Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
80298 MUNICH
GERMANY

ONTVANGEN 2 8 MEI 2020

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

Formalities officer
Vilz, Brigitte

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

Date: 27.05.2020

Reference	Application No./Patent No.
330.002 EPw2	17000713.2 - 1010 / 3229099
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 : 27.05.2020

Unterschrift / Signature:

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

DELTAPATENTS
Fellenoord 370
5611 ZL Eindhoven
the Netherlands
Tel: + 31(0)40 2936800
Fax: + 31(0)40 2366708

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 06.10

BV50040

State of the proceedings

I. European patent N°3 229 099 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°17 000 713.2 which is a divisional application of 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 2018/35 on 29-08-2018. 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 29-05-2019 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), Article 100(b) EPC and Article 100(b) 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 02/01334 A2 (MICROSOFT CORP [US]) 3 January 2002 (2002-01-03)

E12 WO 01/46918 A2 (ARCOT SYSTEMS INC [US]) 28 June 2001 (2001-06-28)

E13 WO 00/67143 A2 (UNICATE BV [NL]; SIPMAN WILHELMUS HENDRIKUS MAR [NL] ET AL.) 9 November 2000 (2000-11-09)

E14 US 5 354 097 A (TEL TEUNIS [NL]) 11 October 1994 (1994-10-11)

V. With a letter, received on 24-10-2019, 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.

VI. With a letter, dated 10-01-2020, the Opponent filed a response to the submission of the Patentee. With a letter, dated 21-04-2020, the Patentee also filed an additional response to the submission of the Opponent.

VII. The following documents were cited by the Patentee in support of his answers:

E17 BIOS Boot Specification Version 1.01, Compaq Computer Corporation Phoenix Technologies Ltd. Intel Corporation, January 11, 1996

E18 Copy of the page "BIOS" found at https://en.wikipedia.org/wiki/BIOS; downloaded on 14-Oct-2019

E20 A press release of Phoenix Technologies and Orbid Corporation Partner

E21 Smart Computing Article - What Is The BIOS Computing Basics. July 1994 • Vol.5 Issue 7

Obtained from http://www.smartcomputing.com/editorial/article.asp?article=articles/1994/july94/pcn0713/pcn0713.asp

Through the Internet Archive

http://web.archive.org/web/20120310002756/http://www.smartcomputing.com/editorial/article.asp?article=articles/1994/july94/pcn0713/pcn0713.asp

E22 IBM Personal Computer XT Hardware Reference Library, Technical Reference

First edition January 1983 (page 2), Linked from https://en.wikipedia.org/wiki/BIOS (note number 12), Obtained from: http://www.reenigne.org/crtc/PC-XT.pdf

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 In parallel to this opposition another opposition has been filed against the patent based on the parent 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.

5 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 creating a run-time environment for user applications,

the method comprising:

M3: providing authentication data in a memory of said electronic device,

M3.1: said memory being a secure part of a Basic In Out System or any other secure location in said electronic device, which authentication data are inaccessible to a user of said electronic device,

M3.2: wherein the authentication data are encrypted when the authentication data are stored in said memory,

M3.3: a decryption key for decrypting the authentication data being incorporated in the electronic device,

M3.4: said decryption key being inaccessible to said user, to any user-operated software and to said operating system,

M3.5: wherein said memory is inaccessible to said operating system of said electronic device, thereby rendering the authentication data inaccessible to said user;

M4: providing authentication software in said electronic device,

M4.1: the authentication data being accessible to said authentication software, wherein authentication software is stored in said secure memory inaccessible to said operating system;

M4.2: activating the authentication software to generate a digital signature from the authentication data,

M4.3: wherein the authentication software is run in a secure processing environment inaccessible to said operating system;

M5: providing the digital signature to the second transaction party.

