Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact

DeltaPatents B.V.
Fellenoord 370
5611 ZL Eindhoven
PAYS-BAS

Formalities officer
Strick, Marina

Date
25.05.2020

Reference	Application No./Patent No.
330.002 EPw	04748654.3 - 1010 / 1634140
Applicant/Proprietor	
Ward Participations B.V.	

EPA/EPO/OEB Formblatt/Form/Formulaire : 2310

Empfangsbescheinigung über den Zugang des vorstehend bezeichneten Schriftstücks
Acknowledgement of receipt of the document specified above
Récépissé du document spécifié ci-dessus

Unter Bezugnahme auf die Mitteilung im ABl EPA 7/2010, 377 wird gebeten, die Empfangsbescheinigung mit Empfangsdatum und Unterschrift zu versehen und **umgehend** an das EPA zurückzusenden:

With reference to the Notice in OJ EPO 7/2010, 377, you are requested to date and sign the acknowledgement of receipt and return it to the EPO **immediately**:

Conformément au communiqué paru au JO OEB 7/2010, 377, vous êtes prié d'indiquer sur le récépissé la date de réception du document, de signer le récépissé et de le renvoyer **sans délai** à l' OEB:

- **über die Online-Dienste des EPA** (als Anlage zu EPA Form 1038) / **through EPO Online Services** (as annex to EPO Form 1038) / **par les services en ligne de l'OEB** (en tant que pièce jointe au formulaire OEB 1038),
- **per Fax / by fax / par téléfax (+49 (0) 89 2399-4465 or +31 (0) 70 340-3016)**
- oder per Post / or by post / ou par courrier.

Empfangen am / Received on / Reçu le :

Unterschrift / Signature:

Empfangsberechtigter/authorised recipient/
le destinataire ou la personne dûment mandatée

Rücksende-Adresse / Return address / Adresse de retour
(Umschlag / envelope / enveloppe ISO C4 / DL / C6/C5 / C6)

Europäisches Patentamt
80298 MÜNCHEN
DEUTSCHLAND

Rücksende-Adresse / Return address / Adresse de retour

EPA/EPO/OEB Form 2936 08.10

MS50949

SAMSUNG 1016

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact

DeltaPatents B.V.
Fellenoord 370
5611 ZL Eindhoven
PAYS-BAS

Date
25.05.2020

Reference	Application No./Patent No.
330.002 EPw	04748654.3 - 1010 / 1634140
Applicant/Proprietor	
Ward Participations B.V.	

Summons to attend oral proceedings pursuant to Rule 115(1) EPC

You are hereby summoned to attend oral proceedings arranged in connection with the above-mentioned European patent.

The matters to be discussed are set out in the communication accompanying this summons (EPO Form 2906).

The oral proceedings, which will be public, will take place before the opposition division

on 07.12.20 at 09.00 hrs in Room 2453
at the EPO, Bayerstr. 34, PschorrHöfe, D-80335 München

No changes to the date of the oral proceedings can be made, except on serious grounds (see OJ EPO 1/2009, 68). If you do not appear as summoned, the oral proceedings may continue without you (R. 115(2) EPC).

Your attention is drawn to Rule 4 EPC, regarding the language of the oral proceedings, and to the Special edition No. 3 OJ EPO 2007, 128, concerning the filing of authorisations for company employees and lawyers acting as representatives before the EPO.

The final date for making written submissions and/or amendments (R. 116 EPC) is 07.10.20.

You are requested to report in good time beforehand to the porter in the EPO foyer. Room 3473 and 3474 are available as waiting rooms.

Parking is available in the underground car park, accessible only via the entrance "Grasserstrasse 2/6". On presentation of the summons to oral proceedings at one of the porters' lodges in the PschorrHöfe, the parking ticket will be revoked.

1st Examiner:	2nd Examiner:	Chairman:
Hijazi, Ali	Kleiber, Michael	Pavón Mayo, Manuel

For the Opposition Division

Annexes:
Confirmation of receipt (Form 2936)
Rule 4 EPC (EPC Form 2043)
Communication (EPO Form 2906)

Europäisches Patentamt • European Patent Office • Office européen des brevets

Registered letter to EPO postal service: 18.05.20

State of the proceedings

I. European patent N°1 634 140 B1 entitled *"METHOD AND SYSTEM FOR PERFORMING A TRANSACTION AND FOR PERFORMING A VERIFICATION OF LEGITIMATE ACCESS TO, OR USE OF DIGITAL DATA"* is based on European patent application N°04 748 654.3 (international application number PCT/NL2004/000 422). The patent Proprietor is
Ward Participations B.V.
De Schaepstal 1, 1251 MZ Laren, NL.
The mention of the grant of the patent was published in European Patent Bulletin 2019/03 on 16-01-2019. The patent claims the following priority: PCT/NL03/00436 filed on 13-06-2003

II. A notice of opposition against the patent has been filed on 16-10-2019 by:

Samsung Electronics Benelux B.V.
Evert van de Beekstraat 310
1118 CX Schiphol, NL

III. The Opponent submitted that the subject-matter of the patent was not patentable according to Article 100(a) EPC (Article 52(1) EPC; Articles 54 and 56 EPC) and Article 100(c) EPC. He requested to revoke the patent in its entirety and auxiliarily to arrange an oral proceedings according to Article 116 EPC.

IV. The following documents were cited by the Opponent in support of his requests:

E1 WO 2004/015579 A1 (TREK 2000 INT LTD [SG]; OOI CHIN SHYAN RAYMOND [SG] ET AL.) 19 February 2004 (2004-02-19)

E2 "Client Security Software Version 5.0 Installation Guide", IBM Client Security Solutions, September 2002 ;

E2a "IBM Improves PC Security System", IBM News room, 4 October 2002 (2002-10-04), pages 1-2, URL:https://www-03.ibm.com/press/us/en/pressrelease/485.wss ;

E2b "Embedded Security Chip and Software - a white paper", IBM Client Security Solutions, 1999, pages 1-6 ;

E2c "Client Security Software Version 1.0 Administrator's Guide", IBM Client Security Solutions, December 1999

E3 US 5 892 900 A (GINTER KARL L [US] ET AL) 6 April 1999 (1999-04-06)

E4 US 2002/007456 A1 (PEINADO MARCUS [US] ET AL) 17 January 2002 (2002-01-17)

E5 US 2002/023215 A1 (WANG YNJIUN P [US] ET AL) 21 February 2002 (2002-02-21)

E6 EP 1 076 279 A1 (HEWLETT PACKARD CO [US]) 14 February 2001 (2001-02-14)

E7 WO 01/17296 A1 (ERICSSON TELEFON AB L M [SE]) 8 March 2001 (2001-03-08)

E8 WO 02/076127 A1 (QUALCOMM INC [US]) 26 September 2002 (2002-09-26)

E9 GB 2 338 381 A (BARCLAYS BANK PLC [GB]) 15 December 1999 (1999-12-15)

E10 EP 1 237 324 A (SANYO ELECTRIC CO [JP]; PFU LTD [JP]; FUJITSU LTD [JP]; HITACHI LTD [J) 4 September 2002 (2002-09-04)

E11 WO 01/84319 A (XTEC INC [US]) 8 November 2001 (2001-11-08)

E12 WO 02/47081 A (SANDISK CORP [US]) 13 June 2002 (2002-06-13)

E13 US 5 802 590 A (DRAVES RICHARD P [US]) 1 September 1998 (1998-09-01)

E14 US 2001/051996 A1 (COOPER ROBIN ROSS [US] ET AL) 13 December 2001 (2001-12-13)

E15 US 2002/112162 A1 (COCOTIS THOMAS ANDREW [US] ET AL) 15 August 2002 (2002-08-15)

E16 US 2002/112171 A1 (GINTER KARL L [US] ET AL) 15 August 2002 (2002-08-15)

E17 US 2003/039362 A1 (CALIFANO ANDREA [US] ET AL) 27 February 2003 (2003-02-27)

E18 BENNET YEE: "Using Secure Coprocessors", THESIS SUBMITTED TO THE SCHOOL OF COMPUTER SCIENCE FOR THE DEGREE OF DOCTOR OF PHILOSOPHY, May 1994

E19 WO 00/67143 A2 (UNICATE BV [NL]; SIPMAN WILHELMUS HENDRIKUS MAR [NL] ET AL.) 9 November 2000 (2000-11-09)

E20 US 5 354 097 A (TEL TEUNIS [NL]) 11 October 1994 (1994-10-11)

E21 GERALD J POPEK ET AL: "Encryption and Secure Computer Networks", ACM COMPUTING SURVEYS, ACM, NEW YORK, NY, US, US, vol. 11, no. 4, December 1979, pages 331-356, ISSN: 0360-0300, DOI: 10.1145/356789.356794

V. With a letter, received on 03-03-2020, the Patentee filed observations concerning the opposition and requested to reject the opposition. Furthermore, he auxiliarily requested oral proceedings according to Article 116 EPC to take place.

Points to be discussed

1 Since both parties have requested oral proceedings as an auxiliary measure, the parties are hereby invited to attend such proceedings.

2 The points which need to be discussed are set out below and a provisional, non-binding opinion of the Opposition Division is given on the positions adopted by the parties. However, the discussion may cover further points according to the circumstances. The parties are asked to make their submissions well in advance of the date of the oral proceedings, i.e. at the latest at the date set in this summons, especially if new sets of claims or lines of argumentations are to be considered during oral proceedings.

3 The attention of all parties is drawn to the Guidelines E-III, 8.5 concerning submissions by the parties.

4 The present patent is based on an application filed before 13.12.2007, i.e. before the EPC 2000 is entered into force, and therefore in accordance with the transitional provisions as decided by the Administrative Council some of the provisions of the EPC 2000 are to be applied while other provisions of the EPC 1973 still apply. As the Euro-PCT at the basis of the patent in suit was still pending on 13.12.2007, Article 54(4) EPC 1973 and therefore Rule 23a EPC 1973 apply in the present case. For the rest, in the present case, no substantial difference could be detected between both provisions to be applied concretely and therefore for simplicity reasons it is referred merely to the EPC 2000, i.e. EPC unless otherwise mentioned.

5 In parallel to this opposition another opposition has been filed against the patent based on a divisional application of the application forming the basis of the patent discussed below. The Opposition Division will have the same composition in both cases and the intention is to have the oral proceedings on two consecutive days. In case the discussions would take longer than foreseen, it is planed to have a third day as a backup in order to avoid any postponement.

6 In order to ease the discussion, the features breakdown used by the opponent for the independent claims is also taken by the Opposition Division.

Claim 1:

M1: Method for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party,

M2: the electronic device having an operating system (48) creating a run-time environment for user applications

M3: and authentication software (54) running in a separate operating environment, independent from and inaccessible to said operating system, (48)

M4: the electronic device having a memory comprising

M4.1: storage locations, part of the memory being accessible to the operating system, (48)

M4.2: part of the memory being a secure area (62) storage locations of which are not reported to the operating system, (48)

the method comprising:

M5: providing authentication data (63A) in the secure area (62) of said electronic device

M5.1: which authentication data (63A) are inaccessible to a user of said electronic device,

M5.2: wherein said secure area (62) is inaccessible to said operating system (48) of said electronic device, thereby rendering the authentication data (63A) inaccessible to said user;

M6: providing authentication software (54) in said electronic device,

M6.1: the authentication data (63A) being accessible to said authentication software, (54) wherein the authentication software (54) is stored in the secure area (62) inaccessible to said operating system;(*) (48)

M6.2: activating the authentication software (54) to generate a digital signature from the authentication data, (63A)

M6.3: wherein the authentication software (54) is run in a secure processing environment inaccessible to said operating system;(*) (48)

M7: providing the digital signature to the second transaction party.

(*) Note: the Druckexemplar mentions a ";" which is not present on the B1 publication of the patent.

Claim 23:

S1: System for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party,

S2: the electronic device having an operating system creating a run-time environment for user applications

S3: and authentication software running in a separate operating environment, independent from and inaccessible to said operating system,

S4: the electronic device having a memory comprising

S4.1: storage locations, part of the memory being accessible to the operating system,

S4.2: part of the memory being a secure area storage locations of which are not reported to the operating system,

the system comprising:

S5: means for providing authentication data in the secure area of said electronic device

S5.1: which authentication data are inaccessible to a user of the electronic device,

S5.2: wherein said secure area is inaccessible to said operating system of said electronic device, thereby rendering the authentication data inaccessible to said user;

S6: means for providing authentication software in said electronic device,

S6.1: the authentication data being accessible to said authentication software, wherein the authentication software is stored in the secure area inaccessible to said operating system;

S6.2: means for activating the authentication software to generate a digital signature from the authentication data,

S6.3: wherein the authentication software is run in a secure processing environment inaccessible to said operating system;

S7: means for providing the digital signature to the second transaction party.

Claim 24:

E1: Electronic device for performing an electronic transaction between a first transaction party and a second transaction party, wherein the electronic device is operated by the first transaction party,

E2: the electronic device having an operating system creating a run-time environment for user applications

E3: and authentication software running in a separate operating environment, independent from and inaccessible to said operating system,

E4: the electronic device having a memory comprising

E4.1: storage locations, part of the memory being accessible to the operating system,

E4.2: part of the memory being a secure area storage locations of which are not reported to the operating system,

E5: the secure area storing authentication data

E5.1: which are inaccessible to a user of the electronic device,

E5.2: wherein said secure area is inaccessible to said operating system of said electronic device, thereby rendering the authentication data inaccessible to said user;

the electronic device comprising:

E6: a memory storing authentication software,

E6.1: the authentication data being accessible to said authentication software, wherein the authentication software is stored in the secure area inaccessible to said operating system;

E6.2: means for activating the authentication software to generate a digital signature from the authentication data,

E6.3: wherein the authentication software is run in a secure processing environment inaccessible to said operating system; and

E7: means for providing the digital signature to the second transaction party.

Article 100(c) EPC

7 Claim 1.

7.1 Generally, the subject-matter of claim 1 appears to be mainly based on claims 1, 26 and 27 of the application as originally filed WO 2004/111752 A2 (in the following called D2, like done by the Opponent). In addition, the operating system, the memory and the authentication software have been further specified based on the description.

7.2 Feature M1.

This feature was already present in claim 1 of D2.

7.3 Feature M2.

The Opponent has challenged the lack of basis of feature M2 in the originally filed application mainly on the ground that the only passage explicitly disclosing this definition (page 13, lines 23-24 of D2) is to be read in the context of the embodiment of Fig. 3 which discloses other components.

The Opposition Division is of the provisional opinion that this feature, although only explicitly present at one place in D2, is nothing more than providing the definition of what an operating system is and generally applies to the whole disclosure (see also point 4 of the decision T 0248/17).

7.4 Feature M3.

Page 7, lines 31-34 discloses that the authentication software is independent from and inaccessible to the operating system on the device. However, it is also specified there that the separate operating environment is in the BIOS or in a console. The Opposition Division has therefore some doubts that this feature has a basis in its present generality in D2.

7.5 Features M4 to M4.2.

The Opponent has argued that no part of D2 discloses a memory which comprises a combination of parts that are accessible and non-accessible to the operating system.

The Opposition Division notes the following:

Feature M4. The claim mentions a memory in general (and not for instance a memory module), while this aspect was already present in claim 1 of D2 (the authentication data is provided in a memory of said electronic device). It is not specified whether this memory is formed of one or several physical memory parts and where this memory is located. Generally speaking a memory must be present in an electronic device as claimed, independently of the embodiment considered, and a memory, as a matter of definition, comprises a storage location. Feature M4 appears therefore to have a basis in D2.

Feature M4.1. Page 11, lines 9-12 of D2 discloses that a secure memory location has to be provided as a part of a secure memory or it may be an encrypted part of a non-secure memory (therefore a non-secure memory is defined). At least a part of this memory is also accessible to the operating system (page 15, lines 11-14). In addition, this feature, as such, appears to be a common aspect of any operating system.

Feature M4.2. Page 14, lines 12-13, it is stated that in or behind the console 52, there is a secure area 62 only accessible to the BIOS. At page 7, lines 28-29, it is stated that the secure part of the device is accessible only to the BIOS. It is further stated (lines 13+) that the secure area 62 comprises applications and storage locations, which are not reported to the operating system 48. Later (lines 35+) it is stated that the secure area may further comprises other ... memory locations. Such a secure area appears therefore to be part of a memory.
Page 15, lines 21+ discloses that the authentication data is stored in a memory that is accessible to an operating system of the device and possibly to a user of said device. Page 18, lines 12+ appears to relate to a similar embodiment as far as this aspect is concerned. However, it is stated in that embodiment that the secure area 62 is not essential for performing the third embodiment (contrary to the part starting at page 15, line 21 which still appears to comprise a secure area 62). As argued indirectly by the Opponent, the embodiment starting at page 18, line 12 does not appear to be covered by claim 1.

The question which still arises is which link, if any, is to be made between features M4.1 and M4.2 and the BIOS (and possibly the console).

In the paragraph bridging pages 5 and 6 it is mentioned that in the context of the installation method a new device contains a BIOS and an existing device also contains such BIOS. It is also specified that the BIOS is used to access a memory location in a memory. This part appears to relate to all described embodiments. See with that regard page 5, line 19 and the reference to Figs. 1, 2, 4 and 6-9, while both Figs. 3 and 5A,B disclose the BIOS; access to a removable memory - Fig. 10 - is also to be done via the BIOS, see e.g. page 13, line 10.

Therefore, in the light of these passages, the Opposition Division has also doubts that the BIOS can be omitted from the combination of features M4-M4.2 without extending the content of the application as filed.

The fact that independent claim 1 of D2 does not mention the BIOS does not provide any technical teaching providing such a justification as the aspects related to the secure area have been taken from the description. The same applies in relation with page 2 of D2 quoted by the Patentee which appears to be directed to a mere repetition of the claims of D2. The decision of the BoA does not appear to provide a justification for the present generality either, as the claim pending at the time did have a reference to the BIOS.

7.6 Features M5 to M5.2.

In section B.I.3. of the notice of opposition, the Opponent argues that there is neither explicit nor implicit support for features M4 to M5.2.

The Opposition Division notes the following:

Features M4 to M4.2 have been discussed in the section above.

Features M5 and M5.1. These features were already present in claim 1 of D2 apart that secure area instead of memory is now used which appears to have a basis in e.g. Fig. 3 (see also the discussion above concerning feature M4.2). Concerning the expression "authentication data", the Opposition Division notes that this feature was present in the claim 1 of D2 which is supposed to cover all embodiments of D2. It is nevertheless noted that the specific embodiments of Figs. 1 and 2 appear to refer to an "authentication table" instead (see e.g. the random table supplier, page 6, line 17 and the random table lines 21-23). It is however noted that page 15, line 12 of D2 appears to provide the idea that an authentication table is an example for authentication data in general. Lastly, it is noted that a table can have one or several dimensions so that any data in a memory could possibly be considered as being part of the authentication table

in the absence of any definition for it. All in all, the Opposition Division is of the provisional opinion that "authentication data" in connection with the secure area as claimed is having a basis in D2, i.e. features M5 and M5.1 have such a basis.

Feature M5.2. This feature is repeating feature M4.2 with a slightly different wording. As the secure area is not reported/inaccessible to the OS it is de facto rendering the data in it inaccessible to the user.

