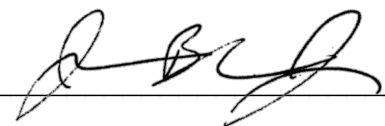


IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

SECOND DECLARATION OF DR. BLACK

I declare that all statements made herein on my own knowledge are true and that all statements made on information and belief are believed to be true, and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

By: _____

John R. Black, Jr.

Date: Nov 28, 2022 _____

Table of Contents

I.	Introduction.....	4
II.	Ward failed to provide evidence that the '480 Patent satisfies the written description requirement	5
A.	The '480 Patent fails to include written description support for “providing a private key in a memory of said electronic device, wherein said memory being a secure part of a Basic In Out System or any other secure location in said electronic device operated by the first transaction party,” (“Feature A”)	5
B.	The '480 Patent fails to include written description support for “[the] private key is inaccessible to a user of said electronic device,” (“Feature B”).....	9
C.	The '480 Patent fails to include written description support for “the private key is encrypted when the private key is stored in said memory,” (“Feature C”).....	12
D.	The '480 Patent fails to include written description support for “the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software,” (“Feature D”) as required by claim 1.	13
III.	Claim Construction.....	15

IV.	The '480 Claims are obvious in view of the grounds identified in my first declaration.....	18
A.	The POR and Expert Testimony are not tied to the prior art references	18
B.	Ellison and Muir render obvious the “decryption key being inaccessible to said user, to any user-operated software and to said operating system” (feature [1d])	18
C.	Ellison and Muir render obvious “authentication software is stored in said secure memory inaccessible to said operating system” (feature [1i])... ..	23
D.	Ellison and Muir render obvious claim 1	24
V.	Conclusion	28

I. Introduction

1. I previously submitted a declaration (“**SAMSUNG-1003**”) in support of a post grant review (PGR) petition (“**Pet.**” or “**Petition**”) challenging the validity of claims 1-19 (“**Challenged Claims**”) of U.S. Patent No. 10,992,480 (“**the ’480 Patent**”). I have reviewed the response by the Patent Owner (hereinafter referred to as “**Ward**”) and the accompanying declaration of Ward’s expert, Dr. Preneel. In this declaration, I provide additional remarks in response to Ward’s Patent Owner Response (“**POR**”) and Dr. Preneel’s declaration in support of the Petitioner Reply.

2. In preparing this declaration, I have reviewed the exhibits supporting the POR and the transcripts of Dr. Preneel’s two depositions on November 1 and 4, 2022 with respect to the ’480 Patent and its parent, U.S. Patent No. 11,063,766 (“**the ’766 Patent**”). I have continued to consider materials through the lens of one of ordinary skill in the art (POSITA) as defined in my previous declaration.

3. I have no financial interest in the outcome of this proceeding. I am being compensated for my work as an expert on an hourly basis. My compensation is not dependent on the outcome of these proceedings or the content of my opinions.

4. In writing this declaration, I have considered the following: my own knowledge and experience, including my work experience in the fields of computer science generally and computer security specifically; my experience in

teaching those subjects; and my experience in working with others involved in those fields. In addition, I have analyzed various publications and materials, in addition to other materials I cite in my declaration.

5. My opinions, as I explained below, are based on my education, experience, and expertise in the fields relating to the '480 Patent. Unless otherwise stated, my testimony below refers to the knowledge of one of ordinary skill in the art as of June 2003. Figures appearing within this document have been prepared with the assistance of Counsel and reflect my understanding of the '480 Patent and the prior art discussed below.

II. Ward failed to provide evidence that the '480 Patent satisfies the written description requirement

A. The '480 Patent fails to include written description support for “providing a private key in a memory of said electronic device, wherein said memory being a secure part of a Basic In Out System or any other secure location in said electronic device operated by the first transaction party,” (“Feature A”)

6. Ward argues that Feature A is supported by the '480 Patent because the independent determinations made by the Board and Hague court are “based on an incorrect interpretation of the term ‘any other secure location’ as it is not linked to the BIOS.” POR, 13. Yet, in support of its argument, Ward offers nothing but

contradictory and unsupported statements that read limitations out of the claims, and rely on irrelevant evidence.

