UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,

Petitioner,

v.

WARD PARTICIPATIONS B.V.,

Patent Owner.

Case IPR2022-00113 (US Patent No. 10,992,480)

Case PGR2022-00007 (US Patent No. 10,992,480)

Case IPR2022-00114 (US Patent No. 11,063,766)

VIDEOCONFERENCE DEPOSITION OF

DR. BART PRENEEL

November 1, 2022

Page 1 - 103 8:06 a.m. EST - 11:48 a.m. EST

REPORTED BY:
Tamara L. Houston
CA CSR No. 7244, RPR, CCRR No. 140
Job Number 22-117173
Ref. 39843-0109IP1; 39843-0109PS1; 39843-0110IP1

REMOTE VIDEOCONFERENCE DEPOSITION OF DR. BART PRENEEL taken on behalf of the Petitioner, commencing from 8:06 a.m. EST to 11:48 a.m. EST, Tuesday, November 1, 2022, before Tamara L. Houston, CSR No. 7244, CCRR, RPR.

APPEARANCE OF COUNSEL:

On behalf of the Petitioner:

FISH & RICHARDSON P.C.
BY: USMAN A. KHAN, PH.D., ESQ.
1000 Maine Avenue SW
Suite 1000
Washington, DC 20024
(202) 626-6383
khan@fr.com

On behalf of the Patent Owner and Witness:

RAMEY LLP
BY: JACOB B. HENRY, ESQ.
5020 Montrose Boulevard
Suite 800
Houston, Texas 77006
(832) 454-1456
jhenry@rameyfirm.com

ALSO PRESENT: Scott Ward, Proprietor

INDEX TO EXAMINATION

WITNESS: DR. BART PRENEEL

QUESTIONS INSTRUCTED NOT TO ANSWER

Page	Line

None

INDEX TO EXHIBITS

DR. BART PRENEEL

SAMSUNG ELECTRONICS CO., LTD. vs. WARD PARTICIPATIONS B.V.

November 1, 2022

Tamara L. Houston, CSR No. 7244, CRR No. 140, RPR

EXHIBIT	DESCRIPTION	PAGE

None.

--o0o--

Tuesday, November 1, 2022, 8:06 a.m. EST

--o0o--

All counsel present stipulate that the witness shall be sworn remotely by the court reporter

*** * ***

Whereupon, DR. BART PRENEEL, having been called as a witness was duly sworn to tell the truth, the whole truth, and nothing but the truth testified as follows:

EXAMINATION BY MR. KHAN:

Q. Good morning. Thank you very much, Dr. Preneel.

MR. KHAN: Jacob, thanks.

BY MR. KHAN:

Q. I wanted, I guess, to first start off with asking you if I'm pronouncing your name correctly.

Is it Dr. Preneel?

A. That's correct. Yes.

Q. Great. I'm joined here by my colleague, Jeremy Monaldo, also with Fish & Richardson.

MR. KHAN: Jacob, is there anybody else at your end who is participating or listening to the proceedings, just for the record?

MR. HENRY: Mr. Scott Ward is present.

MR. KHAN: Okay. Fantastic.

So from Petitioner's side, there is Usman Khan and Jeremy Monaldo with Fish & Richardson. And from patent owner's side, we have their expert, Dr. Preneel; the attorney, Mr. Jacob Henry; and patent owner, Scott Ward.

Is that correct?

MR. HENRY: That's correct.

MR. KHAN: Okay. Thank you.

BY MR. KHAN:

Q. So, Dr. Preneel, I'll start off with some general questions, getting to specifics, but I'll be providing periodic breaks as we go. So, you know, you don't have to go through it -- through without any breaks. You know, you may request a break at any time.

MR. KHAN: And, Tamara, yourself as well, if you need a break, please let me know.

BY MR. KHAN:

Q. I just request that you let me know about five minutes ahead of time or so, a few minutes ahead of time, so that I can wrap up my line of questioning or I at least know when to stop.

Does that work for you?

A. That's fine.

Q. Great.

And during the breaks, do you understand that you are not allowed to discuss the substance of your testimony today until your cross-examination is concluded?

A. I understand that.

Q. Will you agree to let me know if at any point anyone communicates with you in any manner during the course of your cross-examination regarding your testimony?

A. I agree.

Q. Thank you.

Do you understand that your testimony today is sworn testimony taken under oath?

A. I understand that, yes.

Q. And do you understand that the oath you've taken for the deposition today is as solemn as an oath you would take if testifying at trial?

A. I understand that, yes.

Q. Do you understand that the deposition testimony today can be used at trial or in subsequent briefs in these proceedings?

A. I understand that, yes.

Q. And do you understand that you're being deposed today for statements made in your declaration

submitted in support of the '766 patent owner response?

A. Yes, I understand that.

Q. Do you have a copy of the exhibits that were cited in your declaration and a copy of the patent owner response?

A. I do have all these documents in digital format. I don't have them all printed out.

Q. Okay.

A. But I do have a digital format. I can find it, like, if you give me the correct document. But I do have in front of me the patents and my declaration and also the declaration of Dr. Black.

Q. Okay. Fantastic.

So if I -- I'll refer to the documents either by their exhibit numbers or their names. So if you're not clear, please let me know.

A. That's fine.

Q. Great. Thank you.

Before we get started, is there any edit or change that you'd like to make in your declaration?

A. Not at this stage, no.

Q. Okay. Fantastic.

So let's turn to your declaration. That's Exhibit 2009 in the proceedings. And please let me know when you have that in front of you.

A. I have it in front of me. That's fine.
Q. Great. Thank you.
The cover page of your declaration states that this declaration is for US Patent 11,603,766; is that correct?
A. That's correct.
Q. Is it correct that that patent number is a -- includes a typographical error? The patent number that you're referring to is Patent 11,063,766, which is also Exhibit 1001?
A. Yes, that's correct. I see this now. Yes. That's a typo. I confirm that.
Q. Thank you.
And in the header of the cover page and the rest of the pages, you also list the patent number with the same typographical error; is that correct?
A. That's correct, yes.
Q. Okay. And did you review your declaration and the documents in preparation for this deposition today?
A. Yes, I did.
Q. Did counsel tell you how to answer questions in your preparation?
A. Counsel told me to tell the truth.
Q. Have you been deposed before?
A. Not in a patent procedure. I've been a

witness in an international arbitration.

Q. And how many times have you served as a witness?

A. In arbitration, only once.

Q. And in the arbitration, did you have to be deposed?

A. Yes.

Q. Was it one time or multiple times?

A. It was one time. It was a very long session.

Q. Okay. So is it correct that you've been deposed once before in an international arbitration matter but never for a patent-related matter? Is that correct?

A. That's correct. That's correct.

Q. Have you been involved in any other patent matters?

A. I'm the inventor of five patents.

Q. Okay. And have you --

A. And I've also -- I've also consulted several companies on patent questions.

Q. Have you been involved in any other IPR proceedings?

A. Well, for example, I don't -- I'm not sure I fully understand what you mean. But, for example, of course, my research --

(Court reporter requested clarification.)

THE WITNESS: In my research, I've been producing a lot of IPR because we've enjoined projects with the companies and other institutions, and so I've been running very large projects with up to 30 partners, and those projects always had IPR clauses and, of course, also during the running of the projects, so my IPRs have come up.

BY MR. KHAN:

Q. I see. So let me clarify my question, please.

Have you been involved in other post-grant patent matters?

A. I have not been in procedures before except this procedure we're now in, but I've been -- as I mentioned, I have been advising companies of the original patents -- the applicability of patents and how to -- where the patents would apply to their specific case or how they could avoid patents in implementation.

Q. Okay. And just for clarification, in subsequent questions if I ask you "IPR," that would mean inter partes review, not intellectual property rights. My apologies if there's any confusion.

A. My apology.

Q. So in paragraph 18 of your declaration -- could you turn to where it's paragraph 18, please?

A. Yes.
Q. So could you just read your paragraph 18 for me, please?
A. "I have served as expert witness in several IP-related court cases, both in Belgium and abroad."
Q. Yeah. So could you maybe clarify that statement, so what you meant by "several IP-related court cases"?
A. Well, I first -- the court case in the arbitration, this was definitely IP-related, but I've also been involved in a few Belgium court cases related to copyright issues. Also, like, intellectual property played a role.
Q. So is it correct to say that the IP-related court cases, other than the arbitration one, were not patent-related? Is that correct?
A. That's correct, yes.
Q. In your declaration, you -- in paragraph 10 of your declaration -- and let me know when you get there, please.
A. Yes.
Q. In paragraph 10, you start out the paragraph by saying you are a "technical expert in the subject matter areas relevant to this matter, including the design and evaluation of cryptographic algorithms and

protocols, including cryptanalysis, security reductions and proofs, cryptographic hardware and software, secure execution environments, and secure electronic transactions."

Did I read that correct?

A. That's correct.

Q. Is it your opinion that the '766 patent is related to each one of these topics that you've mentioned here? For example, the "cryptographic algorithms, protocols including cryptanalysis, security reductions and proofs, cryptographic hardware and software, secure execution environments, and secure electronics transactions"?

A. Well, the Patent '766 does not discuss in detail cryptographic algorithms and protocols, and it doesn't discuss security reductions and proofs. But, of course, these are like basic signs you need to master to understand fully this patent and to understand the field. But the focus of this patent is indeed cryptographic hardware and software, secure execution environments and secure electronic transactions.

(Court reporter requested clarification.)

THE WITNESS: Secure execution environments and secure electronic transactions.

BY MR. KHAN:

Q. So can you -- so in -- in this sentence, you mentioned that the subject matter areas are relevant, but could you explain to me how cryptanalysis is relevant to the '766 patent?

A. Because if you want -- it's important to understand cryptanalysis because if you want to understand whether the cryptographic algorithms and protocols are secure, and they are used in this scheme. For example, if you look at the related patent LSM, it actually uses hash functions, for example.

(Court reporter requested clarification.)

THE WITNESS: Cryptographic hash functions.

So cryptographic schemes are being used to implement those secure transactions schemes. And, of course, the goal of the patent is not to cryptanalyze or break cryptographic algorithms, but it's important to understand the strengths and weaknesses and limitations to be able to fully understand how a patent -- the patent works.