Therefore, the Opposition Division is of the provisional opinion that the features M5 to M5.2 have a basis in D2, as far as features M4 to M4.2 have such a basis.

7.7 Features M6 to M6.3.

These features were not challenged by the Opponent.

Feature M6 and the first part of feature M6.1 appears to have a basis in claim 1 of D2.

Second part of feature M6.1 (starting at wherein).

Feature M6.2 appears to have a basis in claim 1 of D2. Fig. 3 appears to show that the authentication software is stored in the secure area 62 (see also page 14, lines 31-34).

Feature M6.3 appears to have a basis in claim 27 of D2.

A basis in D2 for these features appears therefore to be present.

7.8 Feature M7.

This feature was not challenged by the Opponent and was present in claim 1 of D2.

8 Independent claim 23.

Claim 23 is directed to a system for performing an electronic transaction, is based on claim 29 of D2 and corresponds for the rest to claim 1 in terms of means for. The same comments as made above for claim 1 apply mutatis mutandis.

9 Independent claim 24.

Claim 24 is directed to an electronic device for performing an electronic transaction and mostly takes back the features of claim 1. The same comments as made above for claim 1 apply mutatis mutandis.

10 Dependent claim 5.

The additional features of claim 5 appear to be based on page 8, lines 28-29 of D2. Whether the authentication software is to be defined in relation with the BIOS as argued by the Opponent will have to be discussed possibly also in connection with the independent claims.

11 Dependent claim 7.

The additional features of claim 7 appear to be based on claim 11 of D2 which depends on claim 10 of D2, itself forming the basis of claim 6 of the patent in suit. No key is present in claim 1 of the patent so that the argumentation of the Opponent cannot be followed.

12 Dependent claim 8.

The additional features of claim 8 appear to originate from page 14, lines 31-34 of D2. Whether these features have been taken out of their context or not will have to be assessed depending on the results of the discussion concerning feature M4.2 which defines the secure area 62.

13 Dependent claim 9.

The additional features of claim 9 appear to originate from page 15, lines 8-10 of D2. Again, whether these features have been taken out of their context or not will have to be assessed depending on the results of the discussion concerning feature M4.2 which defines the secure area 62.

14 Dependent claim 20.

The additional features of claim 20 appear to be based on claim 18 of D2. However, the dependencies of this claim as yet specified (claims 14 to 19) does not appear to have a basis in D2. Claim 18 of D2 was only depending on claims

14 to 17 of D2 which are not corresponding to claims 14 to 19 of the patent. The Opposition Division has doubts that no new combination was thereby introduced.

15 Dependent claim 21.

The parties appear to agree that the relevant part for seeking a basis for this claim is the passage starting at page 19, line 24 to page 20, line 8. The Opponent objects to claim 21 and argues that the specific sequence ("before...") is not explicitly disclosed in D2 and that these features have been extracted and isolated from the embodiment of Fig. 6. The Patentee argues that the above quoted passage is providing a basis for claim 21. The Opposition Division has doubts that this is the case, already because this embodiment appears to refer to the BIOS which is not present in claim 1 on which claim 21 depends but also because these features appear to have been extracted from the embodiment of Fig. 6. It will therefore have to be discussed whether a direct and unambiguous disclosure for claim 21 can be found in D2.

16 Dependent claim 22.

The additional features of claim 22 appear to be partly disclosed at page 8, line 29. Concerning the "two" private encryption keys (one in claim 5 and one in claim 22), this appears to be more a clarity problem than a lack of basis in D2. The general context of D2 appears to relate to digital data in connection with the encryption key, see page 3, lines 7-9. It will have to be discussed whether the new multiple dependencies have a basis in D2.

17 Other dependent claims. The Opposition Division notes provisionally the following:

17.1 Claims 2 to 4 appear to have a basis in claims 5 to 7 of D2.

17.2 Claims 6 and 7 appear to have a basis in claims 10 and 11.

17.3 Claim 10 appears to have a basis in claim 14.

17.4 Claim 11 appears to have some basis in page 19, lines 14-17. However, this part appears to relate to an embodiment possibly not covered by the present independent claims.

17.5 Claim 12 appears to have a basis in claim 15. However, it is not immediately apparent what is the basis for the new dependency structure. Furthermore, this aspect appears to relate to the embodiment where the memory is accessible to the user/OS, see e.g. page 17, lines 20-21, and therefore, it will have to be discussed whether this aspect can be combined with the features of claim 1.

17.6 Claims 13, 14. These claims appear to have some basis at page 17, line 32 to page 18, line 4. However, these parts refer to a second encryption layer not necessarily presently claimed as this aspect is only present starting at claim 12. Furthermore, it is not immediately apparent what is the basis for the new dependency structure.

17.7 Claim 15 appears to have a basis in claim 16.

17.8 Claim 16 appears to have a basis in claim 17, however, here also, it is not immediately apparent what the basis is for the new dependency structure.

17.9 Claims 17, 18 appear to have some basis page 19, lines 5-8. However, this part appears to relate to an embodiment possibly not covered by the independent claims. The reference to Fig. 3 shows that some aspect(s) of the first embodiment might be incorporated in the embodiment of Fig. 5A. The contrary does not appear, however, to be mentioned.

17.10 Claim 19 appears to have some basis page 26, lines 32-35 which, however, also appears to relate to an embodiment (where the memory is accessible to the user/OS) not covered by the present independent claims.

17.11 Claim 25. The only part which appears to provide some basis for this claim is page 12, lines 31-36. However, that this device should contain a BIOS appears mandatory in this passage. A clear basis for this claim is therefore not immediately apparent.

18 As a conclusion, although most of the features of the claims appear to have some basis in D2, it is not always immediately apparent whether the presently claimed combinations (including mixing of different embodiments) can be derived directly and unambiguously from the originally filed application. The provisional opinion of the Opposition Division is therefore that the subject-matter of the patent appears to extend beyond the content of the application as filed.

Article 100(a) in combination with Articles 52, 54 and 56 EPC

19 The Opponent has submitted that the subject-matter of claim 1 is not novel in view of E1, E2/E2a, E3, E5, E6, E8 and auxiliarily not inventive in view of E2/ E2a. The provisional opinion of the Opposition Division is as follows.

20 Validity of the priority claim with regard to the independent claims.

20.1 The Opponent has brought two lines of attack with regard to the priority.

20.1.1 First argumentation, concerning the feature M2.

The Opposition Division refers to point 7.3 above and provisionally does not see that the presence of this feature would lead to a loss of the priority right.

20.1.2 Second argumentation, concerning the absence in claim 1 of the patent in suit of the feature "providing digital data from the second transaction party to the first transaction party".

The Opposition Division tends to follow the argumentation of the Patentee that page 14, lines 10-15 and page 15 (lines 24-26) provides some support for omitting the last feature of claim 1 of the priority document, i.e. this feature is not an essential feature missing in claim 1 of the patent, which would lead to a loss of priority.

In case the Opposition Division would change its opinion on this, e.g. during oral proceedings in the light of arguments submitted by the parties, the Opposition Division has doubts that G 1/15 can be applied as it concerns generic "OR"-claims. Here the absence of an essential feature does not appear to fall under this category.

20.2 Similar considerations apply to independent claims 23 and 24.

21 Novelty over E1.

21.1 E1 has a publication date of 19.02.2004, i.e. after the priority date of the patent in suit (13.06.2003) but before its filing date (14.06.2004). The filing date of E1 is before the priority date of the patent in suit so that the validity of the priority of E1 is of no importance. E1 is a PCT application which had validly entered the European phase on 21.05.2004 in the form of an Euro-PCT application EP 03 713 173 and was still pending at the time of entry into force of the EPC 2000.

Article 158(1) and (2) EPC 1973 applies to the Euro-PCT of E1. In view of the provisional opinion mentioned above concerning the priority of the patent in suit, this document is therefore a document according to Article 54(3), (4) EPC 1973, i.e. only relevant for novelty. For simplicity reasons, reference to E1 is kept in the following, since the WO publication document corresponds to the publication of the Euro-PCT application.

21.2 E1 relates to a secured access to restricted information over the networks (page 1, lines 6+). Figs. 1 to 4 disclose four embodiments of an authentication system to verify a password from a host, Fig. 5 relates to a method for such authentication, Figs. 6-8 are directed to some specific system implementations, Fig. 9 is a block diagram of a SAKE (storage anti-piracy key encryption) implementation, while Figs. 10 and 11 are directed to further embodiments of related methods.

21.3 The Opponent presents an argumentation against the subject-matter of claim 1 by using parts of E1 which relate to Figs. 1, 2, 4, 7 and 9 and which appear to concern different embodiments of the invention disclosed in E1. As argued by the Patentee it is not immediately apparent how these embodiments can be combined, as no real link between them appears to be made in E1. Further to that, at least E1 does not appear to disclose the generation of a digital signature which is understood as a code which can act as a signature. A yes or no (verification of a password) does not appear to be such a signature.

21.4 Therefore, the subject-matter of independent claims 1, 23 and 24 appears to be new in view of E1, inventive step from E1 not being an issue at present (see point 21.1 above).

22 Novelty over E2a/E2.

22.1 Publication dates.

It appears undisputed that E2a has a publication date of 04.10.2002 in view of the date it bears.

Concerning E2, the following is noted:

It is referred in E2a to the Client Security Software, Version 5.0 (which installation guide is E2). There it is stated the availability of this software is scheduled for November 2002 while the Installation Guide itself bares the date of September 2002. All these dates are well before (more than six months) the priority date of the patent in suit. It is further noted that the version 5.1 was announced with a press release dated 15.04.2003 with an availability for May 2003 (https://www-03.ibm.com/press/us/en/pressrelease/240.wss), which is also before the priority date of the patent.

The Opposition Division is therefore of the provisional opinion that the Client Security Software, Version 5.0, was released before the priority date and therefore that E2, being its installation guide, was also available before the priority date.

22.2 E2a/E2 is to be considered as one document or not?

The Opposition Division tends to accept that starting from E2a, the link to E2 is precise enough to justify considering both teachings together. The fact that the E2 was possibly not available at the time E2a was published is not considered by the Opposition Division to prevent this view. The Guidelines G-IV, 8 refers to a decision of the BoA T 153/85 which does not appear to mention such criteria (see section 4.2 of the decision). The Opposition Division tends also to consider that the date to be considered when assessing the combination is the date of the latest of the two, here E2, which is anyway before the priority date of the patent in suit (see section 22.1).

The contrary (starting from E2) does not appear to be true as no mention of the press release appears to be present in E2.

Lastly, the Patentee has expressed some doubts as to whether a press release can be regarded to provide a technical disclosure. The Opposition Division is of the opinion that the state of the art comprises everything made available to the public (Article 54(2) EPC) and therefore that such type of document also belongs to the prior art which must be taken into consideration when assessing the patentability of a claim, as it mentions in it some technical aspects referring to existing systems, i.e. it provides some technical teaching.

22.3 E2a/E2 discloses:

M1: An Embedded Security Subsystem is offered on notebooks and desktops, the user of which is the first transaction party (first paragraph). The second paragraph mentions that the subsystem consists of both a hardware component, the cryptographic security chip, which supports key storage, privacy encryption and digital signatures for authentication of identity, and a downloadable software component, the Client Security Software, which interfaces with the user and with other software applications. The sixth paragraph quoted by the Opponent discloses that the Client Security Software is providing interoperability with IBM Tivoli Access Manager which is used to manage security policies. This allows consistent security policy enforcement across the organization for a wide range of Web and application resources. These resources may be seen as the second transaction party.

M2: See page 3 of E2 which discloses the required operating systems. As mentioned under point 7.3 any such OS is creating a run-time environment for user applications.

M3: Page 1 last sentence of E2 discloses that the Security Chip is encrypting and storing keys. An authentication software is therefore present in a separate environment. However, for similar reasons as those argued by the Patentee, the Opposition Division has doubts that this environment can be qualified as inaccessible to the operating system due to the access to the chip by a software running under the OS (for instance the Client Security Software).

M4,
M4.1: A notebook or desktop as mentioned in E2a comprises such features.

M4.2: The Security Chip includes some memory used to store keys and which can be qualified as providing a secure area, as the Secure Chip is not a normal component (like the hard disk for instance) used to store data (see E2a or page 3 of E2 as quoted above). However, it does not appear to be unambiguously disclosed that these storage locations are not reported to the OS.

M5: As mentioned above, the Security Chip includes some secure area used to e.g. store keys.

M5.1: As mentioned in E2a, second paragraph, the Client Security Software interfaces with the user and with other software applications.The authentication data appears therefore to be generally inaccessible to the user.

M5.2: This feature further repeats the definition of the secure area which was given in M4.2, which the Opposition Division does not see as being disclosed in E2a/E2, while at the same time further defining what is meant with the inaccessibility to the user. Hence, this feature does not appear to be disclosed in E2a/E2.

M6: An authentication software is disclosed in E2a/e2, see feature M3 above.

M6.1: The authentication data of the Secure Chip are accessible to the authentication software of the same chip. However, as mentioned above (M4.2), it does not appear to be disclosed that the secure area (of the chip) is inaccessible to the OS.

M6.2: E2a, second and third paragraph, appears to disclose part of this feature in that signatures are mentioned in connection with the Secure Chip ("supports"). The Opposition Division could not, however, corroborate that the Secure Chip is generating signatures through a software stored in itself.

M6.3: As mentioned in connection with M3, the Opposition Division has some doubts that it is directly an unambiguously disclosed that the secure processing environment of the chip is inaccessible to the OS.

M7: What is done with the signature mentioned in E2a is also not explicitly mentioned in E2a so that this feature also does not appear to be directly and unambiguously disclosed.

22.4 As a conclusion, the subject-matter of claim 1 appears to be novel in view of E2a/E2.

23 Novelty over E3.

23.1 E3 discloses:

M1: See e.g. the Virtual Distribution Environment (VDE) of Fig. 1. Col. 60, lines 8+ mentions that the VDE participants (i.e. each participant is a transaction party) may have an electronic appliance which may be or contains a computer. Fig. 7 discloses an example of VDE electronic appliance.

M2: As at least some of the appliances are meant to be used by consumers, it can be safely assumed that an OS must be present when the appliance is a computer. Such operating system appears to be called Rights Operating System (ROS) 602, see Col. 61, lines 21-22. The ROS is described starting at Col. 80, line 6. The ROS supports user application(s) 608 in addition to rights and auditing operating system functions 604 and other OS functions 606.

M3: Fig. 6 shows a Secure Processing Environment (SPE) 503 which is further described starting at Col. 112, line 1 and which is supported by the hardware resources of a Secure processing Unit (SPU) 500 (Col. 112, lines 12-13). The SPE is understood by the Opposition Division as a software which does not appear to be necessarily part of the SPU 500 as argued by the Opponent. The SPE includes an Authentication Manager 564 which can be seen as an authentication software within the meaning of feature M3. It is however stated at Col. 82, lines 55+ that the ROS manages the hardware (e.g. CPU, memory and encrypt/decrypt engines within the SPU 500). Therefore, the SPE 503 does not appear to be inaccessible to the ROS contrary to the requirement of feature M3. Fig. 7 or Col. 60, lines 13-14 do not appear to provide support for the contention that the ROS is left outside of the SPU 500 or SPE 503.

M4, M4.1: Fig. 7, Col. 82, lines 61+: the ROS managed the hardware like memories other than within SPU. These parts are accessible to the ROS.

M4.2: For this feature, the Opposition Division tends to follow the position of the Patentee. The memory manager 578 is part of the kernel 552 (Fig. 13) which is itself part of the SPE 503 (Fig. 13) itself part of the ROS (Fig. 12). Therefore, the parts of the memory driven by the memory manager do not appear to be "not reported to the operating system", rather merely their use is restricted to some specific processes of the ROS.

M5: From Col. 71, lines 28+ it can be read that sensitive information, such as encryption keys, is stored in the NVRAM 534b. The Opposition Division tends to consider such keys as being authentication data in the general sense of this term.

M5.1, M5.2: The secure area (the NVRAM 534b) is not inaccessible to the operating system (the ROS, see above feature M3) and as a consequence the Opposition Division tends to consider that it is de facto not inaccessible to the user within the meaning of features M5.1 and M5.2.

M6: An authentication software is provided, see above feature M3.

M6.1: The authentication manager 564 is part of the SPE 503 (Col. 112). The authentication data appear therefore to be accessible to the manager (whether they are really accessed and for what purpose does not appear to be disclosed). It is not clear to the Opposition Division where the manager 564 is stored and even if it was accepted that it is stored in the secure area defined in feature M5, this area appears to be accessible to the ROS (see above features M5.1, M5.2).

M6.2: The Opposition Division tends to follow the argumentation of the Patentee. The first line of attack of the Opponent refers to the Ticket Services mention at Col. 130, lines 32+. The tickets mentioned at Col. 131 are requested by the VDE and returned to it, i.e. a digital signature generated by the authentication manager does not appear to be explicitly present in E3. It will have however to be discussed during oral proceedings whether such ticket can be interpreted as being an example of a signature within the meaning of the claim.
The second line of attack refers to the embodiment of Fig. 71 and more specifically to Col. 257, lines 33-36. From this part, it is however not immediately apparent who is generating this signature and whether this signature is provided to the second transaction party (for feature M7)

M6.3: As mentioned in connection with feature M3, the Opposition Division has some doubts that the secure processing environment of the authentication software is inaccessible to the ROS.

M7: In view of the opinion provided above for feature M6.2, this feature does not appear to be disclosed in E3 either.

23.2 As a conclusion, the subject-matter of claim 1 appears to be novel in view of E3.

24 Novelty over E5.

24.1 E5 discloses:

M1: Fig. 2 and e.g. paragraph 0104. The first transaction party is the user of the electronic device which includes the PEAD 200 (see also paragraphs 0067 and 0072), the second transaction party is the server 1302.

M2: The PDAs given as examples in paragraph 0067 comprise implicitly an operating system as in feature M2.

M3: The Opponent has quoted paragraph 0074 for this feature. It is not immediately apparent from this passage why it can be considered that the OS of the PDA (which actually does not appear to be explicitly mentioned in E5) does not have access to the hardware components described in this paragraph.

M4, M4.1: The PDA provided as example can be seen to have some memory (necessary for it's functioning), at least the one used for the PEAD (paragraph 0074).

M4.2: Paragraph 0049 mentions a user identification data block 302, paragraph 0050 mentions user's private key 304 stores in memory portions which can be qualified as a secure area . However, again it could not be corroborated from the explanations of the Opponent where it is disclosed that such secure area is not reported to the OS (directly or indirectly).

M5: Paragraphs 0049 and 0050 appear to disclose this feature, see again the data block 302.

M5.1, M5.2: It is not known if the secure area is inaccessible or not to the operating system and therefore the features M5.1 and M5.2 do not appear to be directly and unambiguously disclosed.

M6: Paragraph 0074 together with e.g. paragraphs 0049-0050 may be seen as disclosing feature M6.

M6.1: As mentioned above for feature M4.2, it is not apparent why the secure area of E5 could be seen as inaccessible to the OS.

