

UNITED STATES PATENT AND TRADEMARK  
OFFICE

BEFORE THE PATENT TRIAL AND APPEAL  
BOARD

---

SAMSUNG ELECTRONICS CO., LTD.,

Petitioner,

v.

WARD PARTICIPATIONS B.V.,

Patent Owner.

---

Case No.: PGR2022-00007

Patent No.: 10,992,480

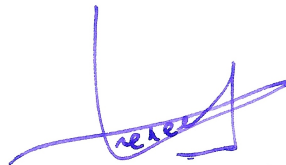
---

**DECLARATION OF BART PRENEEL, PH.D.,  
UNDER 37 C.F.R. § 1.68 IN SUPPORT OF  
PATENT OWNER'S PRELIMINARY RESPONSE**

---

Date: January 28, 2022

Respectfully submitted,



---

Bart Preneel, Ph.D.

## TABLE OF CONTENTS

	PAGE
I. INTRODUCTION .....	1
II. SUMMARY OF OPINIONS .....	1
III. MATERIALS CONSIDERED .....	2
IV. BACKGROUND AND QUALIFICATIONS .....	3
V. UNDERSTANDING OF THE APPLICABLE LEGAL STANDARDS .....	6
VI. BACKGROUND OF THE '480 PATENT AND ITS PROSECUTION HISTORY .....	9
VII.DETAILED UNPATENTABILITY ANALYSIS .....	14
A. Level of Ordinary Skill in the Art .....	15
B. The Disclosure of the '480 Patent to One of Ordinary Skill in the Art .....	16
C. Summary of the Cited References .....	19
1. Ellison – U.S. Patent No. 7,082,615 .....	19
2. Muir – PCT Publication No. WO 01/93212 .....	19
D. Comparison of the '480 Patent to the Cited References .....	20
VIII.CONCLUSION .....	23

**Patent Owner's Exhibit List**

<b>Exhibit No.</b>	<b>Description</b>
2001	Declaration of Bart Preneel, Ph.D.
2002	Remarks of December 23, 2020, Amendment and Response for U.S. Patent Application No. 16/597,773
2003	December 22, 2020, USPTO Examiner Interview Summary
2004	September 18, 2020, Final Office Action for U.S. Patent Application No. 16/597,773
2005	December 17, 2020 USPTO Examiner Interview Summary
2006	<i>Curriculum Vitae</i> of Bart Preneel, Ph.D.
2007	Europass <i>Curriculum Vitae</i> of Bart Preneel, Ph.D.
2008	Publication List of Bart Preneel, Ph.D.

I, Bart Preneel, Ph.D., hereby declare under the penalty of perjury that the following is true and correct. All statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true. I understand that perjury and/or a willful false statement and the like are punishable by fine or imprisonment, or both (18 U.S.C. § 1001) and may jeopardize the validity of the application or any patent issuing thereon.

## **I. INTRODUCTION**

1. I have been retained by Ramey and Schwaller LLP in connection with Samsung Electronics Co., Ltd.'s Petition for post grant review of U.S. Patent No. 10,992,480 ("the '480 Patent").

2. I have been asked to provide opinions regarding whether Samsung Electronics Co., Ltd.'s Petition demonstrates that it is more likely than not that at least one of Claims 1-19 is unpatentable. I understand that this Declaration will be used to respond to the Petition and its supporting materials.

3. I am being compensated at my customary fee of \$247 per hour for work associated with this matter. I am also being reimbursed for reasonable and customary expenses. My compensation does not depend upon the outcome of this post grant review.

## **II. SUMMARY OF OPINIONS**

4. Each limitation is fully supported by the written description of the '480

Patent and that one of ordinary skill in the art would readily recognize the claim limitations based on the disclosure of the '480 Patent.

5. In the '480 Patent, because the authentication software has a private encryption key, the private key forms an integral part of the authentication software component and/or is embedded therein

6. Neither Ellison nor Muir teach or suggest a decryption key for decrypting the private key (used by the first transaction party to digitally sign a transaction) being incorporated in the electronic device.