7. For instance, Ward argues that Feature A is supported because “[t]he encoded authentication table is stored in a secure part of the BIOS, where it may only be retrieved by the BIOS and not by the operating system. This secure part of the BIOS may also be **any other secure location** in the device.” POR, 13. As a preliminary matter, this statement, even if true, relates to the storage of the authentication table, not the recited private key, and is thus not relevant. Second, by asserting that the “secure part of the BIOS” may also be “any other secure location,” Ward effectively reads out one of these terms from the claims as both the “secure part of the BIOS” and “any other secure location” are recited in claim 1 as separate terms.

8. Ward also incorrectly relies on the '480 Patent's FIG. 3 and contends that the secure area 62 may be the claimed “any other secure location.” POR, 14. In support, Ward points to the storage of authentication table and authentication software in the secure area 62. POR, 14. Ward's argument again relies on the erroneous and unsupported notion that storage of the authentication table and authentication software in the secure area 62 discloses storage of the “private key” in the secure area 62. The '480 Patent does not disclose that the authentication table or authentication software are a private key, nor does it disclose storing a

“private key” in the secure area 62. In fact, as noted in my first declaration, during prosecution, the claims were amended to replace “authentication data” with “private key” in order to modify the scope and obtain allowance. SAMSUNG-1002, 91-96, 29-31; SAMSUNG-1003, ¶¶[42]-[43]. Thus, authentication table, authentication software, and private key are not interchangeable terms, and consequently FIG. 3 and its related description do not provide written description support for Feature A.

9. During his deposition, Ward’s expert, Dr. Preneel, conceded that there is no disclosure in the ’480 Patent that the private key is part of the authentication software. In particular, Dr. Preneel acknowledged that the private key may not be part of the authentication software and that he relied on an obviousness standard to conclude that the authentication software *can* store the private key. SAMSUNG-1034, 42:20-43:17. Similarly, his opinion that the private key *can be* authentication data was not based on disclosure in the ’480 Patent, but instead because a POSITA would have found it obvious to be. SAMSUNG-1034, 43:21-44:14. Counsel has informed me that obviousness cannot be relied upon to satisfy a written description requirement. Accordingly, while I am not a lawyer, it appears Dr. Preneel used the incorrect standard to perform his analysis and thus incorrectly conclude that the ’480 Patents have written description support.

10. Dr. Preneel and Ward also incorrectly attempted to equate an “authentication table” or “authentication data” with “bit string.” POR, 5, EX2012, ¶46. For example, in support of its argument that the “authentication table” is equivalent to a “bit string,” Dr. Preneel cites to col. 4, lines 33-39, col. 7, lines 45-48, and col. 10, lines 23-33 of the ’480 Patent. *Id.* During his deposition, Dr. Preneel conceded that none of these sections recite “authentication table.” SAMSUNG-1034, 33:2-16. Thus, Ward has no basis in the ’480 Patent for equating “authentication table” or “authentication data” to “bit string.”

11. In related remarks, Ward contradicts its above-noted position that the secure part of the BIOS may be any other secure location in the device. POR, 13-14. For instance, on page 15 of its response, Ward argues that “‘any other secure location’ is a ‘secure storage location’ *not* in the BIOS but shielded from the operating system by the BIOS.” POR, 15.

12. Ward also attempts to distinguish between “any secure location” and “any other location” in an attempt to conjure written description support for Feature A. POR, 15-16. But such a distinction is unavailing and misses the point. None of the portions cited by Ward disclose that *a private key* is provided in a memory that is a secure part of a BIOS *or any other secure location*.