M6.2: The Opponent has quoted paragraphs 0075-0078 as well as paragraph 0051 in support of his contention that this feature is disclosed in E5. From these passages it is not immediately apparent whether a digital signature is generated by the authentication software. Paragraphs 0075-0078 appear to relate to encryption of data. Paragraph 0051 mentions an electronic signature but when read in combination with paragraph 0096 this could possibly be understood as the user's signature acquired using an "appropriate input device".

M6.3: Here also it does not appear to be disclosed in a direct and unambiguous manner that the secure process environment is inaccessible to the OS.

M7: Feature M7 refers to the digital signature defined in feature M6.2 (generated by the authentication software) which does not appear to be disclosed, so that feature M7 is also not disclosed. Looking at paragraph 0098, it could possibly be agreed that authentication data can be understood as digital signature.

24.2 As a conclusion, the subject-matter of claim 1 appears to be novel in view of E5.

25 Novelty over E6.

25.1 E6 discloses:

M1: See Fig. 14 and paragraph 0160. The first transaction party is the user (A) which uses the host computer 100, the second transaction party is C.

M2: An OS is disclosed, see e.g. paragraph 0124.

M3: See the licensing code components 200 which can be seen as an authentication software and which runs in a protected environment preferably within the trusted module. However, the Opposition Division cannot see a direct and unambiguous disclosure that this environment is independent from and inaccessible from the OS as required by feature M3.

M4, M4.1: Fig. 14 discloses some memory which appears to be accessible to the OS, see e.g. the HDD or the DRAM.

M4.2: The trusted module has some memory comprising some secure area in view of the kind of data stored in it (see e.g. Fig. 15). It is however not immediately apparent that such memory part is not reported to the OS.

M5: See e.g. paragraph 0125, the private key 212.

M5.1, M5.2: It is not known if the secure area is inaccessible or not to the operating system and therefore the features M5.1 and M5.2 do not appear to be directly and unambiguously disclosed.

M6: See e.g. the licensing code components 200 mentioned above, paragraph 0125.

M6.1: See the comments under feature M4.2 above. A secure area of the trusted module being inaccessible to the OS does not appear to be disclosed.

M6.2: See paragraph 0136, a digital signature appears to be generated by the secure executor 204 using the private key 212.

M6.3: As mentioned above, an environment inaccessible to the OS does not appear to be explicitly disclosed.

M7: Paragraph 0160 together with paragraphs 0136 and 0137 appear to disclose this feature.

25.2 As a conclusion, the subject-matter of claim 1 appears to be novel in view of E6.

26 Novelty over E8.

26.1 E8 discloses:

M1: See Fig. 1, the user of a remote terminal 110 being the first transaction party, the "intended recipient entity" of paragraph 1075 being the second transaction party.

M2: No OS appears to be explicitly disclosed, it may however be agreed that some kind of OS must be present, i.e. this feature appears to be implicitly disclosed. For instance, the vault mentioned at paragraph 1061 could be seen as user application needing some kind of OS.

M3: Fig. 3, paragraphs 1033 and 1034 may be seen as disclosing that some kind of authentication software might be present, see also paragraph 1075. However, in the absence of an explicit disclosure of an OS, it cannot be seen that there is a separate operating environment inaccessible to the OS.

M4, M4.1: See Fig. 3.

M4.2: There is a secure memory 254 but again its link to the (undisclosed) OS is not made.

M5: See paragraph 1008 and e.g. the certificates used for authentication.

M5.1, M5.2: Here again, in the absence of an explicit disclosure of an OS, it cannot be confirmed that the secure area is inaccessible to the OS.

M6: See paragraph 1075.

M6.1, M6.3: Again the inaccessibility to the OS does not appear to be directly and unambiguously disclosed.

M6.2, M7: See paragraph 1075.

26.2 As a conclusion, the subject-matter of claim 1 appears to be novel in view of E8.

27 Similar considerations apply to the subject-matter of independent claims 23 and 24 which also appears to be novel.

28 Inventive step.

In view of the provisional opinion of the Opposition Division concerning the ground of Article 100(c) EPC, it appears difficult to provide an opinion on inventive step at this stage. Taking into account the submissions made by the Opponent, it appears, however, that no document is available which discloses the (absence of) link between the OS and a secure area within the meaning of the independent claims. It is therefore at present not immediately apparent how the skilled person would arrive at the claimed subject-matter without exercising inventive skills.

Europäisches Patentamt
European Patent Office
Office européen des brevets

Wichtige Hinweise zur mündlichen Verhandlung

Das Europäische Patentamt verfügt über keine eigenen Dolmetscher. Diese müssen im Bedarfsfall von außerhalb, teilweise sogar aus anderen Ländern, beigezogen werden, was mit einem hohen Aufwand an Kosten und organisatorischen Vorbereitungen verbunden ist. Muss ein Verhandlungstermin kurzfristig abberaumt werden, können Kosten für bestellte Dolmetscher nicht mehr vermieden werden.

Es wird daher gebeten, eine Simultanübersetzung nur bei wirklichem Bedarf in Anspruch zu nehmen. Es wäre wünschenswert, wenn sich die Beteiligten (zweckmäßigerweise gleichzeitig mit der Terminabstimmung) auf die Benutzung einer Amtssprache einigen könnten. Bei Verständigungsschwierigkeiten sind die Mitglieder der Einspruchsabteilung bereit zu helfen.

Die von den Verfahrensbeteiligten bevorzugte (abgestimmte) Verhandlungssprache und ggf. eine notwendige Simultanübersetzung sind dem Amt möglichst vor der in Regel 4(1) EPÜ angegebenen Frist mitzuteilen.

☐ Verfahrenssprache ist **Deutsch**

Von der/dem/den Einsprechenden wurde

☐ Englisch

☐ Französisch benutzt.

Es wird um eilige Mitteilung - möglichst per Telefax an den zuständigen Formalprüfer - gebeten,

möglichst bis

Datum **07.10.20**

1. welche Sprache(n) Sie in der mündlichen Verhandlung verwenden (**Sprechen**)
2. aus welcher Sprache Sie eine Simultanübersetzung benötigen (**Hören**).

Important information concerning oral proceedings

The European Patent Office has no interpreters of its own. When interpreters are needed they have to be brought in from outside, sometimes even from other countries, which is costly and involves considerable organisation. If oral proceedings have to be cancelled at short notice, the cost of interpreters already engaged still has to be borne.

Please therefore make use of simultaneous interpreting facilities only where strictly necessary. If possible the parties should agree on an official language for the proceedings, preferably at the time when they arrange a date. The members of the Opposition Division will be willing to help should any communication problems arise.

The EPO should be told if possible before the period mentioned in Rule 4 (1) EPC which language the parties prefer (agree on) and whether simultaneous interpreting facilities are required.

☒ Language of the proceedings is **English**

The language used by the opponent/s was

☐ German OI - EN

☐ French.

Please inform us urgently - where possible by fax addressed to the formalities officer concerned -

if possible by

Date **07.10.20**

1. which language(s) you intend to use during the oral proceedings (**Speaking**)
2. from which language you need simultaneous interpretation (**Listening**).

Très important Procédure orale

L'Office européen des brevets ne dispose pas de son propre service d'interprètes. Aussi faut-il appel le cas échéant à des interprètes de l'extérieur, qui viennent même parfois de l'étranger, ce qui occasionne de frais élevés et demande un grand travail d'organisation. Si la date d'une procédure orale doit être annulée au dernier moment, il n'est plus possible d'éviter les frais d'interprètes.

Les parties à une procédure sont donc priées de ne demander une traduction simultanée qu'en cas de réel besoin. Il serait souhaitable qu'elles puissent se mettre d'accord en même temps qu'elles conviennent de la date sur l'utilisation d'une langue officielle comme langue des débats. Si les parties éprouvent des difficultés de compréhension lors des débats, les membres de la division d'opposition sont disposés à leur prêter leur assistance.

L'Office doit être avisé si possible avant le début du délai mentionné dans la règle 4(1) CBE de la langue préférée par les parties pour le déroulement des débat (et sur laquelle elles se sont préalablement mises d'accord) et de la nécessité éventuelle d'une traduction simultanée.

☐ La langue de la procédure est le **français**

La langue utilisée par l'opposant/les opposants était

☐ l'allemand

☐ l'anglais.

Prière d'indiquer d'urgence à l'agent des formalités compétent si possible par téléfax

si possible jusqu'au

Date **07.10.20**

1. quelle(s) langue(s) vous utiliserez au cours de la procédure orale (**pour parler**)
2. à partir de quelle langue vous aurez besoin d'une traduction simultanée (**pour écouter**).

Sollten Sie Ihren Antrag auf mündliche Verhandlung zurückziehen oder zum anberaumten Verhandlungstermin nicht erscheinen wollen bzw. aus wichtigem Grund daran gehindert sein, werden Sie gebeten,

- **unverzüglich das Amt - möglichst per Telefax - davon zu benachrichtigen, wobei das Schriftstück mit einem deutlichen Vermerk "Dringend, mündliche Verhandlung am ..." oder sinngemäß gekennzeichnet sein sollte;**
- **in dringenden Fällen** (weniger als 1 Monat vor dem Verhandlungstermin) zusätzlich **auch dem/die anderen Verfahrensbeteiligten** bzw. ihre(n) Vertreter auf schnellstem Weg **direkt zu unterrichten.**

In jedem solchen Fall obliegt der Einspruchsabteilung die Entscheidung, ob die Verhandlung durchgeführt oder abberaumt wird. Es wird jedoch darauf hingewiesen, dass einem Verfahrensbeteiligten, der eine nicht rechtzeitige oder unterbliebene Benachrichtigung zu verantworten hat, die dadurch den anderen Beteiligten verursachten Kosten auferlegt werden können (Art. 104 EPÜ).

Hinweis auf Regel 4 EPÜ

Regel 4
Sprache im mündlichen Verfahren

(1) Jeder an einem mündlichen Verfahren vor dem Europäischen Patentamt Beteiligte kann sich anstelle der Verfahrenssprache einer anderen Amtssprache des Europäischen Patentamts bedienen, sofern er dies dem Europäischen Patentamt spätestens einen Monat vor dem angesetzten Termin mitgeteilt hat oder selbst für die Übersetzung in die Verfahrenssprache sorgt. Jeder Beteiligte kann sich einer Amtssprache eines Vertragsstaats bedienen, sofern er selbst für die Übersetzung in die Verfahrenssprache sorgt. Von diesen Vorschriften kann das Europäische Patentamt Ausnahmen zulassen.

Should you decide to withdraw your request for oral proceedings or not wish to attend on the date set, or if for some special reason you are unable to do so, you are requested

- **to notify the EPO immediately, where possible by fax, marking the document clearly with the words "Urgent, oral proceedings on ..." or similar;**
- **in urgent cases** (less than one month before the date set for the proceedings), additionally to **notify the other party/parties** and/or their representative(s) **direct as rapidly as possible.**

In all such cases the Opposition Division will decide whether the proceedings are to go ahead or be cancelled. You should however note that costs incurred by the other parties may be charged to a party who either fails to notify them or does not do so in good time (Article 104 EPC).

Attention is drawn to Rule 4 EPC

Rule 4
Language in oral proceedings

(1) Any party to oral proceedings before the European Patent Office may use an official language of the European Patent Office other than the language of the proceedings, if such party gives notice to the European Patent Office at least one month before the date of such oral proceedings or provides for interpretation into the language of the proceedings. Any party may use an official language of a Contracting State, if he provides for interpretation into the language of the proceedings. The European Patent Office may permit derogations from these provisions.

Si vous retirez votre requête tendant à recourir à la procédure orale ou si vous ne souhaitez pas vous présenter à la date fixée pour la procédure orale ou ne pouvez vous y présenter pour une raison sérieuse, veuillez

- **en faire avis sans retard à l'Office, si possible par téléfax, en partant sur votre communication clairement la mention "Urgent, procédure orale le ..." ou une indication similaire;**
- **dans les cas urgents** (moins d'un mois avant la date fixée pour la procédure orale) **en faire avis également directement** pas la voie la plus rapide à **l'autre/aux autres partie(s)** ou bien à son/leurs mandataire(s).

Il appartient alors à la division d'opposition de décider si la procédure orale aura lieu ou non. Il est néanmoins souligné que les frais causés aux autres parties par une partie qui est responsable de l'omission d'un tel avis ou de ce que cet avis n'a pas été fait en temps utile peuvent être mis à la charge de cette partie (art. 104 CBE).

Rappel de la Règle 4 CBE

Règle 4
Langues admissibles lors de la procédure orale

(1) Toute partie à une procédure orale devant l'Office européen des brevets peut utiliser une langue officielle de l'Office européen des brevets autre que la langue de la procédure, à condition soit d'en aviser l'Office européen des brevets un mois au moins avant la date de la procédure orale, soit d'assurer l'interprétation dans la langue de la procédure. Toute partie peut utiliser une langue officielle de l'un des Etats contractants à condition d'assurer l'interprétation dans la langue de la procédure. L'Office européen des brevets peut autoriser des dérogations aux présentes dispositions.

(2) Die Bediensteten des Europäischen Patentamts können sich im mündlichen Verfahren anstelle der Verfahrenssprache einer anderen Amtssprache des Europäischen Patentamts bedienen.

(2) In the course of oral proceedings, employees of the European Patent Office may use an official language of the European Patent Office other than the language of the proceedings.

(2) Au cours de la procédure orale, les agents de l'Office européen des brevets peuvent utiliser une langue officielle de l'Office européen des brevets autre que la langue de la procédure.

(3) In der Beweisaufnahme können sich die zu vernehmenden Beteiligten, Zeugen oder Sachverständigen, die sich in einer Amtssprache des Europäischen Patentamts oder eines Vertragsstaats nicht hinlänglich ausdrücken können, einer anderen Sprache bedienen. Erfolgt die Beweisaufnahme auf Antrag eines Beteiligten, so werden die Beteiligten, Zeugen oder Sachverständigen mit Erklärungen, die sie in einer anderen Sprache als in einer Amtssprache des Europäischen Patentamts abgeben, nur gehört, sofern dieser Beteiligte selbst für die Übersetzung in die Verfahrenssprache sorgt. Das Europäische Patentamt kann jedoch die Übersetzung in eine seiner anderen Amtssprachen zulassen.

(3) Where evidence is taken, any party, witness or expert to be heard who is unable to express himself adequately in an official language of the European Patent Office or of a Contracting State may use another language. Where evidence is taken upon request of a party, parties, witnesses or experts expressing themselves in a language other than an official language of the European Patent Office shall be heard only if that party provides for interpretation into the language of the proceedings. The European Patent Office may, however, permit interpretation into one of its other official languages.

(3) Lors de l'instruction, les parties, témoins ou experts appelés à être entendus, qui ne possèdent pas une maîtrise suffisante d'une langue officielle de l'Office européen des brevets ou d'un Etat contractant, peuvent utiliser une autre langue. Si la mesure d'instruction est ordonnée sur requête d'une partie, les parties, témoins ou experts qui s'expriment dans une langue autre qu'une langue officielle de l'Office européen des brevets ne sont entendus que si cette partie assure l'interprétation dans la langue de la procédure. L'Office européen des brevets peut toutefois autoriser l'interprétation dans l'une de ses autres langues officielles.

(4) Mit Einverständnis aller Beteiligten und des Europäischen Patentamts kann jede Sprache verwendet werden.

(4) If the parties and the European Patent Office agree, any language may be used.

(4) Sous réserve de l'accord des parties et de l'Office européen des brevets, toute langue peut être utilisée.

(5) Das Europäische Patentamt übernimmt, soweit erforderlich, auf seine Kosten die Übersetzung in die Verfahrenssprache und gegebenenfalls in seine anderen Amtssprachen, sofern ein Beteiligter nicht selbst für die Übersetzung zu sorgen hat.

(5) The European Patent Office shall, if necessary, provide at its own expense interpretation into the language of the proceedings, or, where appropriate, into its other official languages, unless such interpretation is the responsibility of one of the parties.

(5) L'Office européen des brevets assure à ses frais, en tant que de besoin, l'interprétation dans la langue de la procédure, ou, le cas échéant, dans ses autres langues officielles, à moins que cette interprétation ne doive être assurée par l'une des parties.

(6) Erklärungen von Bediensteten des Europäischen Patentamts, Beteiligten, Zeugen und Sachverständigen, die in einer Amtssprache des Europäischen Patentamts abgegeben werden, werden in dieser Sprache in die Niederschrift aufgenommen. Erklärungen in einer anderen Sprache werden in der Amtssprache aufgenommen, in die sie übersetzt worden sind. Änderungen einer europäischen Patentanmeldung oder eines europäischen Patents werden in der Verfahrenssprache in die Niederschrift aufgenommen.

(6) Statements by employees of the European Patent Office, parties, witnesses or experts, made in an official language of the European Patent Office, shall be entered in the minutes in that language. Statements made in any other language shall be entered in the official language into which they are translated. Amendments to a European patent application or European patent shall be entered in the minutes in the language of the proceedings.

(6) Les interventions des agents de l'Office européen des brevets, des parties, témoins et experts faites dans une langue officielle de l'Office européen des brevets sont consignées au procès-verbal dans cette langue. Les interventions faites dans une autre langue sont consignées dans la langue officielle dans laquelle elles sont traduites. Les modifications apportées à une demande de brevet européen ou à un brevet européen sont consignées au procès verbal dans la langue de la procédure.

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact

Kaufmann, Tobias
Bardehle Pagenberg Partnerschaft mbB
Patentanwälte, Rechtsanwälte
Prinzregentenplatz 7
81675 München
ALLEMAGNE

Formalities officer
Strick, Marina

Date
25.05.2020

Reference	OPPO 01	Application No./Patent No.
S154820EPEIN		04748654.3 - 1010 / 1634140
Applicant/Proprietor		
Ward Participations B.V.		

EPA/EPO/OEB Formblatt/Form/Formulaire : 2310

Empfangsbescheinigung über den Zugang des vorstehend bezeichneten Schriftstücks
Acknowledgement of receipt of the document specified above
Récépissé du document spécifié ci-dessus

Unter Bezugnahme auf die Mitteilung im ABl EPA 7/2010, 377 wird gebeten, die Empfangsbescheinigung mit Empfangsdatum und Unterschrift zu versehen und **umgehend** an das EPA zurückzusenden:

With reference to the Notice in OJ EPO 7/2010, 377, you are requested to date and sign the acknowledgement of receipt and return it to the EPO **immediately**:

Conformément au communiqué paru au JO OEB 7/2010, 377, vous êtes prié d'indiquer sur le récépissé la date de réception du document, de signer le récépissé et de le renvoyer **sans délai** à l' OEB:

- **über die Online-Dienste des EPA** (als Anlage zu EPA Form 1038) / **through EPO Online Services** (as annex to EPO Form 1038) / **par les services en ligne de l'OEB** (en tant que pièce jointe au formulaire OEB 1038),
- **per Fax / by fax / par téléfax (+49 (0) 89 2399-4465 or +31 (0) 70 340-3016)**
- oder per Post / or by post / ou par courrier.