So I do believe that most of cryptography is plain portion to understand the patent and that cryptography consists both of design and analysis, and those are two sides of one coin. And without cryptography, it would not be possible to build some of

those systems.

BY MR. KHAN:

Q. Is there a difference between cryptographic algorithms and protocols and cryptanalysis?

A. Yes, there is a difference, but they are two sides of one coin. The cryptographic algorithm is a mathematical operation in which we take a bit string and you transform this to another bit string possibly under control of a key. Cryptographic protocol is an interaction between two or more parties in which you try to achieve specific security goals within a secure transaction, and again, cryptographic protocols typically use cryptographic algorithms as -- through the parties, and cryptanalysis is the science that studies the security of algorithms and protocols. But you can't have one without the other. They're two sides of a coin.

Q. How are --

A. In order to be able to design and appreciate the security of the system, you need to also understand how they are being broken.

Q. How is -- or how are security reductions and proofs relevant to the '766 patent?

A. Well, of course, this is the academic discipline in which you study these algorithms and

protocols. These are tools and techniques which are also mastered for this specific patent. Those techniques have not been used because in the patent, again, as I said before, you use building blocks to build a larger system. But if you want to establish security carefully, it's important that you can perform such reductions and proofs, that you master those techniques.

Q. And so are you saying that security reductions and proofs is essentially an academic area that is tangentially related to the subject matter here? Could you clarify that, please?

A. I think these are toolboxes developed by academia which I use to study these protocols and algorithms, and I believe they give us new insights in how to study them.

Q. Can you --

A. The academic relevance, I think today, if you look at cryptographic standards today, it is -- both for algorithms and protocols, it will be required that there are security reductions and proofs in those.

Q. Can you give me an example of how the '766 patent uses security reductions and proofs?

A. The '766 patent does not secure -- use security reductions and proofs, but to be able to fully

understand and evaluate the security today, I believe it's essential that you also understand how security reductions and proofs work and how you can prove how the different components result in a secure system.

Again, it's two sides of the coin, and I fully agree with you that to design a system, you don't necessarily need to use the reductions and proofs. But to study and understand the system, you would need those.

But, of course, in the specific question we're discussing here with this patent -- whether something is patent or not or whether patent applies to something, you don't need security and proofs. It's to understand the security of the schemes.

Q. I'm sorry. Can you repeat the last sentence you just said?

A. To decide on the question whether Patent A or B are overlapping or not overlapping or innovative or apply to a certain system, you don't need security reductions and proofs. But to fully understand content, you do need to understand security reductions and proofs. And for this, I believe it -- my skills in this area as expert are relevant to this general area in which the patent is situated.

Q. So is it your position that the '766 patent

claims have nothing to do with security reductions and proofs; it's just for general understanding of the subject matter?

A. It's for general understanding of the subject matter, but also to specifically if you want to study in detail how the components fit together, you would be able to use security reductions and proofs.

Q. I'll repeat my question.

Is it your position that the '766 claims have nothing to do with security reductions and proofs and it is just for understanding of the subject matter?

A. I'm not sure I fully understand your question, what is defined by "subject matter." I mean, the matter of the patent, you don't -- to understand how the system operates in the patent, you don't need to know security and proofs, but to understand the science of how these things are being developed and how they --

(Court reporter requested clarification.)

THE WITNESS: -- how they work together or fit together, you can make use of security reductions and proofs.

BY MR. KHAN:

Q. So in paragraph 10, you use the word "subject matter," which is what I was questioning you about.

So is it not clear to you whether the word --

the phrase where I'm using "subject matter" as used in your declaration, what that entails?

A. To me, entails the subject --

MR. HENRY: Objection. Objection. Substance of the -- or the format of the question. I don't see the word "subject matter" in paragraph 10.

MR. KHAN: I'll read the question of the patent --

MR. HENRY: Oh, I'm sorry. I do see it. Can you ask the question again, please?

MR. KHAN: Yeah. So Dr. Preneel, in his last statement, had mentioned that it wasn't clear to him what I meant when I was asking about subject matter relevance, and I was indicating that I'm quoting his paragraph 10 language that said, "I am a technical expert in the subject matter areas relevant."

BY MR. KHAN:

Q. And so my question was, that term as used in your declaration, is it not clear to you what that term includes, hence the confusion in my question; or is -- I guess I'm trying to understand why there's confusion when that term is used in your declaration.

A. I'm not sure I fully understand what you're asking. I mean, how I define "subject matter areas relevant to this matter"? Is that -- you want me to

define this, or you want to define the scope of this?

Q. I'd like to understand what you're trying to say here. I am trying to understand whether your statement is saying -- when you're saying "subject matter areas relevant to this matter," all right, what are you trying to say to these -- the list that we've been discussing, is this related -- is this related to the specification for context? Is it related to the claims?

I am asking you for clarity, and hence my last questions were related to, is this required in the claims or relevant to the claims or -- or subject matter understanding. So that's why I was, you know, trying to get a better sense of what your -- what you mean by this particular sentence.

A. When I say "subject matter areas relevant to this matter," okay, I mean this is all of the technical and scientific tools you need to fully understand all of the aspects of the technology studied in this patent, which means not only the description and the scope of the techniques, but also to fully understand the security and weaknesses and shortcomings.

Now, if you specifically limit this to whether a certain claim is valid or not or whether -- you need to understand what the scope is of the claim in the

patent, I do think this is limited. I would say the definition would be more limited and restricted to secure execution environments and secure electronic transactions in the first place --

(Court reporter requested clarification.)

THE WITNESS: -- execution environments and secure electronic transactions in the first place, but of course, also cryptographic hardware and software because they are used in the claims, and then cryptographic algorithms and protocols.

The cryptanalysis security reductions and proofs, they are only there to understand security of the schemes and to understand how valuable they would be in a specific context. I hope that helps to clarify.

BY MR. KHAN:

Q. Thank you.

Going back to paragraph 8 of your declaration, just two paragraphs up, would you let me know when you --

A. Yes, I have it in front of me.

Q. Thank you.

You mention in paragraph 8 that, in forming your opinions, you reviewed the '766 patent, the '480 patent, the respective file histories, the exhibits that were submitted by the Petitioner; is that correct?

A. That's correct.

Q. You also mention that you have relied upon your education, experience, and knowledge of engineering practices and principals in the cryptographic algorithm industry; is that correct?

A. That's correct.

Q. In the last sentence on -- in paragraph 8, you mention that, "I have also relied on publication relevant to the technology in this matter"; is that correct?

A. That's correct.

Q. What's the publication that you're referring to in that sentence?

A. Well, I guess it should read "publications" because there was, of course, a large cryptographic literature on this topic, liter- -- on the topic of how to implement secure execution environments.

Q. Which publications are those?

A. I should have to go look up the list. I mean, I don't have the list in front of me. But, of course, I've been working in this area very early on because I was, for example, involved in secure smart cards. There was quite some literature on secure smart cards, and I can provide you details on this.

I've also -- this is, of course, in the period

after patent was filed, so more recently, I've been working myself. So I was -- around 2000, I was involved in TPM, initially called TPCA, Trusted Platform Computing Alliance, which was later renamed to TPM, Trusted Platform Module, and I was an international advisor to this organization. And together with my PhD student, I wrote publications about the security of TPMs. These are trusted modules which are added to a PC to -- and house their security.

And so more recently, I've also worked on developing secure execution environments and the key management in those environments. One example is the literature on Sancus and Sancus 2.0, which is an environment --

(Court reporter requested clarification.)

THE WITNESS: Sancus, S-A-N-C-U-S. Sancus is a Latin word. It's a secure execution environment which we designed about ten years ago.

So what I want to put out with the statement is that I've been active as a researcher in this topic since the late '80s, and that's how I've been keeping up-to-date with the scientific literature on this, but also with industry developments such as what happened in the framework of TCPA and TPM.

BY MR. KHAN:

Q. So in relying -- in forming your opinions and relying on these other publications, are there any of these publications that you used to form your opinions but did not cite in your declaration?

A. I don't think it's the case. I think I refer here to publications are referred is that these publications and this work we did provide me general understanding of the field on what is possible and what is not possible. But I don't think that this general knowledge was literature to specifically cite to this in this deposition -- or in this declaration.

(Court reporter requested clarification.)

THE WITNESS: I would say "literature," I said.

THE REPORTER: "General literature," would that be --

THE WITNESS: Yes.

THE REPORTER: Okay. Thank you.

BY MR. KHAN:

Q. So there's no position here in your declaration that was -- that relied on evidence that you did not cite to; is that --

A. In the publication -- can you please clarify the question? Because I'm not sure I fully understand

it.

Q. My question was that there is -- is it correct to say that there's no missing reference or citation in your declaration that you perhaps may have used to support to -- to develop your opinions here, but did not bring to the record?

A. No, I don't think that it was necessary to add citation literature also because most of the citations are much more recent, but they do develop my general understanding of what is happening because sometimes we can learn things also in hindsight.

Q. Now, you've mentioned that you have a lot of experience in this area. Does that include teaching classes in this subject matter you mentioned in your declaration?

A. Since the late '90s, I've been teaching classes on applied cryptography and network security, but I've also been providing specific industry trainings on secure implementations and on hardware security, which typically involves things like secure execution environments.

Q. In the past five years, how many such classes have you taught?

A. So applied cryptography and network security, so the general cryptography course I've been teaching

every year plus in two classes, and then I think, like, just for industry I would say on this topic two to three.

Q. And how big are these classes?

A. My applied cryptography and network security course has 80 students, and I also have a condensed version of this course with about 5 to 10 students. On my teaching to specific industry is typically group of size 8 to 10.

Q. And the curriculum or the material that's covered in these classes, does that include hardware and software or is it just for one of the two?

A. So the dedicated courses do include both hardware and software.

Q. You mentioned earlier, I think, and also in the context of paragraph 10 again also, you mentioned secure execution environments.

Why is that -- why is that so relevant or important in the '766 patent?

A. Because the '766 patents actually in it claims it has a memory device in the electronic device storing of the private key in a secure area of the electronic device, and it also has authentication software in a secure area inaccessible to the operating system. So it's clear that the scope of the patent and of this

claim is to have a secure execution of an electronic transaction inside a secure environment in a protected memory.

Q. How does secure environment -- what is required for a secure environment to be in place in these computer systems as described in the '766 patent?