7. Neither Ellison nor Muir teach or suggest authentication software is stored in said secure memory inaccessible to said operating system.

8. Neither Ellison nor Muir teach or suggest authentication software is run in a secure processing environment inaccessible to said operating system.

9. Al-Salqan and Searle do not overcome the deficiencies described in the Patent Owner's Response relating to the combination of Ellison and Muir.

### **III. MATERIALS CONSIDERED**

10. In forming my opinions, I reviewed the '480 Patent its respective file history. I considered the Petition and each of the references and unpatentability grounds presented therein. I have considered the exhibits submitted by Petitioner, including the Declaration of Dr. John R. Black, Jr. My opinions are based in part on those materials. I have also relied upon my education, experience, and

knowledge of engineering practices and principals in the cryptographic algorithm industry, as well as my understanding of the applicable legal principals described below. I have also relied on publication relevant to the technology in this matter.

#### **IV. BACKGROUND AND QUALIFICATIONS**

23. I am over eighteen years of age and I am competent to testify as to the matters set forth herein if I am called upon to do so. My *Curriculum Vitae* is attached hereto as Exhibit 2006 and 2007 and provides an accurate identification of my background and experience.

24. I am a technical expert in the subject matter areas relevant to this matter, including design and evaluation of cryptographic algorithms and protocols including cryptanalysis, security reductions and proofs, cryptographic hardware and software, secure execution environments, and secure electronic transactions.

25. I was awarded a Ph.D. in computer science from the Katholieke Universiteit (KU) Leuven in Belgium in 1993. I also hold an Electrical Engineering degree from the Katholieke Universiteit Leuven in Belgium received in 1987.

26. I have been part-time advisor at Philips Research (2005-2011). I am serving on the Board of Directors of two companies (co-founder of the start-up nextAuth and Approach Belgium). I run my own consulting company Arenberg Crypto BV (formely ABT Crypto Aps). I have served on the Advisory Board of several companies including Hypertrust, Intrinsic ID and Nym Technologies and of

the Trusted Computing Platform Alliance (2000-2002). I am serving on the Board of Directors of four non-profit organizations in the area of cybersecurity (International Association for Cryptologic Research, EEMA, Leaders in Security and Cybersecurity Coalition Belgium); I have served as President of the IACR from 2008-2013. I regularly consult for international companies on security architectures and cryptography.

27. I am Full Professor at the Katholieke Universiteit Leuven in Belgium since 2006 (associate professor 2000-2003, professor 2003-2005). Since 2013, I head the COSIC research group which has 95 members (7 professors). I have been Visiting professor at the Technical University of Denmark, TU Graz (Austria), University College London (UK), University of Bergen (Norway), Ruhr-Universität Bochum (Germany) and at the University of Ghent. I am a regular guest lecturer at University of Piraeus (Greece).

28. I have received the following awards: European Information Security Award in the area of academic research (2003), Honorary Certified Information Security Manager (CISM) of the Information Systems Audit and Control Association (ISACA) (2003), RSA Award for Excellence in the Field of Mathematics (2014), Member of the Academia Europaea (since 2014), Fellow IACR (2015), IACR Distinguished Lecturer (2016), Christian Beckman award from IFIP TC-11 (2016), ESORICS Research Excellence Award (2017), IT Person

of the Year, Belgium (2020). I have received several best paper awards (including SAC 2021 and CHES 2021).

29. I am the inventor of five patents including U.S. Patent No. 5,664,016 entitled "Method Of Building Fast MACS From Hash Functions," U.S. Patent No. 8,267,306 entitled "Selection Systems," European Patent No. EP2751949, International Publication No. WO 2013/033235 entitled "Multiple Table Tokenization," U.S. Patent No. 9,396,357 entitled "Physically Unclonable Function (PUF) With Improved Error Correction," and U.S. Publication No. 9,240,885 entitled "Cryptographic Processing Apparatus, Cryptographic Processing Method, And Computer Program Therefor."