Empfangen am / Received on / Reçu le :

Unterschrift / Signature:

Empfangsberechtigter/authorised recipient/
le destinataire ou la personne dûment mandatée

Rücksende-Adresse / Return address / Adresse de retour
(Umschlag / envelope / enveloppe ISO C4 / DL / C6/C5 / C6)

Europäisches Patentamt
80298 MÜNCHEN
DEUTSCHLAND

Rücksende-Adresse / Return address / Adresse de retour

EPA/EPO/OEB Form 2936 08.10

MS50949

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact

Kaufmann, Tobias
Bardehle Pagenberg Partnerschaft mbB
Patentanwälte, Rechtsanwälte
Prinzregentenplatz 7
81675 München
ALLEMAGNE

Date
25.05.2020

Reference	Application No./Patent No.
S154820EPEIN OPPO 01	04748654.3 - 1010 / 1634140
Applicant/Proprietor	
Ward Participations B.V.	

Summons to attend oral proceedings pursuant to Rule 115(1) EPC

You are hereby summoned to attend oral proceedings arranged in connection with the above-mentioned European patent.

The matters to be discussed are set out in the communication accompanying this summons (EPO Form 2906).

The oral proceedings, which will be public, will take place before the opposition division

on 07.12.20 at 09.00 hrs in Room 2453
at the EPO, Bayerstr. 34, PschorrHöfe, D-80335 München

No changes to the date of the oral proceedings can be made, except on serious grounds (see OJ EPO 1/2009, 68). If you do not appear as summoned, the oral proceedings may continue without you (R. 115(2) EPC).

Your attention is drawn to Rule 4 EPC, regarding the language of the oral proceedings, and to the Special edition No. 3 OJ EPO 2007, 128, concerning the filing of authorisations for company employees and lawyers acting as representatives before the EPO.

The final date for making written submissions and/or amendments (R. 116 EPC) is 07.10.20.

You are requested to report in good time beforehand to the porter in the EPO foyer. Room 3473 and 3474 are available as waiting rooms.

Parking is available in the underground car park, accessible only via the entrance "Grasserstrasse 2/6". On presentation of the summons to oral proceedings at one of the porters' lodges in the PschorrHöfe, the parking ticket will be revoked.

1st Examiner:	2nd Examiner:	Chairman:
Hijazi, Ali	Kleiber, Michael	Pavón Mayo, Manuel

For the Opposition Division

Annexes:
Confirmation of receipt (Form 2936)
Rule 4 EPC (EPC Form 2043)
Communication (EPO Form 2906)

Registered letter to EPO postal service: 18.05.20

State of the proceedings

I. European patent N°1 634 140 B1 entitled *"METHOD AND SYSTEM FOR PERFORMING A TRANSACTION AND FOR PERFORMING A VERIFICATION OF LEGITIMATE ACCESS TO, OR USE OF DIGITAL DATA"* is based on European patent application N°04 748 654.3 (international application number PCT/NL2004/000 422). The patent Proprietor is
Ward Participations B.V.
De Schaepstal 1, 1251 MZ Laren, NL.
The mention of the grant of the patent was published in European Patent Bulletin 2019/03 on 16-01-2019. The patent claims the following priority: PCT/NL03/00436 filed on 13-06-2003

II. A notice of opposition against the patent has been filed on 16-10-2019 by:

Samsung Electronics Benelux B.V.
Evert van de Beekstraat 310
1118 CX Schiphol, NL

III. The Opponent submitted that the subject-matter of the patent was not patentable according to Article 100(a) EPC (Article 52(1) EPC; Articles 54 and 56 EPC) and Article 100(c) EPC. He requested to revoke the patent in its entirety and auxiliarily to arrange an oral proceedings according to Article 116 EPC.

IV. The following documents were cited by the Opponent in support of his requests:

E1 WO 2004/015579 A1 (TREK 2000 INT LTD [SG]; OOI CHIN SHYAN RAYMOND [SG] ET AL.) 19 February 2004 (2004-02-19)

E2 "Client Security Software Version 5.0 Installation Guide", IBM Client Security Solutions, September 2002 ;

E2a "IBM Improves PC Security System", IBM News room, 4 October 2002 (2002-10-04), pages 1-2, URL:https://www-03.ibm.com/press/us/en/pressrelease/485.wss ;

E2b "Embedded Security Chip and Software - a white paper", IBM Client Security Solutions, 1999, pages 1-6 ;

E2c "Client Security Software Version 1.0 Administrator's Guide", IBM Client Security Solutions, December 1999

E3 US 5 892 900 A (GINTER KARL L [US] ET AL) 6 April 1999 (1999-04-06)

E4 US 2002/007456 A1 (PEINADO MARCUS [US] ET AL) 17 January 2002 (2002-01-17)

E5 US 2002/023215 A1 (WANG YNJIUN P [US] ET AL) 21 February 2002 (2002-02-21)

E6 EP 1 076 279 A1 (HEWLETT PACKARD CO [US]) 14 February 2001 (2001-02-14)

E7 WO 01/17296 A1 (ERICSSON TELEFON AB L M [SE]) 8 March 2001 (2001-03-08)

E8 WO 02/076127 A1 (QUALCOMM INC [US]) 26 September 2002 (2002-09-26)

E9 GB 2 338 381 A (BARCLAYS BANK PLC [GB]) 15 December 1999 (1999-12-15)

E10 EP 1 237 324 A (SANYO ELECTRIC CO [JP]; PFU LTD [JP]; FUJITSU LTD [JP]; HITACHI LTD [J) 4 September 2002 (2002-09-04)

E11 WO 01/84319 A (XTEC INC [US]) 8 November 2001 (2001-11-08)

E12 WO 02/47081 A (SANDISK CORP [US]) 13 June 2002 (2002-06-13)

E13 US 5 802 590 A (DRAVES RICHARD P [US]) 1 September 1998 (1998-09-01)

E14 US 2001/051996 A1 (COOPER ROBIN ROSS [US] ET AL) 13 December 2001 (2001-12-13)

E15 US 2002/112162 A1 (COCOTIS THOMAS ANDREW [US] ET AL) 15 August 2002 (2002-08-15)

E16 US 2002/112171 A1 (GINTER KARL L [US] ET AL) 15 August 2002 (2002-08-15)

E17 US 2003/039362 A1 (CALIFANO ANDREA [US] ET AL) 27 February 2003 (2003-02-27)

E18 BENNET YEE: "Using Secure Coprocessors", THESIS SUBMITTED TO THE SCHOOL OF COMPUTER SCIENCE FOR THE DEGREE OF DOCTOR OF PHILOSOPHY, May 1994

E19 WO 00/67143 A2 (UNICATE BV [NL]; SIPMAN WILHELMUS HENDRIKUS MAR [NL] ET AL.) 9 November 2000 (2000-11-09)

E20 US 5 354 097 A (TEL TEUNIS [NL]) 11 October 1994 (1994-10-11)

E21 GERALD J POPEK ET AL: "Encryption and Secure Computer Networks", ACM COMPUTING SURVEYS, ACM, NEW YORK, NY, US, US, vol. 11, no. 4, December 1979, pages 331-356, ISSN: 0360-0300, DOI: 10.1145/356789.356794

V. With a letter, received on 03-03-2020, the Patentee filed observations concerning the opposition and requested to reject the opposition. Furthermore, he auxiliarily requested oral proceedings according to Article 116 EPC to take place.

Points to be discussed

1 Since both parties have requested oral proceedings as an auxiliary measure, the parties are hereby invited to attend such proceedings.

2 The points which need to be discussed are set out below and a provisional, non-binding opinion of the Opposition Division is given on the positions adopted by the parties. However, the discussion may cover further points according to the circumstances. The parties are asked to make their submissions well in advance of the date of the oral proceedings, i.e. at the latest at the date set in this summons, especially if new sets of claims or lines of argumentations are to be considered during oral proceedings.

3 The attention of all parties is drawn to the Guidelines E-III, 8.5 concerning submissions by the parties.

4 The present patent is based on an application filed before 13.12.2007, i.e. before the EPC 2000 is entered into force, and therefore in accordance with the transitional provisions as decided by the Administrative Council some of the provisions of the EPC 2000 are to be applied while other provisions of the EPC 1973 still apply. As the Euro-PCT at the basis of the patent in suit was still pending on 13.12.2007, Article 54(4) EPC 1973 and therefore Rule 23a EPC 1973 apply in the present case. For the rest, in the present case, no substantial difference could be detected between both provisions to be applied concretely and therefore for simplicity reasons it is referred merely to the EPC 2000, i.e. EPC unless otherwise mentioned.

5 In parallel to this opposition another opposition has been filed against the patent based on a divisional application of the application forming the basis of the patent discussed below. The Opposition Division will have the same composition in both cases and the intention is to have the oral proceedings on two consecutive days. In case the discussions would take longer than foreseen, it is planed to have a third day as a backup in order to avoid any postponement.

6 In order to ease the discussion, the features breakdown used by the opponent for the independent claims is also taken by the Opposition Division.

Claim 1:

M1: Method for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party,

M2: the electronic device having an operating system (48) creating a run-time environment for user applications

M3: and authentication software (54) running in a separate operating environment, independent from and inaccessible to said operating system, (48)

M4: the electronic device having a memory comprising

M4.1: storage locations, part of the memory being accessible to the operating system, (48)

M4.2: part of the memory being a secure area (62) storage locations of which are not reported to the operating system, (48)

the method comprising:

M5: providing authentication data (63A) in the secure area (62) of said electronic device

M5.1: which authentication data (63A) are inaccessible to a user of said electronic device,

M5.2: wherein said secure area (62) is inaccessible to said operating system (48) of said electronic device, thereby rendering the authentication data (63A) inaccessible to said user;

M6: providing authentication software (54) in said electronic device,

M6.1: the authentication data (63A) being accessible to said authentication software, (54) wherein the authentication software (54) is stored in the secure area (62) inaccessible to said operating system;(*) (48)

M6.2: activating the authentication software (54) to generate a digital signature from the authentication data, (63A)

M6.3: wherein the authentication software (54) is run in a secure processing environment inaccessible to said operating system;(*) (48)

M7: providing the digital signature to the second transaction party.

(*) Note: the Druckexemplar mentions a ";" which is not present on the B1 publication of the patent.

Claim 23:

S1: System for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party,

S2: the electronic device having an operating system creating a run-time environment for user applications

S3: and authentication software running in a separate operating environment, independent from and inaccessible to said operating system,

S4: the electronic device having a memory comprising

S4.1: storage locations, part of the memory being accessible to the operating system,

S4.2: part of the memory being a secure area storage locations of which are not reported to the operating system,

the system comprising:

S5: means for providing authentication data in the secure area of said electronic device

S5.1: which authentication data are inaccessible to a user of the electronic device,

S5.2: wherein said secure area is inaccessible to said operating system of said electronic device, thereby rendering the authentication data inaccessible to said user;

S6: means for providing authentication software in said electronic device,

S6.1: the authentication data being accessible to said authentication software, wherein the authentication software is stored in the secure area inaccessible to said operating system;

S6.2: means for activating the authentication software to generate a digital signature from the authentication data,

S6.3: wherein the authentication software is run in a secure processing environment inaccessible to said operating system;

S7: means for providing the digital signature to the second transaction party.

Claim 24:

E1: Electronic device for performing an electronic transaction between a first transaction party and a second transaction party, wherein the electronic device is operated by the first transaction party,

E2: the electronic device having an operating system creating a run-time environment for user applications

E3: and authentication software running in a separate operating environment, independent from and inaccessible to said operating system,

E4: the electronic device having a memory comprising

E4.1: storage locations, part of the memory being accessible to the operating system,

E4.2: part of the memory being a secure area storage locations of which are not reported to the operating system,

E5: the secure area storing authentication data

E5.1: which are inaccessible to a user of the electronic device,

E5.2: wherein said secure area is inaccessible to said operating system of said electronic device, thereby rendering the authentication data inaccessible to said user;

the electronic device comprising:

E6: a memory storing authentication software,

E6.1: the authentication data being accessible to said authentication software, wherein the authentication software is stored in the secure area inaccessible to said operating system;

E6.2: means for activating the authentication software to generate a digital signature from the authentication data,

E6.3: wherein the authentication software is run in a secure processing environment inaccessible to said operating system; and

E7: means for providing the digital signature to the second transaction party.

Article 100(c) EPC

7 Claim 1.

7.1 Generally, the subject-matter of claim 1 appears to be mainly based on claims 1, 26 and 27 of the application as originally filed WO 2004/111752 A2 (in the following called D2, like done by the Opponent). In addition, the operating system, the memory and the authentication software have been further specified based on the description.

7.2 Feature M1.

This feature was already present in claim 1 of D2.

7.3 Feature M2.

The Opponent has challenged the lack of basis of feature M2 in the originally filed application mainly on the ground that the only passage explicitly disclosing this definition (page 13, lines 23-24 of D2) is to be read in the context of the embodiment of Fig. 3 which discloses other components.

The Opposition Division is of the provisional opinion that this feature, although only explicitly present at one place in D2, is nothing more than providing the definition of what an operating system is and generally applies to the whole disclosure (see also point 4 of the decision T 0248/17).

7.4 Feature M3.

Page 7, lines 31-34 discloses that the authentication software is independent from and inaccessible to the operating system on the device. However, it is also specified there that the separate operating environment is in the BIOS or in a console. The Opposition Division has therefore some doubts that this feature has a basis in its present generality in D2.

7.5 Features M4 to M4.2.

The Opponent has argued that no part of D2 discloses a memory which comprises a combination of parts that are accessible and non-accessible to the operating system.

The Opposition Division notes the following:

Feature M4. The claim mentions a memory in general (and not for instance a memory module), while this aspect was already present in claim 1 of D2 (the authentication data is provided in a memory of said electronic device). It is not specified whether this memory is formed of one or several physical memory parts and where this memory is located. Generally speaking a memory must be present in an electronic device as claimed, independently of the embodiment considered, and a memory, as a matter of definition, comprises a storage location. Feature M4 appears therefore to have a basis in D2.

Feature M4.1. Page 11, lines 9-12 of D2 discloses that a secure memory location has to be provided as a part of a secure memory or it may be an encrypted part of a non-secure memory (therefore a non-secure memory is defined). At least a part of this memory is also accessible to the operating system (page 15, lines 11-14). In addition, this feature, as such, appears to be a common aspect of any operating system.

Feature M4.2. Page 14, lines 12-13, it is stated that in or behind the console 52, there is a secure area 62 only accessible to the BIOS. At page 7, lines 28-29, it is stated that the secure part of the device is accessible only to the BIOS. It is further stated (lines 13+) that the secure area 62 comprises applications and storage locations, which are not reported to the operating system 48. Later (lines 35+) it is stated that the secure area may further comprises other ... memory locations. Such a secure area appears therefore to be part of a memory.
Page 15, lines 21+ discloses that the authentication data is stored in a memory that is accessible to an operating system of the device and possibly to a user of said device. Page 18, lines 12+ appears to relate to a similar embodiment as far as this aspect is concerned. However, it is stated in that embodiment that the secure area 62 is not essential for performing the third embodiment (contrary to the part starting at page 15, line 21 which still appears to comprise a secure area 62). As argued indirectly by the Opponent, the embodiment starting at page 18, line 12 does not appear to be covered by claim 1.

The question which still arises is which link, if any, is to be made between features M4.1 and M4.2 and the BIOS (and possibly the console).

In the paragraph bridging pages 5 and 6 it is mentioned that in the context of the installation method a new device contains a BIOS and an existing device also contains such BIOS. It is also specified that the BIOS is used to access a memory location in a memory. This part appears to relate to all described embodiments. See with that regard page 5, line 19 and the reference to Figs. 1, 2, 4 and 6-9, while both Figs. 3 and 5A,B disclose the BIOS; access to a removable memory - Fig. 10 - is also to be done via the BIOS, see e.g. page 13, line 10.

Therefore, in the light of these passages, the Opposition Division has also doubts that the BIOS can be omitted from the combination of features M4-M4.2 without extending the content of the application as filed.

The fact that independent claim 1 of D2 does not mention the BIOS does not provide any technical teaching providing such a justification as the aspects related to the secure area have been taken from the description. The same applies in relation with page 2 of D2 quoted by the Patentee which appears to be directed to a mere repetition of the claims of D2. The decision of the BoA does not appear to provide a justification for the present generality either, as the claim pending at the time did have a reference to the BIOS.

7.6 Features M5 to M5.2.

In section B.I.3. of the notice of opposition, the Opponent argues that there is neither explicit nor implicit support for features M4 to M5.2.

The Opposition Division notes the following:

Features M4 to M4.2 have been discussed in the section above.

Features M5 and M5.1. These features were already present in claim 1 of D2 apart that secure area instead of memory is now used which appears to have a basis in e.g. Fig. 3 (see also the discussion above concerning feature M4.2). Concerning the expression "authentication data", the Opposition Division notes that this feature was present in the claim 1 of D2 which is supposed to cover all embodiments of D2. It is nevertheless noted that the specific embodiments of Figs. 1 and 2 appear to refer to an "authentication table" instead (see e.g. the random table supplier, page 6, line 17 and the random table lines 21-23). It is however noted that page 15, line 12 of D2 appears to provide the idea that an authentication table is an example for authentication data in general. Lastly, it is noted that a table can have one or several dimensions so that any data in a memory could possibly be considered as being part of the authentication table

in the absence of any definition for it. All in all, the Opposition Division is of the provisional opinion that "authentication data" in connection with the secure area as claimed is having a basis in D2, i.e. features M5 and M5.1 have such a basis.

Feature M5.2. This feature is repeating feature M4.2 with a slightly different wording. As the secure area is not reported/inaccessible to the OS it is de facto rendering the data in it inaccessible to the user.

Therefore, the Opposition Division is of the provisional opinion that the features M5 to M5.2 have a basis in D2, as far as features M4 to M4.2 have such a basis.

7.7 Features M6 to M6.3.

These features were not challenged by the Opponent.

Feature M6 and the first part of feature M6.1 appears to have a basis in claim 1 of D2.

Second part of feature M6.1 (starting at wherein).

Feature M6.2 appears to have a basis in claim 1 of D2. Fig. 3 appears to show that the authentication software is stored in the secure area 62 (see also page 14, lines 31-34).

Feature M6.3 appears to have a basis in claim 27 of D2.

A basis in D2 for these features appears therefore to be present.

7.8 Feature M7.

This feature was not challenged by the Opponent and was present in claim 1 of D2.

8 Independent claim 23.

Claim 23 is directed to a system for performing an electronic transaction, is based on claim 29 of D2 and corresponds for the rest to claim 1 in terms of means for. The same comments as made above for claim 1 apply mutatis mutandis.

9 Independent claim 24.

Claim 24 is directed to an electronic device for performing an electronic transaction and mostly takes back the features of claim 1. The same comments as made above for claim 1 apply mutatis mutandis.

10 Dependent claim 5.

The additional features of claim 5 appear to be based on page 8, lines 28-29 of D2. Whether the authentication software is to be defined in relation with the BIOS as argued by the Opponent will have to be discussed possibly also in connection with the independent claims.

11 Dependent claim 7.

The additional features of claim 7 appear to be based on claim 11 of D2 which depends on claim 10 of D2, itself forming the basis of claim 6 of the patent in suit. No key is present in claim 1 of the patent so that the argumentation of the Opponent cannot be followed.

12 Dependent claim 8.

The additional features of claim 8 appear to originate from page 14, lines 31-34 of D2. Whether these features have been taken out of their context or not will have to be assessed depending on the results of the discussion concerning feature M4.2 which defines the secure area 62.