B. The '480 Patent fails to include written description support for “[the] private key is inaccessible to a user of said electronic device,” (“Feature B”)

13. Ward mischaracterizes the '480 Patent's disclosure to argue that Feature B is described in the '480 Patent. For example, Ward notes that the authentication software has “its own unique serial number, software ID and/or private encryption key,” and then incorrectly and without any support, contends that “[a] POSITA would recognize that since the unique serial number, software ID of the authentication software is private key, the private key forms an integral part of the authentication software component and/or is embedded therein.” POR, 17. But there is simply no disclosure in the '480 Patent that the private key is stored or embedded in the authentication software. At best, the '480 Patent teaches that the authentication software “has” a private encryption key¹ or that the authentication software is used with a private key to sign a digital signature. SAMSUNG-1001, 5:39-40, 13:30-44. But using a private key does not mean that the private key is

¹ The private encryption key recited in 5:40 of the '480 Patent should not be confused with the private key used to generate a digital signature in the '480 Patent's 13:31-44. A key used to encrypt data is not the same as a key used to generate a digital signature, and the '480 Patent does not describe these two terms as being the same. SAMSUNG-1003, ¶¶[174]-[179].

part of or included in the authentication software. For instance, col. 13, lines 30-44 of the '480 Patent discloses that *in a further embodiment*, the authentication software *uses* “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.” SAMSUNG-1001, 13:30-44. This sentence does not state that the authentication software stores the private key such that the private key becomes inaccessible to a user.

14. Ward further claims that “the private key locates in the BIOS.” POR, 20. In support, Ward cites to Preneel ¶ 57, which merely recites claim language from Feature A (which, again, is unsupported); that claim language says that the private key is either in a secure part of the BIOS or some other secure location, and from this Ward concludes the private key is stored in the BIOS. In sum: the '480 *specification* never discloses that the private key is stored in a secure area of the BIOS or any other secure location (see II.A above). Thus, the '480 Patent fails to explain how the private key is protected to make it inaccessible to the user even if at some point it is used by the authentication software.

15. In addition, the '480 Patent is not clear if or how the further embodiment described in col. 13, lines 30-44 combines with earlier described embodiments. For instance, even assuming Ward's argument that the unique serial number, software ID of the authentication software is the private key (which I do not

concede), when such an assumption is combined with the third embodiment illustrated in FIGS. 4 and 5A (which as explained in my first declaration is not what the claims are directed to), such a private key would not be inaccessible to a user at least because the authentication software itself is not inaccessible to a user. SAMSUNG-1001, 9:35-38, 11:23-45; SAMSUNG-1003, ¶¶181-184.

16. Again, the '480 Patent is silent as to how the single disclosure of a private key in col. 13, ln. 31-33 would be combined with earlier embodiments and descriptions in the '480 Patent in a manner that would provide written description support of Feature B. It is indeed notable that the POR cannot provide a single citation to the '480 Patent disclosure to support the statement that “the authentication software 54 includes the private key contained or embedded therein”—which contradicts Ward’s related position noted above that the private key is located in the BIOS. *See, e.g.*, POR, 17, 19, 20.

17. Ward also incorrectly derives that omissions in the '480 Patent disclosure somehow support a disclosure that the authentication software stores the private key. For instance, Ward argues that, because the '480 Patent fails to describe how the authentication software retrieves or handles the private key after a request, such a failure supports a finding that the '480 Patent describes that the private key is with the authentication software. POR, 21. Ward’s argument is logically disconnected. A failure to describe the authentication software’s handling of the

private key does not necessarily mean nor does it provide written description support for Feature B.

C. The '480 Patent fails to include written description support for “the private key is encrypted when the private key is stored in said memory,” (“Feature C”)

18. Ward incorrectly argues that the '480 Patent describes Feature C because, “if the authentication software is encrypted when the authentication software is stored in the memory, the private key must also be encrypted when the authentication software (with the private key) is stored in the memory.” POR, 22. Ward’s argument relies on Ward’s faulty assumption that the authentication software includes the private key, which for the reasons noted above is not described in the '480 Patent. Accordingly, Feature C does not have written description support for the reasons noted above in §§II.A, II.B.