30. I have published more than 500 scientific articles including more than 100 journal publications and 40 book chapters. I am (co-)editor of 28 published books. There are more than 28000 citations to my work in Google Scholar and my h-index is 82.

31. I have served as keynote lecturer or invited speaker at more than 130 conferences or schools in 50 countries (including Asiacrypt, Eurocrypt, Esorics, IFIP SEC, FSE, PKC, CHES)

32. I have served as expert witness in several IP-related court cases (both in Belgium and abroad).

33. In the past five years, I was an expert in the following case:



- *DTS International B.V., v. Samsung Electronics Benelux B.V., et al.*, Case C/09/576280 v HA ZA 19-713 (Case I), (District Court of the Hague).
- *DTS International B.V., v. Samsung Electronics Benelux B.V., et al.*, Case C/09/577703 HA ZA 19-793 (Case II), (District Court of the Hague).

## **V. UNDERSTANDING OF THE APPLICABLE LEGAL STANDARDS**

34. I am not a lawyer; however, I have been informed of the applicable legal standards by counsel.

35. I understand that the Board may not institute post grant review (“PGR”) unless the Petition “information presented in the petition filed under section 321, if such information is not rebutted, would demonstrate that it is more likely than not that at least 1 of the claims challenged in the petition is unpatentable.” It is the Petition’s burden of showing the statutory threshold has been met.

36. The determination of patentability over the prior art requires a two-step analysis. The first step is to properly construe the claims to determine claim scope and meaning. The second step is to compare the construed claims to the prior art on a limitation-by-limitation basis.

37. Patent claims in a PGR are given their broadest reasonable interpretation (“BRI”). The BRI of the claim terms are understood from the perspective of a person of ordinary skill in the art. The claim interpretation begins

with the ordinary and customary meanings of the claim terms. The patent's entire disclosure, including the specification and prosecution history, should be considered to understand the BRI.

38. There are other principals of claim construction that should be taken into account. When an applicant makes a clear statement to distinguish the claimed invention from the prior art, the applicant disclaims such subject matter and narrows the scope of the claim. When the specification describes the invention using phrases such as "the present invention," these phrases describe the invention as a whole and they can limit the scope of the claims.

39. Once the claims of a patent have been construed, the second step is to compare the claim language to the prior art on a limitation-by-limitation basis.

40. A prior art reference can render a patent unpatentable if it anticipates the patent. A prior art reference is said to anticipate if each and every element of the claim is set forth, either expressly or inherently, in a single prior art reference. An anticipatory reference must disclose all elements of the claim, and must disclose those elements as arranged in the claim. A prior art reference that does not expressly disclose a limitation may inherently disclose a limitation if such a feature is necessarily present in that reference. To inherently anticipate, the feature must result from the disclosure.

41. If a claim is not anticipated, a claim can still be unpatentable if the

differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious. The obviousness analysis requires a comparison of the properly construed claim to the prior art on a limitation-by-limitation basis. An analysis of whether claims are obvious includes considering factors such as (1) the scope and content of the prior art, (2) the differences between the prior art and the asserted claims, (3) the level of ordinary skill in the art, and (4) the existence of secondary considerations of non-obviousness.

42. A claim can be obvious when its elements are disclosed in two or more references from the prior art, and there was a reason for a person of ordinary skill to combine those references to obtain the elements as claimed. It is not enough that each of a patent's elements were independently known in the prior art. A skilled artisan needs to have had a reason to combine the teachings of the prior art to achieve the claimed invention with a reasonable expectation of success. It is improper to use hindsight to reconstruct the claims, such as where the prior art gives no indication of which parameters were critical or no direction as to which of many possible choices are likely to be successful. A combination of references that renders one of the references inoperable for its intended purpose, may fail to support a conclusion of obviousness.

