

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO. LTD.,
SAMSUNG ELECTRONICS AMERICA, INC., and
BANK OF AMERICA N.A.,
Petitioner,

v.

WARD PARTICIPATIONS B.V.,
Patent Owner.

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

Record of Oral Hearing
Held: January 26, 2023

Before THU A. DANG, GEORGIANNA W. BRADEN, and
JAMES J. MAYBERRY *Administrative Patent Judges*.

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

APPEARANCES:

ON BEHALF OF THE PETITIONER:

JEREMY MONALDO, ESQ.
Fish & Richardson
1000 Maine Avenue, S.W.
Washington, D.C. 20024

ON BEHALF OF THE PATENT OWNER:

JACOB HENRY, ESQ.
Ramey & Schwaller, LLP
5020 Montrose Blvd.
#800
Houston, TX 77006

The above-entitled matter came on for hearing, by video, on
Thursday, January 26, 2023, commencing at 10:00 a.m., EDT, at the U.S.
Patent and Trademark Office.

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

PROCEEDINGS

1 - - - - -

2 JUDGE DANG: Good morning. We are here today for consolidated oral
3 arguments and IPR 2022-00113, PGR 2022-00007 and IPR 2022-01076
4 challenging patent No. 10,992,480 and IPR 2022-00114 and IPR 2022-
5 01077 challenging patent No. 11,063,766. Samsung Electronics Co., Ltd.,
6 Samsung Electronics America, Inc., and Bank of America N.A. collectively
7 are the Petitioner and Ward Participations B.V., is the Patent Owner. Your
8 panel today includes myself, Judge Thu Dang, Judges Georgianna Braden
9 and James Mayberry.

10 Okay. Let's start with appearances. Who do we have for Petitioner
11 today?

12 MR. MONALDO: Hi, Your Honor. This is Jeremy Monaldo
13 representing Petitioner. I'm joined here with my colleagues, Karl Renner
14 and Usman Khan, Jonathan Driesslein is on the line and Ben Haber from
15 Bank of America is also here with us.

16 JUDGE DANG: Okay. Great. And who do we have for Patent
17 Owner?

18 MR. HENRY: Good morning, Your Honor. Jacob Henry for Patent
19 Owner.

20 JUDGE DANG: Okay. Great. Thank you. Thank you all for joining
21 us, and I have a few administrative details before we get started. First,
22 please be reminded that unless you are speaking please mute yourself

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 because we could have an echo, okay. Two, please refer, when you're
2 speaking, please refer to your demonstratives and exhibits by numbers so we
3 can follow along. There might be an audio lag, so please observe a little
4 pause before you speak and then I would ask that the parties remain on line
5 at the end so that you can answer any questions that our court reporter may
6 have. Please also be reminded that we do have a public line connected
7 today.

8 So with that let's begin. Petitioner, you are to present first. You have
9 90 minutes in total and then please indicate if you'd like any time reserved
10 for rebuttal.

11 MR. MONALDO: Thank you Your Honor. We would like to reserve
12 35 minutes for rebuttal.

13 JUDGE DANG: Thirty five minutes. Okay. So you would like 55
14 minutes; am I correct?

15 MR. MONALDO: I believe so.

16 JUDGE DANG: So, yes. So please begin anytime you're ready.

17 MR. MONALDO: Thank you, Your Honor, may it please the Board.
18 Jeremy Monaldo representing Petitioner.

19 On slide 2 of our demonstratives you'll see that we offer a table of
20 contents that will allow you to quickly identify content in our slides that is
21 relevant to each of the different issues involved in these proceedings. As
22 shown on slide 2, I plan to start with a brief overview of the proceedings and
23 then transition to the first issue related to the written description support for
24 the claims of the '480 patent. After the discussion of written description

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 support, I plan to ask my colleague, Usman Khan, to discuss the remaining
2 issues directed to the prior art challenges involved in these proceedings.

3 In addition to the slides, I plan to reference the PGR petition filed
4 against the '480 patent and I'd ask Your Honors to load the petition and turn
5 to page 25 so that it is ready when we reach that portion of the discussion.
6 So unless Your Honors have any questions at the outset, I'll start the slides
7 and move to slide 4 of our demonstratives to provide a brief overview of
8 these proceedings.

9 As shown on slide 4 today's oral hearing involves two patents, the
10 '480 and the '766. Section 112 arguments were raised against the '480
11 patent and the petition identified four features of claim 1 that lacked written
12 description support. Patent Owner responded to these arguments and I plan
13 to address these arguments later in the presentation.

14 Separately, the Petitioner raised additional written description
15 arguments for claims 2, 4, 5, 16, 18 and 19. These arguments are different
16 than the arguments presented against claim 1 and they can be found in pages
17 25 to 30 of the petition. Patent Owner decided not to defend these claims in
18 its Patent Owner response and waived arguments related to written
19 description support for them. As a result, claims 2, 4, 5, 16, 18 and 19
20 should be canceled as failure to comply with Section 112.

21 Now, this result is notable not just for the patentability of these claims
22 but also for resolution of the PGR eligibility question for the '480 patent that
23 questions whether PGR is appropriate for the '480 patent and turns on
24 whether at least one claim in the '480 patent lacks written description

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 support. Because Patent Owner has not even attempted to defend the lack of
2 support for claims 2, 4, 5, 16, 18 and 19 Patent Owner's actions resolved a
3 lack of support for these claims and also resolves the PGR eligibility
4 question in favor of PGR eligibility.

5 In addition to the Section 112 grounds for the '480 patent, Section 103
6 grounds have been raised against each of the '480 and '766 patents. For
7 these grounds Patent Owner made similar choices to limit its arguments only
8 to the independent claims and only the primary combination of Ellison and
9 Muir. The Patent Owner response does not separately advocate for
10 patentability of any dependent claims and does not substantively address the
11 additional secondary references, Al-Salqan, Searle and Epstein. Because
12 Patent Owners waived these arguments, we plan to focus our discussion of
13 the 103 grounds on the independent claims and Ellison and Muir references.

14 With that background, I'd like to turn us the page 7 of our
15 demonstratives to discuss written description support for claims of the '480
16 patent. As shown on slide 7, before jumping into specific features of claim
17 1, I wanted to discuss four points that provide helpful context for this part of
18 our discussion. First, I'd like to discuss the amendments made during
19 prosecution to add the term private key to the claims. Then I'll briefly touch
20 on the disclosure of private key and the '480 patent, the similarity of claim 1
21 of the '480 patent to a claim that's been found to lack support in a
22 corresponding European patent and significant problems with the analysis
23 performed by Patent Owner's experts.

24 Moving to slide 8, I'll start with the amendments. As shown on slide

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 8 you can see the amendments that Patent Owner made during prosecution
2 to progress the '480 patent to allowance. As shown, Patent Owner added a
3 new decryption feature to the claims and also replaced the term
4 authentication data with the term private key throughout the entire claim set.
5 Patent Owner also adjusted the verb are, used in connection with
6 authentication data with the verb is used in connection with private key.
7 These amendments are important because they demonstrate that the
8 previously claimed authentication data is something different than the
9 claimed private key. The prosecution history thus reveals that these two
10 terms are not interchangeable. Instead, they're distinct and Patent Owner
11 used the narrower term private key to justify allowance.

12 Another important aspect of these amendments is that Patent Owner
13 simply replaced authentication data with private key everywhere the term
14 authentication data appeared in the claims. This type of blanket amendment
15 was made without accounting for the actual disclosure in the '480 patent
16 specification and created significant problems within the claim set. For
17 example, consider dependent claim 2 which, after the amendment and as
18 shown on page 25 of the PGR petition that I asked you to load earlier, recites
19 that the private key is provided by the second transaction part. But as we'll
20 discuss the '480 patent clearly describes the private key as being registered
21 at a third-party. It is not provided by the second party and the blanket
22 amendment to replace this authentication data with the term private key
23 rendered claim 2 nonsensical.

24 If the private key used to create the first party's digital signature is

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 provided by the second party, the key would no longer be private and it
2 would no longer be effective to secure transactions on behalf of the first
3 party. This type of issue is pervasive throughout the claim set based on the
4 type of amendments made during prosecution and as shown on slide 9, the
5 problem is underscored by the complete lack of disclosure of a private key
6 within the specification of the '480 patent.

7 If you turn to slide 9 of our demonstratives, you'll see that the '480
8 patent includes just one paragraph of disclosure related to the claimed
9 private key. This paragraph is located in column 13 near the end of the
10 specification. The paragraph starts with the phrase in a further embodiment
11 signifying that this private key embodiment is a new embodiment that is
12 different and further to what was previously described in the specification.
13 The paragraph also provides limited details as to how the private key is used
14 by the system. It simply indicates that the private key is registered at a third-
15 party and that the private key is needed by the second party to generate the
16 signed digital signature. It says nothing about where the private key is
17 stored. It says nothing about encryption of the private key, and it says
18 nothing about the private key being decrypted in a secure processing
19 environment.

20 JUDGE BRADEN: And counsel, what do you say about Patent
21 Owner's argument regarding figure 3 and the key being contained or
22 embedded in the authentication software 54? Well, if you're going to
23 address that, that's fine. I just want to make sure we get to it.

24 MR. MONALDO: I'll plan to address that for sure. I'll start with

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 figure 3 and I think there's two issues with that and I'll just briefly address it
2 here and I'll certainly follow up later on. But on figure 3 the private key, or
3 there is no private key shown in figure 3. What's shown in figure 3 is an
4 encryption key that's found in the BIOS This encryption key is different
5 than the private key that's put forth in these claims. That encryption key is
6 used to encrypt data that's within the system, but it's not the private key that's
7 used to generate the digital signal signature and that was added to the claims.

8 You can see this in the claims themselves. If you look at the claims at
9 dependent claim 3, what's claimed there is that encryption key that's shown
10 in figure 3. You can see there's an additional key added in claim 3 and that
11 is the encryption key, not the private key and if you look back at the
12 prosecution record, which I was doing yesterday, you can see that when
13 Patent Owner made these amendments to introduce private key into the
14 claims, claim 3 previously said private encryption key. So they changed
15 that. They got rid of private and they just left it as encryption key,
16 signifying the difference between the two different keys in the claims and so
17 the notion that figure 3 has in any way support the claim limitations added
18 related to the private key is completely false and we don't see any
19 description, and I'll get to it a little bit more later about the authentication
20 software, including the private key.

21 JUDGE BRADEN: All right. Thank you, counselor.

22 JUDGE DANG: Counselor, this is Judge Dang.

23 MR. MONALDO: Yes.

24 JUDGE DANG: I have a question. So the specification does discuss

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 a private encryption key, right, and so you're saying a private encryption key
2 is different from private key?

3 MR. MONALDO: That's correct. The private key that was added to
4 the claims is a key that's used to create the digital signature. The patent
5 specification mentions private encryption key just one time in column 5 and
6 that encryption key is that encryption key that we see in figure 3, which is
7 different than a key that's used to create a digital signature. It performs
8 encryption, and the system uses that encryption to encrypt the data that's
9 stored within the system. It does not use that key to create the digital
10 signature, and that is the private key that is discussed and introduced in
11 column 13 and which we see on slide 9.