Claim 23:

S1: System for performing an electronic transaction between a first transaction party and a second transaction 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,

the system comprising:

S3: means for providing authentication data in a memory of said electronic device, , [sic]

S3.1: said memory being a secure part of a Basic In Out System or any other secure location in said electronic device, which authentication data are inaccessible to a user of the electronic device, , [sic]

S3.2: wherein the authentication data are encrypted when the authentication data are stored in said memory,

S3.3: a decryption key for decrypting the authentication data being incorporated in the electronic device,

S3.4: said decryption key being inaccessible to said user, to any user-operated software and to said operating system,

S3.5: wherein said memory is inaccessible to said operating system of said electronic device, thereby rendering the authentication data inaccessible to said user;

S4: means for providing authentication software in said electronic device,

S4.1: the authentication data being accessible to said authentication software, wherein the authentication software is stored in a secure memory location inaccessible to said operating system;

S4.2: means for activating the authentication software to generate a digital signature from the authentication data,

S4.3: wherein the authentication software is run in a secure processing environment inaccessible to said operating system;

S5: means for providing the digital signature to the second transaction party; and

S6: means for providing digital data from the second transaction party to the first 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,

the electronic device comprising:

E3: a memory storing authentication data ,

E3.1: said memory being a secure part of a Basic In Out System or any other secure location in said electronic device, which authentication data are inaccessible to a user of the electronic device, , [sic]

E3.2: wherein the authentication data are encrypted when the authentication data are stored in said memory,

E3.3: a decryption key for decrypting the authentication data being incorporated in the electronic device,

E3.4: said decryption key being inaccessible to said user, to any user-operated software and to said operating system,

E3.5: wherein said memory is inaccessible to said operating system of said electronic device, thereby rendering the authentication data inaccessible to said user;

E4: a memory storing authentication software,

E4.1: the authentication data being accessible to said authentication software, wherein the authentication software is stored in a secure memory location inaccessible to said operating system;

E4.2: means for activating the authentication software to generate a digital signature from the authentication data,

E4.3: wherein the authentication software is run in a secure processing environment inaccessible to said operating system; and

E5: means for providing the digital signature to the second transaction party.

Article 100(c) EPC

6 Claim 1.

6.1 Generally, the subject-matter of claim 1 appears to be mainly based on claims 1, 12, 14, 26 and 27 of the parent 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, the BIOS and the authentication software have been further specified based on the description.

6.2 Feature M1.

This feature was already present in claim 1 of D2.

6.3 Feature M2.

The Opponent has challenged in his two letters 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 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).

6.4 Feature M3.

This feature was already present in claim 1 of D2.

6.5 Features M3.1 and M3.5.

The authentication data and the memory.

6.5.1 Formally, feature M3.2 was present in claim 14 of D2 while the end of feature M3.1 (which authentication ...) was present in claim 1 of D2. However, feature M3.1 also defines the memory as being part of a BIOS or any other secure location. Therefore it has to be assessed from where in D2 this feature is coming from and what is the consequence on feature M3.2.

6.5.2 The Patentee first refers to page 6, lines 8-13. Here it is stated that the BIOS may be employed to securely store certain digital data. How the BIOS is employed and how the security is achieved (e.g. specific memory or encryption) is not mentioned in this part.

6.5.3 The Patentee also refers to page 14, lines 13-17 in support of the contention that secure location is not part of the BIOS. However, lines 12-13 defines that the secure area 62 is in or behind the console 52 and is only accessible to the BIOS. This is a very specific teaching which is not present in claim 1.

6.5.4 The Patentee further refers to claim 13 of D2. Here it is stated that the authentication data is provided in the BIOS. It is, however, not specified that this is done in a "secure part" of it.

6.5.5 The reference from the Patentee to the decision T 248/17 does not appear to provide a basis for this aspect either as the claim at the time was not trying to define the memory in the same manner as in present claim 1. Page 2, lines 22-23, 34 which were quoted in r. 3.1 mention that the authentication data is inaccessible to a user (not that the memory is somehow specific). Again, the fact that the authentication data are stored inaccessible to the user does not necessary imply some specificity of the memory as the data could be merely encrypted rendering it inaccessible to the user. Similarly, claim 1 of D2 does not provide more details on the memory but merely that the authentication data is inaccessible to the user. The discussion done in this part of the decision of the BoA appears more to relate to equating or not the authentication data with the authentication table.