A. Well, we can start with Claim 1. You have -- of course, in this case you have an electronic device. It has an operating system. And on top of that, there is user applications, and then secondly, there is a secure operating environment independent of the operating system. So it's very important that the operating system and there's also the user applications cannot access this secure environment because the user environment is easily compromised and, in general for these transactions, the users are not trusted.

So you want to get a separation with the secure electronic environment on the one hand where you do the --

(Court reporter requested clarification.)

THE WITNESS: -- to do the computation, so to execute the authentication software, and on the other hand, the operating system and the user applications.

And, of course, to create a secure environment, you then need a secure memory or memory

location which is, again, not accessible to the operating system. And the secure area needs a private key for computing the secure transaction and also needs software, again, to compute a secure transaction.

And then the matter to authenticate this software, these are the elements described in the '766 patents.

BY MR. KHAN:

Q. So my question was a little bit different. I'm going to repeat it.

My question was, what is required for a secure execution environment? I understand you're telling me what Claim 1 is saying, but I'm asking you, you know, more generally, what's required for a secure execution environment?

A. In general, what you want is -- I think that there is a separation between, on the one hand, the user side and, on the other hand, typically also the operating system and, on the other hand, the environment itself. So it is not possible for user software or for compromised user software or for operating system software or compromised operating system software to access the secure environment.

Q. So how do the systems operating in these secure execution environments create that -- that

ability to sort of make the operating system -- that division there you're talking about, the inaccessibility, how does the secure execution environment do that?

A. Well, typically you have a layer below the operating system that separates the operating system from some other piece of software, for example, the console, or you try to fully implement this in hardware. And so what you try to do is try separate the memory and the code from a secure environment from that from the regular environment.

Q. So is the console typically between the operating system and some other layer? Is that what you're saying?

A. The console would sit at the same level as the operating system, and there is a layer below that actually separates those two. And you can see the console as a simplified operating system that's only there to run the secure environment, just as the operating system is there to run the user applications.

Q. I see.

So -- so the console is like an operating system except it's not used to run the user applications that are receiving user input; is that correct?

A. It's typically much more restricted in

functionality, which makes it also easier to make it secure.

Q. I see.

So is it possible to have multiple operating systems in a computer?

A. Yes, it is.

Q. And one of those could act like the console?

A. Yes. It would be called -- the operating system would be called a console then.

Q. I see.

Turning to paragraph 20 of your declaration. Can you let me know when you get there?

A. Yes, I have that.

Q. So I'll read it for the record. Paragraph 20 states, "I understand that the board may not institute post-grant review unless the petition 'information presented in the petition filed under Section 321, if such information is not rebutted, would demonstrate that it is more likely than not that at least one of the claims challenged in the petition is unpatentable.'" End quotes there.

Is that a correct reading of paragraph 20?

A. That's correct.

Q. The first sentence. Yeah. Okay.

Did you apply this standard in --

A. Yes, I did.
Q. Okay. What does the -- in paragraph 22, two paragraphs down, you mention that the, "Patent claims in an IPR are given their broadest reasonable interpretation ('BRI')"; is that correct?
A. That's correct. Yes.
Q. Did you apply the BRI standard to review the '766 patent?
A. Yes, I did.
Q. In paragraph 20, you mention post-grant review, and in paragraph 22 you mention IPR.
Can you tell me what the difference between a PGR and IPR is?
A. So I see two times in 20 and 21 post-grant review. Maybe I misunderstood your question, but...
Q. So I'll repeat my question. In paragraph 20, you mention "post-grant review." In paragraph 22, you say "patent claims in an IPR."
My question is, what's the difference between a PGR and an IPR?
A. It must be a typo because the version I have in front of me says "PGR."
Q. I'm sorry. What does it say?
A. This must be a problem that occurred because, in fact, the version I have in front of me says "patent

claims in a PGR," the correct statement. So there may have been some editing error in both.

Q. Okay.

A. So the correct version is PGR as far as I understand.

Q. So I will maybe -- I'd like to make sure we have the same copy. So what I can do is I can drop the file for the exhibit into the chat and then --

A. I have the file in front of me. I mean, I have the two files in front of me, the one --

Q. My concern is --

A. Yes, I know it says IPR, but it should be PGR.

Q. My concern is that the version that you're looking at is not the same one that's filed.

A. Okay.

Q. And I'd like to make sure that as we move forward we're looking at the same document so that they're not -- there is no confusion.

So I am going to send you the filed version, or if your counsel would like to send you the filed version, that is also okay. I would prefer to send it to you, but if -- unless your counsel has any objection to that --

MR. HENRY: No, I'd prefer that you do it.

MR. KHAN: Okay. Great. Give me one second,

please. I'll send it to you.
BY MR. KHAN:
Q. Dr. Preneel, please let me know when you have the file open.
A. I have it open in front of me. I also have the printout of it next to my own version which I have my notes on. That's why I was using that version.
Q. Okay. So moving -- moving forward, I think I'll be referring to the filed document, right --
A. Yes.
Q. -- and asking you questions accordingly. I don't know the contents of whatever else you're looking at, so I'd rather not have you look there.
MR. KHAN: So -- but, Ms. Houston, do you have a copy -- were you able to download a copy too?
COURT REPORTER: I was. Thank you so much.
MR. KHAN: Great.
BY MR. KHAN:
Q. Okay. Up until -- I'd just like to confirm, up until now, the questions I've been asking you, were they consistent with the copy that you had seen?
A. Yes, they were.
Q. And your opinion is consistent with the file that I just sent you, Exhibit 2009, a copy of --
A. Yes, it is. Yes.

Q. Okay. So I'm going to ask -- pick up from where we just were.

In the Exhibit 2009 that we are looking at, in paragraph 20, is it correct that your paragraph 20 states, "I understand that the board may not institute post-grant review ('PGR') unless the petition" -- and I'll stop there.

Is that correct?

A. That's correct, yes.

Q. In paragraph 22, you state that the, "Patent claims in an IPR are given their broadest reasonable interpretation ('BRI')."

Is that correct?

A. That's correct, yes.

Q. And you use the BRI standard for your opinions; is that correct?

A. That's correct, yes.

Q. Can you tell me what the difference is between a PGR and an IPR?

A. Well, the post-grant review was the first phase in which there was a petition and there was a request to go to a IPR procedure. And my understanding is we're now in the IPR procedure. So first there was an indication that there's -- it's more likely than not that at least one of the claims challenged in the

petition is unpatentable, and then this question is actually sorted out in the IPR procedure. That's my understanding.

Q. And so is it your understanding that first we are in a PGR and then we move to an IPR?

A. Yes.

Q. And we didn't discuss it at the outset, but make it clear now. As you know, we have a second deposition scheduled for Friday. And just to make it -- I guess the lines a little bit -- well, just to facilitate our discussion, what I was planning on doing is questioning you on the '766 patent today and the '480 patent on Friday. Does that sound okay to you?

A. That's fine, yes.

Q. Okay. So my questions today will be limited to your '766 declaration. Is that okay?

A. That's fine.

Q. Great.

In paragraph 22, you mention that, and I'll quote, "The BRI of the claim terms is understood from the perspective of a person of ordinary skill in the art."

Is that correct?

A. That's correct.

Q. Who is a person of ordinary skill in the art?

A. I think that somebody -- I don't remember whether my -- my working definition, but it's somebody who had a basic knowledge of a specific subject matter of the patent. This typically is somebody, say, with a bachelor degree with a few years of experience or somebody with a master degree or PhD degree, I think in this case, who would understand the subject matter necessary to -- as we discussed earlier, to apply and understand the patent.

Q. So is it your position that a person of ordinary skill in the art is someone who has a bachelor's or master's or PhD degree in the subject matter areas that you noted in paragraph 10, which was cryptographic algorithms and protocols, cryptanalysis --

(Court reporter requested clarification.)

MR. KHAN: I'm really sorry.

THE REPORTER: That's okay.

BY MR. KHAN:

Q. So I'll continue. Maybe I'll repeat my question.

So is it your opinion that a person of ordinary skill in the art, as you note in paragraph 22, is a person who has a bachelor's or a master's or a PhD degree in the subject matter areas that you've listed in paragraph 10, which include "the design and evaluation

of cryptographic algorithms and protocols, including cryptanalysis, security reductions and proofs, cryptographic hardware and software, secure execution environments, and secure electronic transactions"?

A. First, I don't think that a bachelor degree in most cases is sufficient because it's quite advanced matter.

Second, these degrees, of course, don't exist. I mean, you have degrees of computer science or electrical engineering where you have -- typically to understand these matters, you get basic notions of computer science and computer architecture, and then hopefully or ideally such a person should also have at least some courses on computer security or cybersecurity and cryptography.

Q. So is it your position that a person of ordinary skill in the art would have a bachelor's, master's, or PhD degree in electrical engineering focused on the topics you just mentioned? Is that correct?

A. I think you need to have a general understanding of either computer science or electrical engineering courses. Typically -- CS courses typically have some courses on computer architecture which you would need to understand the hardware, and the EE

courses typically have some computer science subject matters, so that would be the general degree, so to have a general understanding of what's happening or how computers operate and how the systems work. And having it would -- I would assume that somebody has also some course in cybersecurity or applied cryptography.

Q. Does --

A. Then in this moment to be an expert in cryptanalysis or -- I don't expect this person to be an expert for the cryptanalysis or security proofs but to have a general understanding of what these things are, what the security proof is, or what these notions are at a very high level. And I think I also already repeated that I don't believe that a bachelor degree is sufficient to be -- in this matter, a person of ordinary skill in the art would need to have at least several years of industry experience, given the scope of most bachelor programs.

Q. So is it correct to say that you think at least a master's or a PhD degree with work experience is -- is what is needed to be a person of ordinary skill in the art?

A. I don't think I said that. I think I said a bachelor degree with a few years of experience or a master degree or a PhD degree because during master or

PhD degree, this experience can also be acquired.

Q. Do you think having a doctorate degree is what a person of ordinary skill in the art would have?

A. No. That's not necessary.

Q. But it's possible?

A. They could have this, yes, but it's not essential to have a doctor's degree.

Q. Which year did you get your PhD in?

A. 1993.

Q. So is it correct to say it's been about 29 years since you got your PhD?

A. That's correct.

Q. So how do you understand the perspective of a person of ordinary skill in the art minus -- I'm sorry, let me scratch that, please.