12 JUDGE DANG: But that private encryption key is part of the
13 authentication software; is that correct?

14 MR. MONALDO: I'd have to look back at the disclosure, but I'm not
15 sure it says that it's part of or it's just used by the authentication software. I
16 don't think it is actually part of the authentication software, but I have to
17 look at that.

18 JUDGE DANG: Thank you so much.

19 MR. MONALDO: Okay. Great. So moving to slide 10, I just wanted
20 to briefly discuss the European proceeding that found the claims of the
21 corresponding European patent to lack written description support and I
22 raised the European proceeding here, not because Europe has the same
23 standard for written description as we do here in the US, it doesn't. Or that
24 Your Honors are in any way bound by the decision in Europe, you're not.

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 But simply to point out that a similar claim was found to lack support in the
2 same disclosure by an independent third-party. We view this as persuasive
3 and that the record of this proceeding demonstrates that the same problems
4 that the European Court found with claim 1 of the EP099 patent are present
5 in claim 1 of the '480 patent which is actually narrower, it has additional
6 issues introduced by the private key amendments made during prosecution.

7 As shown on slide 10 you'll see that claim 1 of the EP099 patent is
8 very similar to claim 1 of the '480 patent. The differences lie in the
9 amendments that Patent Owner made to the '480 patent during prosecution.
10 These differences are highlighted in the text of the claims on slide 10 and as
11 you can see the differences relate to the introduction of the private key and
12 the additional limitation of the private key is decrypted in secure processing
13 environment. These differences creates problems for the support of the
14 claims of the '480 patent over and beyond the issues that the European Court
15 found that the claims of the corresponding European patent. Now, despite
16 these differences, claim 1 of the '480 patent retains much of the claim to
17 claim 1 of the EP099 patent and it suffers from the same problems that the
18 European Court found with that claim. I'll plan to discuss those problems in
19 more detail on later slides

20 Now, as a final introductory point, I'd like to turn to slide 11 of our
21 demonstratives to review testimony provided by Patent Owner's expert
22 during deposition. As shown on slide 11 Patent Owner's expert admitted
23 during deposition that he used the wrong standards for evaluating written
24 description support in his declaration. First as shown on the top of slide 11,

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 the declaration submitted by Patent Owner's expert included the wrong
2 standard for claim interpretation. In paragraph 37 of the declaration Patent
3 Owner's expert clearly states that he applied the broadest reasonable
4 interpretation standard in interpreting the claims of the '480 patent and he
5 later confirmed this was true during his deposition.

6 This is impactful for the written description arguments because in
7 evaluating support for the claim subject matter, Patent Owner's expert was
8 assessing an overly broad interpretation of the claims. This impacted the
9 expert's analysis as the application of the broadest reasonable interpretation
10 standard caused Patent Owner's expert to view the relevant claim language
11 in an overly broad and sweeping manner that required less than appropriate
12 from the specification to establish written description support. This
13 treatment demonstrates that Patent Owner's expert has very limited
14 experience with these types of proceedings and was willing to accept
15 information that was given to him by Patent Owner's counsel without
16 confirming its accuracy.

17 Perhaps more impactful is the testimony Patent Owner's expert
18 offered at the lower portion of slide 11. In this testimony, Patent Owner's
19 expert confirmed that he evaluated the written description of the '480 patent
20 using the obviousness standard. But obviousness is not the proper standard
21 by which we evaluate written description support. So in his testimony,
22 Patent Owner's expert confirmed that he viewed the claim language more
23 broadly than appropriate and then applied an obviousness analysis in
24 attempting to match his overly broad interpretation to disclosure in the '480

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 patent. This is quite simply incorrect. It confirms that Patent Owner's
2 expert should be given very little, if any, weight in these proceedings.

3 Now, with that background, I'll turn to slide 12 and the four features
4 of independent claim 1 that we've identified as lacking written description
5 support in the '480 patent. Although the briefing addresses each of these
6 features in the interest of time, I'll focus our discussion on the first feature
7 listed on slide 12 denoted as feature A.

8 Moving to slide 13. As shown on the upper left portion of slide 13
9 feature A recites providing a private key in a memory of said electronic
10 device and then confirms that said memory is a secure part of a basic in out
11 system BIOS or any other secure location in said electronic device. The
12 '480 patent however is limited to secure storage that is neither within the
13 BIOS or shielded by the BIOS. You can see this in figure 3 on the lower left
14 portion of slide 13 where the secure area is quite clearly shielded by the
15 BIOS. There's no disclosure in the '480 patent of "any other secure location
16 that is divorced from the BIOS" and as a consequence the '480 patent does
17 not reasonably convey possession of an invention where the secure memory
18 is located in any other secure location of the device. This analysis is similar
19 to the analysis in Europe, where the European Court found a similar claim as
20 lacking support in the same disclosure provided by the '480 patent and that
21 analysis applies here in an even more convincing manner because unlike in
22 Europe, claim 1 of the '480 patent is limited to storage of the private key in a
23 secure part of the BIOS or any other secure location.

24 As we've already discussed, the '480 patent provides only one

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 paragraph of disclosure related to the claim private key and that paragraph
2 offers no details on whether the private key is stored on the electronic device
3 or where that private key would be stored on the electronic device. Instead,
4 paragraph clearly states that the private key is registered at a third-party, a
5 third-party, not the electronic device performing the transaction. The ‘480
6 patent never describes that the private key is stored at the electronic device
7 at all, much less that the private key is stored in a secure part of the BIOS or
8 any other secure location.

9 Faced with this dilemma Patent Owner’s sole recourse has been to
10 argue that the private key is part of the authentication software, and that
11 storage of the authentication software equates to disclosure of storage of the
12 private key. Now, even assuming that Patent Owner was correct, which we
13 do not agree with, that does not cure the problem found by the European
14 Court. It does not cure the lack of disclosure of secure storage in a location
15 that is not linked to the BIOS. Now that said, as mentioned, Patent Owner
16 is incorrect in its premise. There’s simply no disclosure in the ‘480 patent of
17 the private key being stored in the authentication software and Patent
18 Owner’s own expert confirmed this during deposition.

19 You can see this testimony on slide 15 and its supported testimony.
20 So as shown by the first question highlighted on slide 15, we asked Patent
21 Owner’s expert whether the private key might not be an integral part of the
22 authentication software and Patent Owner’s expert confirmed that is correct.
23 The private key might not be part of the authentication software. At the
24 lower portion of slide 15 we probed further and Patent Owner’s expert

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 confirmed that he was using the obviousness standard when he concluded
2 that the private key can be an integral part of the authentication software.
3 But as we discussed, that is not the proper standard for written description.
4 The standard is more exacting and requires a disclosure that conveys
5 possession of the specific features set forth in the claims. A finding that a
6 feature could have been present or was obvious is simply not enough and
7 highlights the problem with Patent Owner's argument and incorrect
8 assessment formed by their expert, and to your question earlier, Judge
9 Braden. Here, Patent Owner's expert has admitted that the private key is not
10 an integral part of the software. It's not disclosed. He thinks that it would
11 have been obvious, but that's not the standard.

12 Now unless there are any questions on this feature claim 1, I'll simply
13 note that similar issues exist for the other three features of claims 1 shown
14 on slides 17 through 20 which we've discussed in detail in the briefing, but
15 asking questions and given the time that we have remaining I'd like to turn
16 things over to my colleague, Usman Khan, to discuss the prior art, but just
17 wanted to pause here to see if there are any questions on the written
18 description support arguments. Okay. Thank you, Your Honors. Hearing
19 no questions, I'll ask Usman to continue the presentation.

20 MR. KHAN: Good morning, Your Honors. May it please the Board.
21 My name is Usman Khan and I'll be addressing the prior art related issues.

22 I'd like to start by giving Your Honors an overview of the Ellison
23 reference which is the primary reference asserted in the grounds. In doing
24 so I'll ask for your patience as the first two slides are somewhat detail heavy,

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 but hopefully the benefit of providing an overview of Ellison we can move
2 through the subsequent issues a little faster when we have better
3 understanding of how Ellison maps to the claim features.

4 So I would like to request, Your Honors, to please turn to slide 25.
5 Slide 25, you can see here it's directed to the Ellison reference. Ellison, like
6 the '480 patent, is directed to providing a secure, isolated environment that
7 protects data from external attacks such as corrupt code or viruses, which
8 can be fairly commonplace in E-commerce and business transactions. To
9 provide this protection, Ellison teaches a specific architecture, as shown here
10 in figures 1A and 1B.

11 As can be seen on the left side of the slide in figure 1a, the operating
12 architecture can be split into two very distinct areas. One is the normal
13 execution area that's shown as the white half of the upper portions of the
14 rings in figure 1A and the second being the isolated execution area we
15 highlighted in red text and that's depicted as a gray half of the lower portions
16 of the rings. The operating architecture also depicts different levels of
17 hierarchy of privilege. Ring zero, which is located in the centermost --
18 which is the centermost ring, encompasses the most privileged components.
19 On the other hand, ring 3, the outermost ring has the least privileged
20 components. So user accessibility is typically in the reverse direction where
21 ring 3 encompasses the most user interaction and has user applications with
22 lower level of privilege, such as applications 42 and applets 46.

23 It can be seen here in figure 1A that several important components or
24 modules such as the primary operating system 12, hardware drivers 14,

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 software drivers 13, are all based in the normal execution mode of ring zero.
2 On the other side, the OS nub 16 that's highlighted in yellow and the
3 processor nub that's highlighted in green, are located in the isolated
4 execution region. This depiction of the logical architecture is shown in
5 another manner in figure 1B on the right side of the slide.

6 Figure 1B includes two duplicate depictions of the physical memory
7 60 on the left and the right side of the figure. Memory 60 is split into an
8 isolated area 70 that's highlighted in blue and a non-isolated area 80.
9 Between the two depictions of the memories are modules in the normal
10 execution region. Those are on the left side of the line in the middle of the
11 figure and modules in the isolated execution region which is shown on the
12 right side of the line in the middle of the figure 1B. As can be seen here in
13 figure 1B, applications 42 1 to N, the primary OS 12, software drivers 13
14 and hardware drivers 14 are all located in the normal execution area. In
15 contrast, the OS nub 16, process nub 18 and applets are located in the
16 isolated execution areas.

17 As noted in the bottom of this slide, applets 46 1 to K are tamper
18 resistant and cannot even be accessed by the primary OS 12. This
19 corresponds to what's shown in figure 1A with the operating system 12
20 located in the normal execution mode, whereas the primary nub and the
21 applets are located in the isolated execution level.

22 Looking further at figure 1B, as shown by the arrows that extend from
23 the OS nub 16 and processor nub 18 to the memory 60, the OS nub and
24 processor nub, here they are again highlighted in yellow and green can

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 access the isolated area 70 of memory 60 in addition to the non-isolated
2 area. In contrast, the operating system is limited to accessing only the non-
3 isolated areas of memory, as shown by the arrows extended from OS 12 to
4 only the non-isolated areas 80.

