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 PGR2022-00007
Patent 10,992,480

PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

EXHIBIT LIST

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

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

SAMSUNG-1003 Declaration and Curriculum Vitae of Dr. Black

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

SAMSUNG-1005 Stipulation by Petitioner

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SAMSUNG-1024 [RESERVED]

SAMSUNG-1025 [RESERVED]

SAMSUNG-1026 [RESERVED]

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

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

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

SAMSUNG-1030 Declaration of Ashley Bolt

SAMSUNG-1031 [RESERVED]

SAMSUNG-1032 Second Declaration of Dr. Black

SAMSUNG-1033 Transcript of Dr. Preneel Deposition for IPR2022-00114

SAMSUNG-1034 Transcript of Dr. Preneel Deposition for PGR2022-00007 and IPR2022-00113

I. Introduction

In the Patent Owner Response ("**POR**"), Patent Owner (hereafter referred to as "**Ward**") argued that claims 1-19 ("**Challenged Claims**") of U.S. Patent No. 10,992,480 ("**the '480 Patent**") have written description support and are not rendered obvious by the instituted prior art grounds. Ward's arguments as to why the '480 Patent's claims have written description rely on improper mixing of embodiments, reading limitations out of the claims, and incorrectly using the term "private key" in an interchangeable manner with authentication software and authentication table. In terms of the prior art, as explained in more detail below, Ward's arguments against the prior art references mischaracterize either the references or Petitioner's mappings, and thus fail to demonstrate that the asserted grounds do not render the Challenged Claims obvious. SAMSUNG-1032, ¶1-5.

II. The claims of the '480 Patent lack written description support

The test for adequate written description support "requires an objective inquiry into the four corners of the specification from the perspective of a person of ordinary skill in the art. Based on that inquiry, the specification must describe an invention understandable to that skilled artisan and show that the inventor actually invented the invention claimed." *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d at 1351. The test is not whether a claimed element is obvious in light of

the specification. And, even if Ward argues that combining the embodiments to arrive at the claimed features would have been obvious, such obviousness cannot be used to cure a lack of written description. *See Lockwood*, 1571-72; *Intuitive Surgical, Inc.,* 11-15 (explaining that embodiments cannot be mixed to satisfy the written description requirement even if obvious to do so and that "the disclosure must convey with reasonable clarity to one skilled in the art that the inventors possessed the invention claimed."). As explained below, Ward and Ward's expert cannot demonstrate possession of the invention and instead improperly mix embodiments and rely on obviousness.

A. Ward's expert testimony cannot be relied upon because Ward's expert used the wrong standards to assess written description support

In his declaration, Dr. Preneel, Ward's expert, stated that he used the broadest reasonable interpretation standard to interpret the claims. EX2012, ¶26. Thus, the standard that Dr. Preneel used to interpret the claims was not the plain and ordinary meaning standard used for post-grant proceedings, and his understanding of the scope of the claims in attempting to demonstrate support is therefore incorrect. SAMSUNG-1034, 15:9-16:2; SAMSUNG-1033, 31:2-9, 34:10-17.

In addition, Dr. Preneel indicated that he used the obviousness standard when reviewing the '480 Patent and considering written description support.

SAMSUNG-1034, 19:3-20:19. Accordingly, Dr. Preneel used the wrong claim construction standard and coupled that with an obviousness analysis in an attempt to justify support for the claimed features. But, the lack of written description cannot be cured based on obviousness of a patent disclosure. *See Lockwood v. American Airlines, Inc.,* 107 F.3d 1565, 1571-72 (Fed. Cir. 1997); *Intuitive Surgical, Inc. v Ethicon LLC*, IPR2019-01110, Paper 30 at 11-15 (Nov. 20, 2020). Thus, Dr. Preneel's testimony and Ward's arguments, that rely on Dr. Preneel's testimony, should not be given any weight.

B. 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"

Ward argues that the above-noted "providing …" feature (hereinbelow referred to as "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. SAMSUNG-1032, ¶6.

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. SAMSUNG-1032, ¶7.

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; SAMSUNG-1032, ¶11.

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 the Petition, 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; Pet. 9. 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. SAMSUNG-1032, ¶8.

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.

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.