You're an expert in this area as you have noted in your declaration according to you. How do you understand the perspective of someone who just has ordinary skill in the art, given that you are an expert, what a person of ordinary skill in the art thinks? How would you understand that?

A. Well, I work on a daily basis with some of those people because I do also teach a second year bachelor course, so I am very well aware of what bachelor students know and do not understand. I also

teach at first and second year master level, where they are slightly more advanced students. I think every year I supervise about five master thesis, so these are students who are at the end of their master and you see how they become more mature and what they understand about these kind of topics and how they develop their skills.

I -- on a regular basis, I consult for industry, and very often the people I deal with there are not PhDs but people with technical experience, sometimes very experienced people, sometimes more junior people, and we discuss technical matters exactly on these kind of topics. So I'm not sitting in an ivory tower and I'm just talking to experts. In fact, I interact and train people at every age of experience, and I interact a lot with people in the industry as well.

Q. So you mention in your answer, if I can repeat -- please correct me if I'm wrong here. You mention that, in part -- you can understand the perspective of a POSITA, in part, at least because you have undergraduate students with bachelor's degrees; is that correct?

A. That's correct, yes.

Q. Didn't you mention also earlier that having a

bachelor degree alone is not enough?

A. I mentioned that, but I just -- I understand what is still needed to go beyond that. So I think I understand what people understand and know at specific level of experience in their training. And so, yes, based on my experience with these students, I can confirm that that would not be sufficient even after completion of their bachelor degree.

Q. So does that mean your interaction with bachelor students does not inform the perspective of a person of ordinary skill in the art?

A. I respectfully disagree with this. It does inform me because it shows what -- that they are not there at this young level, so it actually also helps to understand what is needed because you see what is actually missing.

Q. So by talking to your bachelor students, you understand what they don't know?

A. Exactly.

Q. Have you had discussions with them about what they don't know?

A. I do, of course.

Q. And does that include the subject matter of the '766 patent?

A. We tend not to discuss patents, but we do

discuss application, in this case, of discrete [phonetic] mathematics, and we understand what the limited understanding is of systems and complexity of things fitting together, so we do understand how they can apply scientific results to real-life systems and what their concerns are, what their difficulties are.

Q. Have you discussed the '766 patent with your students or your colleagues?

A. No, I have not.

Q. So your thoughts on the perspective of a POSITA are not based on conversations with people you consider POSITAs; is that correct?

A. That's not correct because, as I mentioned earlier, I worked with a PC student and we wrote scientific articles on the security of TPMs, and these are trusted platform modules, and they are very similar ideas. They use secure execution environments for their cryptographic keys, and so we actually are looking at how to -- a better security of these components. And so at that moment, this person was somebody who had a master's degree working towards his PhD degree, so I would consider this person at that stage to be a POSITA.

So I do have -- worked with people at the POSITA level on specific -- unrelated to the specific patent but on related problems, mainly secure execution

environments and cryptographic transactions, secure transactions.

BY MR. KHAN:

Q. When was -- this PhD thesis that you're referring to, what date was that PhD thesis?

A. I would have to look it up, but I would say work was probably done between 2004 and 2008 or so, 2009, something like this.

Q. Does a POSITA's understanding have any timing elements to it?

A. Well, I guess POSITA means state of the art, so of course that evolves with time, of course.

Q. And what time would that be?

A. I guess a time when the invention was filed.

Q. So when it comes to the '776 patent, the filing date of the '766 patent, which would be June 14, 2004; is that correct?

A. That's correct.

Q. And the '480 patent is the same family that had a filing date, I think, in -- well, we can get to that when we talk about the '480. I don't want to mix it.

A. Okay.

MR. KHAN: Okay. So we've been going for about an hour. If you think we can maybe take a five-,

ten-minute break. Does that work for you?

THE WITNESS: That's fine for me.

MR. KHAN: Mr. Henry, does that work for you?

MR. HENRY: Yes.

MR. KHAN: Great. So maybe we can reconvene in ten minutes.

Ms. Houston, does that work?

COURT REPORTER: Of course. Thank you.

(Recess: 9:12 a.m. to 9:24 a.m.)

BY MR. KHAN:

Q. Dr. Preneel, during the break, did you communicate with your patent owner's counsel?

A. No, I did not.

Q. Can I ask you to turn to paragraph 7 of your declaration, please?

A. Yes.

Q. In paragraph 7, you state, "Al-Salqan and Searle do not overcome the deficiencies described in the patent owner's response relating to the combination of Ellison and Muir."

Is that correct?

A. That's correct.

Q. Did you read or review the patent owner response?

A. I did.

Q. So did you read it before or after writing your declaration?

A. I read it before writing my declaration.

Q. Do you agree with all of the contents of the patent owner response?

A. Obviously I don't agree with all of the contents because that's what I try to make here in my declaration.

Q. So you --

A. Maybe I misunderstood your question. Excuse me. The patent owner response or did you say the petitioner's response? Sorry.

Q. I said the patent owner response.

A. Okay. I agree, of course, with what is in there. Excuse me. I did read that correction before I wrote my deposition [sic], and I do agree with what is in there.

Q. And did you write the declaration?

A. Yes, I wrote the declaration.

Q. Did you write any part of the patent owner response?

A. I did not.

Q. Did you -- let me ask you -- I'm sorry. One second, please.

In writing your declaration, did you discuss

the contents of your declaration with counsel?

A. Yes, I did.

Q. Did you attempt to make sure that your comments and arguments were consistent or the same as the patent owner response?

A. There were some consultations, and I did my best to write on my technical opinions, but in the end if there would be deviations -- which I haven't seen -- that would not be deliberate in any case.

Q. So is it correct to say that if there is any difference, it is not your intention to make it different? Is that correct?

A. That's correct, yes.

Q. Do you have --

(Court reporter requested clarification.)

BY MR. KHAN:

Q. Do you have a copy of the patent owner response with you, Dr. Preneel?

A. I don't have it printed, I believe.

Q. Okay. Let me --

A. If you show it -- it would be nice if it could be projected or if you could just mail it to me so I'm sure I have the right version.

Q. Yes, I'll drop it in the chat box like last time.

A. Okay.

Q. I'm sorry. I'm sorry. Please disregard that copy.

Okay. I'm going to share my screen with you, if that's okay.

A. That is fine.

Q. Okay. Can you see my screen?

A. Yes, I can.

Q. Okay. I have shown on my screen the patent owner response.

Can you confirm that this is the patent owner's response?

A. That's correct, yes.

Q. I'm turning to page 24, and page 24, the last paragraph here reads, "The usage protector 250 are loaded into the execution space by processor nub loader 52."

There's some citations there. And then it states, "These loaded modules are stored in mass storage device 170 which can be a CD-ROM 172, floppy diskettes 174, and a hard drive 176."

There's a cite to Exhibit 1006 and then a cite to Exhibit 2009, paragraph 54. Is that correct?

A. That's correct. Yes.

Q. The last citation there, Exhibit 2009,

paragraph 54, do you agree that that is a citation to your declaration?

A. I don't know the number by hand of the exhibit. If you confirm that my declaration is 2009, then I confirmed it, yes.

Q. Okay. Then can you turn to paragraph 54 of your declaration, please.

I'll stop sharing right now.

Could you read paragraph 54 for me, please.

A. "The goal of usage protector 250 is" --

(Court reporter requested clarification.)

THE WITNESS: "The goal of usage protector 250 is to protect the secure processing environment itself and not the transactions."

BY MR. KHAN:

Q. So, Dr. Preneel, paragraph 54 speaks to the goal of the usage protector, correct?

A. That's correct.

Q. And there are no citations in this paragraph, correct?

A. That's correct.

Q. The paragraph includes no statement about a storage device, correct?

A. That's correct.

Q. The paragraph includes no description of

loading the usage protector, correct?

A. That's correct.

Q. And paragraphs 50 to 72 of your declaration do not include a single citation; is that correct?

A. That's correct.

Q. Okay. So in -- I'm sorry. I'll pause there.

Now I'd like to ask you to open up a copy of the '766 patent.

A. Yes, I have it in front of me.

Q. Thank you.

In paragraph 41 of your declaration, you state that, "The '766 patent claims a novel, method, and system for performing an electronic transaction or electronic verification or identification without requiring additional hardware."

Is that correct?

A. That's correct.

Q. It also states that in your opinion, "The interventions claimed in the '766 patent represented significant steps forward in electronic transaction technology and verification of legitimate access to, or use of digital data."

Is that correct?

A. That's correct.

Q. What are the -- can you explain what the '766

patent is referring to when they are saying "without requiring additional hardware"?

A. There was really two approaches to make secure transactions processors, and one is providing additional hardware to secure keys -- to secure potentially the software to complete the transaction, and to isolate this, but one can also do this with existing methods. For example, by modifying the BIOS and by only -- software-only methods. And so I think this particular paragraph refers to the fact that it can also be done without additional hardware.

Q. And what hardware is that?

A. You mean which -- the one which is not added or the --

Q. Yes. Which hardware is not added?

A. There will not -- for example, not add hardware circuits to, for example, separate memory. Or you would not have special additional hardware to store cryptographic keys or to perform cryptographic computations. So if you go back 20 years ago, people weren't particularly thinking of having the smart card, and they would issue it by a bank, and during the transaction it's like a smart card --

(Court reporter requested clarification.)

THE WITNESS: So 20 years ago, you would have

been thinking of securing transactions by performing them inside a smart card provided by a bank, and a secure environment would then be the smart card, and the smart card would be the additional hardware.

BY MR. KHAN:

Q. You mentioned that using potential software secure -- sorry, you could use potential software to secure a transaction.

Did I repeat that correctly?

A. That's correct, yes.

Q. What kind of software is typically used to secure the transaction? And this is, again, you know, going back where we were talking about, I think, when the filing date or -- you know, at the filing date or around that time for the '766 patent, what was the software that would be used to secure transactions?

A. Well, at the time transactions were just carried out in browsers. There was no additional software or hardware provided. People just entered transaction data, including payment data, in a browser -- on a regular browser on a regular computer using a regular operating system on regular hardware. And, of course, this exposes the credit card information, also the transaction itself to attacks on either the operating system or on the browser or the

user application.