5 The snippet at the bottom of the slide, again, makes it abundantly
6 clear that OS 12 does not have access to components in the isolated
7 execution area, whereas OS nub 16 and processor nub 18 do. Indeed
8 Ellison's disclosure, particularly in its discussion in columns 3 to 8
9 explained in detail that OS nub 16 and processor nub 18 are part of
10 executive entities that operate in a secure environment associated with the
11 isolated area 70 and the isolated execution mode. Thus, Ellison consistently
12 in its figures and its description describes OS nub 16 and processor nub 18
13 as being distinct from the primary operating system 12.

14 Now turning to the next slide, slide 26, figures 1C and 2 provide some
15 additional insight into how Ellison's system works, particularly how it
16 protects the isolated execution areas. For example, figure 1C shows several
17 components using Ellison's system. Starting at the top of figure 1C, a
18 plurality of processors are shown including a processor 110 that includes a
19 normal execution part and a separate isolated execution circuitry 115 that's
20 highlighted in yellow. As noted in the bottom left of the slide, the isolated
21 execution circuitry 115 allows the isolated execution mode operations to be
22 performed. The isolated execution circuitry works with the memory control
23 hub MCH 130 and the input output controller hub ICH 150 to protect the
24 isolated area 156 of the memory. These components can even control the

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 types of buses, the read or write cycles and instructions that can be used to
2 perform operations involving the sensitive data for storage in the isolated
3 area of the memory.

4 For example, Ellison explains that the processor nub can be stored in
5 an encrypted form in memory 160. Only when an particular isolation
6 installation instruction is invoked by the processor nub loader 52 does such
7 an installation begin, and that installation is then performed in a secure
8 manner by transferring the encrypted processor nub into an isolated area and
9 then operations such as decryption and verification of the integrity, et cetera
10 are performed to ensure that no corrupt code can enter the isolated area.

11 After the processor nub is ready and the processor nub is configured to
12 verify and load the OS nub into the isolated area.

13 More generally, the isolated area control 135 that's shown as part of
14 the MCH 130, it's also highlighted in yellow, these modules are specifically
15 configured to protect the isolated area ensure control over any data going
16 into or out of the isolated execution area. This ensures that a component
17 such as a primary OS or a user application can't just enter or contaminate the
18 isolated area and it allows a logical architecture shown in figures 1A and 1B
19 in the previous slides to be implemented so that you can create the difference
20 between the normal execution mode and the isolated execution mode.

21 Now, as a result of this type of protection, Ellison can then implement
22 a secure platform, which is shown on the right side in figure 2. The secure
23 platform can be used to perform several operations, such as key generation
24 for digital signature generation, which we'll describe more in figure 3C in

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 the subsequent slide. But this secure platform as shown in figure 2 includes
2 several components that we just discussed, like the OS nub 16, the processor
3 nub and additional modules like the key generator and usage protector 250
4 to perform various cryptographic operations. Importantly, as noted in the
5 snippet at the bottom right side of slide 26, all of these components operate
6 within the isolated execution environment, and thus highly sensitive
7 cryptographic operations can be performed securely without compromising
8 the security of the system.

9 Turning next briefly to slide 30.

10 JUDGE DANG: Excuse me, counselor. This is Judge Dang. I have a
11 question. The isolation area is an isolation execution area; right? So what
12 Ellison is doing is protecting the execution of these applications; right? So
13 my question is, is there any protection of the storage areas?

14 MR. KHAN: Yes, there is protection of the storage areas. As shown
15 in figure 1B the processor nub and the OS nub are the only elements that can
16 access the isolated areas and those are protected from any type of external
17 user interference from an operating system that provides that protection.

18 JUDGE DANG: Thank you. Thank you very much.

19 MR. KHAN: So yes, turning to slide 30. Slide 30 figure 3C which
20 I've just earlier referenced and this slide shows the internal components of
21 the usage protector and specifically it's showing an example of how the
22 usage protector can be used to generate a digital signature. For example,
23 here a protected private key that's outlined in red can be decrypted and then
24 used to generate a digital signature. As noted in the bottom half of the

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 passage on the right side of the slide the private key can be used to encrypt
2 and digest the message, producing a signature that can then subsequently be
3 stored and retrieved and so returning to slide 25, as I just explained in this
4 manner Ellison discloses a system in which data can be securely stored and
5 processed to perform operations such as the generation of a digital signature
6 and it does this by implementing a logic architecture in any device in which
7 the system includes a normal execution region and an isolated execution
8 region.

9 Now, at the beginning of my discussion of Ellison I had noted that
10 Ellison mentions the need for such systems, particularly performing
11 transactions with other devices, E-commerce transactions, et cetera. Ellison
12 explains that in the case that a system can be beneficial for systems
13 involving E-commerce, but does not really speak to the details of how such
14 transactions with other devices are performed, and that's why our second
15 reference Muir comes in.

16 If Your Honors could turn to slide 27. Slide 27, very quickly going
17 through Muir, it shows -- there is a depiction of figure 5 here on the right
18 side of the figure -- very clearly shows how there's a system in which the
19 digital signature can be sent from one electronic to another electronic device
20 in support of an electronic transactions between two devices and turning to
21 slide 28. Here it shows Muir's figure 3. Muir, like Ellison recognizes the
22 importance of storing data securely and thus proposes an architecture in
23 which a private key is stored in a restricted space of a virtual smart hard
24 driver.

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 In the background section of Muir, Muir discusses how earlier
2 systems had disadvantage because they required additional hardware to just
3 physical smart cards which led to several compatibility issues and another
4 problem with the earlier systems is the private keys were exposed to the
5 operating system, and so Muir proposes this architecture shown here in
6 figure 3 in which a virtual smart card can be used and includes, just like
7 Ellison, a restricted space and Muir also goes to talk about how this
8 restricted space includes a private key that can be use to generate a digital
9 signature which is then sent to other devices.

10 Turning to slide 29. Our petition proposes several reasons why a
11 POSITA would have combined Ellison and Muir and why such a
12 combination would have been predictable and foreseeable, including that,
13 for example, that both the references discuss the need for such systems and
14 electronic business transactions additionally be reducing hardware and
15 implementing sworn software, performance costs can be reduced and
16 Ellison's system can also be implemented in a multi-part system.

17 Now, Patent Owner doesn't dispute these reasons for combining the
18 references. Instead, Patent Owner argues against the teachings of the
19 references themselves and in light of those alleged teachings, the
20 combinations would not have been obvious.

21 As an example, and turning to slide 31, as noted in the box in the
22 bottom right side of slide 31, Ellison argues that combining Muir with
23 Ellison would nullify the purpose of Ellison because any request to create a
24 digital signature would come through the primary OS operating with the

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 driver 155 without even touching the isolated execution environment of
2 Ellison. But this is incorrect. As shown in Ellison's figure 2 here, a
3 protected private key 204 is obtained by the usage protector highlighted in
4 yellow, which we match to an authentication software in the claims and
5 that's obtained from the OS nub 16 highlighted in blue, and recall from what
6 I described earlier that all these components are part of a secure platform in
7 an isolated execution environment.

8 And going back one slide to slide 30, again, looking at figure 3C
9 recall that Ellison teaches generating the digital signature within the usage
10 protector using that private key, and so when we turn back to slide 31, Patent
11 Owner's contention that any request to create a digital signature would not
12 even touch the isolated execution environment is simply incorrect. Ellison's
13 teachings of generating a digital signature are performed entirely within that
14 isolated execution environment.

15 Now, to the extent Patent Owner's remarks are focused solely on the
16 creation of a request for a digital signature, such a feature is not recited in
17 the claims, it's not relevant. But even if such a request were to be generated
18 by a user application and come through a primary OS, as explained earlier in
19 the overview of Ellison, Ellison implements several modules like the MCH
20 and the ICH that ensure that only authorized instructions and commands can
21 be processed to protect the integrity of the isolated execution environment
22 and the security platform. Any request from the OS would be discarded if
23 not authorized properly.

24 Now if Your Honors could please turn to slide 32. One of Patent

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 Owner's main arguments against the Ellison and Muir combination is that
2 several features related to the inaccessibility of the operating system, here
3 noted such as features [1.d] and [1pre-2] of the '480 and [1.f] of the '766
4 patent. But these features are not satisfied and the reason is because
5 Ellison's primary operating system 12 alone on its own cannot correspond to
6 the claimed operating system (audio interference).

7 But before doing so -- in the next few slides I'll explain why Patent
8 Owner's position is incorrect -- but before doing so I wanted to clarify and
9 apologize for an error in the following two slides. Slides 33 and 34. Slide
10 33 at the top includes a snippet of feature [1.d] and slide 34 at the top
11 includes a snippet of feature [1pre-2]. Those snippets should be switched.
12 So slide 33 actually relates to [1pre-2] and slide 34 relates to [1.d]. So
13 apologies for the error and if there was any confusion because of that.

14 So turning to slide 33 which relates the feature [1pre-2], Patent Owner
15 argues that feature [1pre-2] is not rendered obvious by Ellison because, as I
16 just mentioned Patent Owner argues both the operating system OS 12 and
17 the OS nub 16 must correspond to the claimed OS, not just the operating
18 system. That's Patent Owner's position. Now both OS 12 and OS nub 16
19 must correspond to the claimed operating system.

20 But this is incorrect for several reasons. As I explained earlier,
21 Ellison describes that OS nub 16 is a distinct and separate entity from OS 12.
22 OS nub operates within the isolated execution area, primary OS does not.
23 Moreover, there's nothing preventing Ellison's system from having multiple
24 operating systems. In fact, as Your Honors will see, in slide 7 of Patent

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 Owner's demonstratives they include a snapshot of Ellison's column 7,
2 lines 32 to 58 and that snapshot, that actually explicitly recites operating
3 systems in plural indicating that Ellison's system would have included, or at
4 least contemplated, multiple operating systems. Patent Owner has not
5 provided any reason why Ellison's system could not have two or more
6 operating systems, one, that is configured to operate in normal execution
7 mode and the other in the isolated execution mode. In fact it was just
8 consistent with the disclosure in Ellison and the claim does not require all
9 operating systems in a system to create a run time environment for that to
10 not have access to the authentication software.

11 On slide 33, as shown in the right Ellison's figure 1B clearly shows
12 that the primary OS highlighted in yellow is located in the normal execution
13 area and supports user applications 42 highlighted in red. Like, for example,
14 by creating a run time environment for application pages 82 used by those
15 applications. Recall also that the OS cannot access any area of the isolated
16 execution environment for memory and that includes the usage protector
17 250. For these reasons Ellison renders obvious feature [1pre-2].

18 Now turning to slide 34 which again relates to feature [1.d], that's the
19 decryption key. In the petition we map the OSNK and which is the
20 operation system will take two or three to the decryption key as shown here
21 in figure two, the OSNK which is the operation system new key 203 to the
22 decryption key. As shown here in figure 2, the OSNK 203, it's highlighted
23 in yellow in the box in figure 2, that's generated within the secure platform
24 and supplied to the usage protector 250 which as we note here, is a trusted

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 agent and the secure platform again is implemented within the isolated
2 execution environment.