19. In addition, even if Ward’s argument is to be considered, the '480 Patent does not disclose that the authentication software is encrypted. Thus, even the conditional argument set forth by Ward, does not provide written description support for Feature C for this additional reason.

D. The '480 Patent fails to include written description support for “the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software,” (“Feature D”) as required by claim 1.

20. Ward relies on the decryption of authentication software as described in the authentication software installation process as allegedly supporting Feature D.

POR, 24-26; SAMSUNG-1001, 6:61-8:11. But this description does not support Feature D for several reasons.

21. First, Ward confuses the private key used to sign a digital signature with the private encryption key that the authentication software “has.” For instance, Ward argues that, “[s]ince the authentication software has the private key, the private key is decrypted.” POR, 25. Even if this statement is assumed to be correct (which I do not concede), the key that the authentication software has is “its own ... private encryption key.” SAMSUNG-1001, 5:39-40. As I explained in my first declaration (*see* SAMSUNG-1003, ¶¶175-182), the '480 Patent does not teach that the private encryption key in the authentication software is the private key used to sign a digital signature, as is required by the claims. Accordingly, there is no support in the '480 Patent that the same private key is decrypted and used to generate a digital signature.

22. Second, in describing how the '480 Patent's second embodiment supports Feature D, Ward again turns to the '480 Patent's third embodiment, which is not

compatible with the second embodiment, as I explained in my first declaration.

POR, 24-26; SAMSUNG-1003, ¶¶181-184. For example, Ward contends that the '480 Patent's disclosure at 9:42-49 teaches that "authentication data should only be decrypted in a secure processing environment" and that "such a secure processing environment may only be accessible to selected software applications, *preferably not* to user-operated software applications." POR, 25. This description is part of the third installation method of the '480 Patent in which authentication data "is stored in a memory that is accessible to an operating system of the device and possibly to a user of said device," which is not compatible with the '480 Patent's second embodiment shown in FIG. 3, to which the claims are directed.

23. Third, even if the different embodiments are mixed (which they cannot be), the disclosure relied upon by Ward at best teaches a preference not to provide access to user-operated software applications, not that the "secure processing environment [is] inaccessible to said user and *to any* user-operated software."

24. Finally, Ward provides a list of citations on pages 26-34 for alleged support of claim 1 without accompanying explanations. But the list of citations suffers from the same or similar deficiencies noted above with respect to Features A-D.

III. Claim Construction

25. In the Board's Institution Decision (ID), the Board construed the storage limitations in claims 1 and 16-18. In particular, the Board determined that "the term 'stored in said secure memory inaccessible to said operating system' encompasses "being held in any secure location that is inaccessible to the operating system for an undefined amount of time." ID, 25-26. In response, Ward does not offer its own construction ("[n]o formal claim constructions are necessary"). POR, 8. Rather, Ward contends that "[w]hen data/a data file (e.g., a program or a private key) is stored in **permanent memory** (hard disk, floppy disk, non-volatile memory also known as flash memory), it remains there until it is deleted" and that "[t]he main conclusion is that data (or software) remains stored in the original location (**permanent memory**) ... independent of where read/retrieved data or software is subsequently 'held', 'located', or 'executed' or whether the retrieved data or software are stored/buffered in another memory as well." POR, 72, 73. Ward's arguments are incorrect for several reasons.

26. 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.

27. 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.

28. Specifically, Ward’s argument contends that if a prior art reference discloses that “authentication software” is loaded into secure memory inaccessible to the operating system, but the authentication software is loaded from permanent memory (e.g., a hard disk) and that permanent memory source is not inaccessible to the operating system, then the prior art reference fails to disclose “wherein the authentication software is stored in the secure area inaccessible to the operating system.” In other words, Ward’s view seems to be that the authentication software must *always* reside in secure memory inaccessible to the operating system, despite this requirement not being stated in the claim. The basis for this seems to rest on Ward’s claim that storing authentication software in memory that *is* accessible to the operating system would be insufficient because “it will not allow to achieve the intended goals of the system.” POR, 74, citing EX2012, ¶124. This reasoning fails for several reasons.