Q. So at that time there were no cryptographic keys?

A. Cryptographic keys were used inside the browser. So already in 1993, '94, the SSL protocol was created, which later became TLS protocol, and that protocol provided a secure channel between a browser on the one hand and a server at the merchant on the other. For the secure channel, cryptographic keys were used, but there was no cryptography used to protect the transaction itself. It was just entered through the secure channel and transferred to the other side.

Q. So at that time were digital signatures used?

A. It depends on the context and the setting. Very specifically, digital signatures, at least of the definition which is also used in this patent, which also includes what cryptographers call MAC algorithms or symmetric key signatures, they were in use already since the '80s in the banking sector.

Digital signatures were also in use using public key technology in the credit card sector, you have read specifications for which I was a reviewer in the early '90s. This technology was, at that time, rolled out in Europe late '90s but not yet in the US. It came much later in the US, but in Europe, it was

available. Digital signatures were also used, for example, in -- I would say not in the US but several countries in Europe including Belgium --

(Court reporter requested clarification.)

THE WITNESS: Belgium, that's the country where I live -- Belgium and Estonia were issued digital or electronic identity cards, and you could compute with those digital signatures. So the answer is, yes, signatures were used, but not for Internet transactions.

BY MR. KHAN:

Q. I see.

So as of 2003, you're saying digital signatures were used but maybe for other applications, not for Internet applications; is that correct?

A. They were used for electronic transactions as described in the patent but not when implemented on the Internet.

Q. I see.

And the digital signatures that are used, are they -- as of 2003, are they also -- are they used -- are they generated using a private key or a public key or at that -- 2003, how were the digital signatures generated?

A. As I mentioned in my previous answer, there is two options. One is based on symmetric cryptography,

which cryptographers call MAC algorithms, or message authentication codes, and in that case the signer and the verifier or sender and recipient share a secret key. And that is the model used in most banking cards, typically debit cards, and it's still also used in a number of debit cards, credit card transactions today.

But in some other settings, in typically credit card payments following the EMV specifications -- and those specifications were created in '93, '94, '95, so first half of the '90s -- their digital signatures were used that used a private key to sign a transaction and a public key to verify the transaction.

And this was rolled out by EMV under the term "combined data authentication." Combined because you would use both a digital signature based on asymmetric keys and a second digital signature based on a MAC algorithm with shared keys. So at the time of the invention, both technologies were in use for financial transactions.

Q. And at that time in 2003, did they -- specifically June 2003, did they have architecture that would be able to secure the private key and allow for secure transactions to occur?

A. I think definitely there were several banks and this is -- I was aware of this, but most of those

things were proprietary protocols. For example, in Europe, there were several banks that actually used software-based solutions to secure digital banking with private keys stored somewhere on the user device, typically encrypted under a user password.

Q. And in 2003, in June 2003, how would they -- so you mentioned that there were several protocols.

How would they secure the private key? Like what would these protocols do?

A. For the majority of transactions, the private key was stored in a smart card issued by the bank or the financial institution, and this was a problem because, of course, a smart card -- it's hard to connect a smart card with a PC platform. There were banking solutions that provided this but not for retail banking, so there were wholesale banking applications where you could use a smart card to authorize your transactions. But this was deemed to be too complex and too expensive to support for retail applications. So this was used for business-to-business scenario.

For retail applications, so for consumer transactions, this private key was just stored somewhere on the device or in the browser encrypted using very often the password of the user.

Q. As you said, the private key would be in a --

stored in an encrypted form in the memory.

A. But as a very weak encryption because it was the password of the user.

Q. I see.

A. And sometimes it was not encrypted at all. There were applications where it was stored in Clear.

Q. And how would the private key be -- scratch that.

You mentioned that the private key would be encrypted perhaps using the user's password, login information; is that correct?

A. That's correct.

Q. When it was -- when the private key was stored in memory and in encrypted format, was it protected in any way or was it left vulnerable for anyone to take?

A. It was not protected in any way. So both the encryption process itself and the outcome of the crypto private key was available in clear. And, again, I'm referring here to the scenario on a PC, not the scenario where a smart card is used.

Q. So when the encryption or decryption was performed, where -- where would that be performed?

A. Just on the regular processor in normal software, and so both the operating system and the user software had access to this.

Q. Would that be in a -- I guess, would that be in a secure area where they did --

A. No --

Q. -- perform the encryption or the decryption?

A. No, it was done in what we call insecure memory.

Q. I see.

Now, in paragraph -- going back to paragraph 31, you -- the second statement in that paragraph, you also mentioned that the '766 patent represented some "significant steps forward."

What are these significant steps forward?

A. The step forward is the idea of creating two environments, on the one hand -- I'm now referring here to Figure 3, the operating system. And then the secure environment run by the console, and there was a secure area, and this area has secure storage of the key but also secure storage of authentication software. And in addition, the key would be encrypted and also decrypted all in a secure environment. So even if the user application, say, the browser or the operating system would be compromised, it would not be possible to get access to the keys or to manipulate authentication software in the secure environment. So it was like creating a smart card inside the computer.

Q. What prevents the operating system from accessing the secure area?

A. The BIOS prevents this because the operating system has to use the BIOS, and the BIOS, you cannot just use it. You have to go to an API call, so it's called the vector table, so it's a regulated interface, and this BIOS would deny access to certain places in memory to the operating system.

Q. Can you explain -- can you indicate what a BIOS -- what it stands for and what its function is?

A. A BIOS is the basic input/output system. It's active when the system starts up, when the system boots, as we say with technical terms. So when the computer starts up, the first program run will be the BIOS, and the BIOS will prepare the computer for working.

And then secondly, during operation of the system, the BIOS will mediate access to memory and to other devices such as printers or network ports on the computer. So the operating system, it wants to use memory or wants to use certain ports, it has to go through the BIOS, and the BIOS can give access or -- in the example of the design in Figure 3 -- also, in certain cases, deny access.

Q. So is it correct to say that the BIOS can permit access or restrict access to the secure area?

A. That's correct, yes.
Q. Thereby rendering the secure area inaccessible to the operating system; is that correct?
A. That's correct.
Q. Can the BIOS be split into different areas?
A. It's possible to make the BIOS more complex and to have more complex designs, and as I mentioned, the BIOS has already two functions, the startup function and the operating function. So in practice, yes, it is possible to do this. But that depends, of course, on the design of the system, whether it's done or not.
Q. What about in Figure 3 of the '766 patent, is that -- is that just one BIOS, or is it a BIOS that has different parts?
A. That's one BIOS, but in this particular example, the BIOS may contain also an encryption key that can be used in the secure operation of -- secure operation environments.
Q. So it's one BIOS -- so if I understood you correctly, it -- in Figure 3 of the '766 patent, there's one BIOS, not divided, by --
A. That's correct.
Q. Okay. It includes an encryption key 46?
A. Yes.
Q. Can you turn to column 6, line 62, of the

patent.

Is it correct -- I'll read lines 61 to 62.

Is it correct to say that lines 61 and 62 read, "The encoded authentication table is stored in a secure part of the BIOS"?

A. Yes.

Q. So is there an unsecured part of the BIOS?

A. Well, I think in this particular sentence, what is meant by "secure part" is part that cannot be read by the operating system. So "secure" is here defined as the operating system cannot read or write this. And BIOS is typically ROM, so it can't be rewritten. But other parts, of course, can be read by the operating system because it's needed to boot the system or to perform certain actions.

Q. So is it -- is it accurate to say that the BIOS can include a secure part and an insecure part, and the insecure part is the one that communicates with the operating system 48?

A. I think it's a bit more complex. I think there is -- the BIOS consists of multiple pieces of software, and part of it regulates the traffic, right, and then it may give you access to certain part of the BIOS or certain part of the system, and the other parts implement a specific access.

Q. So more specifically when you say that it -- there are certain parts that give you access to certain parts of the system and other parts that implement a specific access, could you be a little more precise in that? I'm not sure which part is giving access to what. So if you could explain that to me, that would be --

A. Well, the core -- the core is that the operating system will ask for access during operation of the system. And then access will be implemented, which means, for example, a connection will be set up with the printer if the BIOS allows this or with the network or with part of the memory, or the BIOS may say, no, you cannot access this or this function is not available to you. So there is code needed to implement the access, and there is code needed to regulate the access in the first place.

Q. So when the patent says there is a "secure part of the BIOS," are they referring to just code, that's the secure part of the BIOS? What are they referring to when they say "secure part of the BIOS"?

A. Obviously it's data which cannot be read. That secure part is data which cannot be read by the operating system. The operating system asks to read it, it will be denied. That's why we call it secure BIOS.

Q. So is that data being handled by a secure

processor or stored in a secure memory? What -- what makes that secure part of the BIOS?

A. There is part of -- if the operating system wants to read it, it will not get permission to do this. That's why we call it secure part of the BIOS.

Q. So I'm asking about which part is secure, which part's not secure, and your answer has been whether the BIOS gives permission or not.

So I'm going to ask again. Which part of the BIOS is secure? Which part is insecure? Not whether one part gives permission or not. I'm trying to understand when the patent -- '766 patent says "the secure part of the BIOS," which part of the BIOS does that include?

A. I think, Counselor, that the answer is as I gave before. Secure part is the part which cannot be read by the operating system, so there is part of the BIOS that denies access to it where the operating system has no read access.

Q. And what components form that secure part?

A. That part of the BIOS that decides about access.

Q. So my question was, what components form the secure part?

A. So would you mean what is -- maybe to -- to

make sure I understand the question, what are the components of the secure part of the BIOS; is that the question?

Q. Yes.

A. What is in there? What comes in the secure part? So there can be cryptographic keys, there can be data for authentication of transactions, and also it could be -- authentication software could also be stored in there.

(Court reporter requested clarification.)

THE WITNESS: Authentication software.

BY MR. KHAN:

Q. But in Figure 3, isn't it the case that the authentication software is in the secure area 62?

A. Yes. But it could also be stored in the BIOS.

Q. So in the BIOS in Figure 3, the authentication software is not part of the secure part?

A. That's right, but you didn't ask me what was stored in Figure 3. You asked me what can be in the secure part of the BIOS, and I gave you an answer to that question.

Q. Okay. So let me rephrase my question.

In Figure 3, what forms the secure part of the BIOS?