3 Now as we discussed earlier in figure 3C, the usage protector 250 uses
4 this OSNK 203 to decrypt a private key which is then used to generate a
5 digital signature and so what we see from the teachings of Ellison is that the
6 OSNK is limited to the isolated execution environment and is used to
7 perform decryption. This isolated execution environment cannot be
8 accessed by the primary OS, the user of any user operated software, because
9 it remains in the secure platform and so for this additional reason we think
10 that feature [1.d] is rendered obvious by the teachings of Ellison and Muir.

11 Now turning to the next slide, slide 35, Patent Owner has the same
12 similar argument against feature [1.f]. So I'm not going to repeat our
13 rationale here but the same thing applies for feature [1.f]. I just wanted to
14 make a note of that.

15 I also understand that I'm running up against time and so in the
16 interest of time I wanted to leave Your Honors with one final note and that's
17 regarding feature [1pre-4] of the '766 patent. So if I could ask Your Honors
18 to turn to slide 47, please. Slide 47 here, again, this feature [1pre-4] of the
19 '766 which recites that the electronic device comprises a system for
20 accessing a memory location in the memory and wanting the system for
21 accessing the memory location is configured to selectively record the storage
22 locations of the secure area.

23 Now, in the petition we offered two mappings for this particular
24 feature. One mapping is based on the teachings of Ellison, the other is based

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 on the teachings of Muir. In the response, Patent Owner offered some
2 remarks with respect to the second mapping addressing the teachings of
3 Muir but they were silent as to the mapping based on Ellison. We pointed
4 this out in our Petitioner reply in the '766 and in spite of us pointing that out
5 Patent Owner offered no response to the first mapping, which is somewhat
6 telling and so we wanted to make that note here to Your Honors that there
7 remains at least one mapping that on the record is unrebutted in spite of our
8 note to Patent Owner multiple times at this point.

9 With that, Your Honors, I conclude my talk today and if you have any
10 questions, I'd be happy to answer them.

11 JUDGE DANG: This is Judge Dang. I have, I guess, a broad
12 question. How are you -- can you clarify how are you combining Ellison
13 and Muir on a broad level?

14 MR. KHAN: Yes. So, yes. So as we discussed Ellison provides a
15 system architecture on one device that can provide a secure environment for
16 performing cryptographic operations. That includes the generation of a
17 digital signature and it even alludes to the fact that that signature is used for
18 a message; right? And you think about it, for electronic transactions, you
19 really don't need to generate a digital signature unless you're going to be
20 communicating with another device; right? The digital signature indicates
21 your identity, the first just identity, the sender's identity. But Ellison doesn't
22 go into the details of, you know, sending it to another device. Muir does and
23 our combination is basically that Muir explicitly teaches I'm going to take
24 this digital signature that I generated and send it to another device. That's

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 the last feature of the independent claim and it's basically that simple
2 combination of these two, where Ellison is focused on the system. It tells
3 you it generates a digital signature so it's explicitly telling you it's sending it
4 to another device, well Muir does that and Muir was based on the same
5 concepts as well as providing security, implementing a digital signature on a
6 secure environment. That's how we see the two come together at a high
7 level.

8 JUDGE DANG: Thank you.

9 MR. KHAN: With no further questions thank you very much, Your
10 Honors. Petitioner has no further comments.

11 JUDGE DANG: Okay. Great. Well, then you have 40 minutes left.
12 Patent Owner, you can begin any time and, I'm sorry, would you like to
13 reserve any time?

14 MR. HENRY: Good morning, Your Honor. Jacob Henry for the
15 Patent Owner. Yes, Your Honor, I would like to reserve 20 minutes if it's --

16 JUDGE DANG: So then, yes, 70 minutes. Thank you so much.

17 MR. HENRY: You're very welcome indeed. With all due respect,
18 I'm going to go ahead and turn off my video just because, unless you want it
19 on, I'm going to go ahead and turn it off because it's been giving the issues.

20 JUDGE DANG: That's fine, yes.

21 MR. HENRY: You all know what I look like. Not that much to look
22 like.

23 JUDGE DANG: Okay, thank you.

24 MR. HENRY: Thirty years ago, maybe, but not today. So I'm going

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 to go ahead and turn off my video. You can hear me if you want me to turn
2 it back on for some reason, I'll be happy to do that.

3 May it please the Board. I had intended to proceed in sort of one
4 order, but I think that I will proceed in another, if I may, just because I think
5 it'll mean I'm less likely to forget some things that I needed to say.
6 Obviously, this is -- we're actually talking about three cases and two patents
7 so it's fairly complicated for everybody concerned. So I ask you to please
8 bear with me on that.

9 So the first thing I'd like to do is address the issue of support for some
10 subject matter and the '480 patent and also reply to some of the things that
11 were said by opposing counsel before getting into the analysis of the prior
12 art. So if you are so inclined just to make it easier to follow, if you'd like to
13 go to page 14 of my demonstrative exhibit. See, there were basically four
14 reasons why four elements that were issues for the Board about whether or
15 not support was present. So I'll come back to that momentarily.

16 Before I do, I'd like to say a few things about what was said by
17 opposing counsel in their excellent argument. One is that comments were
18 made or the argument was made, excuse me, that if Petitioner did not
19 respond, the point of the claim or a specific point -- I'm paraphrasing, of
20 course -- made by the other side, that that constitutes sort of an agreement
21 that that element had been proven. Obviously, just to remind, I know you all
22 know the law but I think it's worth emphasizing that the burden is on the
23 Petitioner. So I'll leave it at that if I may.

24 I heard a lot of discussion about what happened in Europe and I think

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 you should make up their own minds and more or less ignore what happened
2 in Europe. I don't think it's that illuminating. There's a lot of stuff to read if
3 you're so inclined, but it's not very helpful and I think you all can read it for
4 yourselves and make up your own mind using American jurisprudence and
5 that's what I encourage you to do. But I would like -- it's worth noting that
6 the Europeans specifically found that authentication data and the bits strings
7 and the stuff in the authentication table, it's the same and I'll come back to
8 that. But that those elements were supported in that they were basically
9 interchangeable terms.

10 I'd like to address the issue of private key. I thought I heard someone
11 say that the private key is not necessarily used for decryption and the issue
12 came up with regard to private key and the drawing in my exhibit, excuse
13 me, demonstrative exhibit on page 4 that the encryption key illustrated there
14 is or is not a private key. Here's my position on the private key business.
15 Private keys are used for encryption and decryption. That's (indiscernible),
16 full stop as I understand it. I have never seen anything, nothing I've learned
17 has indicated to me otherwise that that's not what was intended by the Patent
18 Owner or anybody in this discussion. That's what they're used to do. They
19 encrypt data, and then they're used to draft (phonetic) keys that are properly
20 held by the other side and the other side, they are used to decrypt it.

21 With regard to the experts --

22 JUDGE DANG: Mr. Henry? This is Judge Dang. I have a question
23 along the line of the private key be, also could be, an encryption key, but it
24 also, according to the claim, has to be for the digital signature, no?

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 MR. HENRY: Yes.

2 JUDGE DANG: Thank you.

3 MR. HENRY: True. However, I'm sorry I'm not an expert on this
4 subject, but I've read (phonetic) a lot and my understanding is that a process
5 involved in creating the digital signature is related to encryption. So not --
6 one is not divorced from the other.

7 JUDGE DANG: Okay. Thank you.

8 MR. HENRY: You're welcome, Your Honor. Okay.

9 JUDGE MAYBERRY: Excuse me, counsel.

10 MR. HENRY: Yes, sir.

11 JUDGE MAYBERRY: Judge Mayberry. Along the same line of
12 questioning. Again, the claim recites that we have a private key that's used
13 to generate a digital signature and then in column 5, at least the '480 patent
14 discloses, and I'm at lines 39 and 40, that the authentication software has its
15 own unique serial number, software ID and/or private encryption key. If I
16 understood Petitioner's argument earlier, it was that this private encryption
17 key it's used for encryption, sure, but encrypting data that was not a digital
18 signature and it seems like in some of your arguments you're directing us to
19 the private encryption language there in column 5 to support written
20 description support for the claimed private key. So can you address
21 Petitioner's argument that it's clearly different private encryption as
22 disclosed at column 5 and private key as recited in claim 1, that they're
23 different?

24 MR. HENRY: Yes. I will give it my very best, bearing in mind that I

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 was not a patent attorney with this application was filed. It's not the best --

2 JUDGE MAYBERRY: Excuse me, counsel. Maybe I can help out
3 and ask my question a little differently. Can you point us to where in the
4 record there are arguments and supporting evidence to show that they are the
5 same, the private encryption key and private key?

6 MR. HENRY: The one location is and the deposition of our expert,
7 Dr. Preneel, was asked by opposing counsel when we say -- I think I'm
8 answering your question, I apologize -- and when we say a private, this is
9 page 52 and 53, line 22.

10 "Q When we say a private encryption key, that is the key that is
11 private that is used to perform encryption; is that correct?"

12 "A I think we've been therefore. So private means you don't make
13 it public. But as I explained, the term encryption key can also -- is also
14 sometimes used for other cryptologic algorithms such as authentication
15 programs."

16 So I think that what the expert had in mind there was generation
17 deciding algorithms which is what our patent is primarily about.

18 JUDGE MAYBERRY: Okay. Thank you.

19 MR. HENRY: You're welcome. And returning to the issue of the
20 standard used by our expert, Dr. Preneel, in evaluating the support for the
21 claim terms, Dr. Preneel entered the claims that were answered. His
22 understanding of the law of what leads to adequate support from combined
23 elements -- combined pieces within a disclosure is actually not relevant. If
24 you read the record he was plainly asked, the gist of it being his point was

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 I'm reading what's in front of me, I'm using plain normal language. He said
2 how do you construe the claims? Well, under the broadest reasonable
3 interpretation. The fact that he was reading the claim as having the broadest
4 reasonable interpretation does not somehow mean that there's less support.
5 As I understand it I don't think that means there's less support in a
6 disclosure for that claimed element. I think he was just using his common
7 sense like any scientist would do and was mainly caught off guard a little bit
8 by the question.

9 Okay. So I'm going to turn then to some of the issues about support,
10 the subject matter and this is maybe a little murky but I'll ask you to please
11 bear with me. So, again, if you'd like my frame of reference is the
12 demonstrative exhibit page 14, claim (1) providing a private key in a
13 memory of said electronic device wherein said memory is being a secure
14 part of a BIOS or in any other secure location in said electronic device
15 operated by the first transaction party.

16 There are various groups of support for that claimed element but I'm
17 not going to read them all in detail, but I am going to point to them within
18 the '480 patent which is Petitioner's Exhibit 1006. No, I'm sorry. Scratch
19 that last comment. That's not Petitioner's (indiscernible). But in any case
20 the '480 patent in column 7, lines 6 through 8 it notes,

21 "Compared to a new computer device, further steps are necessary in
22 the above-described installation method to install the necessary software and
23 the authentication table in a secure memory location of the device. Such a
24 secure memory location may be a part of the secure memory or it may be an

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 encrypted part of a non-secure memory.”