13 Dependent claim 9.

The additional features of claim 9 appear to originate from page 15, lines 8-10 of D2. Again, whether these features have been taken out of their context or not will have to be assessed depending on the results of the discussion concerning feature M4.2 which defines the secure area 62.

14 Dependent claim 20.

The additional features of claim 20 appear to be based on claim 18 of D2. However, the dependencies of this claim as yet specified (claims 14 to 19) does not appear to have a basis in D2. Claim 18 of D2 was only depending on claims

14 to 17 of D2 which are not corresponding to claims 14 to 19 of the patent. The Opposition Division has doubts that no new combination was thereby introduced.

15 Dependent claim 21.

The parties appear to agree that the relevant part for seeking a basis for this claim is the passage starting at page 19, line 24 to page 20, line 8. The Opponent objects to claim 21 and argues that the specific sequence ("before...") is not explicitly disclosed in D2 and that these features have been extracted and isolated from the embodiment of Fig. 6. The Patentee argues that the above quoted passage is providing a basis for claim 21. The Opposition Division has doubts that this is the case, already because this embodiment appears to refer to the BIOS which is not present in claim 1 on which claim 21 depends but also because these features appear to have been extracted from the embodiment of Fig. 6. It will therefore have to be discussed whether a direct and unambiguous disclosure for claim 21 can be found in D2.

16 Dependent claim 22.

The additional features of claim 22 appear to be partly disclosed at page 8, line 29. Concerning the "two" private encryption keys (one in claim 5 and one in claim 22), this appears to be more a clarity problem than a lack of basis in D2. The general context of D2 appears to relate to digital data in connection with the encryption key, see page 3, lines 7-9. It will have to be discussed whether the new multiple dependencies have a basis in D2.

17 Other dependent claims. The Opposition Division notes provisionally the following:

17.1 Claims 2 to 4 appear to have a basis in claims 5 to 7 of D2.

17.2 Claims 6 and 7 appear to have a basis in claims 10 and 11.

17.3 Claim 10 appears to have a basis in claim 14.

17.4 Claim 11 appears to have some basis in page 19, lines 14-17. However, this part appears to relate to an embodiment possibly not covered by the present independent claims.

17.5 Claim 12 appears to have a basis in claim 15. However, it is not immediately apparent what is the basis for the new dependency structure. Furthermore, this aspect appears to relate to the embodiment where the memory is accessible to the user/OS, see e.g. page 17, lines 20-21, and therefore, it will have to be discussed whether this aspect can be combined with the features of claim 1.

17.6 Claims 13, 14. These claims appear to have some basis at page 17, line 32 to page 18, line 4. However, these parts refer to a second encryption layer not necessarily presently claimed as this aspect is only present starting at claim 12. Furthermore, it is not immediately apparent what is the basis for the new dependency structure.

17.7 Claim 15 appears to have a basis in claim 16.

17.8 Claim 16 appears to have a basis in claim 17, however, here also, it is not immediately apparent what the basis is for the new dependency structure.

17.9 Claims 17, 18 appear to have some basis page 19, lines 5-8. However, this part appears to relate to an embodiment possibly not covered by the independent claims. The reference to Fig. 3 shows that some aspect(s) of the first embodiment might be incorporated in the embodiment of Fig. 5A. The contrary does not appear, however, to be mentioned.

17.10 Claim 19 appears to have some basis page 26, lines 32-35 which, however, also appears to relate to an embodiment (where the memory is accessible to the user/OS) not covered by the present independent claims.

17.11 Claim 25. The only part which appears to provide some basis for this claim is page 12, lines 31-36. However, that this device should contain a BIOS appears mandatory in this passage. A clear basis for this claim is therefore not immediately apparent.

18 As a conclusion, although most of the features of the claims appear to have some basis in D2, it is not always immediately apparent whether the presently claimed combinations (including mixing of different embodiments) can be derived directly and unambiguously from the originally filed application. The provisional opinion of the Opposition Division is therefore that the subject-matter of the patent appears to extend beyond the content of the application as filed.

Article 100(a) in combination with Articles 52, 54 and 56 EPC

19 The Opponent has submitted that the subject-matter of claim 1 is not novel in view of E1, E2/E2a, E3, E5, E6, E8 and auxiliarily not inventive in view of E2/ E2a. The provisional opinion of the Opposition Division is as follows.

20 Validity of the priority claim with regard to the independent claims.

20.1 The Opponent has brought two lines of attack with regard to the priority.

20.1.1 First argumentation, concerning the feature M2.

The Opposition Division refers to point 7.3 above and provisionally does not see that the presence of this feature would lead to a loss of the priority right.

20.1.2 Second argumentation, concerning the absence in claim 1 of the patent in suit of the feature "providing digital data from the second transaction party to the first transaction party".

The Opposition Division tends to follow the argumentation of the Patentee that page 14, lines 10-15 and page 15 (lines 24-26) provides some support for omitting the last feature of claim 1 of the priority document, i.e. this feature is not an essential feature missing in claim 1 of the patent, which would lead to a loss of priority.

In case the Opposition Division would change its opinion on this, e.g. during oral proceedings in the light of arguments submitted by the parties, the Opposition Division has doubts that G 1/15 can be applied as it concerns generic "OR"-claims. Here the absence of an essential feature does not appear to fall under this category.

20.2 Similar considerations apply to independent claims 23 and 24.

21 Novelty over E1.

21.1 E1 has a publication date of 19.02.2004, i.e. after the priority date of the patent in suit (13.06.2003) but before its filing date (14.06.2004). The filing date of E1 is before the priority date of the patent in suit so that the validity of the priority of E1 is of no importance. E1 is a PCT application which had validly entered the European phase on 21.05.2004 in the form of an Euro-PCT application EP 03 713 173 and was still pending at the time of entry into force of the EPC 2000.

Article 158(1) and (2) EPC 1973 applies to the Euro-PCT of E1. In view of the provisional opinion mentioned above concerning the priority of the patent in suit, this document is therefore a document according to Article 54(3), (4) EPC 1973, i.e. only relevant for novelty. For simplicity reasons, reference to E1 is kept in the following, since the WO publication document corresponds to the publication of the Euro-PCT application.

21.2 E1 relates to a secured access to restricted information over the networks (page 1, lines 6+). Figs. 1 to 4 disclose four embodiments of an authentication system to verify a password from a host, Fig. 5 relates to a method for such authentication, Figs. 6-8 are directed to some specific system implementations, Fig. 9 is a block diagram of a SAKE (storage anti-piracy key encryption) implementation, while Figs. 10 and 11 are directed to further embodiments of related methods.

21.3 The Opponent presents an argumentation against the subject-matter of claim 1 by using parts of E1 which relate to Figs. 1, 2, 4, 7 and 9 and which appear to concern different embodiments of the invention disclosed in E1. As argued by the Patentee it is not immediately apparent how these embodiments can be combined, as no real link between them appears to be made in E1. Further to that, at least E1 does not appear to disclose the generation of a digital signature which is understood as a code which can act as a signature. A yes or no (verification of a password) does not appear to be such a signature.

21.4 Therefore, the subject-matter of independent claims 1, 23 and 24 appears to be new in view of E1, inventive step from E1 not being an issue at present (see point 21.1 above).

22 Novelty over E2a/E2.

22.1 Publication dates.

It appears undisputed that E2a has a publication date of 04.10.2002 in view of the date it bears.

Concerning E2, the following is noted:

It is referred in E2a to the Client Security Software, Version 5.0 (which installation guide is E2). There it is stated the availability of this software is scheduled for November 2002 while the Installation Guide itself bares the date of September 2002. All these dates are well before (more than six months) the priority date of the patent in suit. It is further noted that the version 5.1 was announced with a press release dated 15.04.2003 with an availability for May 2003 (https://www-03.ibm.com/press/us/en/pressrelease/240.wss), which is also before the priority date of the patent.

The Opposition Division is therefore of the provisional opinion that the Client Security Software, Version 5.0, was released before the priority date and therefore that E2, being its installation guide, was also available before the priority date.

22.2 E2a/E2 is to be considered as one document or not?

The Opposition Division tends to accept that starting from E2a, the link to E2 is precise enough to justify considering both teachings together. The fact that the E2 was possibly not available at the time E2a was published is not considered by the Opposition Division to prevent this view. The Guidelines G-IV, 8 refers to a decision of the BoA T 153/85 which does not appear to mention such criteria (see section 4.2 of the decision). The Opposition Division tends also to consider that the date to be considered when assessing the combination is the date of the latest of the two, here E2, which is anyway before the priority date of the patent in suit (see section 22.1).

The contrary (starting from E2) does not appear to be true as no mention of the press release appears to be present in E2.

Lastly, the Patentee has expressed some doubts as to whether a press release can be regarded to provide a technical disclosure. The Opposition Division is of the opinion that the state of the art comprises everything made available to the public (Article 54(2) EPC) and therefore that such type of document also belongs to the prior art which must be taken into consideration when assessing the patentability of a claim, as it mentions in it some technical aspects referring to existing systems, i.e. it provides some technical teaching.

22.3 E2a/E2 discloses:

M1: An Embedded Security Subsystem is offered on notebooks and desktops, the user of which is the first transaction party (first paragraph). The second paragraph mentions that the subsystem consists of both a hardware component, the cryptographic security chip, which supports key storage, privacy encryption and digital signatures for authentication of identity, and a downloadable software component, the Client Security Software, which interfaces with the user and with other software applications. The sixth paragraph quoted by the Opponent discloses that the Client Security Software is providing interoperability with IBM Tivoli Access Manager which is used to manage security policies. This allows consistent security policy enforcement across the organization for a wide range of Web and application resources. These resources may be seen as the second transaction party.

M2: See page 3 of E2 which discloses the required operating systems. As mentioned under point 7.3 any such OS is creating a run-time environment for user applications.

M3: Page 1 last sentence of E2 discloses that the Security Chip is encrypting and storing keys. An authentication software is therefore present in a separate environment. However, for similar reasons as those argued by the Patentee, the Opposition Division has doubts that this environment can be qualified as inaccessible to the operating system due to the access to the chip by a software running under the OS (for instance the Client Security Software).

M4,
M4.1: A notebook or desktop as mentioned in E2a comprises such features.

M4.2: The Security Chip includes some memory used to store keys and which can be qualified as providing a secure area, as the Secure Chip is not a normal component (like the hard disk for instance) used to store data (see E2a or page 3 of E2 as quoted above). However, it does not appear to be unambiguously disclosed that these storage locations are not reported to the OS.

M5: As mentioned above, the Security Chip includes some secure area used to e.g. store keys.

M5.1: As mentioned in E2a, second paragraph, the Client Security Software interfaces with the user and with other software applications.The authentication data appears therefore to be generally inaccessible to the user.

M5.2: This feature further repeats the definition of the secure area which was given in M4.2, which the Opposition Division does not see as being disclosed in E2a/E2, while at the same time further defining what is meant with the inaccessibility to the user. Hence, this feature does not appear to be disclosed in E2a/E2.

M6: An authentication software is disclosed in E2a/e2, see feature M3 above.

M6.1: The authentication data of the Secure Chip are accessible to the authentication software of the same chip. However, as mentioned above (M4.2), it does not appear to be disclosed that the secure area (of the chip) is inaccessible to the OS.

M6.2: E2a, second and third paragraph, appears to disclose part of this feature in that signatures are mentioned in connection with the Secure Chip ("supports"). The Opposition Division could not, however, corroborate that the Secure Chip is generating signatures through a software stored in itself.

M6.3: As mentioned in connection with M3, the Opposition Division has some doubts that it is directly an unambiguously disclosed that the secure processing environment of the chip is inaccessible to the OS.

M7: What is done with the signature mentioned in E2a is also not explicitly mentioned in E2a so that this feature also does not appear to be directly and unambiguously disclosed.

22.4 As a conclusion, the subject-matter of claim 1 appears to be novel in view of E2a/E2.

23 Novelty over E3.

23.1 E3 discloses:

M1: See e.g. the Virtual Distribution Environment (VDE) of Fig. 1. Col. 60, lines 8+ mentions that the VDE participants (i.e. each participant is a transaction party) may have an electronic appliance which may be or contains a computer. Fig. 7 discloses an example of VDE electronic appliance.

M2: As at least some of the appliances are meant to be used by consumers, it can be safely assumed that an OS must be present when the appliance is a computer. Such operating system appears to be called Rights Operating System (ROS) 602, see Col. 61, lines 21-22. The ROS is described starting at Col. 80, line 6. The ROS supports user application(s) 608 in addition to rights and auditing operating system functions 604 and other OS functions 606.

M3: Fig. 6 shows a Secure Processing Environment (SPE) 503 which is further described starting at Col. 112, line 1 and which is supported by the hardware resources of a Secure processing Unit (SPU) 500 (Col. 112, lines 12-13). The SPE is understood by the Opposition Division as a software which does not appear to be necessarily part of the SPU 500 as argued by the Opponent. The SPE includes an Authentication Manager 564 which can be seen as an authentication software within the meaning of feature M3. It is however stated at Col. 82, lines 55+ that the ROS manages the hardware (e.g. CPU, memory and encrypt/decrypt engines within the SPU 500). Therefore, the SPE 503 does not appear to be inaccessible to the ROS contrary to the requirement of feature M3. Fig. 7 or Col. 60, lines 13-14 do not appear to provide support for the contention that the ROS is left outside of the SPU 500 or SPE 503.

M4, M4.1: Fig. 7, Col. 82, lines 61+: the ROS managed the hardware like memories other than within SPU. These parts are accessible to the ROS.

M4.2: For this feature, the Opposition Division tends to follow the position of the Patentee. The memory manager 578 is part of the kernel 552 (Fig. 13) which is itself part of the SPE 503 (Fig. 13) itself part of the ROS (Fig. 12). Therefore, the parts of the memory driven by the memory manager do not appear to be "not reported to the operating system", rather merely their use is restricted to some specific processes of the ROS.

M5: From Col. 71, lines 28+ it can be read that sensitive information, such as encryption keys, is stored in the NVRAM 534b. The Opposition Division tends to consider such keys as being authentication data in the general sense of this term.

M5.1, M5.2: The secure area (the NVRAM 534b) is not inaccessible to the operating system (the ROS, see above feature M3) and as a consequence the Opposition Division tends to consider that it is de facto not inaccessible to the user within the meaning of features M5.1 and M5.2.

M6: An authentication software is provided, see above feature M3.

M6.1: The authentication manager 564 is part of the SPE 503 (Col. 112). The authentication data appear therefore to be accessible to the manager (whether they are really accessed and for what purpose does not appear to be disclosed). It is not clear to the Opposition Division where the manager 564 is stored and even if it was accepted that it is stored in the secure area defined in feature M5, this area appears to be accessible to the ROS (see above features M5.1, M5.2).

M6.2: The Opposition Division tends to follow the argumentation of the Patentee. The first line of attack of the Opponent refers to the Ticket Services mention at Col. 130, lines 32+. The tickets mentioned at Col. 131 are requested by the VDE and returned to it, i.e. a digital signature generated by the authentication manager does not appear to be explicitly present in E3. It will have however to be discussed during oral proceedings whether such ticket can be interpreted as being an example of a signature within the meaning of the claim.
The second line of attack refers to the embodiment of Fig. 71 and more specifically to Col. 257, lines 33-36. From this part, it is however not immediately apparent who is generating this signature and whether this signature is provided to the second transaction party (for feature M7)

M6.3: As mentioned in connection with feature M3, the Opposition Division has some doubts that the secure processing environment of the authentication software is inaccessible to the ROS.

M7: In view of the opinion provided above for feature M6.2, this feature does not appear to be disclosed in E3 either.

23.2 As a conclusion, the subject-matter of claim 1 appears to be novel in view of E3.

24 Novelty over E5.

24.1 E5 discloses:

M1: Fig. 2 and e.g. paragraph 0104. The first transaction party is the user of the electronic device which includes the PEAD 200 (see also paragraphs 0067 and 0072), the second transaction party is the server 1302.

M2: The PDAs given as examples in paragraph 0067 comprise implicitly an operating system as in feature M2.

M3: The Opponent has quoted paragraph 0074 for this feature. It is not immediately apparent from this passage why it can be considered that the OS of the PDA (which actually does not appear to be explicitly mentioned in E5) does not have access to the hardware components described in this paragraph.

M4, M4.1: The PDA provided as example can be seen to have some memory (necessary for it's functioning), at least the one used for the PEAD (paragraph 0074).

M4.2: Paragraph 0049 mentions a user identification data block 302, paragraph 0050 mentions user's private key 304 stores in memory portions which can be qualified as a secure area . However, again it could not be corroborated from the explanations of the Opponent where it is disclosed that such secure area is not reported to the OS (directly or indirectly).

M5: Paragraphs 0049 and 0050 appear to disclose this feature, see again the data block 302.

M5.1, M5.2: It is not known if the secure area is inaccessible or not to the operating system and therefore the features M5.1 and M5.2 do not appear to be directly and unambiguously disclosed.

M6: Paragraph 0074 together with e.g. paragraphs 0049-0050 may be seen as disclosing feature M6.

M6.1: As mentioned above for feature M4.2, it is not apparent why the secure area of E5 could be seen as inaccessible to the OS.

M6.2: The Opponent has quoted paragraphs 0075-0078 as well as paragraph 0051 in support of his contention that this feature is disclosed in E5. From these passages it is not immediately apparent whether a digital signature is generated by the authentication software. Paragraphs 0075-0078 appear to relate to encryption of data. Paragraph 0051 mentions an electronic signature but when read in combination with paragraph 0096 this could possibly be understood as the user's signature acquired using an "appropriate input device".

M6.3: Here also it does not appear to be disclosed in a direct and unambiguous manner that the secure process environment is inaccessible to the OS.

M7: Feature M7 refers to the digital signature defined in feature M6.2 (generated by the authentication software) which does not appear to be disclosed, so that feature M7 is also not disclosed. Looking at paragraph 0098, it could possibly be agreed that authentication data can be understood as digital signature.

24.2 As a conclusion, the subject-matter of claim 1 appears to be novel in view of E5.

25 Novelty over E6.

25.1 E6 discloses:

M1: See Fig. 14 and paragraph 0160. The first transaction party is the user (A) which uses the host computer 100, the second transaction party is C.

M2: An OS is disclosed, see e.g. paragraph 0124.

M3: See the licensing code components 200 which can be seen as an authentication software and which runs in a protected environment preferably within the trusted module. However, the Opposition Division cannot see a direct and unambiguous disclosure that this environment is independent from and inaccessible from the OS as required by feature M3.

M4, M4.1: Fig. 14 discloses some memory which appears to be accessible to the OS, see e.g. the HDD or the DRAM.

M4.2: The trusted module has some memory comprising some secure area in view of the kind of data stored in it (see e.g. Fig. 15). It is however not immediately apparent that such memory part is not reported to the OS.

M5: See e.g. paragraph 0125, the private key 212.

M5.1, M5.2: It is not known if the secure area is inaccessible or not to the operating system and therefore the features M5.1 and M5.2 do not appear to be directly and unambiguously disclosed.

M6: See e.g. the licensing code components 200 mentioned above, paragraph 0125.

M6.1: See the comments under feature M4.2 above. A secure area of the trusted module being inaccessible to the OS does not appear to be disclosed.