A. In Figure 3, the secure part of the BIOS is

the encryption key stored in the BIOS, and also there will be -- but this is more technical -- those functions that give access at the start of the console and started with secure parts.

Q. Is the secure part of the BIOS --

A. Yes.

Q. -- admitted to the encryption key?

A. Yes.

Q. I'm sorry, I didn't hear that. What was that?

A. Yes, that's the encryption key.

Q. So you -- you would agree that no other parts of the BIOS, other than the encryption key, form the secure part of the BIOS in Figure 3?

A. That's correct. Yes.

Q. And what do you think the patent means when it says "secure area"?

A. I think it means the box and dotted lines in Figure 3, "secure area." It's a part of memory which is not accessible to the operating system where we have authentication software, recovery application, secure storage location, and then also block 58 which could, for example, contain a log file of transactions.

Q. Is it correct that the authentication software and other data that is shown in Figure 3 as being part of the secure area that they're stored in inaccessible

memory? Is that correct?

A. That's correct, because the BIOS will deny access to the operating system of this area.

Q. And that inaccessible memory restricts access to the operating system; is that correct?

A. That's correct.

Q. How is access to these memory locations restricted?

A. This happens because the operating system cannot just read a value as to the passing of the BIOS, to ask access, and if the operating system requires access to a secure area, the BIOS will deny this. So it's the BIOS that regulates access to the secure area.

Q. So you had mentioned here that one of the points of novelty in -- that the point of novelty -- sorry. Let me scratch that.

You had mentioned earlier that the point of novelty of the '766 patent is that it provides this separation that allows you to have a secure area that is not accessible from -- by the operating system and that that was something new in 2003.

Is that correct?

A. Well, that's only part of the story. The newer thing is also that this is -- the secure part also contains authentication software and can be used for

secure transactions.

Q. I'll have you turn to column 4, please, lines 16 to 18. I'll read it. The sentence there says, "A secure storage location and/or an encryption system are not essential to the BIOS system with respect to the present invention."

Is that correct?

A. That's correct.

Q. So how does the '766 system work without a secure storage location?

A. Well, there is also the embodiment in Figure 5 where you actually modify the hardware and have secure storage of keys and authentication software and hardware in a separate hardware area.

Q. In that embodiment, the operating system can access the authentication software; is that correct?

A. It cannot because access is mediated by the BIOS, and, again, the BIOS will limit access to the hardware. That's the role of the --

Q. Can a user -- sorry. Can a user access the hardware?

A. No. Not directly. The user has to go to the operating system. The operating system goes to the BIOS, and then the BIOS goes to the hardware. And so the BIOS mediates the access.

Q. Which system is more secure, Figure 5A or Figure 3?

A. I think it all depends on your threat level, depending what the adversary --

(Court reporter requested clarification.)

THE WITNESS: Threat level, what the assumptions are you make about the opponent. But, of course, Figure 5 requires modifying the hardware, so it will be more complex and expensive, but if it's done well, it will give you a higher level of security against certain attacks. For some other attacks, the two systems are equivalent.

BY MR. KHAN:

Q. So you're saying that the embodiment in Figure 5A, to be precise, is more secure than the one in Figure 3?

A. I don't think that's what I said. I said for certain attacks, this embodiment in Figure 5A will be more resistant. Against other attacks, it will not make a difference. It depends on your threat level whether you care about the difference or not.

Q. So in looking at Figure 3 and Figure 5A of the '766 patent, is it your understanding that the secure area, Box 62 in Figure 3, is secure because it is preventing access from the operating system?

A. Yes.

Q. And what would happen if a system in Figure 3, for example, has multiple operating systems? Would it -- would the secure area have to be protected from all of the operating systems?

A. That is correct, yes.

Q. Can the console access the secure area?

A. It can access the data, but typically it will only send instructions to the software running in secure area and will make sure it actually runs as requested. So actually it will recall API calls. It will give a request to, for example, authenticate a piece of data with a specific key and will get the answer. But there is no need for the console to, for example, read the keys. That's how you would implement the settings.

Q. So earlier you had mentioned that the console is like an operating system.

A. It's a highly simplified operating system, so it makes it easier to make it secure.

Q. Okay. So would it be fair to say that in some cases you could have an operating system that speaks to the secure area and other operating systems are not in communication -- are prevented access to the secure area?

A. I would consider it as a very bad design

decision to replace a console by an operating system.

Q. And why is that?

A. Because operating systems typically are much more complex, and more complex systems are more likely to have bugs and flaws, and so you actually open additional attack factors into your system. So preferably the console should be as simple as possible.

Q. So a simple OS would do the job, not a complex one; is that correct?

A. Well, I think simple OS is like an oxymoron. OS has to do so many tasks. Typically OSs are not simple.

Q. So I'm trying to understand, then. Is it then your position that the console is not an operating system?

A. It's a highly stripped-down operating system with only very minimal functionality, and some experts would no longer call it an operating system. That's why they call it a console, because it doesn't have the typical task that an operating system has.

Q. Okay. Thank you.

MR. KHAN: I think I'll pause there. Maybe we can take our next ten-minute break. Does that sound okay to everyone?

THE WITNESS: Fine for me.

MR. HENRY: Fine.

(Recess: 10:17 a.m. to 10:32 a.m.)

BY MR. KHAN:

Q. Picking up where we were, turning to Figure 3, Dr. Preneel, of the '766.

Do you have that in front of you?

A. Yes, I do.

Q. Great.

So Figure 3 shows a secure area 62 including authentication software 54; is that correct?

A. That's correct.

Q. How does the authentication software get stored in the secure area?

A. Can you clarify what you mean by "get stored"? Get loaded in there or get stored in there, because --

Q. I mean, maybe you can clarify that. Is the authentication software stored in the secure area, or is it loaded in the secure area in the '766 patent?

A. Yes, this will be -- it depends on how the -- operator but will be in a separate part of memory that is, as we discussed before, controlled by the BIOS and not accessible to the operating system, and the authentication software will be running in there. And so I -- which is as a piece of RAM, so random access memory which is separate, not accessible to the

operating system and where the software is run.

Q. So if I understood you correctly, you're saying that the authentication software is stored in the RAM where it's not accessible to the operating system; is that correct?

A. Yes.

Q. And how does it get onto the RAM?

A. It will be loaded at boot time.

Q. At what time?

A. At boot time of the computer. At startup time.

Q. I see.

So it's loaded there, and as a result, it's stored onto the RAM and then --

A. Right.

Q. -- the BIOS protects it from the operating system?

A. That's correct.

Q. Okay. Figure 5A, the authentication software is in the hardware; is that correct?

A. That's correct.

Q. Which part of the hardware is it on?

A. Will be stored somewhere in -- I mean, there can be many solutions. It doesn't -- I don't think it necessary to specifically specify this in more detail,

but it can be nonvolatile memory somewhere.

(Court reporter requested clarification.)

THE WITNESS: Nonvolatile memory -- NVM, nonvolatile memory, somewhere. But it can also be baked into the hardware if your processor would be -- I mean, processors have also -- can also have software run inside the processor chip itself. It can be inside the processor chip as well.

BY MR. KHAN:

Q. Sorry. It could be in a nonvolatile memory or a ROM of the processor; is that correct?

A. That could be external or internal to the processor.

Q. And if it's external to the processor, how is it protected?

A. Well, in principle, the software only has to be protected against modification, and then you would use standard protection techniques. It's just the same way as your boot software is protected through the standard software authentication techniques with a secure boot mechanism.

Q. So if a person of ordinary skill in the art were to look at Figure 5A, I understand that the authentication softwares and the hardware -- it's your understanding that the possible implementations there

are one in which it could be part of the ROM in the processor or one where it could be external to the processor but with some standard well-known software protection?

A. With boot protection -- with boot protection mechanisms. But I think specifically if it would be stored inside the processor, then no additional protection would be needed because the processor area is believed to be a secure area by itself.

Q. Okay. In -- in both in Figure 5A or Figure 3, how is the authentication software stored and -- and so I think in Figure 3 you said that it's a RAM, right? So how is it stored? Where is it -- where does that code come from that's creating this authentication software? How does it create that memory space for the authentication software?

A. I'm not sure I fully understand your question. Memory space is allocated to this secure area, so you don't have to create it. It's existing space in RAM.

Q. How is it allocated?

A. It's allocated because the BIOS decides which space is for the regular operating system and user and which part is for the secure part. So the allocation of memory I understand is deciding which --

(Court reporter requested clarification.)

THE WITNESS: So the allocation is deciding which part of the memory is for the applications and the operating system on the one hand and which is for the secure environment on the other hand, and this decision is made by the BIOS.

BY MR. KHAN:

Q. And how does the BIOS determine which memory spaces to allocate to a secure area and which ones to a nonsecure area?

A. It depends on the size that's needed. Typically, the secure area will be simpler because it has less functions. It will get a smaller space than the regular applications and operating system.

Q. Is it possible to change the configuration of a system, for example, to store the authentication software from in a secure area and then into the hardware?

A. Figure 5A describes how authentication software is stored into the hardware.

Q. Yes. My question was, is it possible, for example, to change from Figure 3 to Figure 5A, or Figure 5A to Figure 3, so you have the different places where you might want to configure the authentication software? Is that possible?

A. That's correct, but of course, for Figure 5,

you definitely have to change the hardware. So you cannot just, for a given system, choose between one or the other option. It's different design decisions.

Q. So is it correct to say that you could have a system such as the one shown in Figure 3 and include the authentication software in the secure area and subsequently decide that you want to implement -- modify that system so that you have the authentication software in the hardware and therefore configure the hardware in order to accommodate the authentication software? Is that correct?

A. That would require a different design with different hardware.

Q. And a different --

A. You have flexibility of where it was stored in your design of authentication software; that's correct. And if you store it -- you can store it in the option of Figure 3 or you can store it in the hardware option of Figure 5A. These are two embodiments of the invention. Maybe it's important to point out that authentication software itself need not be secret. You just have to make sure that it's correct.

Q. Sorry. What need not be secret?

A. The authentication software itself.

Q. Authentication software itself. Okay.

A. Of course, the keys used in the software have to be secret but not the software itself. It may be secret, but it doesn't need to be secret.