2 Either way it’s secure. That was column 7, lines 6 through 8.

3 Column 9, lines 7 through 19 recites,

4 “An authentication table may be securely stored in the secure storage
5 location 60 in such a part of the computer commonly seen as part of the
6 BIOS, the authentication table is unreachable for the operating system and
7 thus for the user. With the authentic table securely stored in the secure
8 location 60, this software should run in an environment in the BIOS, thus
9 showing that the authentication table is preventing the authentication table
10 from being accessible to the operating system at any time.”

11 We have further evidence about its security. In another installation
12 method, column 9, lines 35 to 43 in the ‘480 patent, that’s column 9, 35
13 through 43, we discuss -- the Patent Owner discusses the installation method
14 for the claimed invention and recites,

15 “The authentication data, for example, the authentication table, is
16 stored in the memory that is accessible to an operating system and possibly
17 to a user of the device. To prevent that the user might obtain this
18 authentication data, the authentication data are encrypted. Thus, the user
19 may only obtain encrypted authentication data.”

20 So that’s an example of the fact that there’s (audio interference) one
21 of the ways that we make data secure in the invention is by encrypting it and
22 encrypting it in a way that makes that data unreadable and inaccessible to the
23 user of the device. Just keeping in mind this data is intended to go -- it may
24 seem odd, but that encrypted data is ultimately intended to be used in a

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 transaction with a third party. It's out there (phonetic), someone else is
2 going to decrypt it, not the device.

3 At column 10, lines 25 to 33. The patent recites,
4 "After installation of the authentication software, the authentication
5 software obtains a master bit string according to cell 202. A master bit
6 string may be a large array of characters, for example, 2,048 numbers. The
7 MBS master bit string may be embedded in the authentic software package
8 and in that case may not be obtained separately."

9 So it's in an encrypted master bit string, and then I'm not going to
10 read the rest of them to you but I will point to column 10, lines 59 through
11 67. That's column 10, lines 59 through 67 of the '480 patent and column 13,
12 lines 30 through 36 which recites,

13 "The authentication software may be provided with a system for
14 signing a digital signature according to the present invention, at least a part
15 of the software identification number or any other application identifying
16 character string therein after referred to as a private key."

17 The next point was the private key being inaccessible to a user of the
18 electronic device. Column 9, lines 42 through 47 specifically recites,

19 "To prevent the authentication data from becoming accessible to a
20 user, the authentication data should only be decrypted in a secure processing
21 environment such as a ring zero processing environment which is embedded
22 in a processing unit, commonly used in personal computers."

23 Also see column 10, lines 25 through 33. "After the installation
24 already," (indiscernible) elsewhere so I'm not going to say it again. But

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 again, the inaccessibility of the key can be supported by column 10, lines 25
2 through 33.

3 The third point relates to the private key being encrypted when the
4 private key is stored in the memory. First of all, I point out again that in
5 Europe, you can make up your own mind, but it is worth noting that in
6 Europe the authentication table, excuse me, the authentication data was
7 inaccessible to the user and it was co-extensive with the terminology
8 authentication table which (indiscernible) I note it is our position that the
9 private key as claimed reads on those elements and I think it's worth noting
10 at this point the position that the Patent Owner, or excuse me, the fact that
11 during prosecution the attorney prosecuting the application was willing to
12 amend the claims to get an allowance absent additional information does not
13 necessarily mean that the patent attorney's read on the claim term is the
14 same as the meaning of the claim term asserted today. It is all too often
15 possible that the patent attorney may have been wanting to get along to go
16 along, to get an allowed application and absent additional information from
17 the record it shouldn't be treated as any one particular thing or another,
18 except for what plain English tells us the words mean.

19 Also, again –

20 JUDGE MAYBERRY: Excuse me, counsel.

21 MR. HENRY: Yes.

22 JUDGE MAYBERRY: This is Judge Mayberry again. If I heard you
23 right you said the private key as claimed reads on the terms authentication
24 table or authentication data; is that correct?

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 MR. HENRY: I did and maybe I misspoke. I'm talking about the bit
2 strings and the authentication table data that are in -- bear with me.

3 JUDGE MAYBERRY: So this is the master bit string, the MBS?

4 MR. HENRY: Yes, yes, Your Honor. Thank you.

5 JUDGE MAYBERRY: So the MBS is the same as a private key?

6 MR. HENRY: The MBS -- the private key is stored as an MBS.

7 JUDGE MAYBERRY: As an MBS.

8 MR. HENRY: Yes.

9 JUDGE MAYBERRY: And where in the specification do we note
10 that? Where is that described?

11 MR. HENRY: Sorry, I can't remember at this point. I think I
12 addressed that --

13 JUDGE MAYBERRY: Is that what you directed us to in column 13?

14 MR. HENRY: I know I directed you to it.

15 JUDGE MAYBERRY: So it's column 13, starting at line 31. It says,
16 "In a further embodiment the authentication software may be provided
17 with a system for signing a digital signature according to the present
18 invention using at least a part of a software identification number wherein
19 the other application identifying character string thereafter referred to as a
20 private key."

21 MR. HENRY: Yes.

22 JUDGE MAYBERRY: So that disclosure, that description is
23 describing a MBS?

24 MR. HENRY: Yes. Yes, Your Honor. It's (audio interference) only

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 one if memory serves, and it typically does, but that is, yes.

2 JUDGE MAYBERRY: Okay.

3 MR. HENRY: And that's one to be within, generally within the
4 secure area 62 which is found in figure 3 of the '480 and the '766 patents.
5 So, again, the issue about the private key staying encrypted when stored in
6 memory, Dr. Preneel was asked. This is in page 23, 24 to 33 about private
7 keys during his deposition on the '480 patent which is Exhibit No. 1034 and
8 the question was asked,

9 "Q Well, my question is very -- because you used the word 'either,'
10 I'm trying to understand that do you mean, then, that all cryptography
11 private keys can just be either bit strings or algebraic objects?"

12 "A I think, indeed, that that's the case in all crypto systems that are
13 being used and that are being described in textbooks."

14 "Q Is that the case for the disclosure in the '480 patent as well?"

15 "A Yes, it is."

16 I think it's may not be too strong to say that -- disregard. Last point
17 was that the encryption, excuse me, I note that the encryption of the bit
18 string when stored in a secure part of the BIOS which is also -- the
19 encryption of the bit string when stored in the secured part of the BIOS is
20 inherently inaccessible to the operating system as claimed, and I direct you
21 to column 7, lines 45 through 65 of the '480 patent as well. I'm not going to
22 read you that cite but, again, that is column 7, lines 45 through 65 that deals
23 with encryption the storage of the key, and pointing forward to the Board an
24 issue raised was the private key is decrypted in a secure processing

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 environment inaccessible to said user and to any user operated software.

2 I would direct you to column 9, lines 42 through 46 which recites,

3 “To prevent the authentication data becomes accessible to a user, the

4 authentication data should only be decrypted in a secure processing

5 environment such as a ring zero processing environment which is embedded

6 in a processing unit of a commonly used personal computer. Such a secure

7 processing environment may only be accessible to selected software

8 applications and preferably not a user operating the software application.

9 Further, a decryption algorithm in a decryption key should not be attainable

10 to any user.”

11 If I may, this last comment if you will from the ‘480 patent sort of

12 dovetails nicely with the introduction that I’d like to make about the alleged

13 obviousness of the claimed invention and that is that the Ellison disclosure is

14 related to systems and methods for providing secure transaction, excuse me,

15 Ellison is related to protecting internal components of a device from

16 unscrupulous attacks. Okay.

17 If I could I’d like to direct your attention to page 2 of my

18 demonstrative exhibit sheet and --

19 JUDGE DANG: Mr. Henry, I’m sorry.

20 MR. HENRY: Yes.

21 JUDGE DANG: Can I interrupt before we go to the prior art

22 references. Can we go back to I guess point one, issue one for the written

23 description?

24 MR. HENRY: Yes.

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 JUDGE DANG: Can you point out where the limitation “or any other
2 secure location” was disclosed in the ‘480 patent? You see “providing a
3 private key in the memory, the memory being a secure part of the BIOS or
4 any other secure location in the device.” So do you, you know, I apologize
5 if I missed it but can you point to any section in the ‘480 for that?

6 MR. HENRY: That’s all right. That’s a great question and that’s one
7 of those if you blink you could miss it maybe. I know I was talking pretty
8 fast. I don’t want to rehash everything that I said and I say this with respect.
9 I thought that I covered that. The verbiage is not necessarily the private key;
10 right? Keeping in mind a key is taught by the bit string and the
11 authentication data. All of that, the authentication data is stored when it’s --
12 it's stored in the secure area. So my page demonstrative exhibit slide 4
13 which is figure 3 from the ‘766 patent and the ‘480 patent, we see that
14 there’s a secure area and there’s lots of discussions about such things being
15 stored there.

16 Alternatively, it’s encrypted. For example, column 9, lines 35 through
17 43. “In a preferred installation method,” and again it’s worth pointing out
18 there was some discussion about, well, you know, you have embodiments,
19 there’s different embodiments and it’s not that you can’t read anything from
20 one embodiment into another. That is -- I don’t think that’s the standard.
21 You have to use common sense when reading a patent disclosure and if it,
22 for example, a claimed invention that works a certain way and they tell you
23 how to install it in a certain way and part of that installation includes putting,
24 I don’t know, element X in there because it’s necessary. Element X is part

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 of the invention. It's taught (indiscernible).

2 So returning to your question. You asked about the storage of the
3 private key other than in a BIOS. Well, one example was column 9, 35
4 through 43. It recites,

5 "In a third preferred installation method, illustrated in Fig. 4, the
6 authentication data, for example, authentication table," keeping in mind
7 what I said about what the expert said earlier, "this information is stored in a
8 memory that is accessible to an operating system and possibly to a user of
9 said device,"

10 But it's to prevent that becoming available, it should be prevented
11 through encryption. That's the user may only obtain encrypted
12 authentication data which is basically useless if it's encrypted. Given that
13 we're trying to use this for a transaction with a third party the information is
14 only possibly usable by that third party. There are other -- can I just give
15 you some other examples, Your Honor?

16 JUDGE DANG: Yes, that's fine. Thank you.

17 MR. HENRY: Okay. Column 10, lines 25 through 33. Column 10,
18 lines 59 through 67. Column 13, line 30 through 36. I've been talking here
19 for about half an hour, does that sound about right? I've been talking for
20 half an hour.

21 JUDGE DANG: That's correct. Thank you. You can proceed.

22 MR. HENRY: Right, Your Honor. Thank you. Okay. I'm just
23 pausing for dramatic effect. Let's talk about then the alleged teachings of
24 the prior art and the claim subject matter. As written in Ellison, Ellison

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 reminds us redesigning operating systems creates software compatibility
2 issues and causes tremendous investment and development efforts. Put
3 another way, redesigning software systems and operating systems is not easy
4 and that's how Ellison viewed it in -- prior to 2004.

5 With that in mind I'd like to point out that Ward's patents, Patent
6 Owner's patents, are directed to systems and methods for providing secure
7 transactions between parties. Ellison, on the other hand, is directed to a
8 system for protecting internal components of a device from unscrupulous
9 attacks. The problems to which they are directed are different and their
10 solutions are also different and the fact that one is able to go out and find
11 another effort (phonetic) that deals with interacting with third party
12 transactions and the attempt to tack it on is simply not there, it's untenable,
13 and I'll explain why. I'm referring of course to Newark (phonetic).