M6.2: See paragraph 0136, a digital signature appears to be generated by the secure executor 204 using the private key 212.

M6.3: As mentioned above, an environment inaccessible to the OS does not appear to be explicitly disclosed.

M7: Paragraph 0160 together with paragraphs 0136 and 0137 appear to disclose this feature.

25.2 As a conclusion, the subject-matter of claim 1 appears to be novel in view of E6.

26 Novelty over E8.

26.1 E8 discloses:

M1: See Fig. 1, the user of a remote terminal 110 being the first transaction party, the "intended recipient entity" of paragraph 1075 being the second transaction party.

M2: No OS appears to be explicitly disclosed, it may however be agreed that some kind of OS must be present, i.e. this feature appears to be implicitly disclosed. For instance, the vault mentioned at paragraph 1061 could be seen as user application needing some kind of OS.

M3: Fig. 3, paragraphs 1033 and 1034 may be seen as disclosing that some kind of authentication software might be present, see also paragraph 1075. However, in the absence of an explicit disclosure of an OS, it cannot be seen that there is a separate operating environment inaccessible to the OS.

M4, M4.1: See Fig. 3.

M4.2: There is a secure memory 254 but again its link to the (undisclosed) OS is not made.

M5: See paragraph 1008 and e.g. the certificates used for authentication.

M5.1, M5.2: Here again, in the absence of an explicit disclosure of an OS, it cannot be confirmed that the secure area is inaccessible to the OS.

M6: See paragraph 1075.

M6.1, M6.3: Again the inaccessibility to the OS does not appear to be directly and unambiguously disclosed.

M6.2, M7: See paragraph 1075.

26.2 As a conclusion, the subject-matter of claim 1 appears to be novel in view of E8.

27 Similar considerations apply to the subject-matter of independent claims 23 and 24 which also appears to be novel.

28 Inventive step.

In view of the provisional opinion of the Opposition Division concerning the ground of Article 100(c) EPC, it appears difficult to provide an opinion on inventive step at this stage. Taking into account the submissions made by the Opponent, it appears, however, that no document is available which discloses the (absence of) link between the OS and a secure area within the meaning of the independent claims. It is therefore at present not immediately apparent how the skilled person would arrive at the claimed subject-matter without exercising inventive skills.

Europäisches Patentamt
European Patent Office
Office européen des brevets

Wichtige Hinweise zur mündlichen Verhandlung

Das Europäische Patentamt verfügt über keine eigenen Dolmetscher. Diese müssen im Bedarfsfall von außerhalb, teilweise sogar aus anderen Ländern, beigezogen werden, was mit einem hohen Aufwand an Kosten und organisatorischen Vorbereitungen verbunden ist. Muss ein Verhandlungstermin kurzfristig abberaumt werden, können Kosten für bestellte Dolmetscher nicht mehr vermieden werden.

Es wird daher gebeten, eine Simultanübersetzung nur bei wirklichem Bedarf in Anspruch zu nehmen. Es wäre wünschenswert, wenn sich die Beteiligten (zweckmäßigerweise gleichzeitig mit der Terminabstimmung) auf die Benutzung einer Amtssprache einigen könnten. Bei Verständigungsschwierigkeiten sind die Mitglieder der Einspruchsabteilung bereit zu helfen.

Die von den Verfahrensbeteiligten bevorzugte (abgestimmte) Verhandlungssprache und ggf. eine notwendige Simultanübersetzung sind dem Amt möglichst vor der in Regel 4(1) EPÜ angegebenen Frist mitzuteilen.

☐ Verfahrenssprache ist **Deutsch**

Von der/dem/den Einsprechenden wurde

☐ Englisch

☐ Französisch benutzt.

Es wird um eilige Mitteilung - möglichst per Telefax an den zuständigen Formalprüfer - gebeten,

möglichst bis

Datum **07.10.20**

1. welche Sprache(n) Sie in der mündlichen Verhandlung verwenden (**Sprechen**)
2. aus welcher Sprache Sie eine Simultanübersetzung benötigen (**Hören**).

Important information concerning oral proceedings

The European Patent Office has no interpreters of its own. When interpreters are needed they have to be brought in from outside, sometimes even from other countries, which is costly and involves considerable organisation. If oral proceedings have to be cancelled at short notice, the cost of interpreters already engaged still has to be borne.

Please therefore make use of simultaneous interpreting facilities only where strictly necessary. If possible the parties should agree on an official language for the proceedings, preferably at the time when they arrange a date. The members of the Opposition Division will be willing to help should any communication problems arise.

The EPO should be told if possible before the period mentioned in Rule 4 (1) EPC which language the parties prefer (agree on) and whether simultaneous interpreting facilities are required.

☒ Language of the proceedings is **English**

The language used by the opponent/s was

☐ German OI - EN

☐ French.

Please inform us urgently - where possible by fax addressed to the formalities officer concerned -

if possible by

Date **07.10.20**

1. which language(s) you intend to use during the oral proceedings (**Speaking**)
2. from which language you need simultaneous interpretation (**Listening**).

Très important Procédure orale

L'Office européen des brevets ne dispose pas de son propre service d'interprètes. Aussi faut-il appel le cas échéant à des interprètes de l'extérieur, qui viennent même parfois de l'étranger, ce qui occasionne de frais élevés et demande un grand travail d'organisation. Si la date d'une procédure orale doit être annulée au dernier moment, il n'est plus possible d'éviter les frais d'interprètes.

Les parties à une procédure sont donc priées de ne demander une traduction simultanée qu'en cas de réel besoin. Il serait souhaitable qu'elles puissent se mettre d'accord en même temps qu'elles conviennent de la date sur l'utilisation d'une langue officielle comme langue des débats. Si les parties éprouvent des difficultés de compréhension lors des débats, les membres de la division d'opposition sont disposés à leur prêter leur assistance.

L'Office doit être avisé si possible avant le début du délai mentionné dans la règle 4(1) CBE de la langue préférée par les parties pour le déroulement des débat (et sur laquelle elles se sont préalablement mises d'accord) et de la nécessité éventuelle d'une traduction simultanée.

☐ La langue de la procédure est le **français**

La langue utilisée par l'opposant/les opposants était

☐ l'allemand

☐ l'anglais.

Prière d'indiquer d'urgence à l'agent des formalités compétent si possible par téléfax

si possible jusqu'au

Date **07.10.20**

1. quelle(s) langue(s) vous utiliserez au cours de la procédure orale (**pour parler**)
2. à partir de quelle langue vous aurez besoin d'une traduction simultanée (**pour écouter**).

Sollten Sie Ihren Antrag auf mündliche Verhandlung zurückziehen oder zum anberaumten Verhandlungstermin nicht erscheinen wollen bzw. aus wichtigem Grund daran gehindert sein, werden Sie gebeten,

- **unverzüglich das Amt - möglichst per Telefax - davon zu benachrichtigen, wobei das Schriftstück mit einem deutlichen Vermerk "Dringend, mündliche Verhandlung am ..." oder sinngemäß gekennzeichnet sein sollte;**
- **in dringenden Fällen** (weniger als 1 Monat vor dem Verhandlungstermin) zusätzlich **auch dem/die anderen Verfahrensbeteiligten** bzw. ihre(n) Vertreter auf schnellstem Weg **direkt zu unterrichten.**

In jedem solchen Fall obliegt der Einspruchsabteilung die Entscheidung, ob die Verhandlung durchgeführt oder abberaumt wird. Es wird jedoch darauf hingewiesen, dass einem Verfahrensbeteiligten, der eine nicht rechtzeitige oder unterbliebene Benachrichtigung zu verantworten hat, die dadurch den anderen Beteiligten verursachten Kosten auferlegt werden können (Art. 104 EPÜ).

Hinweis auf Regel 4 EPÜ

Regel 4
Sprache im mündlichen Verfahren

(1) Jeder an einem mündlichen Verfahren vor dem Europäischen Patentamt Beteiligte kann sich anstelle der Verfahrenssprache einer anderen Amtssprache des Europäischen Patentamts bedienen, sofern er dies dem Europäischen Patentamt spätestens einen Monat vor dem angesetzten Termin mitgeteilt hat oder selbst für die Übersetzung in die Verfahrenssprache sorgt. Jeder Beteiligte kann sich einer Amtssprache eines Vertragsstaats bedienen, sofern er selbst für die Übersetzung in die Verfahrenssprache sorgt. Von diesen Vorschriften kann das Europäische Patentamt Ausnahmen zulassen.

Should you decide to withdraw your request for oral proceedings or not wish to attend on the date set, or if for some special reason you are unable to do so, you are requested

- **to notify the EPO immediately, where possible by fax, marking the document clearly with the words "Urgent, oral proceedings on ..." or similar;**
- **in urgent cases** (less than one month before the date set for the proceedings), additionally to **notify the other party/parties** and/or their representative(s) **direct as rapidly as possible.**

In all such cases the Opposition Division will decide whether the proceedings are to go ahead or be cancelled. You should however note that costs incurred by the other parties may be charged to a party who either fails to notify them or does not do so in good time (Article 104 EPC).

Attention is drawn to Rule 4 EPC

Rule 4
Language in oral proceedings

(1) Any party to oral proceedings before the European Patent Office may use an official language of the European Patent Office other than the language of the proceedings, if such party gives notice to the European Patent Office at least one month before the date of such oral proceedings or provides for interpretation into the language of the proceedings. Any party may use an official language of a Contracting State, if he provides for interpretation into the language of the proceedings. The European Patent Office may permit derogations from these provisions.

Si vous retirez votre requête tendant à recourir à la procédure orale ou si vous ne souhaitez pas vous présenter à la date fixée pour la procédure orale ou ne pouvez vous y présenter pour une raison sérieuse, veuillez

- **en faire avis sans retard à l'Office, si possible par téléfax, en partant sur votre communication clairement la mention "Urgent, procédure orale le ..." ou une indication similaire;**
- **dans les cas urgents** (moins d'un mois avant la date fixée pour la procédure orale) **en faire avis également directement** pas la voie la plus rapide à **l'autre/aux autres partie(s)** ou bien à son/leurs mandataire(s).

Il appartient alors à la division d'opposition de décider si la procédure orale aura lieu ou non. Il est néanmoins souligné que les frais causés aux autres parties par une partie qui est responsable de l'omission d'un tel avis ou de ce que cet avis n'a pas été fait en temps utile peuvent être mis à la charge de cette partie (art. 104 CBE).

Rappel de la Règle 4 CBE

Règle 4
Langues admissibles lors de la procédure orale

(1) Toute partie à une procédure orale devant l'Office européen des brevets peut utiliser une langue officielle de l'Office européen des brevets autre que la langue de la procédure, à condition soit d'en aviser l'Office européen des brevets un mois au moins avant la date de la procédure orale, soit d'assurer l'interprétation dans la langue de la procédure. Toute partie peut utiliser une langue officielle de l'un des Etats contractants à condition d'assurer l'interprétation dans la langue de la procédure. L'Office européen des brevets peut autoriser des dérogations aux présentes dispositions.

(2) Die Bediensteten des Europäischen Patentamts können sich im mündlichen Verfahren anstelle der Verfahrenssprache einer anderen Amtssprache des Europäischen Patentamts bedienen.

(2) In the course of oral proceedings, employees of the European Patent Office may use an official language of the European Patent Office other than the language of the proceedings.

(2) Au cours de la procédure orale, les agents de l'Office européen des brevets peuvent utiliser une langue officielle de l'Office européen des brevets autre que la langue de la procédure.

(3) In der Beweisaufnahme können sich die zu vernehmenden Beteiligten, Zeugen oder Sachverständigen, die sich in einer Amtssprache des Europäischen Patentamts oder eines Vertragsstaats nicht hinlänglich ausdrücken können, einer anderen Sprache bedienen. Erfolgt die Beweisaufnahme auf Antrag eines Beteiligten, so werden die Beteiligten, Zeugen oder Sachverständigen mit Erklärungen, die sie in einer anderen Sprache als in einer Amtssprache des Europäischen Patentamts abgeben, nur gehört, sofern dieser Beteiligte selbst für die Übersetzung in die Verfahrenssprache sorgt. Das Europäische Patentamt kann jedoch die Übersetzung in eine seiner anderen Amtssprachen zulassen.

(3) Where evidence is taken, any party, witness or expert to be heard who is unable to express himself adequately in an official language of the European Patent Office or of a Contracting State may use another language. Where evidence is taken upon request of a party, parties, witnesses or experts expressing themselves in a language other than an official language of the European Patent Office shall be heard only if that party provides for interpretation into the language of the proceedings. The European Patent Office may, however, permit interpretation into one of its other official languages.

(3) Lors de l'instruction, les parties, témoins ou experts appelés à être entendus, qui ne possèdent pas une maîtrise suffisante d'une langue officielle de l'Office européen des brevets ou d'un Etat contractant, peuvent utiliser une autre langue. Si la mesure d'instruction est ordonnée sur requête d'une partie, les parties, témoins ou experts qui s'expriment dans une langue autre qu'une langue officielle de l'Office européen des brevets ne sont entendus que si cette partie assure l'interprétation dans la langue de la procédure. L'Office européen des brevets peut toutefois autoriser l'interprétation dans l'une de ses autres langues officielles.

(4) Mit Einverständnis aller Beteiligten und des Europäischen Patentamts kann jede Sprache verwendet werden.

(4) If the parties and the European Patent Office agree, any language may be used.

(4) Sous réserve de l'accord des parties et de l'Office européen des brevets, toute langue peut être utilisée.

(5) Das Europäische Patentamt übernimmt, soweit erforderlich, auf seine Kosten die Übersetzung in die Verfahrenssprache und gegebenenfalls in seine anderen Amtssprachen, sofern ein Beteiligter nicht selbst für die Übersetzung zu sorgen hat.

(5) The European Patent Office shall, if necessary, provide at its own expense interpretation into the language of the proceedings, or, where appropriate, into its other official languages, unless such interpretation is the responsibility of one of the parties.

(5) L'Office européen des brevets assure à ses frais, en tant que de besoin, l'interprétation dans la langue de la procédure, ou, le cas échéant, dans ses autres langues officielles, à moins que cette interprétation ne doive être assurée par l'une des parties.

(6) Erklärungen von Bediensteten des Europäischen Patentamts, Beteiligten, Zeugen und Sachverständigen, die in einer Amtssprache des Europäischen Patentamts abgegeben werden, werden in dieser Sprache in die Niederschrift aufgenommen. Erklärungen in einer anderen Sprache werden in der Amtssprache aufgenommen, in die sie übersetzt worden sind. Änderungen einer europäischen Patentanmeldung oder eines europäischen Patents werden in der Verfahrenssprache in die Niederschrift aufgenommen.

(6) Statements by employees of the European Patent Office, parties, witnesses or experts, made in an official language of the European Patent Office, shall be entered in the minutes in that language. Statements made in any other language shall be entered in the official language into which they are translated. Amendments to a European patent application or European patent shall be entered in the minutes in the language of the proceedings.

(6) Les interventions des agents de l'Office européen des brevets, des parties, témoins et experts faites dans une langue officielle de l'Office européen des brevets sont consignées au procès-verbal dans cette langue. Les interventions faites dans une autre langue sont consignées dans la langue officielle dans laquelle elles sont traduites. Les modifications apportées à une demande de brevet européen ou à un brevet européen sont consignées au procès verbal dans la langue de la procédure.

State of the proceedings

I. European patent N°1 634 140 B1 entitled *"METHOD AND SYSTEM FOR PERFORMING A TRANSACTION AND FOR PERFORMING A VERIFICATION OF LEGITIMATE ACCESS TO, OR USE OF DIGITAL DATA"* is based on European patent application N°04 748 654.3 (international application number PCT/NL2004/000 422). The patent Proprietor is
Ward Participations B.V.
De Schaepstal 1, 1251 MZ Laren, NL.
The mention of the grant of the patent was published in European Patent Bulletin 2019/03 on 16-01-2019. The patent claims the following priority: PCT/NL03/00436 filed on 13-06-2003

II. A notice of opposition against the patent has been filed on 16-10-2019 by:

Samsung Electronics Benelux B.V.
Evert van de Beekstraat 310
1118 CX Schiphol, NL

III. The Opponent submitted that the subject-matter of the patent was not patentable according to Article 100(a) EPC (Article 52(1) EPC; Articles 54 and 56 EPC) and Article 100(c) EPC. He requested to revoke the patent in its entirety and auxiliarily to arrange an oral proceedings according to Article 116 EPC.

IV. The following documents were cited by the Opponent in support of his requests:

E1 WO 2004/015579 A1 (TREK 2000 INT LTD [SG]; OOI CHIN SHYAN RAYMOND [SG] ET AL.) 19 February 2004 (2004-02-19)

E2 "Client Security Software Version 5.0 Installation Guide", IBM Client Security Solutions, September 2002 ;

E2a "IBM Improves PC Security System", IBM News room, 4 October 2002 (2002-10-04), pages 1-2, URL:https://www-03.ibm.com/press/us/en/pressrelease/485.wss ;

E2b "Embedded Security Chip and Software - a white paper", IBM Client Security Solutions, 1999, pages 1-6 ;

E2c "Client Security Software Version 1.0 Administrator's Guide", IBM Client Security Solutions, December 1999

E3 US 5 892 900 A (GINTER KARL L [US] ET AL) 6 April 1999 (1999-04-06)

E4 US 2002/007456 A1 (PEINADO MARCUS [US] ET AL) 17 January 2002 (2002-01-17)

E5 US 2002/023215 A1 (WANG YNJIUN P [US] ET AL) 21 February 2002 (2002-02-21)

E6 EP 1 076 279 A1 (HEWLETT PACKARD CO [US]) 14 February 2001 (2001-02-14)

E7 WO 01/17296 A1 (ERICSSON TELEFON AB L M [SE]) 8 March 2001 (2001-03-08)

E8 WO 02/076127 A1 (QUALCOMM INC [US]) 26 September 2002 (2002-09-26)

E9 GB 2 338 381 A (BARCLAYS BANK PLC [GB]) 15 December 1999 (1999-12-15)

E10 EP 1 237 324 A (SANYO ELECTRIC CO [JP]; PFU LTD [JP]; FUJITSU LTD [JP]; HITACHI LTD [J) 4 September 2002 (2002-09-04)

E11 WO 01/84319 A (XTEC INC [US]) 8 November 2001 (2001-11-08)

E12 WO 02/47081 A (SANDISK CORP [US]) 13 June 2002 (2002-06-13)

E13 US 5 802 590 A (DRAVES RICHARD P [US]) 1 September 1998 (1998-09-01)

E14 US 2001/051996 A1 (COOPER ROBIN ROSS [US] ET AL) 13 December 2001 (2001-12-13)

E15 US 2002/112162 A1 (COCOTIS THOMAS ANDREW [US] ET AL) 15 August 2002 (2002-08-15)

E16 US 2002/112171 A1 (GINTER KARL L [US] ET AL) 15 August 2002 (2002-08-15)

E17 US 2003/039362 A1 (CALIFANO ANDREA [US] ET AL) 27 February 2003 (2003-02-27)

E18 BENNET YEE: "Using Secure Coprocessors", THESIS SUBMITTED TO THE SCHOOL OF COMPUTER SCIENCE FOR THE DEGREE OF DOCTOR OF PHILOSOPHY, May 1994

E19 WO 00/67143 A2 (UNICATE BV [NL]; SIPMAN WILHELMUS HENDRIKUS MAR [NL] ET AL.) 9 November 2000 (2000-11-09)

E20 US 5 354 097 A (TEL TEUNIS [NL]) 11 October 1994 (1994-10-11)

E21 GERALD J POPEK ET AL: "Encryption and Secure Computer Networks", ACM COMPUTING SURVEYS, ACM, NEW YORK, NY, US, US, vol. 11, no. 4, December 1979, pages 331-356, ISSN: 0360-0300, DOI: 10.1145/356789.356794

V. With a letter, received on 03-03-2020, the Patentee filed observations concerning the opposition and requested to reject the opposition. Furthermore, he auxiliarily requested oral proceedings according to Article 116 EPC to take place.

