However, like Ward's OS argument noted-above, the '766 Patent imposes no requirement that both applets 42_1-42_K and applets 46_1-46_K must be mapped to the claimed "user applications." For example, claim 1 does not recite "all user applications" or any other limitation that would require all applets (or even both applets 42_1-42_K and applets 46_1-46_K) in Ellison's system to be mapped to the claimed "user applications." Thus, Ward's "user applications" argument also fails. SAMSUNG-1032, ¶17.

766 IPR: PR, 7.

Ellison



766 IPR: EX1006, FIG. 1A; EX1003, p61; Pet., 27.

46

Issue 8

EMC renders obvious accessing a memory and selectively reporting memory locations, as recited in 766 feature [1pre-4]

[1pre-4]	wherein the electronic device comprises a system for accessing a memory location in the memory, wherein the system for accessing the memory location is configured to selectively report the storage locations of the secure area,

766 IPR: Pet., v; EX1001, 18:21-25.

FISH.

EMC renders obvious "selectively reporting …"

[1pre-4]	wherein the electronic device comprises a system for accessing a memory location in the memory, wherein the system for accessing the memory location is configured to selectively report the storage locations of the secure area,

766 IPR: Pet., v; EX1001, 18:21-25.

Muir

Virtual smart card driver 155 also includes an address pointer 171 to restricted memory space 170. In alternate embodiments, address pointer 171 may point to a number of addresses or locations for restricted memory space 170. In one embodiment, hidden memory space 170 is contiguous. Alternatively, hidden memory space 170 may be non-contiguous. In one embodiment, virtual smart card driver 155 uses address pointer 171 to send data to and retrieve data from restricted memory space 170.

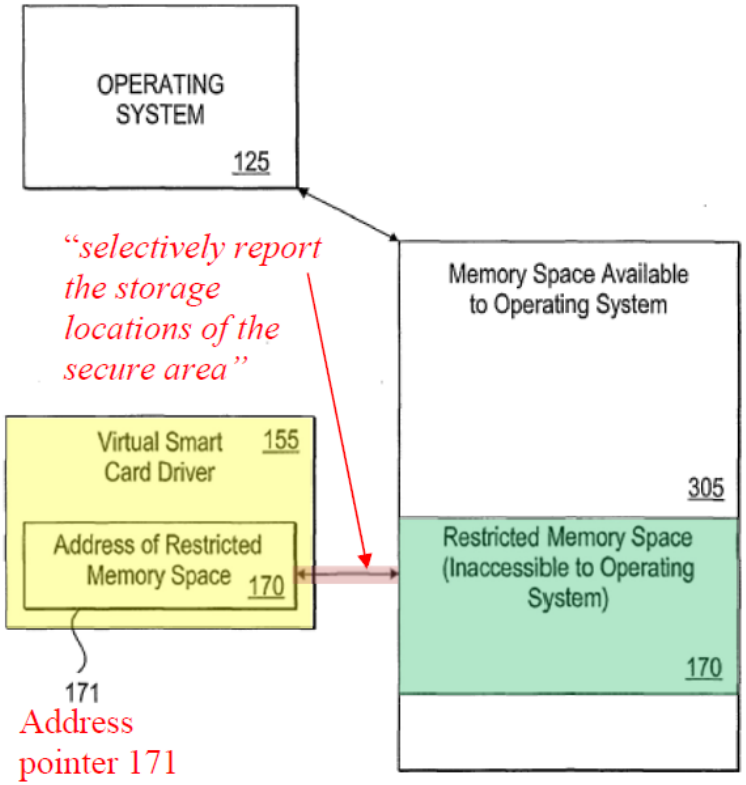
776 IPR: EX1008, p13-¶1.

Dr. Black's 2nd Dec.

- Pet. relied upon Muir's disclosure of selective reporting of the locations of the restricted memory space 170.

776 IPR: EX1032, ¶25.

Muir



766 IPR: EX1008, FIG. 6; EX1003, p71; Pet., 37.

EMC renders obvious "accessing a memory"

Ellison

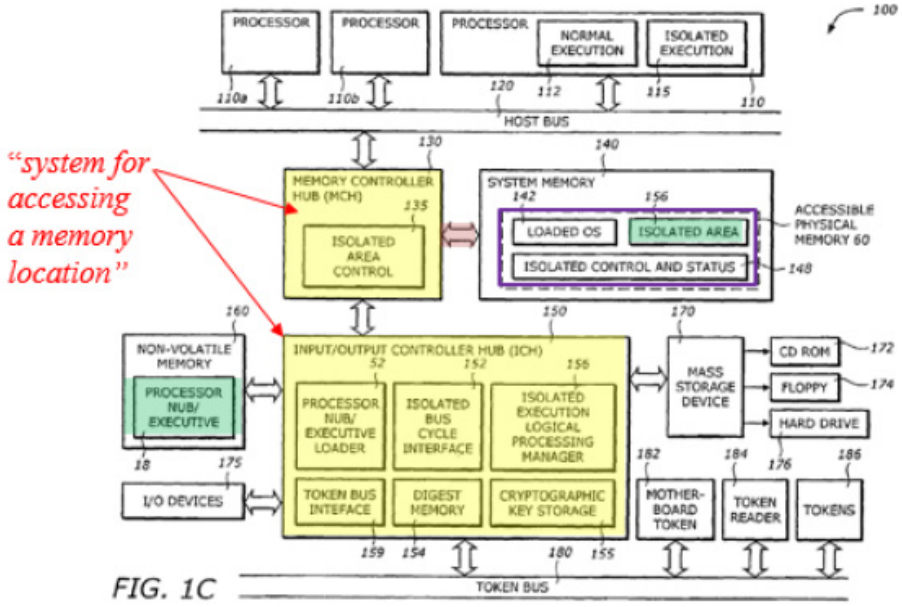


FIG. 1C

776 IPR: EX1006, FIG. 1C; EX1003, p70; Pet., 36.

35 can be used, including using programmable configuring registers. The ICH **150** has a number of functionalities that are designed to support the isolated execution mode in addition to the traditional I/O functions. In particular, the ICH **150** includes an isolated bus cycle interface **152**, the
40 processor nub loader **52** (shown in FIG. **1**A), a digest memory **154**, a cryptographic key storage **155**, an isolated execution logical processor manager **156**, and a token bus interface **159**.

776 IPR: EX1006, 6:35-43.

Dr. Black's 1st. Dec.

108. SAMSUNG-1006, 5:57-67. In addition, an input/output controller hub (ICH) 150 can be integrated with the MCH 130, controls access and connection to non-volatile memory 160, and "support[s] the isolated execution mode in addition to the traditional I/O functions." SAMSUNG-1006, 4:38-56, 6:27-7:32, FIG. 1C (reproduced below). Because MCH 130 and ICH 150 control and configure the system memory 140 (which includes physical memory 60 and isolated (memory) area 156/70) and the memory 160, it would have been obvious to a POSITA that Ellison's MCH 130 and ICH 150 would have ***access to a memory location in the isolated area 70 and the memory 160*** and would have been "***configured to selectively report the storage locations of the secure area***" as part of its control and configuration of system memory 140. SAMSUNG-1006, 5:57-6:26. Reporting of the secure locations would have been selective because such locations would not have been reported to components (e.g., OS 12) that are not allowed to access the secure locations while being reported to other components (e.g., processor 110 in isolated execution mode 115) with access. A POSITA would have found it obvious that Ellison's MCH 130 and ICH 150 are "a system for accessing a memory location in the memory."

776 IPR: EX1003, ¶108.

FISH.