29. First, and primarily, reading additional limitations into the claim based on perceived “intended goals of the system” would be improper. To my knowledge, satisfying the intended goals of a system is not required to establish obviousness.

30. Second, from a more technical standpoint, it is entirely conceivable that loading authentication software from a storage device that *is* accessible by the

operating system would not represent a security weakness: it is common practice that security *algorithms* are public but the security *keys* are secret. Indeed, it was a known and common practice to load an algorithm from public storage into secure memory and only then is the key introduced and the algorithm executed (within secure memory). This principle, named “Kerckhoffs’s Principle” after the 19th century Dutch scientist Auguste Kerckhoffs, can be informally stated as “the security of a cryptosystem should not rely on the secrecy of the algorithm but solely on the secrecy of the key.”²

31. Lastly, during his deposition, Dr. Preneel acknowledged in his declaration and deposition that reading and writing operations “involves some sort of buffering” and that buffering involves “stor[ing] the data on a buffer at least temporarily.” SAMSUNG-1033, 82:20-84:24. Accordingly, it would have been obvious to a POSITA that when Ellison’s usage protector 250 (authentication software) is operating in the isolated execution environment of the secure platform 200, the usage protector 250 would have been stored in the same isolated execution environment, even if for a short period of time.

² See Kerckhoffs, Auguste, “La Cryptographie Militaire,” Jan 1883, available at http://petitcolas.net/kerckhoffs/crypto_militaire_1.pdf (in French)

IV. The '480 Claims are obvious in view of the grounds identified in my first declaration

A. The POR and Expert Testimony are not tied to the prior art references

32. As a preliminary matter, Ward's POR includes remarks from page 39 to 52 characterizing the prior art references. The support for these statements is not linked to the prior art references, but is instead derived from Dr. Preneel's declaration, which itself has no citations to the prior art references. In other words, pages 39-52 include primarily attorney arguments and references to statements by Ward's paid expert that are not tethered to the prior art references. During the deposition, Dr. Preneel confirmed that paragraphs 52-71 and 76-95 (that are relied upon in pages 39-52 of the POR) have no citations at all (other paragraphs have minimal citations if any). SAMSUNG-1034, 45:2-46:4. Effectively, the statements in pages 39-52 of the POR are disconnected from the prior art references.

B. Ellison and Muir render obvious the "decryption key being inaccessible to said user, to any user-operated software and to said operating system" (feature [1d])

33. Ward argues that the combination of Ellison and Muir (referred to as EMC) does not render obvious [1d] because, according to Ward, Ellison's primary operating system (OS) 12 was incorrectly mapped to the claimed operating system

and because Ellison's isolated environment region is allegedly not accessible to the operating system. POR, 55. In particular, Ward argues that:

a POSITA would understand that the counterpart of "user applications" of the '480 Patent includes applications 42₁-42_N and applets 46₁ to 46_K, correspondingly, *the counterpart of "operating system" of the '480 Patent in Ellison is the operating system including normal execution mode and isolated execution mode, not only the primary operating system (OS) 12 operating in the normal execution mode, thus, the operating system should include the processor nub 18 and the operating system nub 16 which operate in the isolated execution mode.*

POR, 59.

34. But Ward's arguments represent a fundamental misunderstanding of Ellison's disclosure for the following reasons.

35. First, there is no reason why Ellison's OS 12 cannot be the only OS mapped to the claimed OS. As a preliminary matter, OS 12 satisfies Ward's description of an operating system, and thus even Ward cannot dispute that OS 12 is an operating system. Moreover, while not entirely clear, Ward's argument appears to rest on

the idea that to be properly mapped to the claimed operating system, the operating system must execute the normal and isolated execution modes. POR, 59. But neither the intrinsic record nor the prosecution history impose such a requirement on the claimed OS. And Ward has not provided any evidence to support their argument.