43. When considering combinations of references, it is important to

consider the references as a whole, including portions that would lead a person of ordinary skill away from the claimed invention. If, upon reading a reference, a person of ordinary skill would be discouraged from following the reference, or would be led in a different direction from that taken by the applicant, then a reference is said to teach away.

44. There are multiple factors relevant to determining the level of ordinary skill in the pertinent art, including (1) the levels of education and experience of persons working in the field at the time of the invention; (2) the sophistication of the technology; (3) the types of problems encountered in the field; and (4) the prior art solutions to those problems.

45. Finally, I understand that patent claims can be both independent and dependent. A claim that stands on its own is called an independent claim. A dependent claim is one that refers to another claim, incorporates its limitations, and adds additional limitations. If the prior art does not anticipate or render obvious an independent claim, it cannot anticipate or render obvious any dependent claim that further limits that independent claim.

## **VI. BACKGROUND OF THE '480 PATENT AND ITS PROSECUTION HISTORY**

46. The '480 Patent claims a novel, method and system for performing a electronic transaction or electronic verification or identification without requiring

additional hardware. '480 Patent col. 1, ln. 53-56. In my opinion, the inventions claimed in the '480 Patent represented significant steps forward in electronic transaction technology and verification of legitimate access to, or use of digital data.

47. The '480 Patent claims a method and system 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 '480 Patent's claimed invention improves digital file transmission security between two parties while also providing a method for tracing the file. This is advantageous because vast amounts of digital information, including highly sensitive transactions, are being handled electronically every day.

48. Three significant components of the inventive systems enable two party transactions: (1) secure private key and authentication software on a first party's device; (2) generation of a digital signature sent to a second party; and (3) embedding of a digital signature in the transaction file. This provides a more secure way to interact in a digital world because of the integrated security functionality to mitigate the risks related to unwarranted security access by operating systems. Additionally, strong authentication is not dependent on any client – server exchange of credentials. This avoids the exposure of usernames, passwords, and PINS at any time of the transaction and renders stolen credentials or phished data useless in the protected environments.

*1. The '480 Specification*

49. The '480 Patent was filed on October 9, 2019. '480 Patent, Cover. I understand that '480 Patent has an effective filing date of June 13, 2003 because it claims priority to an earlier PCT application PCT/NL03/00436. '480 Patent, Cover. The '480 Patent has 19 claims, including four independent claims. (1, 16, 17, 18).

50. The '480 Patent generally relates to a “method and system for performing a transaction and for performing a verification of legitimate access to, or use of digital data.” '480 Patent, Cover.

51. The '480 Patent explains one configuration of a device according to the disclosed subject matter:

The device consists of several components, commonly referred to as hardware 42. Exemplary hardware components are a processor, a hard drive, or other memory and a keyboard.

All the hardware devices are controlled by the BIOS 44. The BIOS 44 is a software package stored in a read-only memory (ROM), usually located on a main board, which is one of the hardware components of an electronic device.

The BIOS 44 controls most of the instructions and data flowing from one component to another. Data or instructions coming from one component and addressed to another need to pass through the BIOS 44. The BIOS 44 may check whether the instructions to the other component are allowed or not, as not every component is accessible

for any other component.

The BIOS 44 may comprise an encryption key 46. Such an encryption key 46 may be used to encrypt data and only another party who knows the encryption key 46 may be able to decrypt the data.

The operating system 48 creates a run-time environment for any user applications. Therefore, it may be stated that the operating system 48 is an interface between a user and the hardware 42. A user may instruct the operating system 48 to run an application 50. If the application 50 needs data that are stored on the hard drive, the application 50 requests the data from the operating system 48. The operating system 48 in turn requests the data through the BIOS 44 from the hardware 42, i.e. the hard drive. The data coming from the hardware 42 pass through the BIOS 44 and the operating system 48 before they arrive at the requesting application 50. Via this protocol the BIOS 44 may control the accessibility of certain data or hardware devices 42 and thus the use of particular software. It may prohibit, for example, the operating system 48 to access certain parts of a hard drive or start certain applications.