Q. And in Figure 3, is the authentication software secret or no?

A. Well, it it's in a protected environment, so it could be secret.

Q. But is it or is it not?

A. It's an independent decision. The design does not force you to make it public. You can make it public and have this design, or you can keep it secret and have this design.

Q. I see. So in Figure 3, the authentication software, it may or may not be secret depending on the design choice?

A. That's correct.

Q. And when you say "secret," are you using that as another word for secure or, like, what are you --

A. Secret means it is available to the public for inspection.

Q. And is it available to the operating system?

A. Well, you can hide it from the operating system, or you can -- if it's available to the public, obviously it's also accessible to the operating system. I mean, it can run it itself --

(Court reporter requested clarification.)

THE WITNESS: Yes. So I think it's a bit of a rhetorical issue, so you can have the software secret or not. It doesn't matter. It can be a public standard, or it can be a proprietary secret standard. In both cases, it's protected by secure area, but of course, it's a public standard, everybody can know how it looks like. That doesn't change the access of the operating system. That's a different question.

BY MR. KHAN:

Q. I'm a little confused. If you could just clarify the last two statements that were made. Reading from the transcription, so I'll try to summarize, but please feel free to correct me. I think you had mentioned that if it's available to the public, it's also accessible to the operating system; is that correct?

A. This may be an unfortunate formulation. Accessible, that's -- I mean, it's just available to everybody, so also to the software, it doesn't mean the operating system can run it, so I would say "accessible" is not the correct term because "accessible" means the operating system can run it.

Q. So the authentication software could be in the secure area and be available to the public or may not be

available to the public; is that correct?

A. That's correct.

Q. And when you say "available," what does that mean?

A. The description is known. The code itself is known.

Q. The code is known. I see.

A. Yeah.

Q. But your -- your position is that even though the code may be known, the software itself cannot be accessed by the operating system; is that correct?

A. That's correct. So the software, while being run, cannot be inspected or accessed or stopped by the operating system, and the operating system does not see the particular values processed inside a secure area.

Q. So the authentication software that we are referring to here, is that simply just allocated memory spaces, or is there any data that is part of the authentication software as well?

A. Authentication software is a computer program. The computer program consists of instructions and data.

Q. So the authentication software is a program that includes instructions and data; is that correct?

A. That's correct. Yes.

Q. So when you are loading the authentication

software to store it in the secure area, where is that -- where is that data and instruction coming from?

A. That depends on the design. That could be in the BIOS, or that could be also in an external memory.

Q. And after it's been stored in the authentication -- sorry, in the allocated memory spaces, is the authentication software generally removed from the BIOS or the external memory?

A. No, it will remain there as well.

Q. Why?

A. Because that's -- the BIOS is a ROM memory. It's memory you can only read and not write. So you can load software from there, but after you load it, it will still remain in there for next time you want to load it.

Q. If it's in the external memory, the external memory gets deleted, does that affect the authentication software in the secure area?

A. It would not affect it, but of course, if you want to load it next time, it would no longer be possible. So in practice, you would leave it there.

Q. So when your authentication software is coming from an external memory, it is possible for that external memory to get deleted and remove the authentication software that was stored in that external memory?

A. I don't think that makes sense from an engineering point of view to do this.

Q. My question was, is it possible for the external memory that stores the authentication software to be deleted such that the authentication software is no longer on the external memory?

A. That would happen, and then the next time you boot the computer, it would no longer -- the process would no longer work. It's similar as you would take a smart card and destroy the smart card. Well, then you can -- the next time, you cannot make -- you cannot use it anymore.

Q. But the authentication software that's stored in the secure area is still working even after the external memory gets deleted, right?

A. Until -- yes, until the computer is booted down.

Q. So whatever data is stored in the authentication software remains there even though the external memory might have been deleted; is that correct?

A. That's correct, yes.

(Audio interruption.)

BY MR. KHAN:

Q. When the authentication software is stored in

the allocated memory space, let's say it's coming from external memory, how does that -- the -- does the -- is the authentication software stored in a permanent memory space necessarily?

A. I think we discussed this before. The authentication software gets loaded from the nonvolatile memory and gets then loaded into RAM --

(Court reporter requested clarification.)

THE WITNESS: From external memory, which is nonvolatile memory, and gets stored into RAM, which is obviously temporary memory.

BY MR. KHAN:

Q. And I think you had also said that in some other implementations, it can be stored on the ROM --

A. That's correct, yes.

Q. -- in the processor; is that correct?

A. That's correct.

Q. And is the ROM temporary or permanent memory?

A. The ROM is permanent.

MR. KHAN: Just one second.

BY MR. KHAN:

Q. Could we turn to Claim -- so I'm hearing the echo again.

Can we turn to Claim 1 of the '766. Dr. Preneel, if could you let me know when you get

there.

A. That's fine. I have it in front of me.

Q. And in Claim 1, is it correct that the claim recites, "The electronic device having an operating system creating a run-time environment for user applications and authentication software running in a separate operating environment"? That's in column 18, lines 13 to 16.

A. That's correct.

Q. Is that correct?

A. That's correct.

Q. Is it correct that Claim 1 does not recite a BIOS?

A. That's correct.

(Audio disruption.)

BY MR. KHAN:

Q. Turning to paragraph 94 of your declaration, Dr. Preneel, if you could let me know when you're there.

A. Yes.

Q. You have a statement in paragraph 94 saying, about one, two, three -- seven -- six lines down, "However, every such read/data retrieval involves some sort of buffering: Most programming languages and operating systems buffer at least part of the I/O operations."

Do you see that?

A. I see that, yes.

Q. What's your understanding of what "buffering" means?

A. It means that there is no magic way to immediately transfer a byte or a series of bytes from the memory -- from one memory to the RAM of the processor.

And memories are typically read off in larger blocks and also the speeds of reading from the memory and writing to the other location are not always the same. So you have in between a buffer where information that's transferred is stored in between information being read from the source memory while -- before it's being written to the destination memory.

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

A. That's correct.

Q. And how long does the buffering normally take?

A. That depends on the relative speeds and on the

data sizes, of course.

Q. Could you give me an example?

A. Of course. I think main memory read speeds are on the order of -- data does not come from cache memory. It's hundreds of nanoseconds or delays before data can be read, and data comes also in quite large blocks. For example, if you --

(Court reporter requested clarification.)

THE WITNESS: -- if you read from hard disks, then it comes in blocks of 512 bytes, and this is typical order. It might be due to buffer, it needs to have several of those blocks, and so this is order of magnitude of those things. So you may have to store data for milliseconds and you may have to buffer kilobytes of data.

BY MR. KHAN:

Q. So while maybe -- so because you read -- correct me if I'm wrong. As you're reading certain chunks of memory and you'd store those chunks until you were able to write those chunks of memory and perhaps the duration of storage in the buffer may depend on the speed of your processor and the --

A. The latency and the speeds of the memory reads.

(Court reporter requested clarification.)

BY MR. KHAN:

Q. Okay. Can I ask you to open up the Ellison reference? That's Exhibit 1006, please.

A. Yes, I have it in front of me.

Q. Okay. And then may I ask you to turn to Figure 1C, please.

A. Can you repeat that? 1C?

Q. 1C, yes.

A. Okay. At this time I have that, yes.

Q. Okay. Thank you.

In Figure 1C, is it correct that there is a mass storage device 170?

A. Yes, that's correct.

Q. Is it correct that the system that's shown in Figure 1C also includes a CD-ROM 172, floppy drive 174, hard drive 176?

A. That is correct.

Q. Is it also true that this system includes I/O devices 175?

A. Yes, it does.

Q. Is it also correct that it includes a nonvolatile memory 160 that includes a processor nub 18?

A. Yes, it does.

Q. And typically what types of devices may be the I/O devices 175?

A. Of course, you have to go back a while. I guess it could have been screens or printers. At that time, we also -- I think we started seeing USB ports.

Q. And how about nonvolatile memory? What -- do you know what -- typically what would a nonvolatile memory be like, or what are different implementations of a nonvolatile memory?

A. A nonvolatile memory is typically an E2PROM I see with -- that can store information. It can also be rewritten. But even if the device overall loses power, the information stays in the memory.

Q. Is it correct that the nonvolatile memory can be a flash memory?

A. Yes, E2PROM is the same as flash, for your clarification. That's the informal name for E2PROM memory.

Q. Is the system in Ellison, through the I/O devices, capable of communicating with another device?

A. Yes, it can.

Q. In Figure 1C, do you see the ICH unit, input/output controller hub, 150?

A. Yes, I see this.

Q. What's the operation of the ICH 150?

A. Can you clarify the question? You mean the function? You mean how it works? What the goals are?

Or what specifically do you want to know?

Q. Yeah, so maybe I can -- I can be a little more precise here. Excuse that.

The ICH 150 includes a processor nub/executive loader; is that correct?

A. That's correct.

Q. Do you know what that loader -- how does that loader work -- loader at 52 work?

A. Well, I think that refers there to look at Figure 1A where it shows where this processor nub/executive loader is located in the isolated execution environment of Ellison and more specifically in the Ring-0.

(Court reporter requested clarification.)

BY MR. KHAN:

Q. Okay. And you mentioned the isolated environment.

What's -- scratch that. Sorry. The -- so system Figure 1 -- sorry.

Figure 1C also shows an MCH, the memory controller hub 130; is that correct?

A. That's correct.

Q. Is it possible to have multiple MCHs and multiple ICHs in Ellison's system?

A. As an engineer, I would say, yes, it's

possible. My general opinion is that the Ellison design is incredibly complex, and to have the value of making it even more complex is hard to see. But technically it would be feasible.

Q. And can the MCH be integrated with the ICH?

A. You can do that, but then you have a different design, but again different considerations, different security requirements. You can take all these blocks here and combine them in different ways, and you every time have different designs with different properties.

Q. Okay. Can I turn your attention to column 4 of Ellison at lines 46 to 51.

A. Okay. Shall I read it?

Q. Yes, please.

A. "The MCH may be integrated into a chipset that integrates multiple functionalities such as the isolated execution mode, host-to-peripheral bus interface" --

(Court reporter requested clarification.)

THE WITNESS: -- "host-to-peripheral bus interface, and memory control."

I think that's --

BY MR. KHAN:

Q. Could you read the next line too, please.

A. "Similarly, the ICH may also be integrated into a chipset together or separate from the MCH to

perform I/O functions."