36. Second, there is no reason why Ellison's OS 12 cannot be the only OS mapped to the claimed OS. 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, 54-57. 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 42₁-42_K, which are user applications in the non-isolated region. SAMSUNG-1006, 2:57-4:29, FIGS. 1A, 1B. In contrast, applets 46₁-46_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.

37. Third, Ward's argument that the prior art fails to render [1d] obvious rises and falls with Ward's erroneous understanding of the claimed operating system. In particular, Ellison's OSNK 203 had been mapped to the "decryption key," in part, because it is located 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;

SAMSUNG-1003, ¶101. In the mapping of feature [1d] described in my first declaration, I had previously explained 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; SAMSUNG-1003, ¶101. 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. SAMSUNG-1006, 8:12-32; SAMSUNG-1003, ¶101. Ward argues that because OS nub 16 and processor nub 18 have access to the OSNK 203, EMC fails to render [1d] obvious. POR, 61-65. However, this argument is based on Ward’s erroneous assertion that the claimed OS should be mapped to processor nub 18 and OS nub 16, in addition to OS 12. For the reasons already noted above, Ward’s argument has no merit and fails.

38. Fourth, Ward’s arguments are not based on a correct understanding of Ellison. For example, Ward contends that, “[w]hen a transaction is performed on Ellison’s operating system, an attack can invade into the operating

system to alter the execution mode of applets 46₁ to 46_K from isolated execution mode to normal execution mode, or invade into the isolated execution mode of operating system and control the operating system nub 16 which operate in the isolated execution mode to access the secure platform 200 to steal the decryption key and information in the memory of the isolated area 70.” POR, 65. Ward provides no citations or support for its conclusory assertion. In fact, OS nub 16 and other components of Ellison’s system that are part of the isolated execution region cannot be attacked in the manner Ward claims. Ellison explicitly teaches that “[t]he secure platform 200 includes the OS nub 16, the processor nub 18, ... and a usage protector 250, *all operating within the isolated execution environment.*” SAMSUNG-1006, 8:25-32. In some embodiments, the protected private key 204 can be *generated by the platform 200*, and “[o]nly the OS nub 16 can retrieve and decrypt the encrypted private key for subsequent use.” SAMSUNG-1006, 8:40-65. Separately, applets 46₁ to 46_K are located in Ring-3 of the isolated execution environment, and thus would also be protected from external attacks, in contrast to Ward’s unfounded assertions. SAMSUNG-1006, 3:9-32, FIG. 1A.

39. For at least the foregoing reasons, it is still my opinion that EMC renders [1d] obvious.

C. Ellison and Muir render obvious “authentication software is stored in said secure memory inaccessible to said operating system” (feature [1i])

40. Ward’s argument that the prior art fails to render [1i] obvious rises and falls with Ward’s erroneous understanding of the claimed operating system and that the claimed OS should be mapped to processor nub 18 and OS nub 16, in addition to OS 12. POR, 67-68. For the reasons noted above, this argument is without merit. Accordingly, EMC renders [1i] obvious for the reasons I noted in my first declaration. SAMSUNG-1003, ¶¶108-109.

41. Ward also relies on language that is not recited in the claims to argue that feature [1i] is not rendered obvious by EMC. For instance, Ward argues that EMC does not render [1i] obvious because “Ellison does not teach or suggest authentication software for securing user transactions.” POR, 48. Even if true (and it is not), neither [1i] nor claim 1, as a whole, requires or recites storing authentication *for securing transactions*, which Ward argues is the “essential difference.” POR, 48. Thus, this argument lacks relevance and is untethered to the claims.