14 Now if I could, please, refer you to slide No. 3 of Patent Owner's
15 demonstrative exhibits there's a few items I'd like to highlight before I get
16 into the meat of my arguments. Claim 1 of the '766 patent, I would say that
17 it deals -- what I'd like to talk about today relate to three overarching
18 portions of that claim. One is the memory and another is the operating
19 system, and a third is the authentication software and of course everything
20 that I say applies with that (indiscernible) to the other independent claims of
21 the '766 patent and actually substantially to the '480 patent as well. Should
22 be self evident where that's true.

23 Again, so let's talk about what I wanted to say about the memory.
24 With the memory involved is that '766 with regard to memory recites,

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 “The electronic device having a memory comprising storage
2 locations, part of the memory being accessible to the operating system and
3 part of the memory being a secure area. Wherein the electronic device
4 comprises a system for accessing a memory location in the memory wherein
5 the system for accessing the memory location is configured to selectively
6 report the storage locations of the secure area.” The operating system.

7 Claim 1 recites it partly with regard to the operating system. The
8 electronic device having an operating system creating a run time
9 environment for user applications and authentication software running in a
10 separate operating environment independent from and inaccessible to the
11 operating system. Wherein the storage locations of that secure area are not
12 reported to the operating system while, at the same time, are reported to the
13 authentication software which is running in the separate operating
14 environment.

15 With regard to the authentication software, claim 6, excuse me, claim
16 1 recites in part the electronic device having an operating system creating a
17 run time environment for user applications and authentication software
18 running in a separate operating environment independent from and
19 inaccessible to the operating system. Wherein the authentication software is
20 stored in the secured area and is inaccessible to the operating system.

21 It is our position then that Ellison and Muir do not teach the claimed
22 memory. The claimed invention is directed towards a single network having
23 various attributes, either as part of a modified block or as a separate part of a
24 hard drive, a reconfigurable consul or an encrypted part of user accessible

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 memory.

2 In contrast, in Ellison there are multiple memories. For example, if
3 you look at figure 1B and figure 1C of Ellison you will see that there are
4 multiple memories including elements 60, 154, 155, 160 and 170. Indeed,
5 the fact that Ellison requires so many memories to operate is an indication of
6 its difference from Patent Owner's claimed invention and of the
7 incombability of Ellison's teachings with Muir. For example, if you look
8 at figure 1C of Ellison you will see that there are three separate buses, each
9 of which would be reconfigured substantially to make it somehow operable
10 with the teaching of Muir.

11 Turn now to the operating system.

12 JUDGE MAYBERRY: Excuse me, counsel. This is Judge Mayberry.

13 MR. HENRY: Yes, sir.

14 JUDGE MAYBERRY: How do you respond to the general
15 convention that the article A in patent claim drafting, so a memory means
16 one or more, not a single?

17 MR. HENRY: What you said is true, however if I say a memory --
18 I'll rephrase. One or more memories or something like that and then I
19 further talk about the memory, the memory, the memory, the memory.
20 Obviously I'm talking about the same memory.

21 JUDGE MAYBERRY: Oh, yes. I agree with that.

22 MR. HENRY: Yes.

23 JUDGE MAYBERRY: So your point isn't that there's a single
24 memory, it's just that the memories have to do everything that's recited as

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 part of the memory?

2 MR. HENRY: Yes. We have a single memory that's doing the
3 claimed -- that complies with the claimed subject matter so that any, in order
4 to teach that memory that recited memory would have to have the same
5 attributes, so standing alone --

6 JUDGE MAYBERRY: I'm sorry. Meaning that the prior art would
7 have to disclose a single memory?

8 MR. HENRY: No. The prior art would have to disclose a single
9 memory that's operating in the manner that our single memory is operating.
10 There may be other memories doing other things.

11 JUDGE MAYBERRY: Okay. Thank you.

12 MR. HENRY: You're welcome. It's a fair question. And I was
13 discussing the operating system. I specifically would like to point you to the
14 language about the operating system in claim 1 from the '766 patent which
15 recites wherein the storage locations of the secure area are not reported to
16 the operating system, while at the same time they are -- I'm paraphrasing
17 here -- while at the same time they are reported to be authentication software
18 which is running in a separate operating environment...the method
19 comprising, et cetera, et cetera. Okay. First of all, likewise our claim is
20 directed to one operating system having various attributes. Not the slices
21 (phonetic) of an operating system, an operating system, and I refer to this in
22 one of my surreplies and that is Ellison says in discussing figure 1A of
23 Ellison, Ellison says 1A shows an operating system architecture. This is
24 what an operating system looks like and remember, we're talking about

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 what's going on in approximately the year 2004. There's nothing at all in
2 the '480 patent that would lead one to believe that we were talking about
3 multiple operating systems doing multiple things and slicing and dicing the
4 operating system. It's an operating system that does stuff, there's no special
5 meaning to it. It's just an operating system. That's obviously what they --
6 to me that's what the Patent Owner had in mind, that's what the patent
7 describes and I think by and large Ellison kind of does the same thing.
8 Ellison says, well, here's what the operating system architecture looks like
9 and then they start getting into some of the pieces, but overall it's an
10 operating system. My argument does not rest solely on that point, however
11 it's definitely worth noting.

12 Okay. So back to the operating system. The Petitioner has argued
13 that Muir teaches an operating system that cannot access the usage protector.
14 This is not correct. That is the usage protector 250 of Ellison has been
15 mapped by the Petitioner on to the authentication software. So, again,
16 Petitioner argues that Muir teaches an operating system that cannot access
17 usage protector, excuse me, Ellison teaches -- I misspoke -- that cannot
18 access the usage protector. But that's not correct.

19 If you look at Ellison, for example, Ellison operating system 12, it can
20 access OSNK, the key 203, and so the OS 12 which the Petitioner treats as
21 the operating system just said it's not a correct mapping but we'll assume for
22 argument's sake that that's true. Even there the operating --

23 JUDGE BRADEN: I'm sorry, counselor. So are you saying that
24 Ellison's 12 is not an operating system?

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 MR. HENRY: It is not the operating system in the sense that it's been
2 claimed. It's certainly --

3 JUDGE BRADEN: Okay. Because I'm looking at Ellison's figure
4 1B and it literally says primary OS, well I mean No. 12 is labeled as primary
5 OS so I'm not sure how to square that with what you just said.

6 MR. HENRY: Can I get there?

7 JUDGE BRADEN: Oh, absolutely.

8 MR. HENRY: I think I'm -- it's a fair question. I'm cautiously
9 optimistic that it's going to get there. I know that it says it's the primary OS
10 but there are other OS's doing things or other systems doing things in
11 Ellison in conjunction, and moreover that operating system OS 12 does not
12 -- I hope to show -- have the attributes of the claimed operating system.

13 So, for example, the OS 12 knows about the location of the key 203
14 which is shown in figure 1A because it can access that key. But let's talk --
15 importantly we need to address the issue of the mapping of the usage
16 protector 250. Ellison does not name -- does not identify by name where the
17 usage protector 250 is stored; okay? How can we be unambiguously certain
18 and infer that the usage protector is inaccessible in a raised (phonetic)
19 situation to OS 12 if we don't even know where it is?

20 I'm going to say more about the authentication software which is
21 element 250 and, again, what I'm about to say with regard to authentication
22 software obviously applies to '480 because it too claims authentication
23 software in the independent claims.

24 Wherein the authentication software is stored in the secure area

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 inaccessible to the operating system. I would point you to column 7, lines
2 33 through 39 of Ellison which states, and see also figure 1C of Ellison.

3 “The mass storage device 170 stores archived information such as
4 code, for example, processor nub 18, programs, files, data, applications. For
5 example, applications 42, also applets 46 and operating systems. The mass
6 storage device may include compact disks, RAMs, floppy diskettes and hard
7 drive 176 and other storage devices.”

8 The operating system, however you slice it, must have access to mass
9 storage device 170 as said device 170 stores the applications and the applets
10 by Ellison’s own terms. Without access by the operating system, thereto no
11 electronic transaction could even take place. Moreover, the mass storage
12 device contains code, even processor nub 18 can be described as code,
13 according to Ellison, contains code and programs. Ellison does not disclose
14 any limitations or restrictions in relation to this point so OS nub 16, key
15 generator 240 and usage protector 250 can be stored in the mass storage
16 device 170 and is accessible by the operating system in Ellison.

17 Likewise I point you to column 8, lines 33 through 34.

18 “OS nub or OS executive component 16 is part of the operating
19 system running on the secure platform.”

20 Ellisons own terms. Those are part of the operating system as
21 described by Ellison.

22 Returning to column 7, Ellison also points out that the invention of
23 Ellison can be implemented solely in software and in that case the elements
24 of Ellison’s invention are code segments and they’re used to perform

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 necessary tasks. The program or code segments are stored in a processor
2 read only medium such as the floppy diskettes that I pointed to earlier . We
3 can thus see that the key generator 240 and the usage protector 250 are
4 elements of the Ellison invention obviously and they are accessible to the
5 operating system when stored in this processor readable medium.

6 So ask yourself in this situation at least, how is isolated execution
7 even possible if this software implement embodiment is utilized? At least in
8 that embodiment there can't be isolated execution. Ellison does not teach a
9 secure processing environment because in each instance of a secure
10 processing environment according to Ward, the secured item has to be
11 inaccessible to the operating system or user. That is not the case with
12 Ellison.

13 I'd like to turn now to the discussion of the private key. So if you
14 could please, I would direct your attention to page 11 of Patent Owner's
15 exhibits which demonstrates claim 1 of the '480 patent. There are three big
16 sort of topics or chunks of the '480 patent that I'd like to address. There's
17 the private key, the authentication software and the decryption key.

18 With regard to the private key, claim 1 recites that providing a private
19 key in a memory said electronic device, said memory being a secured part of
20 a BIOS or another location in said electronic device which private key is
21 inaccessible to a user of said electronic device wherein the private key is
22 encrypted when the key is stored in said memory and a decryption key for
23 decrypting the private key is incorporated in the electronic device. Said
24 decryption key is inaccessible to the user in (indiscernible).

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 Again, with regard to the private key the claim recites user operated
2 software wherein said memory is inaccessible to said operating system of
3 said electronic device, thereby rendering the private key inaccessible to the
4 user wherein -- unless it's decrypted, excuse me, unless it's encrypted.
5 Wherein the private key is decrypted in a secure processing environment
6 inaccessible to said user and to any user operated software.

7 The authentication software, specifically I point you to the language
8 providing authentication software in said electronic device, the private key
9 being accessible to the authentication software wherein authentication
10 software is stored in the secure memory which is inaccessible to the
11 operating system.

12 With regard to the decryption key, the claim recites in part providing a
13 private key in a memory of said electronic device, said memory being a
14 secure part of a BIOS or another secure location in said electronic device
15 which private key is inaccessible to the user of the electronic device,
16 wherein the private key is encrypted and the private key is stored in said
17 memory, a decryption key for decrypting the private key being incorporated
18 in the electronic device. Said encryption key be, again, now I'm repeating
19 myself, but the decryption key is inaccessible to said user.