I think that's consistent with my statement that you can combine these things. There is still different engineering approaches whether you combine those as separate building blocks on the same chip or multiple chips in a larger encapsulation or whether you really integrate this into a single device. And, yes, all these options are possible, and you actually get designs, I would argue, with different security and performance properties.

Q. I see.

So when the memory controller, MCH, is designed separately from the ICH and then compare that to the scenario where they're integrated together, is it -- is it accurate to say that the combined unit of the MCH and the ICH would be performing functions that are greater than just memory control? Right? That they would incorporate some of the functionalities of the ICH as noted in the blocks in Figure 1C such as the isolated execution logical processing manager and the other units there, the token bus interface.

Is that a fair statement to say that when you combine these two units, essentially perform the combination of the two, would it be limited to any one particular operation?

A. I think it would indeed be possible to combine these two in one operation, although I think in practice, you would still have two separate -- it would still be implemented in practice as two separate units inside the same housing or inside the same -- because their functions are very different.

Q. Okay.

MR. KHAN: I think we've come up to the one-hour mark. So I like using this as a good place to take a short break and come back in ten minutes, if that works for everyone.

THE WITNESS: That's fine.

MR. HENRY: Fine with me.

(Recess: 11:19 a.m. to 11:27 a.m.)

MR. KHAN: We have no further questions. So if Mr. Henry would like to redirect, or its his now.

MR. HENRY: Excellent. I do have a few questions.

EXAMINATION BY MR. HENRY:

Q. Dr. Preneel, can you please clarify what is the console in the '766 patent?

A. So the console is a simple piece of software that is being called by the BIOS and that manages access to the secure area. And so this console provides application programming interface, so an interface to

which calls can be made to authenticate specific transactions. It would even be possible in this case to actually go directly from user application to this --

(Court reporter requested clarification.)

THE WITNESS: I will repeat slowly.

It would be possible to also go directly from user application to the console API and bypassing the BIOS because the console can also manage access to the secure area.

BY MR. HENRY:

Q. All right. Then what distinguishes the console as depicted in Figure 3 from that depicted in Figure 5A?

A. Obviously in Figure 3, the console gets access to the secure area which is sitting in software above, and the console provides application interface to calls, for example, authentication software to authenticate transactions. In Figure 5, this authentication software is implemented in the hardware environment, and so if you would make from the user application a call to console, it would then call BIOS and hardware to get authentication software run.

So it remains the central place to invoke the authentication software. In Figure 3 is application -- authentication software runs in secure area in RAM. In

Figure 5A, it runs in the hardware environments.

Q. I'd like you to turn your attention to the subject of the keys, specifically the encryption key.

How does the use of the encryption key as set forth in the '766 patent -- what's -- let me be more specific.

In the embodiment that's more or less depicted in Figure 3 of the '766 patent, we have an encryption key, but you did agree that, you know, keys preexisted this patent application. So how does the use of the encryption key in the '766 patent, at least as depicted in Figure 3, how does it make -- count as a step forward distinguishing it from the prior art?

A. Because first, this encryption key makes this BIOS unique and specific for a particular user device or a particular user. And second, this BIOS encryption key can be used in the secure area to access other keys or it could also be used in principle in authentication software because a cryptographic key is a bit string that can also be used with authentication software. But typically, I would say it would be used to control access to other keys, and so it helps to protect the secure area and the key material in the secure area.

Q. All right. So how does that -- what you just described, how does that differentiate the claims of the

'766 patent, or specifically, say Claim 1, from the disclosure of Ellison?

MR. KHAN: Objection -- sorry. Objection. Form. And these -- the scope of the redirect should be based on the questions that I asked.

MR. HENRY: Well, you asked about Ellison.

MR. KHAN: I did not ask how they differentiated from Claim 1, which is your question.

MR. HENRY: All right. Are you going to let him answer the question?

THE WITNESS: So in Claim 1, in '766, a private key is provided in the secure area of the electronic device where it's inaccessible to the user and it's inaccessible to the operating system and it's also inaccessible to the users, and it can be directly used in an electronic transaction to protect the transaction of the user.

The Ellison patent also uses obviously cryptographic keys, but those keys are used to protect -- to separate and protect the secure environment from the regular environment. That's the fundamental difference.

BY MR. HENRY:

Q. Okay. You were asked previously, I think, about -- I'm paraphrasing, of course, but -- your

comment about -- in your declaration, you made a comment about the '766 patent being -- serve as a major step forward or having major steps forward over the prior art, right?

A. That's correct, yes.

Q. Can you please clarify again what are the major steps over the prior art?

A. I think the prior art was that, as I mentioned, people were doing transactions online already, and they're doing transactions in the physical world using bank cards, and online transactions were performed using browsers, and without providing a secure environment, which meant that if your device was compromised by malware, that would affect the user application or the operating system. That could also compromise transactions and lead to fraudulent transactions.

And so by providing in a simple and elegant way a secure environment, '766 makes it possible -- I think it's particular on an existing device without adding complex and expensive hardware and changing all of the software, but just software changes allowed secure transactions on an ordinary machine. It also provided options with much simpler hardware changes to provide secure transactions on an ordinary machine.

So I think many people had ideas on how to build very complex architectures for much more secure computers with secure and less secure environments, but '766 shows it's possible that if one focuses on transactions, and not on complete computer architectures, to actually have a simple and elegant solution that provides the necessary isolation and protection.

Q. During your earlier testimony, you discussed the topic of the authentication software possibly being -- for example, that's Number 54, authentication software -- being -- you used the term "public but nevertheless secure."

A. Yes.

Q. Can you please explain, at least for my edification, how it can be both public and secure?

A. It's important to understand that in cryptography there is an important principle called Kerckhoffs' principle -- K-E-R-C-K-H-O-F-F-S, apostrophe, the name is Kerckhoffs -- which states that the cryptographic method should remain secure, even if the algorithm itself is publicly known. The security of the algorithm should only rely on the secrecy of the key. And so authentication algorithm can be public, also the software or hardware implementing

authentication algorithm can be public. One only needs a secret key in the software to get protection of the transaction.

And in that sense, it does not matter whether the authentication software in the form of software -- software is actually public or not. Even if it's made publicly available for inspection, even if it follows a common standard, still the provided solution can be secure under the condition that there is a secret key in the secure area that can be input to the authentication software.

MR. HENRY: I don't have any more redirect questions. I pass the witness.

MR. KHAN: Thank you. I have one or two quick follow-up questions.

FURTHER EXAMINATION BY MR. KHAN:

Q. Dr. Preneel, you mentioned early in the redirect that the -- the BIOS could be bypassed because the console has the capabilities by itself to restrict access; is that correct?

A. That is correct, yes.

Q. Can you point to me where in the '766 patent it says the BIOS can be bypassed?

A. I'm afraid I would need more time to look this up.

Q. You can take your time.

A. I'm afraid that I can't point to a specific passage, but I also don't find the place where this would be made impossible.

Q. So what I understand you are saying is that your characterization of the BIOS was not something you found disclosed in the patent but something that you think is within the realm of possibility; is that correct?

A. This was a specific comment where we pointed out that one could implement the whole system also in bypassing the BIOS. I think what I said previously about the BIOS is still correct. That's essentially the BIOS -- and this is also what follows on Figure 3, that normally the user application goes to the OS and the BIOS, and the BIOS plays the role of separator or decider who gets access to the secure part of the memory.

Q. I can appreciate that. I think my comment was more directed towards, you know, the bypassing of the BIOS, right, and the console being able to fill in for the BIOS. And I think you were unable to find support when asked, and that's why I was clarifying your position in that you think it's possible, but it's not disclosed.

A. I could not point, indeed, to a location where it is disclosed.

Q. Thank you.

Also, was there anything in the redirect that -- Mr. Henry just asked you the questions. Was there anything in the redirect that contradicted what you said earlier, or do you think it was consistent with your --

A. I think it was consistent. I've tried my very best to be consistent. To the best of my recollection, I have been consistent.

MR. KHAN: Thank you very much. I have no further questions.

THE WITNESS: Thank you.

COURT REPORTER: Counsel, may I get transcript requests on the record, please?

MR. KHAN: Yes, if we could get a rough draft, like, soon -- like, as soon as possible, and then when do you think we can get the official transcript by?

COURT REPORTER: When would you like it?

MR. KHAN: What are the options?

COURT REPORTER: May we go off the record?

(Discussion off the record.)

THE REPORTER: And, Mr. Henry, did you want a copy, sir?

MR. HENRY: Yes, please.

(Whereupon the proceedings concluded at 11:48 a.m.)

ERRATA SHEET

NAME OF CASE: SAMSUNG ELECTRONICS CO., LTD. V. WARD PARTICIPATIONS B.V.
DATE OF DEPOSITION: NOVEMBER 1, 2022
NAME OF WITNESS: DR. BART PRENEEL

Reason Codes:

1: To clarify the record.
2: To conform to the facts.
3: To correct transcription error.

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

_____ _____
DR. BART PRENEEL DATED

DECLARATION UNDER PENALTY OF PERJURY

I, DR. BART PRENEEL, do hereby certify under penalty of perjury that I have read the foregoing transcript of my deposition taken on November 1, 2022; that I have made such corrections as appear noted on the Deposition Errata Page(s), attached hereto, signed by me; that my testimony as contained herein, as corrected, is true and correct.

This Declaration is executed this _____ day of _____, 20___, at _____, California.

_____

DR. BART PRENEEL

STATE OF CALIFORNIA)
) ss.
)

I, Tamara Houston, RPR, CCRR, CSR No. 7244, a Certified Shorthand Reporter in the State of California, duly empowered to administer oaths, do hereby certify:

That, prior to being examined, the witness named in the foregoing deposition was by me duly sworn to testify to the truth, the whole truth, and nothing but the truth;

That said deposition was taken down by me in shorthand at the time and place therein named, and thereafter reduced to typewriting by computer-aided transcription under my direction;

That the dismantling, unsealing, or unbinding of the original transcript will render the reporter's certification null and void.

I further certify that I am not interested in the event of the action.

In witness whereof, I have hereunto subscribed my name.

Dated: November 8, 2022

Tamara L. Houston

TAMARA L. HOUSTON
CSR 7244, RPR, CCRR 140