'480 Patent at 8:12–48.

## *2. The '480 Patent's Prosecution History*

52. I understand that the Patent Office will either allow a patent application to issue, or it will reject the application and allow the applicant to respond. This is referred to as patent prosecution, and the record of this back-and-

forth with the Patent Office is called the prosecution history.

53. The '480 Patent was filed with the Patent Office on October 9, 2019 and issued on April 27, 2021. '480 Patent, Cover.

54. The '480 Patent was rejected a number of times before it was allowed. Patent Owner made statements during the prosecution that inform my understanding of the invention and the claims.

55. For example, the applicant distinguished the present claims over the prior art by arguing that the prior art did not disclose wherein the private key is decrypted in a secure environment inaccessible to said user and to any user-operated software:

Specifically, Proudler, Constable, Dryer, and Unicate are entirely silent with respect to an encrypted private key. As a result, none of Proudler, Constable, Dryer, or Unicate, either alone or in combination, can disclose a decryption key for decrypting the private key. Accordingly, any proposed combination of the prior art fails to disclose at least the feature of “wherein the **private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software,**” as recited in each of independent claims 1, 26, 27, and 28, emphasis added.

Ex. 2002, p. 11. The Examiner agreed that this feature was not disclosed by any of the prior art references:



See attached. The amendments were discussed. The examiner agreed that the amendments would overcome the currently relied upon prior art. The examiner indicated that the amendments will need to be filed with an RCE. This is due to the scope of the proposed language being a broader version of previous claim 16, that does not include the allowable subject matter from claim 11. The addition of clarifying that the authentication data is a private key, is an important distinction over the currently relied upon prior art, which does not teach or suggest encrypting the private signature key for storage by another inaccessible key.

Ex. 2003, p. 2.

56. These statements by Patent Owner, in combination with the specification, inform my understanding of the claims.

## **VII. DETAILED UNPATENTABILITY ANALYSIS**

57. In my opinion, the Petition does not demonstrate that more likely than not at least 1 of Claims 1-19 are unpatentable. I disagree with the Petition's and Dr. Black's description of the cited references and their comparison of the cited reference to the claims.

58. I first consider the level of ordinary skill. Next, I explain the understanding one of ordinary skill would have of the written description of the '480 Patent. I then provide a summary of the cited references.<sup>1</sup> Finally, I compare

---

<sup>1</sup> The Petition also relies upon U.S. Patent No. 6,546,626 ("Al-Salqan") and U.S. Patent No. 6,683,954 ("Searle") to argue that certain dependent claims are obvious. Petition, p. 2. I do not specifically address Al-Salqan or Searle here because the Petition has not demonstrated that it is more likely than not of prevailing with respect to the independent claims. I reserve the right to do so to the extent I am

and identify the difference between the cited references and the claims of the '480 Patent. In my analysis, I applied the same priority date that Dr. Black applied: June 13, 2003. Ex. 1003, ¶9.

**A. Level of Ordinary Skill in the Art**

59. The Petition and Dr. Black claim that a person of ordinary skill in the art of the '480 Patent would have “a Bachelor’s degree in an academic discipline emphasizing the design of electrical, computer, or software technologies, in combination with at least two years of related work experience with software security technologies, such as cryptography or encryption/decryption systems, or in the development of hardware and software for carrying out secure electronic transactions,” or alternatively “a Masters or Doctor of Philosophy degree in a relevant academic discipline with less than a year of related work experience in the same discipline.” Petition at p. 3.

60. It is unclear what the Petition or Dr. Black mean by a “relevant academic discipline.” However, for the purpose of my Declaration, I will accept their proposed level of ordinary skill because it is my opinion that even to such a person the '480 Patent is not rendered obvious over the cited references.

---

requested to provide further opinions in this matter.

**B. The Disclosure of the '480 Patent to One of Ordinary Skill in the Art**

61. Each limitation is fully supported by the written description of the '480 Patent and that one of ordinary skill in the art would readily recognize the claim limitations based on the disclosure of the '480 Patent.