20 Ellison and Muir do not teach the claimed private key. Specifically,
21 providing a private key in a memory of said electronic device, said memory
22 being part of the BIOS or the other secure location which private key is
23 inaccessible to a user of said electronic device.

24 If you would look please at, for example, figure 1C of Ellison which

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 is illustrated on slide 12 of Patent Owner's demonstrative exhibits on page
2 12, the MCH 130, that is the memory controller nub does not -- there's no
3 description of it providing a private key in the secure part of the claimed
4 BIOS. The same goes for the ICH 150. The secure part of the BIOS is a
5 part of RAM that is inaccessible by the user of the operating system. It does
6 not report to or otherwise communicate with MCH 130 or 150 so they are
7 necessarily accessible to the user. That's our position.

8 Ellison and Muir do not teach the claimed authentication software. I
9 ask you to consider the following question. Where in Ellison does Ellison
10 recite that element 250 authenticates anything? I know that authentication
11 software does in the '480 patent. It's involved in authenticating a
12 transaction, but I don't see what's getting authenticated by 250. In any case,
13 if indeed Ellison were somehow authenticating transactions is asserted with
14 outside parties, it would be using applications 42 in figure 1A, see figure 1A,
15 and those applications would be authenticated. Those re the only
16 applications. If you're transacting business 42 of Ellison, you're going to be
17 using those applications.

18 Likewise, if Muir's teachings were somehow incorporated into
19 Ellison, its sign-in software would probably be or would be within one of the
20 drivers, it teaches drivers, it would be one of the drivers 13 and 14 and the
21 same ring (phonetic) environment as primary OS 12 and would be using one
22 of the applications 42 in normal execution mode of Ellison. The
23 authentication software 250 which is the usage protection component, is not
24 stored in the secure area which is inaccessible to the operating system

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 because it's in on 70 (phonetic) and Ellison and Muir do not teach the
2 claimed encryption key.

3 If you could turn your attention to Ellison, figure 2 which is on page 8
4 of Patent Owner's demonstrative exhibits, you will see that in OS nub 16
5 there are three clouds that are drawn around public key. There's a nub 201
6 and a private key 204. They're stored in nub 16. Likewise, in processor nub
7 18 we see a cloud around the BKO 202 which Ellison also discloses as being
8 stored in nub 18.

9 On the other hand, key generator 240 and usage protector 250 do not
10 contain any such clouds. Key generator 240 in Ellison does not store a
11 decrypt key 203 but instead regenerates an OSNK 203 from BKO 202 and
12 from OS nub ID 201 and provides that OSNK 203 and to usage protector
13 250. I think it's fair to say that in the absence of clouds and the usage
14 protector 250, for example it's plain that the usage protector does not contain
15 storage of any current. The decrypt key 203 is thus not incorporated in the
16 electronic device as is claimed by the '480 patent.

17 Muir does not cure this deficiency of Ellison. Muir discloses a
18 regeneration of the decrypt key. For example, on the third paragraph of page
19 16 --

20 JUDGE BRADEN: Counselor, what do you say about Petitioner's
21 argument that the entirety of 200 is the secure platform that includes OS nub
22 16 and usage protector 250 and therefore, I think they said, that because only
23 the OS nub 16 can retrieve the private key and OS nub 16 is within the
24 secure platform of 200, it would have been obvious that the cryptographic

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 key storage 155 and non-volatile flash memory 160 are the secure storage
2 locations? I mean, they're all within the secured platform 200, so why
3 wouldn't that be correct?

4 MR. HENRY: They're outskirting (phonetic) 170. Moreover, to do
5 anything --

6 JUDGE BRADEN: I'm looking at figure 2 of Ellison which is
7 Exhibit 1006 and it's got 200 and it's got the usage protector 250 and it's got
8 OS nub 16. How do I read that?

9 MR. HENRY: Well, that figure does show that but, like I pointed out,
10 first of all it doesn't tell us -- Ellison doesn't tell us where the usage
11 protector resides specifically. But it does tell us that --

12 JUDGE BRADEN: So this figure 2 isn't telling us that it resides on
13 secure platform 200?

14 MR. HENRY: I wouldn't say that it's not stored in 200, 200 is a
15 description of it running but it's stored in 170.

16 JUDGE BRADEN: Okay. I think I understand your position. Okay.
17 Thank you.

18 MR. HENRY: You're welcome.

19 JUDGE DANG: Mr. Henry, this is Judge Dang. What you just
20 pointed to, I believe Petitioner pointed to the position of your expert where
21 he indicated that they are buffered in the area, in the platform 200, and why
22 isn't that a storage?

23 MR. HENRY: It's placed there when being used. But that's still
24 different from when it's stored.

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 JUDGE DANG: Okay. Thank you.

2 MR. HENRY: You're welcome, Your Honor. I was talking about the
3 decrypt key. It is our position that there's no indication in either Ellison or
4 Muir to securely store or incorporate the decrypt key to make the decrypt
5 key inaccessible to the user in the operating system.

6 I would like to make the following point and return you to what was
7 said by Ellison. Redesigning operating systems, creating software for
8 compatibility issues causes tremendous investment in development efforts.
9 Can one really say with any certainty that a person of skill in the year 2004
10 would, when presented with Ellison and Muir, have arrived at Patent
11 Owner's claimed invention? If the answer is maybe or possibly, not sure,
12 don't know for sure, then you must find that the claims of Ward's patents are
13 valid over Ellison and Muir. I'll reserve the time for (indiscernible).

14 JUDGE DANG: Okay. Great. Thank you. You have 25 minutes.
15 Petitioner, you can begin any time you're ready and I want to make sure, so I
16 think, yes, you have 40 minutes; right?

17 MR. MONALDO: Your Honor, would you like to take a few minute
18 break just to let the parties go to the bathroom and just --

19 JUDGE DANG: Okay. Yes. Yes, so why don't we take a few
20 minutes break?

21 MR. MONALDO: Okay. Great. Thank you.

22 (Break.)

23 JUDGE DANG: Petitioner, you can begin any time you're ready.
24 You have 40 minutes.

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 MR. MONALDO: Thank you, Your Honor. I'll try to be brief. I'll
2 start first with claims 2, 4, 5, 16, 18 and 19. During Patent Owner's
3 presentation he rightly confirmed that the burden was on Petitioner to
4 demonstrate unpatentability of these claims but you'll note that he left it at
5 burden because he had to. The Patent Owner response didn't make any
6 argument for support for these claims and our point is simply that Patent
7 Owner waived arguments for support of these claims.

8 Now a scheduling order at page 10 warned Patent Owner that
9 arguments not raised in the Patent Owner response may be deemed waived.
10 Patent Owner chose not to heed this warning and instead chose to waive
11 arguments for support of these claims. That is our point. There's no contest
12 that claims 2, 4, 5, 16, 18 and 19 are supported.

13 The next topic I wanted to address was this notion of the private key
14 used to generate the digital signature and the encryption key used for
15 encryption. Judge Mayberry, you asked Patent Owner's counsel for support
16 for his statement that these two keys are one and the same. But notably
17 Patent Owner's counsel could not point to any support in the '480 patent
18 itself for this position. Instead, he turned to page 52 of the deposition
19 transcript of his own expert.

20 First, Patent Owner's briefing never cited this exhibit and the
21 arguments you heard are new arguments that are brought before oral
22 hearing. Also, if you look at the testimony at that portion of the deposition
23 transcript the expert clearly refers to different keys. The encryption key for
24 encryption and the private key for generating digital signature. If you keep

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 reading that testimony from page 52 through page 56 Patent Owner's expert
2 again confirms that his testimony is based on the incorrect obviousness
3 standard and he also admits that the '480 patent does not say, does not
4 describe that the software ID or private key is an encryption. For these
5 reasons, this testimony actually supports our position that the '480 patent
6 describes two different keys.

7 You'll also note that Patent Owner never addressed our argument
8 about claims 3 and 4. These claims clearly show you that they're two
9 different keys. They're present in the claim set. Claim 3 introduces an
10 encryption key and as mentioned earlier during prosecution this was
11 changed from private encryption key simply to encryption key. So when the
12 patent says private encryption key, the prosecution history tells you that it
13 means the encryption key, not the private key in claim 1.

14 Claim 4 also clearly differentiates the two keys where the encryption
15 key is claimed as being used to encrypt the private key itself from claim 1.
16 Two different keys clearly set forth in the claims never addressed by Patent
17 Owner.

18 The next point I'd like to make is this conflation of authentication
19 table and bit string for the claimed private key. There's nothing in the patent
20 that says these terms were used interchangeably or synonymously. In fact,
21 the prosecution history clearly tells you that, as we discussed, the term
22 authentication data was changed to the narrow term private key. These
23 terms are differentiated and shown to be distinct through the amendments
24 that were made during prosecution. Patent Owner's counsel tries to discount

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 that prosecution history as just the attorney's view of the claims during
2 prosecution and that view, you know, really doesn't matter. It should be
3 disregarded. You should still look at the claims and you should look at the
4 specification. You should think of the meaning for yourself. You shouldn't
5 consider what the prosecuting attorney thought when the prosecution
6 attorney was making these amendments. That is clearly not the law. The
7 prosecution history is part of the intrinsic record and it informs the
8 construction of these claims. In that prosecution history there's a clear
9 difference between authentication data and private key and description of
10 things (indiscernible) authentication data in the specification cannot support
11 the same things for the private key.

12 JUDGE DANG: Counsel, what about the section where we pointed
13 out about the private key where it did say that it could be a character string
14 herein after referred to as a private key. That's in column I think 13.

15 MR. MONALDO: Yes. That's a good question, Your Honor. So
16 column 13 is talking about, as we said before, a further embodiment, a new
17 embodiment that introduces this private key. So that is something that's new
18 and it's not the rest of the specification that came before that. It says
19 hereinafter, after that point it could be referred to as a private key. So it's
20 not telling you that everything I described before could be a private key and
21 you could just substitute that word wherever you see software ID or bit
22 string or anything like that. That's not what that paragraph is telling you and
23 additionally, that paragraph elaborates on what the private key is and that
24 private key is something that's registered that a third party can use to

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 generate the digital signature. It's nothing different than the encryption key
2 and the bit strings and everything else that was discussed prior to that
3 paragraph. Does that answer your question, Your Honor?

4 JUDGE DANG: Yes. My question, I guess is that then you would
5 say that the MBS is not the same thing as this bit string?

6 MR. MONALDO: As the private key?

7 JUDGE DANG: Yes.

8 MR. MONALDO: Yes. Our position certainly is the MBS and the bit
9 string is not something that can be described as a private key. That never is
10 described in the patent. It talks about a bit string and it talks about a private
11 key and those two things are different. They're used differently in the
12 specification. The private key is registered and this bit string MBS that's
13 described earlier is some different portion of data that is used differently and
14 frankly there's nothing in the specification that actually links the term
15 private key to bit string. Not even in column 13, if you go to column 13 it
16 doesn't say the bit string MBS is the private key and there's nothing --

17 JUDGE DANG: Thank you.

18 MR. MONALDO: You're welcome, Your Honor. All right. Great.
19 On that point I'll just note that Patent Owner's counsel referred to Europe
20 and Europe finding some of these things that are changeable. I'll simply
21 point out that the claims in Europe didn't involve a private key at all. So
22 anything from that record, there's nothing in that record that supports the
23 notion that private key is synonymous with these other types of data that
24 would be described in the '480 patent.