Points to be discussed

1 Since both parties have requested oral proceedings as an auxiliary measure, the parties are hereby invited to attend such proceedings.

2 The points which need to be discussed are set out below and a provisional, non-binding opinion of the Opposition Division is given on the positions adopted by the parties. However, the discussion may cover further points according to the circumstances. The parties are asked to make their submissions well in advance of the date of the oral proceedings, i.e. at the latest at the date set in this summons, especially if new sets of claims or lines of argumentations are to be considered during oral proceedings.

3 The attention of all parties is drawn to the Guidelines E-III, 8.5 concerning submissions by the parties.

4 The present patent is based on an application filed before 13.12.2007, i.e. before the EPC 2000 is entered into force, and therefore in accordance with the transitional provisions as decided by the Administrative Council some of the provisions of the EPC 2000 are to be applied while other provisions of the EPC 1973 still apply. As the Euro-PCT at the basis of the patent in suit was still pending on 13.12.2007, Article 54(4) EPC 1973 and therefore Rule 23a EPC 1973 apply in the present case. For the rest, in the present case, no substantial difference could be detected between both provisions to be applied concretely and therefore for simplicity reasons it is referred merely to the EPC 2000, i.e. EPC unless otherwise mentioned.

5 In parallel to this opposition another opposition has been filed against the patent based on a divisional application of the application forming the basis of the patent discussed below. The Opposition Division will have the same composition in both cases and the intention is to have the oral proceedings on two consecutive days. In case the discussions would take longer than foreseen, it is planed to have a third day as a backup in order to avoid any postponement.

6 In order to ease the discussion, the features breakdown used by the opponent for the independent claims is also taken by the Opposition Division.

Claim 1:

M1: Method for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party,

M2: the electronic device having an operating system (48) creating a run-time environment for user applications

M3: and authentication software (54) running in a separate operating environment, independent from and inaccessible to said operating system, (48)

M4: the electronic device having a memory comprising

M4.1: storage locations, part of the memory being accessible to the operating system, (48)

M4.2: part of the memory being a secure area (62) storage locations of which are not reported to the operating system, (48)

the method comprising:

M5: providing authentication data (63A) in the secure area (62) of said electronic device

M5.1: which authentication data (63A) are inaccessible to a user of said electronic device,

M5.2: wherein said secure area (62) is inaccessible to said operating system (48) of said electronic device, thereby rendering the authentication data (63A) inaccessible to said user;

M6: providing authentication software (54) in said electronic device,

M6.1: the authentication data (63A) being accessible to said authentication software, (54) wherein the authentication software (54) is stored in the secure area (62) inaccessible to said operating system;(*) (48)

M6.2: activating the authentication software (54) to generate a digital signature from the authentication data, (63A)

M6.3: wherein the authentication software (54) is run in a secure processing environment inaccessible to said operating system;(*) (48)

M7: providing the digital signature to the second transaction party.

(*) Note: the Druckexemplar mentions a ";" which is not present on the B1 publication of the patent.

Claim 23:

S1: System for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party,

S2: the electronic device having an operating system creating a run-time environment for user applications

S3: and authentication software running in a separate operating environment, independent from and inaccessible to said operating system,

S4: the electronic device having a memory comprising

S4.1: storage locations, part of the memory being accessible to the operating system,

S4.2: part of the memory being a secure area storage locations of which are not reported to the operating system,

the system comprising:

S5: means for providing authentication data in the secure area of said electronic device

S5.1: which authentication data are inaccessible to a user of the electronic device,

S5.2: wherein said secure area is inaccessible to said operating system of said electronic device, thereby rendering the authentication data inaccessible to said user;

S6: means for providing authentication software in said electronic device,

S6.1: the authentication data being accessible to said authentication software, wherein the authentication software is stored in the secure area inaccessible to said operating system;

S6.2: means for activating the authentication software to generate a digital signature from the authentication data,

S6.3: wherein the authentication software is run in a secure processing environment inaccessible to said operating system;

S7: means for providing the digital signature to the second transaction party.

Claim 24:

E1: Electronic device for performing an electronic transaction between a first transaction party and a second transaction party, wherein the electronic device is operated by the first transaction party,

E2: the electronic device having an operating system creating a run-time environment for user applications

E3: and authentication software running in a separate operating environment, independent from and inaccessible to said operating system,

E4: the electronic device having a memory comprising

E4.1: storage locations, part of the memory being accessible to the operating system,

E4.2: part of the memory being a secure area storage locations of which are not reported to the operating system,

E5: the secure area storing authentication data

E5.1: which are inaccessible to a user of the electronic device,

E5.2: wherein said secure area is inaccessible to said operating system of said electronic device, thereby rendering the authentication data inaccessible to said user;

the electronic device comprising:

E6: a memory storing authentication software,

E6.1: the authentication data being accessible to said authentication software, wherein the authentication software is stored in the secure area inaccessible to said operating system;

E6.2: means for activating the authentication software to generate a digital signature from the authentication data,

E6.3: wherein the authentication software is run in a secure processing environment inaccessible to said operating system; and

E7: means for providing the digital signature to the second transaction party.

Article 100(c) EPC

7 Claim 1.

7.1 Generally, the subject-matter of claim 1 appears to be mainly based on claims 1, 26 and 27 of the application as originally filed WO 2004/111752 A2 (in the following called D2, like done by the Opponent). In addition, the operating system, the memory and the authentication software have been further specified based on the description.

7.2 Feature M1.

This feature was already present in claim 1 of D2.

7.3 Feature M2.

The Opponent has challenged the lack of basis of feature M2 in the originally filed application mainly on the ground that the only passage explicitly disclosing this definition (page 13, lines 23-24 of D2) is to be read in the context of the embodiment of Fig. 3 which discloses other components.

The Opposition Division is of the provisional opinion that this feature, although only explicitly present at one place in D2, is nothing more than providing the definition of what an operating system is and generally applies to the whole disclosure (see also point 4 of the decision T 0248/17).

7.4 Feature M3.

Page 7, lines 31-34 discloses that the authentication software is independent from and inaccessible to the operating system on the device. However, it is also specified there that the separate operating environment is in the BIOS or in a console. The Opposition Division has therefore some doubts that this feature has a basis in its present generality in D2.

7.5 Features M4 to M4.2.

The Opponent has argued that no part of D2 discloses a memory which comprises a combination of parts that are accessible and non-accessible to the operating system.

The Opposition Division notes the following:

Feature M4. The claim mentions a memory in general (and not for instance a memory module), while this aspect was already present in claim 1 of D2 (the authentication data is provided in a memory of said electronic device). It is not specified whether this memory is formed of one or several physical memory parts and where this memory is located. Generally speaking a memory must be present in an electronic device as claimed, independently of the embodiment considered, and a memory, as a matter of definition, comprises a storage location. Feature M4 appears therefore to have a basis in D2.

Feature M4.1. Page 11, lines 9-12 of D2 discloses that a secure memory location has to be provided as a part of a secure memory or it may be an encrypted part of a non-secure memory (therefore a non-secure memory is defined). At least a part of this memory is also accessible to the operating system (page 15, lines 11-14). In addition, this feature, as such, appears to be a common aspect of any operating system.

Feature M4.2. Page 14, lines 12-13, it is stated that in or behind the console 52, there is a secure area 62 only accessible to the BIOS. At page 7, lines 28-29, it is stated that the secure part of the device is accessible only to the BIOS. It is further stated (lines 13+) that the secure area 62 comprises applications and storage locations, which are not reported to the operating system 48. Later (lines 35+) it is stated that the secure area may further comprises other ... memory locations. Such a secure area appears therefore to be part of a memory.
Page 15, lines 21+ discloses that the authentication data is stored in a memory that is accessible to an operating system of the device and possibly to a user of said device. Page 18, lines 12+ appears to relate to a similar embodiment as far as this aspect is concerned. However, it is stated in that embodiment that the secure area 62 is not essential for performing the third embodiment (contrary to the part starting at page 15, line 21 which still appears to comprise a secure area 62). As argued indirectly by the Opponent, the embodiment starting at page 18, line 12 does not appear to be covered by claim 1.

The question which still arises is which link, if any, is to be made between features M4.1 and M4.2 and the BIOS (and possibly the console).

In the paragraph bridging pages 5 and 6 it is mentioned that in the context of the installation method a new device contains a BIOS and an existing device also contains such BIOS. It is also specified that the BIOS is used to access a memory location in a memory. This part appears to relate to all described embodiments. See with that regard page 5, line 19 and the reference to Figs. 1, 2, 4 and 6-9, while both Figs. 3 and 5A,B disclose the BIOS; access to a removable memory - Fig. 10 - is also to be done via the BIOS, see e.g. page 13, line 10.

Therefore, in the light of these passages, the Opposition Division has also doubts that the BIOS can be omitted from the combination of features M4-M4.2 without extending the content of the application as filed.

The fact that independent claim 1 of D2 does not mention the BIOS does not provide any technical teaching providing such a justification as the aspects related to the secure area have been taken from the description. The same applies in relation with page 2 of D2 quoted by the Patentee which appears to be directed to a mere repetition of the claims of D2. The decision of the BoA does not appear to provide a justification for the present generality either, as the claim pending at the time did have a reference to the BIOS.

7.6 Features M5 to M5.2.

In section B.I.3. of the notice of opposition, the Opponent argues that there is neither explicit nor implicit support for features M4 to M5.2.

The Opposition Division notes the following:

Features M4 to M4.2 have been discussed in the section above.

Features M5 and M5.1. These features were already present in claim 1 of D2 apart that secure area instead of memory is now used which appears to have a basis in e.g. Fig. 3 (see also the discussion above concerning feature M4.2). Concerning the expression "authentication data", the Opposition Division notes that this feature was present in the claim 1 of D2 which is supposed to cover all embodiments of D2. It is nevertheless noted that the specific embodiments of Figs. 1 and 2 appear to refer to an "authentication table" instead (see e.g. the random table supplier, page 6, line 17 and the random table lines 21-23). It is however noted that page 15, line 12 of D2 appears to provide the idea that an authentication table is an example for authentication data in general. Lastly, it is noted that a table can have one or several dimensions so that any data in a memory could possibly be considered as being part of the authentication table

in the absence of any definition for it. All in all, the Opposition Division is of the provisional opinion that "authentication data" in connection with the secure area as claimed is having a basis in D2, i.e. features M5 and M5.1 have such a basis.

Feature M5.2. This feature is repeating feature M4.2 with a slightly different wording. As the secure area is not reported/inaccessible to the OS it is de facto rendering the data in it inaccessible to the user.

Therefore, the Opposition Division is of the provisional opinion that the features M5 to M5.2 have a basis in D2, as far as features M4 to M4.2 have such a basis.

7.7 Features M6 to M6.3.

These features were not challenged by the Opponent.

Feature M6 and the first part of feature M6.1 appears to have a basis in claim 1 of D2.

Second part of feature M6.1 (starting at wherein).

Feature M6.2 appears to have a basis in claim 1 of D2. Fig. 3 appears to show that the authentication software is stored in the secure area 62 (see also page 14, lines 31-34).

Feature M6.3 appears to have a basis in claim 27 of D2.

A basis in D2 for these features appears therefore to be present.

7.8 Feature M7.

This feature was not challenged by the Opponent and was present in claim 1 of D2.

8 Independent claim 23.

Claim 23 is directed to a system for performing an electronic transaction, is based on claim 29 of D2 and corresponds for the rest to claim 1 in terms of means for. The same comments as made above for claim 1 apply mutatis mutandis.

9 Independent claim 24.

Claim 24 is directed to an electronic device for performing an electronic transaction and mostly takes back the features of claim 1. The same comments as made above for claim 1 apply mutatis mutandis.

10 Dependent claim 5.

The additional features of claim 5 appear to be based on page 8, lines 28-29 of D2. Whether the authentication software is to be defined in relation with the BIOS as argued by the Opponent will have to be discussed possibly also in connection with the independent claims.

11 Dependent claim 7.

The additional features of claim 7 appear to be based on claim 11 of D2 which depends on claim 10 of D2, itself forming the basis of claim 6 of the patent in suit. No key is present in claim 1 of the patent so that the argumentation of the Opponent cannot be followed.

12 Dependent claim 8.

The additional features of claim 8 appear to originate from page 14, lines 31-34 of D2. Whether these features have been taken out of their context or not will have to be assessed depending on the results of the discussion concerning feature M4.2 which defines the secure area 62.

13 Dependent claim 9.

The additional features of claim 9 appear to originate from page 15, lines 8-10 of D2. Again, whether these features have been taken out of their context or not will have to be assessed depending on the results of the discussion concerning feature M4.2 which defines the secure area 62.

14 Dependent claim 20.

The additional features of claim 20 appear to be based on claim 18 of D2. However, the dependencies of this claim as yet specified (claims 14 to 19) does not appear to have a basis in D2. Claim 18 of D2 was only depending on claims

14 to 17 of D2 which are not corresponding to claims 14 to 19 of the patent. The Opposition Division has doubts that no new combination was thereby introduced.

15 Dependent claim 21.

The parties appear to agree that the relevant part for seeking a basis for this claim is the passage starting at page 19, line 24 to page 20, line 8. The Opponent objects to claim 21 and argues that the specific sequence ("before...") is not explicitly disclosed in D2 and that these features have been extracted and isolated from the embodiment of Fig. 6. The Patentee argues that the above quoted passage is providing a basis for claim 21. The Opposition Division has doubts that this is the case, already because this embodiment appears to refer to the BIOS which is not present in claim 1 on which claim 21 depends but also because these features appear to have been extracted from the embodiment of Fig. 6. It will therefore have to be discussed whether a direct and unambiguous disclosure for claim 21 can be found in D2.

16 Dependent claim 22.

The additional features of claim 22 appear to be partly disclosed at page 8, line 29. Concerning the "two" private encryption keys (one in claim 5 and one in claim 22), this appears to be more a clarity problem than a lack of basis in D2. The general context of D2 appears to relate to digital data in connection with the encryption key, see page 3, lines 7-9. It will have to be discussed whether the new multiple dependencies have a basis in D2.

17 Other dependent claims. The Opposition Division notes provisionally the following:

17.1 Claims 2 to 4 appear to have a basis in claims 5 to 7 of D2.

17.2 Claims 6 and 7 appear to have a basis in claims 10 and 11.

17.3 Claim 10 appears to have a basis in claim 14.

17.4 Claim 11 appears to have some basis in page 19, lines 14-17. However, this part appears to relate to an embodiment possibly not covered by the present independent claims.

17.5 Claim 12 appears to have a basis in claim 15. However, it is not immediately apparent what is the basis for the new dependency structure. Furthermore, this aspect appears to relate to the embodiment where the memory is accessible to the user/OS, see e.g. page 17, lines 20-21, and therefore, it will have to be discussed whether this aspect can be combined with the features of claim 1.

17.6 Claims 13, 14. These claims appear to have some basis at page 17, line 32 to page 18, line 4. However, these parts refer to a second encryption layer not necessarily presently claimed as this aspect is only present starting at claim 12. Furthermore, it is not immediately apparent what is the basis for the new dependency structure.

17.7 Claim 15 appears to have a basis in claim 16.

17.8 Claim 16 appears to have a basis in claim 17, however, here also, it is not immediately apparent what the basis is for the new dependency structure.

17.9 Claims 17, 18 appear to have some basis page 19, lines 5-8. However, this part appears to relate to an embodiment possibly not covered by the independent claims. The reference to Fig. 3 shows that some aspect(s) of the first embodiment might be incorporated in the embodiment of Fig. 5A. The contrary does not appear, however, to be mentioned.

17.10 Claim 19 appears to have some basis page 26, lines 32-35 which, however, also appears to relate to an embodiment (where the memory is accessible to the user/OS) not covered by the present independent claims.

17.11 Claim 25. The only part which appears to provide some basis for this claim is page 12, lines 31-36. However, that this device should contain a BIOS appears mandatory in this passage. A clear basis for this claim is therefore not immediately apparent.

18 As a conclusion, although most of the features of the claims appear to have some basis in D2, it is not always immediately apparent whether the presently claimed combinations (including mixing of different embodiments) can be derived directly and unambiguously from the originally filed application. The provisional opinion of the Opposition Division is therefore that the subject-matter of the patent appears to extend beyond the content of the application as filed.

Article 100(a) in combination with Articles 52, 54 and 56 EPC

19 The Opponent has submitted that the subject-matter of claim 1 is not novel in view of E1, E2/E2a, E3, E5, E6, E8 and auxiliarily not inventive in view of E2/ E2a. The provisional opinion of the Opposition Division is as follows.

20 Validity of the priority claim with regard to the independent claims.

20.1 The Opponent has brought two lines of attack with regard to the priority.

20.1.1 First argumentation, concerning the feature M2.

The Opposition Division refers to point 7.3 above and provisionally does not see that the presence of this feature would lead to a loss of the priority right.

20.1.2 Second argumentation, concerning the absence in claim 1 of the patent in suit of the feature "providing digital data from the second transaction party to the first transaction party".

The Opposition Division tends to follow the argumentation of the Patentee that page 14, lines 10-15 and page 15 (lines 24-26) provides some support for omitting the last feature of claim 1 of the priority document, i.e. this feature is not an essential feature missing in claim 1 of the patent, which would lead to a loss of priority.

In case the Opposition Division would change its opinion on this, e.g. during oral proceedings in the light of arguments submitted by the parties, the Opposition Division has doubts that G 1/15 can be applied as it concerns generic "OR"-claims. Here the absence of an essential feature does not appear to fall under this category.

20.2 Similar considerations apply to independent claims 23 and 24.

21 Novelty over E1.

21.1 E1 has a publication date of 19.02.2004, i.e. after the priority date of the patent in suit (13.06.2003) but before its filing date (14.06.2004). The filing date of E1 is before the priority date of the patent in suit so that the validity of the priority of E1 is of no importance. E1 is a PCT application which had validly entered the European phase on 21.05.2004 in the form of an Euro-PCT application EP 03 713 173 and was still pending at the time of entry into force of the EPC 2000.

Article 158(1) and (2) EPC 1973 applies to the Euro-PCT of E1. In view of the provisional opinion mentioned above concerning the priority of the patent in suit, this document is therefore a document according to Article 54(3), (4) EPC 1973, i.e. only relevant for novelty. For simplicity reasons, reference to E1 is kept in the following, since the WO publication document corresponds to the publication of the Euro-PCT application.