SAMSUNG-1034, 43:4-17

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, 43:25-44:14 (“Q [(Dr. Khan)]. 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 [(Dr. Preneel)]. That is correct.”). As noted above, obviousness cannot be relied upon to demonstrate possession of the invention.

Dr. Preneel and Ward also incorrectly attempt 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." SAMSUNG-1032, ¶10.

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***. SAMSUNG-1032, ¶12.

C. The '480 Patent fails to include written description support for "[the] private key is inaccessible to a user of said electronic device"

Ward mischaracterizes the '480 Patent's disclosure to argue that the above-noted "private key is inaccessible …" feature (hereinbelow referred to as "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. SAMSUNG-1032, ¶13

At best, the '480 Patent teaches that the authentication software "has" a private encryption key[1] 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 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-

[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].

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. SAMSUNG-1032, ¶13.

Ward further contends that "the private key locates in the BIOS." POR, 20. But the BIOS is not in the secure area 62, and there is no disclosure that the private key is stored in a secure part of the BIOS. In fact, the '480 Patent teaches that the authentication software is placed in a part of the BIOS that is accessible to the operating system (and hence to the user) during installation before it is moved to a secure part of the BIOS. SAMSUNG-1001, 7:43-48. 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. SAMSUNG-1032, ¶14.

In support of its contentions, Ward cites to Dr. Preneel (EX2012)'s ¶ 57, which merely recites claim language from Feature A (which, again, is unsupported). The recited claim language states 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.B), and even the unsupported *claim itself* support Ward's claim that the private key is stored in the BIOS. SAMSUNG-1032, ¶14.

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 Patent Owner's argument that the unique serial number or software ID of the authentication software is the private key (which Petitioner does not concede), when such an assumption is combined with the third embodiment illustrated in FIGS. 4 and 5A (which as explained in the petition 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; Petition, 22-24. SAMSUNG-1032, ¶15.

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; SAMSUNG-1032, ¶16. During his deposition, Dr. Preneel conceded that when he states that private key can be authentication data, it is also possible that the private key is not authentication data. SAMSUNG-1034, 44:7-9 ("Q (Dr. Khan)]. it's also possible

that the private key cannot be authentication data; is that correct? A [(Dr. Preneel)]. That is correct.").

Ward also incorrectly contends that omissions in the '480 Patent disclosure somehow support 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. SAMSUNG-1032, ¶17.

D. The '480 Patent fails to include written description support for "the private key is encrypted when the private key is stored in said memory"

Ward incorrectly argues that the '480 Patent describes that "the private key is encrypted when the private key is stored in said memory," (hereinbelow referred to as "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 §§III.A-III.B. SAMSUNG-1032, ¶18.

In addition, even if Ward's argument is to be considered, the '480 Patent does not disclose that the authentication software is encrypted. SAMSUNG-1032, ¶19. Thus, even the conditional argument set forth by Ward, does not provide written description support for Feature C for this additional reason.

E. 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"

Ward relies on the decryption of authentication software as described in the authentication software installation process as allegedly supporting that "the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software," (hereinbelow referred to as "Feature D"). POR, 24-26; SAMSUNG-1001, 6:61-8:11. But this description does not support Feature D for several reasons. SAMSUNG-1032, ¶20.

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 Petitioner does not concede), the key that the authentication software has is "its

own … private encryption key." SAMSUNG-1001, 5:39-40. As explained in the petition (*see* Pet. 19-21), 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. SAMSUNG-1032, ¶21.

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 explained in the petition. POR, 24-26; Pet., 21-24. 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. Thus, Ward again incorrectly mixes incompatible embodiments in an attempt to cobble together support for Feature D.

Intuitive Surgical, Inc. v Ethicon LLC, IPR2019-01110, Paper 30 at 11-15 (Nov. 20, 2020). SAMSUNG-1032, ¶22.

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." SAMSUNG-1032, ¶23.

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. Missing in these pages and in the POR is any rebuttal to Petitioner's written description challenge to claims 2, 4, 5, 16, 18, and 19. SAMSUNG-1032, ¶24. These arguments and the opportunity to show support for these claims is thus waived by Ward. *See* also §V.

III. Claim Construction

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. SAMSUNG-1032, ¶25.

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.