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 The next point I'd like to make is just the authentication software
2 again. Patent Owner's counsel continues to say the private key is integral in
3 authentication software but as we discussed earlier in our presentation,
4 Patent Owner's expert admitted that the private key might not be part of the
5 authentication software. You can see this in the testimony we discussed at
6 slide 15 of our demonstratives. Patent Owner's counsel never addressed this
7 testimony and he tried to explain away his expert's use of the wrong claim
8 construction standard but he never really addressed the improper use of the
9 obviousness standard and did not specifically address the testimony that his
10 own expert provided that said that the private key might not be a part of the
11 authentication software.

12 Now, as a final point on written description. Judge Dang, you asked
13 Patent Owner's counsel for support for the private key being stored in "any
14 other secure locations" at the end of the presentation on written description
15 from Patent Owner's side. Now Patent Owner's counsel could not provide a
16 clear answer. He mentioned the use of common sense. You have to use
17 common sense to fill in details that are missing from the specification and
18 that is the same problem with his own expert's use of the obviousness
19 standard. The standard is not obviousness. It's not common sense. It's
20 what does the specification reasonably convey to a person of skill that the
21 inventors possessed when they wrote the disclosure for the patent.

22 You'll also, and I thought it was interesting that in response to that
23 question, Patent Owner's counsel pointed to just three points in the
24 specification, column 9, lines 35 to 43, column 10, lines 25 to 33 and then

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 column 13, lines 30 to 36. The column 13 disclosure is the private key
2 paragraph that we discussed at length and does not specify where the private
3 key is stored. Column 9 and column 10, that disclosure is interestingly
4 directed to the third embodiment shown in figure 5. In that embodiment the
5 secure area is not used, instead encryption is used to create the data.

6 This third embodiment does not align with the remainder of the
7 claims. You can see this clearly at column 9, line 35. It says in the third
8 installation method illustrated in figure 4 the authentication data, the
9 authentication table, is stored in a memory that is accessible to an operating
10 system of the device and possibly to a user of said device. Inaccessible
11 memory, this claims requires the memory to be inaccessible to both the user
12 and the operating system. So these references to column 9 and column 10
13 are simply improper because that embodiment relates to something different
14 than what's in the claims.

15 Now this issue pervades many of Patent Owner's arguments as Patent
16 Owner bounces all over the specification hunting and trying to find support
17 for all of these features that are set forth in these claims and Patent Owner
18 regularly cites to the second embodiment which is shown in figure 3 which
19 has a secure area for certain features and then turns to the third embodiment
20 shown in figure 5 for other features. As we discussed in our briefing and as
21 found by the European Court, these embodiments are distinct and cannot be
22 mixed to provide written description support for the claims of the '480
23 patent.

24 Now unless there are any questions on written description support, I

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 think I'll turn it over to my colleague, Usman Khan, to discuss the prior art.

2 JUDGE DANG: Thank you.

3 MR. MONALDO: Thank you, Your Honors.

4 MR. KHAN: Thank you, Your Honors, and thank you, Jeremy. In
5 my last (indiscernible) Your Honors asked a question how Ellison protected
6 the isolated memory and I had briefly pointed to figure 1B as shown in our
7 slides 25. So I thought maybe it would just help if I could revisit that and
8 also provide a little more information to the extent it's beneficial to Your
9 Honors.

10 So in 1B can see these arrows are coming out of the OS 12, primary
11 OS 12 and that's in the normal execution mode and that normal execution
12 mode modules, none of them have any arrows that point towards the isolated
13 area 70. There's just no access that Ellison's system provides to the normal
14 execution modules to the isolated area, In contrast, when you look at the
15 right side you can see that the OS nub and the processor nub have access to
16 the isolated area but that's only components that are within the isolated
17 execution region that's on the right side of the figure.

18 Now, in addition to this figure, I also wanted to point Your Honors,
19 again, to the extent it may be beneficial, column 3, lines 32 to 49 of Ellison
20 which further explain that the isolated area is protected by both the processor
21 and the chips set in the computer system, that the isolated region is always
22 protected by an access channel and access to this region is permitted only
23 from certain buses in particular read and write cycles that are issued by the
24 processor executing in the isolated execution mode; right?

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 They also say that the isolated execution mode can only be initialized
2 using a privileged instruction in the processor combined with the processor
3 nub loader 52. So, again, Ellison's system goes to large lengths to maintain
4 the integrity of its isolated area and that's the way the system works because
5 if it didn't provide that protection, then there's no point of having the secure
6 region and the whole entire point of Ellison is to be able to provide a secure
7 region that's not accessible to the primary operating system because as
8 described in the background, that's where a lot of attacks used to come from.

9 Now, in discussing Ellison opposing counsel had constantly pointed to
10 the memory 170 and all these components were stored in memory 170 but I
11 think that bears a little bit of a misunderstanding there as to the role of what
12 memory 170 is.

13 If Your Honors may turn to actually slide 7, Patent Owner's
14 demonstratives. Slide 7 includes a depiction there of the various memory
15 units including the memory 170 but it also includes a description of that
16 memory on the right side and at the very first line you can see that it says the
17 mass storage device 170 stores archived information such as and then it lists
18 a bunch of items. In other words, the memory 170 is an archive memory.
19 It's used to store stuff that's already been used, not currently being used;
20 right? The Ellison system very clearly describes how it obtains secure data
21 and protects it in the isolated memory and, for example, even as I mentioned
22 earlier the processor nub that is stored in non-volatile memory, that's
23 embedded and when it's taken from the non-volatile memory it's stored in
24 the isolated memory and there, sorry, it's encrypted, and there when it's

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 taken to the isolated area it can be decrypted using a decryption key. So
2 there is very clear disclosure in Ellison how these components in the isolated
3 execution mode are protected constantly from the time it's installed onwards
4 and Patent Owner's reference to 170 is simply incorrect. It's inconsistent
5 with the teachings of Ellison and also we just don't point to that memory as
6 part of our mapping.

7 In discussing the memory I'd also note that the claims require, and
8 this goes to one of Your Honor's other questions regarding what the memory
9 is in the claim. I want to note that the independent claims recite memory in
10 a rather broad manner; right? The claims explicitly recite that the memory
11 can be stored in multiple places like a BIOS or any other secret location in
12 the electronic device. The claim doesn't require whether the memory is a
13 logical one or a physical one or anything like that. It just requires the
14 memory to be in a secure location and what we have pointed to is the
15 isolated area of the memory as shown in figure 1B and some of the other
16 figures. We think that satisfies the claim limitation.

17 With that, I'd also like to address one more comment that Patent
18 Owner made regarding the usage protector and why it should not be mapped
19 to the authentication software and there was a comment made by Patent
20 Owner's counsel that there's nothing authenticating about the usage
21 protector. Well, if I could direct your attention to slide 30 of Petitioner's
22 demonstratives. Slide 30 shows figure 3C and we discussed this figure in
23 my earlier remarks. Figure 3C shows the usage protector which we map to
24 the authentication software and here you can see that one of the primary

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 functions, as shown in figure 3C, is to generate a signature using the private
2 key. Well, a private key is used specifically for authentication purposes;
3 right? So the usage protection is performing an authentication operation
4 when it's generating a digital signature using a private key; right? So the
5 notion that the usage protector is nothing to do with authentication is simply
6 incorrect.

7 And I'd also like to note here that the private key, and my colleague
8 Jeremy Monaldo also kind of alluded to this, private key can be used for
9 different purposes; right? It's like a key to a door, keeping several different
10 keys to several different doors; right? Some private keys can be used for
11 embedding, sorry, encrypting or decrypting. Others can be used for
12 generating a digital signature. You know, we just don't see that connection
13 where they combine them. In Ellison it's very clear as required by the claim
14 and as shown here in figure 3C that the private key is used to generate a
15 digital signature, and that we feel like Ellison -- the authentication software,
16 the usage protector, very clearly satisfies the claim limitation of an
17 authentication software generating a digital signature using a private key.

18 With that, I have no further comments. Did Your Honors have any
19 questions?

20 JUDGE DANG: Yes. This is Judge Dang. I think Patent Owner also
21 questioned your OS, Ellison's OS 12 as not being the OS claimed. Do you
22 have any further comments on that?

23 MR. KHAN: Yes. I think in my other comments I had mentioned
24 that Ellison very clearly distinguishes between the OS nub 16 and primary

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 OS. That's in these multiple figures in its description indicating, for
2 example, that the OS nub can access -- it's in the isolated execution area, it
3 can access the isolated memory. Primary OS cannot. Also Patent Owner's
4 counsel did not address the fact that the OS system can have multiple OS's,
5 right, and Ellison's system has an OS that operates in the isolated execution
6 mode OS nub, and then finally, Your Honors, that operates in the normal
7 execution mode. There's no reason that these two must be mapped to the
8 claimed operating system. The Patent Owner just doesn't provide any
9 reason why that's the case.

10 JUDGE DANG: Okay. Thank you.

11 MR. KHAN: Okay. Thank you, Your Honors.

12 JUDGE DANG: And Mr. Henry, are you ready? You have 25
13 minutes. Any time you're ready.

14 MR. HENRY: Your Honor, I'm sorry. Just thinking about my
15 answer. I may have nothing further to articulate except I do have one
16 comment in coming, that is that was in column 3, lines 33 through 39 recites
17 one concept of the isolated execution architecture is the creation of an
18 isolated region in the system memory, referred to as an isolated area which
19 is protected by both the processor and the chip segment (phonetic) in the
20 computer system.

21 The isolated region 35 may also be in cache memory protected by a
22 translation of designed (phonetic) access check can thus see that the system
23 memory and the mentioned cache memory are volatile memories and they're
24 not for permanent storage such as the 170 mass storage communicated in

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

1 Ellison.

2 My only other further comment is that I mentioned using common
3 sense. Reasonableness always requires using common sense. That's all for
4 Patent Owner.

5 JUDGE DANG: Great. Thank you so much. So the panel would like
6 to thank both parties for the presentations today. We will issue a final
7 written decision in due course and with that, we are adjourned. As a
8 reminder, parties please stay on the line and answer any questions that the
9 court reporter may have. Thank you so much.

10 (Whereupon, at 12:30 p.m., the oral hearing was
11 concluded.)

IPR2022-00113 (Patent 10,992,480)
PGR2022-00007 (Patent 10,992,480)
IPR2022-01076 (Patent 10,992,480)
IPR2022-00114 (Patent 11,063,766)
IPR2022-01077 (Patent 11,063,766)

PETITIONER:

Walter Renner
Jeremy Monaldo
Usman Khan
FISH & RICHARDSON P.C.
axf-ptab@fr.com
jjm@fr.com
khan@fr.com

PATENT OWNER:

Jacob B. Henry
William Ramey
RAMEY LLP
jhenry@rameyfirm.com
wramey@rameyfirm.com