21.2 E1 relates to a secured access to restricted information over the networks (page 1, lines 6+). Figs. 1 to 4 disclose four embodiments of an authentication system to verify a password from a host, Fig. 5 relates to a method for such authentication, Figs. 6-8 are directed to some specific system implementations, Fig. 9 is a block diagram of a SAKE (storage anti-piracy key encryption) implementation, while Figs. 10 and 11 are directed to further embodiments of related methods.

21.3 The Opponent presents an argumentation against the subject-matter of claim 1 by using parts of E1 which relate to Figs. 1, 2, 4, 7 and 9 and which appear to concern different embodiments of the invention disclosed in E1. As argued by the Patentee it is not immediately apparent how these embodiments can be combined, as no real link between them appears to be made in E1. Further to that, at least E1 does not appear to disclose the generation of a digital signature which is understood as a code which can act as a signature. A yes or no (verification of a password) does not appear to be such a signature.

21.4 Therefore, the subject-matter of independent claims 1, 23 and 24 appears to be new in view of E1, inventive step from E1 not being an issue at present (see point 21.1 above).

22 Novelty over E2a/E2.

22.1 Publication dates.

It appears undisputed that E2a has a publication date of 04.10.2002 in view of the date it bears.

Concerning E2, the following is noted:

It is referred in E2a to the Client Security Software, Version 5.0 (which installation guide is E2). There it is stated the availability of this software is scheduled for November 2002 while the Installation Guide itself bares the date of September 2002. All these dates are well before (more than six months) the priority date of the patent in suit. It is further noted that the version 5.1 was announced with a press release dated 15.04.2003 with an availability for May 2003 (https://www-03.ibm.com/press/us/en/pressrelease/240.wss), which is also before the priority date of the patent.

The Opposition Division is therefore of the provisional opinion that the Client Security Software, Version 5.0, was released before the priority date and therefore that E2, being its installation guide, was also available before the priority date.

22.2 E2a/E2 is to be considered as one document or not?

The Opposition Division tends to accept that starting from E2a, the link to E2 is precise enough to justify considering both teachings together. The fact that the E2 was possibly not available at the time E2a was published is not considered by the Opposition Division to prevent this view. The Guidelines G-IV, 8 refers to a decision of the BoA T 153/85 which does not appear to mention such criteria (see section 4.2 of the decision). The Opposition Division tends also to consider that the date to be considered when assessing the combination is the date of the latest of the two, here E2, which is anyway before the priority date of the patent in suit (see section 22.1).

The contrary (starting from E2) does not appear to be true as no mention of the press release appears to be present in E2.

Lastly, the Patentee has expressed some doubts as to whether a press release can be regarded to provide a technical disclosure. The Opposition Division is of the opinion that the state of the art comprises everything made available to the public (Article 54(2) EPC) and therefore that such type of document also belongs to the prior art which must be taken into consideration when assessing the patentability of a claim, as it mentions in it some technical aspects referring to existing systems, i.e. it provides some technical teaching.

22.3 E2a/E2 discloses:

M1: An Embedded Security Subsystem is offered on notebooks and desktops, the user of which is the first transaction party (first paragraph). The second paragraph mentions that the subsystem consists of both a hardware component, the cryptographic security chip, which supports key storage, privacy encryption and digital signatures for authentication of identity, and a downloadable software component, the Client Security Software, which interfaces with the user and with other software applications. The sixth paragraph quoted by the Opponent discloses that the Client Security Software is providing interoperability with IBM Tivoli Access Manager which is used to manage security policies. This allows consistent security policy enforcement across the organization for a wide range of Web and application resources. These resources may be seen as the second transaction party.

M2: See page 3 of E2 which discloses the required operating systems. As mentioned under point 7.3 any such OS is creating a run-time environment for user applications.

M3: Page 1 last sentence of E2 discloses that the Security Chip is encrypting and storing keys. An authentication software is therefore present in a separate environment. However, for similar reasons as those argued by the Patentee, the Opposition Division has doubts that this environment can be qualified as inaccessible to the operating system due to the access to the chip by a software running under the OS (for instance the Client Security Software).

M4,
M4.1: A notebook or desktop as mentioned in E2a comprises such features.

M4.2: The Security Chip includes some memory used to store keys and which can be qualified as providing a secure area, as the Secure Chip is not a normal component (like the hard disk for instance) used to store data (see E2a or page 3 of E2 as quoted above). However, it does not appear to be unambiguously disclosed that these storage locations are not reported to the OS.

M5: As mentioned above, the Security Chip includes some secure area used to e.g. store keys.

M5.1: As mentioned in E2a, second paragraph, the Client Security Software interfaces with the user and with other software applications.The authentication data appears therefore to be generally inaccessible to the user.

M5.2: This feature further repeats the definition of the secure area which was given in M4.2, which the Opposition Division does not see as being disclosed in E2a/E2, while at the same time further defining what is meant with the inaccessibility to the user. Hence, this feature does not appear to be disclosed in E2a/E2.

M6: An authentication software is disclosed in E2a/e2, see feature M3 above.

M6.1: The authentication data of the Secure Chip are accessible to the authentication software of the same chip. However, as mentioned above (M4.2), it does not appear to be disclosed that the secure area (of the chip) is inaccessible to the OS.

M6.2: E2a, second and third paragraph, appears to disclose part of this feature in that signatures are mentioned in connection with the Secure Chip ("supports"). The Opposition Division could not, however, corroborate that the Secure Chip is generating signatures through a software stored in itself.

M6.3: As mentioned in connection with M3, the Opposition Division has some doubts that it is directly an unambiguously disclosed that the secure processing environment of the chip is inaccessible to the OS.

M7: What is done with the signature mentioned in E2a is also not explicitly mentioned in E2a so that this feature also does not appear to be directly and unambiguously disclosed.

22.4 As a conclusion, the subject-matter of claim 1 appears to be novel in view of E2a/E2.

23 Novelty over E3.

23.1 E3 discloses:

M1: See e.g. the Virtual Distribution Environment (VDE) of Fig. 1. Col. 60, lines 8+ mentions that the VDE participants (i.e. each participant is a transaction party) may have an electronic appliance which may be or contains a computer. Fig. 7 discloses an example of VDE electronic appliance.

M2: As at least some of the appliances are meant to be used by consumers, it can be safely assumed that an OS must be present when the appliance is a computer. Such operating system appears to be called Rights Operating System (ROS) 602, see Col. 61, lines 21-22. The ROS is described starting at Col. 80, line 6. The ROS supports user application(s) 608 in addition to rights and auditing operating system functions 604 and other OS functions 606.

M3: Fig. 6 shows a Secure Processing Environment (SPE) 503 which is further described starting at Col. 112, line 1 and which is supported by the hardware resources of a Secure processing Unit (SPU) 500 (Col. 112, lines 12-13). The SPE is understood by the Opposition Division as a software which does not appear to be necessarily part of the SPU 500 as argued by the Opponent. The SPE includes an Authentication Manager 564 which can be seen as an authentication software within the meaning of feature M3. It is however stated at Col. 82, lines 55+ that the ROS manages the hardware (e.g. CPU, memory and encrypt/decrypt engines within the SPU 500). Therefore, the SPE 503 does not appear to be inaccessible to the ROS contrary to the requirement of feature M3. Fig. 7 or Col. 60, lines 13-14 do not appear to provide support for the contention that the ROS is left outside of the SPU 500 or SPE 503.

M4, M4.1: Fig. 7, Col. 82, lines 61+: the ROS managed the hardware like memories other than within SPU. These parts are accessible to the ROS.

M4.2: For this feature, the Opposition Division tends to follow the position of the Patentee. The memory manager 578 is part of the kernel 552 (Fig. 13) which is itself part of the SPE 503 (Fig. 13) itself part of the ROS (Fig. 12). Therefore, the parts of the memory driven by the memory manager do not appear to be "not reported to the operating system", rather merely their use is restricted to some specific processes of the ROS.

M5: From Col. 71, lines 28+ it can be read that sensitive information, such as encryption keys, is stored in the NVRAM 534b. The Opposition Division tends to consider such keys as being authentication data in the general sense of this term.

M5.1, M5.2: The secure area (the NVRAM 534b) is not inaccessible to the operating system (the ROS, see above feature M3) and as a consequence the Opposition Division tends to consider that it is de facto not inaccessible to the user within the meaning of features M5.1 and M5.2.

M6: An authentication software is provided, see above feature M3.

M6.1: The authentication manager 564 is part of the SPE 503 (Col. 112). The authentication data appear therefore to be accessible to the manager (whether they are really accessed and for what purpose does not appear to be disclosed). It is not clear to the Opposition Division where the manager 564 is stored and even if it was accepted that it is stored in the secure area defined in feature M5, this area appears to be accessible to the ROS (see above features M5.1, M5.2).

M6.2: The Opposition Division tends to follow the argumentation of the Patentee. The first line of attack of the Opponent refers to the Ticket Services mention at Col. 130, lines 32+. The tickets mentioned at Col. 131 are requested by the VDE and returned to it, i.e. a digital signature generated by the authentication manager does not appear to be explicitly present in E3. It will have however to be discussed during oral proceedings whether such ticket can be interpreted as being an example of a signature within the meaning of the claim.
The second line of attack refers to the embodiment of Fig. 71 and more specifically to Col. 257, lines 33-36. From this part, it is however not immediately apparent who is generating this signature and whether this signature is provided to the second transaction party (for feature M7)

M6.3: As mentioned in connection with feature M3, the Opposition Division has some doubts that the secure processing environment of the authentication software is inaccessible to the ROS.

M7: In view of the opinion provided above for feature M6.2, this feature does not appear to be disclosed in E3 either.

23.2 As a conclusion, the subject-matter of claim 1 appears to be novel in view of E3.

24 Novelty over E5.

24.1 E5 discloses:

M1: Fig. 2 and e.g. paragraph 0104. The first transaction party is the user of the electronic device which includes the PEAD 200 (see also paragraphs 0067 and 0072), the second transaction party is the server 1302.

M2: The PDAs given as examples in paragraph 0067 comprise implicitly an operating system as in feature M2.

M3: The Opponent has quoted paragraph 0074 for this feature. It is not immediately apparent from this passage why it can be considered that the OS of the PDA (which actually does not appear to be explicitly mentioned in E5) does not have access to the hardware components described in this paragraph.

M4, M4.1: The PDA provided as example can be seen to have some memory (necessary for it's functioning), at least the one used for the PEAD (paragraph 0074).

M4.2: Paragraph 0049 mentions a user identification data block 302, paragraph 0050 mentions user's private key 304 stores in memory portions which can be qualified as a secure area . However, again it could not be corroborated from the explanations of the Opponent where it is disclosed that such secure area is not reported to the OS (directly or indirectly).

M5: Paragraphs 0049 and 0050 appear to disclose this feature, see again the data block 302.

M5.1, M5.2: It is not known if the secure area is inaccessible or not to the operating system and therefore the features M5.1 and M5.2 do not appear to be directly and unambiguously disclosed.

M6: Paragraph 0074 together with e.g. paragraphs 0049-0050 may be seen as disclosing feature M6.

M6.1: As mentioned above for feature M4.2, it is not apparent why the secure area of E5 could be seen as inaccessible to the OS.

M6.2: The Opponent has quoted paragraphs 0075-0078 as well as paragraph 0051 in support of his contention that this feature is disclosed in E5. From these passages it is not immediately apparent whether a digital signature is generated by the authentication software. Paragraphs 0075-0078 appear to relate to encryption of data. Paragraph 0051 mentions an electronic signature but when read in combination with paragraph 0096 this could possibly be understood as the user's signature acquired using an "appropriate input device".

M6.3: Here also it does not appear to be disclosed in a direct and unambiguous manner that the secure process environment is inaccessible to the OS.

M7: Feature M7 refers to the digital signature defined in feature M6.2 (generated by the authentication software) which does not appear to be disclosed, so that feature M7 is also not disclosed. Looking at paragraph 0098, it could possibly be agreed that authentication data can be understood as digital signature.

24.2 As a conclusion, the subject-matter of claim 1 appears to be novel in view of E5.

25 Novelty over E6.

25.1 E6 discloses:

M1: See Fig. 14 and paragraph 0160. The first transaction party is the user (A) which uses the host computer 100, the second transaction party is C.

M2: An OS is disclosed, see e.g. paragraph 0124.

M3: See the licensing code components 200 which can be seen as an authentication software and which runs in a protected environment preferably within the trusted module. However, the Opposition Division cannot see a direct and unambiguous disclosure that this environment is independent from and inaccessible from the OS as required by feature M3.

M4, M4.1: Fig. 14 discloses some memory which appears to be accessible to the OS, see e.g. the HDD or the DRAM.

M4.2: The trusted module has some memory comprising some secure area in view of the kind of data stored in it (see e.g. Fig. 15). It is however not immediately apparent that such memory part is not reported to the OS.

M5: See e.g. paragraph 0125, the private key 212.

M5.1, M5.2: It is not known if the secure area is inaccessible or not to the operating system and therefore the features M5.1 and M5.2 do not appear to be directly and unambiguously disclosed.

M6: See e.g. the licensing code components 200 mentioned above, paragraph 0125.

M6.1: See the comments under feature M4.2 above. A secure area of the trusted module being inaccessible to the OS does not appear to be disclosed.

M6.2: See paragraph 0136, a digital signature appears to be generated by the secure executor 204 using the private key 212.

M6.3: As mentioned above, an environment inaccessible to the OS does not appear to be explicitly disclosed.

M7: Paragraph 0160 together with paragraphs 0136 and 0137 appear to disclose this feature.

25.2 As a conclusion, the subject-matter of claim 1 appears to be novel in view of E6.

26 Novelty over E8.

26.1 E8 discloses:

M1: See Fig. 1, the user of a remote terminal 110 being the first transaction party, the "intended recipient entity" of paragraph 1075 being the second transaction party.

M2: No OS appears to be explicitly disclosed, it may however be agreed that some kind of OS must be present, i.e. this feature appears to be implicitly disclosed. For instance, the vault mentioned at paragraph 1061 could be seen as user application needing some kind of OS.

M3: Fig. 3, paragraphs 1033 and 1034 may be seen as disclosing that some kind of authentication software might be present, see also paragraph 1075. However, in the absence of an explicit disclosure of an OS, it cannot be seen that there is a separate operating environment inaccessible to the OS.

M4, M4.1: See Fig. 3.

M4.2: There is a secure memory 254 but again its link to the (undisclosed) OS is not made.

M5: See paragraph 1008 and e.g. the certificates used for authentication.

M5.1, M5.2: Here again, in the absence of an explicit disclosure of an OS, it cannot be confirmed that the secure area is inaccessible to the OS.

M6: See paragraph 1075.

M6.1, M6.3: Again the inaccessibility to the OS does not appear to be directly and unambiguously disclosed.

M6.2, M7: See paragraph 1075.

26.2 As a conclusion, the subject-matter of claim 1 appears to be novel in view of E8.

27 Similar considerations apply to the subject-matter of independent claims 23 and 24 which also appears to be novel.

28 Inventive step.

In view of the provisional opinion of the Opposition Division concerning the ground of Article 100(c) EPC, it appears difficult to provide an opinion on inventive step at this stage. Taking into account the submissions made by the Opponent, it appears, however, that no document is available which discloses the (absence of) link between the OS and a secure area within the meaning of the independent claims. It is therefore at present not immediately apparent how the skilled person would arrive at the claimed subject-matter without exercising inventive skills.

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact

DeltaPatents B.V.
Fellenoord 370
5611 ZL Eindhoven
PAYS-BAS

Date
25.05.2020

Reference	Application No./Patent No.
330.002 EPw	04748654.3 - 1010 / 1634140
Applicant/Proprietor	
Ward Participations B.V.	

Summons to attend oral proceedings pursuant to Rule 115(1) EPC

You are hereby summoned to attend oral proceedings arranged in connection with the above-mentioned European patent.

The matters to be discussed are set out in the communication accompanying this summons (EPO Form 2906).

The oral proceedings, which will be public, will take place before the opposition division

on 07.12.20 at 09.00 hrs in Room 2453
at the EPO, Bayerstr. 34, PschorrHöfe, D-80335 München

No changes to the date of the oral proceedings can be made, except on serious grounds (see OJ EPO 1/2009, 68). If you do not appear as summoned, the oral proceedings may continue without you (R. 115(2) EPC).

Your attention is drawn to Rule 4 EPC, regarding the language of the oral proceedings, and to the Special edition No. 3 OJ EPO 2007, 128, concerning the filing of authorisations for company employees and lawyers acting as representatives before the EPO.

The final date for making written submissions and/or amendments (R. 116 EPC) is 07.10.20.

You are requested to report in good time beforehand to the porter in the EPO foyer. Room 3473 and 3474 are available as waiting rooms.

Parking is available in the underground car park, accessible only via the entrance "Grasserstrasse 2/6". On presentation of the summons to oral proceedings at one of the porters' lodges in the PschorrHöfe, the parking ticket will be revoked.

1st Examiner:	2nd Examiner:	Chairman:
Hijazi, Ali	Kleiber, Michael	Pavón Mayo, Manuel

For the Opposition Division

Annexes:
Confirmation of receipt (Form 2936)
Rule 4 EPC (EPC Form 2043)
Communication (EPO Form 2906)

Europäisches Patentamt • European Patent Office • Office européen des brevets

Registered letter to EPO postal service: 18.05.20

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact

Kaufmann, Tobias
Bardehle Pagenberg Partnerschaft mbB
Patentanwälte, Rechtsanwälte
Prinzregentenplatz 7
81675 München
ALLEMAGNE

Date
25.05.2020

Reference	Application No./Patent No.
S154820EPEIN OPPO 01	04748654.3 - 1010 / 1634140
Applicant/Proprietor	
Ward Participations B.V.	

Summons to attend oral proceedings pursuant to Rule 115(1) EPC

You are hereby summoned to attend oral proceedings arranged in connection with the above-mentioned European patent.

The matters to be discussed are set out in the communication accompanying this summons (EPO Form 2906).

The oral proceedings, which will be public, will take place before the opposition division

on 07.12.20 at 09.00 hrs in Room 2453
at the EPO, Bayerstr. 34, PschorrHöfe, D-80335 München

No changes to the date of the oral proceedings can be made, except on serious grounds (see OJ EPO 1/2009, 68). If you do not appear as summoned, the oral proceedings may continue without you (R. 115(2) EPC).

Your attention is drawn to Rule 4 EPC, regarding the language of the oral proceedings, and to the Special edition No. 3 OJ EPO 2007, 128, concerning the filing of authorisations for company employees and lawyers acting as representatives before the EPO.

The final date for making written submissions and/or amendments (R. 116 EPC) is 07.10.20.

You are requested to report in good time beforehand to the porter in the EPO foyer. Room 3473 and 3474 are available as waiting rooms.

Parking is available in the underground car park, accessible only via the entrance "Grasserstrasse 2/6". On presentation of the summons to oral proceedings at one of the porters' lodges in the PschorrHöfe, the parking ticket will be revoked.

1st Examiner:	2nd Examiner:	Chairman:
Hijazi, Ali	Kleiber, Michael	Pavón Mayo, Manuel

For the Opposition Division

Annexes:
Confirmation of receipt (Form 2936)
Rule 4 EPC (EPC Form 2043)
Communication (EPO Form 2906)

Registered letter to EPO postal service: 18.05.20