62. In the '480 Patent, because the authentication software has a private encryption key, the private key forms an integral part of the authentication software component and/or is embedded therein.

63. The '480 Patent does not provide that the authentication software would have (undefined) access to its own private key by requesting such access from any other software component.

64. Because the private key can be an integral part of the authentication software, disclosure relating to the authentication software also includes the private key embedded therein.

65. Since the authentication software 54 includes the private key contained or embedded therein and the authentication software 54 is stored in secure area 62, the private key would be provided in secure memory location 54 of the Secure Area 62.

66. Based on (1) the extensive disclosure in the '480 Patent of the authentication software stored in a memory of the electronic device, wherein the

memory is part of a BIOS or any other secure location and (2) the disclosure that a private key is an integral part of the authentication software, the claim limitation of “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,” is fully supported in the '480 Patent specification.

67. In the '480 Patent, if the authentication software with the private key is encrypted, it would be inaccessible to a user of the device.

68. In the '480 Patent, if the operating system 48 cannot gain specified access, such access is also denied to the user.

69. The feature of “which private key is inaccessible to a user of said electronic device,” is fully supported in the '480 Patent specification.

70. In the '480 Patent, the principle of decryption, re-encryption and re-encrypted storage of an authentication table can be readily applied to any authentication data that are used to perform unique digital signing according to the '480 Patent, including the private key of the authentication software.

71. In the '480 Patent, the feature of “wherein the private key is encrypted when the private key is stored in said memory,” is fully supported in the '480 Patent specification.

72. Ring 0 processing, also known as kernel mode processing, is a particular execution mode of the processor that that is inaccessible by the operating

system and, therefore, the user-operated software.

73. The written description of the '480 Patent supports the authentication software including a private key and describes the secure processing environment (not accessible to user-operated software programs) in which the authentication software decrypts authentication data(which the private key is).

74. Because the bit string is provided by the second party, network administrator, and stored with data identifying the first transaction party, the '480 Patent describes the claim feature of claim 2.

75. In the '480 Patent, the TTP may also be the second transaction party and the authentication data are encrypted by the TTP/second transaction party.

76. In the '480 Patent, a private key can be authentication data.

77. In the '480 Patent, the first start-up of the computer, which may initiate the authentication software to decrypt the bit string sufficient describes retrieval of a decryption key associated with the encryption key and decrypts the private key at its first use.

78. A POSITA would recognize that based on the '480 Patent, a processor must be configured for an operating system in order for the device to run.

79. Processors support kernel mode processing, *e.g.* Ring 0 processing.

80. A POSITA would recognize that the '480 Patent discloses a processor configured for an operation system and for activating the authentication software

wherein the authentication software is run in a secure processing environment inaccessible to the operating system.

### **C. Summary of the Cited References**

#### *1. Ellison – U.S. Patent No. 7,082,615*

81. Ellison is fundamentally different than the claims of the '480 Patent. Ellison is directed toward an operating architecture 50 with ring-0 10, ring-1 20, ring-2 30, ring-3 40, and a processor nub loader 52, the operating architecture 50 having two modes of operation: normal execution mode and isolated execution mode. Ellison col 2, ln.64-67; col. 3, ln. 4-7; and FIG. 1A. In the isolated execution mode, there is secure platform 200 that includes an OS nub 16, a processor nub 18, a key generator 240, a hashing function 220, and a usage protector 250 all operating within an isolated execution environment. Ellison col. 8, ln. 25-30. Ellison's isolated execution architecture allegedly prevents attacks and vulnerabilities in electronic and software systems. Ellison col. 2, ln. 40-61.

82. The isolated execution environment relates to and is dependent on ring 0 architecture of the processor. *See* Ellison's FIG. 1A. Ellison discloses that critical modules are **loaded** into the execution space by processor nub 52. *See* Ellison col. 6, ln. 27-67. This module loading implies that the modules are stored in non-volatile memory, from which they are loaded into the execution space.