42. Relatedly, Ward also mischaracterizes the EMC combination (as described in my first declaration) and advances arguments that are not pertinent to the

advanced EMC combination. For example, Ward argues that EMC fails because Muir's virtual smart card driver 155 is not stored in a secure memory. POR, 48. But, I had not previously described Muir's virtual smart card driver 155 as being stored in a secure memory. Rather, as explained in Section VI.C of my first declaration, one of the reasons the Ellison and Muir combination would have been obvious is because Muir discloses a restricted space 170 that stores a private key 167 (similar to the manner in which Ellison handles its private key). SAMSUNG-1008, pp. 3-¶¶3, 7-¶¶1; SAMSUNG-1003, ¶¶¶63-68. Muir is relied upon, in part, for its disclosure of generating and transmitting an encrypted digital signature in a secure manner to another device. SAMSUNG-1008, p. 3-¶¶¶1-3; Pet. 46-51. The EMC does not bodily incorporate all aspects of Muir's virtual smart card driver 155 or device 110, as Ward represents. For at least the foregoing reasons, Ward's arguments that EMC does not render obvious [1i] are unavailing and incorrect.

D. Ellison and Muir render obvious claim 1

43. Ward contends that EMC does not render obvious claim 1 in view of the above-noted arguments and also because a POSITA would not have looked to Muir to cure the deficiencies of Ellison. POR, 39, 68. The above-noted arguments have been addressed, and Ward only offers conclusory statements without any accompanying evidence in support of the latter argument. POR, 68. As noted

above, on pages 39-51 of the POR, Ward makes numerous conclusory assertions without support. Because Ward does not provide supporting rationale, I will attempt to respond to any arguments pertinent to the claims or the asserted combination.

44. For example, Ward incorrectly argues that:

Ellison cannot be combined with Muir's pointer 171 to restricted memory space 170 without also incorporating Muir's Virtual Smart Card Driver 155. 91. Indeed, 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.

POR, 41-42.

45. First, this argument is without merit at least because the only support for this argument is Dr. Preneel's declaration, which simply repeats the same statements without any citations or supporting explanations.

46. Second, Ward's contention that the digital signature would not even touch the isolated execution environment contradicts Ellison's teachings, which disclose that the signature generator 320 in the usage protector 250 (which operates in a

secure isolated execution environment) generates the digital signature.

SAMSUNG-1006, FIG. 3C, 10:63-11:30, 8:55-65; SAMSUNG-1003, ¶¶[110].

Ellison explains how a private key 204 can be stored in OS Nub 16 and used by usage protector 250 to generate a digital signature. SAMSUNG-1006, FIGS. 2,

3C. For instance, Ellison discloses that “[t]he 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.” SAMSUNG-1006, 3:15-21. A “processor nub loader

52 operates only in the isolated execution mode” and verifies and loads processor

nub 18, which further verifies and loads OS nub 18. SAMSUNG-1006, 3:7-8,

3:32-61. The OS nub 16 is verified when being loaded into the isolated area 70.

SAMSUNG-1006, 3:50-61. The OS nub 16 operates within the isolated execution

environment, and has access to a public and private key pair unique for platform

200. SAMSUNG-1006, 3:60-67. Platform 200 includes the OS nub 16 and a key

generator 240—“*all operating within the isolated execution environment.”*

SAMSUNG-1006, 8:25-32. In some embodiments, the protected private key 204

can be *generated by the platform 200*, and “[o]nly 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.” SAMSUNG-1006, 8:40-65. In other embodiments in which the private key 204 is subsequently stored in a key storage 164 of non-volatile flash memory 160, the private key 204 is protected because “it cannot be calculated from its associated public key 205,” whereas generally “the public key 205 is used as a decryption key to decrypt the signature, revealing the digest value.” *Id.*

47. As can be appreciated from the foregoing, Ellison describes how the OS nub 16 can be securely loaded in isolated area 70 and run in an isolated execution environment without ever going through the primary OS 12—contrary to Ward’s assertions. SAMSUNG-1006, 8:40-65.

48. 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 disclose 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.

V. Conclusion

49. In conclusion, Ward did not provide any arguments that indicated my analysis provided in my first declaration was incorrect. Therefore, I maintain that the Challenged Claims are obvious for the various reasons noted in my first declaration.