For the purposes of this PGR proceeding, Petitioner agrees with the Board's construction for the reasons articulated in the Institution Decision. ID, 24-26. 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. SAMSUNG-1032, ¶31.

IV. The '480 Claims are invalid in view of the prior art grounds advanced in the Petition

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

As a preliminary matter, Ward's POR includes remarks from pages 39-52 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 expert that are not tethered to the prior art references. During 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 largely disconnected from the prior art references and thus should carry minimal, if any, weight. SAMSUNG-1032, ¶32.

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])

Ward argues that the combination of Ellison and Muir (referred to as EMC) does not render obvious [1d] because Petitioner incorrectly mapped Ellison's primary operating system (OS) 12 to the claimed operating system and incorrectly posits that Ellison's isolated environment region is 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 42_1-42_N and applets 46_1 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. But Ward's arguments represent a fundamental misunderstanding of Ellison's disclosure for the following reasons. SAMSUNG-1032, ¶¶33-34.

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 hinge on the argument 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 failed to provide any evidence of the same. SAMSUNG-1032, ¶35.

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, 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 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, ¶36.

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, Petitioner has mapped Ellison's OSNK 203 to the "decryption key" 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; Pet. 64-66. In mapping feature [1d], Petitioner 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; Pet., 65. 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; Pet. 65. 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. SAMSUNG-1032, ¶37.

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 46_1 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 46_1 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; SAMSUNG-1032, ¶38.

For at least the foregoing reasons, EMC renders [1d] obvious. SAMSUNG-1032, ¶39.

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

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 noted in the petition. Pet., 71-72; SAMSUNG-1032, ¶40.

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 (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. SAMSUNG-1032, ¶41.

Relatedly, Ward also mischaracterizes Petitioner's EMC combination 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, Petitioner did not argue that Muir's virtual smart card driver 155 is stored in a secure memory. Rather, as explained in Section IV.A.3 of the petition, 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; Pet., 45, 48. 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. 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. SAMSUNG-1032, ¶42.

D. Ellison and Muir render obvious claim 1

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 and Petitioner disagrees with Ward's characterizations. Because Ward does not provide supporting rationale, Petitioner will make a good faith attempt to respond to any arguments pertinent to the claims or the asserted combination. SAMSUNG-1032, ¶43.

For example, Ward incorrectly argues that Ellison cannot be combined with Muir's pointer 171 and combining Muir with Ellison would nullify the purpose of Ellison. POR, 41-42.

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. SAMSUNG-1032, ¶¶44-45.

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. Pet., 72-73; 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 can be 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*.; SAMSUNG-1032, ¶46.

As indicated above, 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; SAMSUNG-1032, ¶47.

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.

V. Other Prior Art Grounds

Ward does not advance any particular arguments against the other grounds or dependent claims. Thus, Ward does not provide any specific arguments related to the other prior art grounds and references presented in the petition. These

arguments are thus waived and cannot be raised in Patent Owner's sur-reply or subsequent briefs. *Google LLC v. Uniloc 2017 LLC*, IPR2020-00447, Paper 21 at 9-10 (May 11, 2021); *SAP Am., Inc. v. Versata Dev. Group, Inc*., CBM2012-00001, Paper 81 at 2-4 (Sept. 13, 2013). Therefore, Petitioner maintains its arguments pertaining to these grounds and references. SAMSUNG-1032, ¶49.

Respectfully submitted,

Dated November 28, 2022

/Usman Khan/

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

Attorneys for Petitioner

CERTIFICATION UNDER 37 CFR § 42.24(d)

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petitioners' Reply to Patent Owner's Response totals 5,592, which is less than the 5,600 allowed under 37 CFR § 42.24.

Respectfully submitted,

Dated November 28, 2022

/Usman Khan/

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

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(1) and 42.6(e)(4)(iii), the undersigned certifies that on November 28, 2022, a complete and entire copy of this Petitioner's Reply to Patent Owner's Response and accompanying exhibits were provided by email to the Patent Owner by serving the email correspondence addresses of record as follows:

Jacob B. Henry
William P. Ramey, III
RAMEY LLP
5020 Montrose Blvd., Ste. 800
Houston, Texas 77006

Email: jhenry@rameyfirm.com
wramey@rameyfirm.com
uspto@rameyfirm.com

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