#### *2. Muir – PCT Publication No. WO 01/93212*

83. Muir is also fundamentally different than the claims of the '480 Patent and cannot cure the deficiencies noted above with respect to Ellison. Muir is directed toward a computing system 110 that includes an application 120, a device operating system 125, a smart card interface 150, and a virtual smart card 151. Muir p. 7, para. 4.

84. Virtual smart card 151 includes Virtual Smart Card Driver 155 and memory 140 which includes a restricted memory space 170. Muir p. 7, para. 4. Smart card driver 155 is outside of memory 140. *See* Muir FIG. 3. Virtual Smart Card Driver 155 is software code, which upon execution, emulates a physical smart card and can intercept commands from the device operating system 125 to process the commands. Muir p. 8, para. 4. Virtual Smart Card Driver 155 uses the restricted memory 170 to store private keys 167 and may further use restricted memory space 170 to store encrypted and decrypted data. Muir p. 9, para 3.

**D. Comparison of the '480 Patent to the Cited References**

85. It is my opinion that none of the cited references render the claims of the '480 Patent unpatentable. I will now compare the cited references to the '480 Patent. I focus on the independent claims. Because I conclude that the independent claims of the '480 Patent are patentable over the cited references, the dependent claims are likewise patentable over the cited references.

86. It is my opinion that none of the cited references render the claims of

the '480 Patent unpatentable. I will now compare the cited references to the '480 Patent. I focus on the independent claims. Because I conclude that the independent claims of the '480 Patent are patentable over the cited references, the dependent claims are likewise patentable over the cited references.

87. The OSNK 203 is used to decrypt the register values or to sign the software to be run in the secure processing environment—not to sign a transaction between a first and second transaction party.

88. It is unclear where the OSNK key 203 is stored or whether it is generated every time it is needed.

89. Ellison's OSNK 203 is generated by the key generator 240 after the device has been put in circulation.

90. Neither Ellison nor Muir teach or suggest authentication software is stored in said secure memory inaccessible to said operating system.

91. The goal of usage protector 250 is to protect the software and registry states in the secure environment, that is to protect the secure environment itself and not to protect electronic transactions by a user (first transaction party).

92. The execution environment of Ellison's usage protector 250 is not the same as where usage protector 250 is stored.

93. There is not a single instance in Ellison disclosing where the usage protector 250 is stored.



94. Muir's Virtual Smart Card Driver 155 is fully accessible because it is stored in one of fixed disk 225, RAM 205 or ROM 204, or other memory devices within computer system 110.

95. None of Muir's fixed disk 225, RAM 205 or ROM 204, or other memory devices within computer system 110 are secure memory.

96. Neither Ellison nor Muir teach or suggest authentication software is run in a secure processing environment inaccessible to said operating system.

97. Ellison's failure to disclose the storage location of usage protector 250 implies the primary OS 12 would have access to usage protector 250 for running in the normal execution environment.

98. Ellison's drivers 13, 14 all run in normal execution mode and any combination of Ellison and Muir would require Muir's Virtual Smart Card Driver 155, which also runs openly accessible to the operating system.

99. Ellison fails to disclose encryption of usage protector 250.

100. Ellison's primary OS 12 would always have access to the usage protector 250 and could subsequently run the usage protector 250 in the normal execution environment.

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

102. 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.

103. Al-Salqan and Searle do not overcome the deficiencies described in the Patent Owner's Response relating to the combination of Ellison and Muir.

104. Because each of the independent claims 1, 16, 17 and 18 are patentable over the cited references, each of the dependent claims are patentable over the cited references. I reserve the right to present arguments that the dependent claims are patentable over the cited references to the extent the Board institutes PGR and I am asked to provide additional opinions in this matter.

## **VIII. CONCLUSION**

105. It is my opinion that the Petition does not present information that would demonstrate that it is more likely than not that at any of the claims challenged are unpatentable.