6.5.6 The Opponent appears to put some emphasis on the difference between the authentication table and authentication data in general. The Opposition Division does not see any good reason at present to deviate from the conclusion reached by the BoA on this aspect in a similar context, i.e. some secure location being claimed. The authentication data is not any data in general but is, according to feature M4.2, suitable to be used by an authentication software to generate a digital signature, an example of it being an authentication table (page 15, line 12 of D2). This level of generality does not appear to be linked to the fact that it is stored or not in a memory accessible to the OS, and therefore it seems that the skilled person would derive from this that any authentication

data can be used as long as it is related to the generation of a signature. The Opponent further argues (item b, pages 16-17 of the notice of opposition) that D2 teaches a different treatment of authentication data and authentication table. The Opposition Division does not share this view: the only reason there is a difference of treatment appears to be due to the storage location (inaccessible or accessible). In fact the embodiment of Fig. 4, page 15 does not suggest any difference of treatment: on the contrary, it is specified that an example of the data can be an authentication table and nowhere it appears to be made any distinction depending on these two types of data.

6.5.7 The Opposition Division sees the following passages of the description as being relevant to assess feature M3.1, especially the relation between the BIOS and the secure memory location:

6.5.7.1 Page 5, line 36. Here a secure storage/memory location is mentioned but it should be associated with the BIOS. Authentication data/table is not mentioned here so this passage does not appear to provide an adequate basis.

6.5.7.2 Page 6, line 10. See point 6.5.2 above.

6.5.7.3 Page 9, line 33. A secure part of the BIOS is disclosed but to embed the authentication software, not the authentication data to be used by it.

6.5.7.4 Page 12, line 11. Here also, this passage mentions a secure part of the BIOS used to store the authentication software.

6.5.7.5 Page 12, lines 27-28. This passage mentions storing the authentication table in encrypted form in a secure part of the BIOS.

6.5.7.6 Page 14, lines 12-27. See also point 6.5.3 above. The authentication table is stored in the location 60 which is in the secure area behind the console itself linked to the BIOS.

6.5.7.7 Page 10, lines 21-30. This passage has been quoted by both the Opponent and the Patentee and appears to be the most relevant to the point at stake.

As mentioned above under point 6.5.6 it is provisionally assumed that when authentication table is mentioned in D2 a basis can be found to generalise to authentication data within the meaning of claim 1 in general.

In this part, it is disclosed at line 22 that "The encoded authentication table is stored in a secure part of the BIOS, where it may only be retrieved by the BIOS and not by the operating system". The Opposition Division considers therefore

that the first part of feature M3.1 (the memory being a secure part of the BIOS) together with feature M3.5 (which defines the non-accessibility to the OS) have their basis in the quoted sentence.

Furthermore, it is stated in this passage that "This secure part of the BIOS may also be any other secure location in the device. For instance, it may be a separate part of a hard drive of a computer, which part may not be accessible to the operating system, but only to the BIOS and/or authentication software" (emphasis added). Concerning the authentication software, page 8, lines 24-25 mentions that it is embedded or installed in the BIOS. This appears to be the only possibility disclosed and this appears also to imply a link to the BIOS. The Opposition Division considers therefore that the second part of feature M3.1 ("or any other secure location"), even together with feature M3.5, does not have a direct and unambiguous basis in the above quoted sentences as the link to the BIOS (directly or via the console) appears to be missing.

As a conclusion, the first alternative of feature M3.1 appears to have a basis in D2, contrary to the second alternative. It is also noted that feature M3.5 refers to "said memory" while feature M3.1, 2nd alternative, refers to "any other secure location" which does not help to be sure that a link between both features is at all envisaged.

6.6 Feature M3.2.

Encryption of the authentication data.

Cells 16 and 36 of Figs. 1 and 2 of D2 specify that it should be ensured that the (authentication) table is encrypted again, meaning it was encrypted at the first place. This is confirmed by page 9, lines 11-19 which discloses that the bit string (including the random table) is embedded in an encrypted manner.

6.7 Features M3.3 and M3.4.

The decryption key.

Feature M3.3. The Opposition Division could not identify where this feature in its present generality is disclosed: at present it could be that the decryption key is always "incorporated" in the electronic device (e.g. in a/the memory). What appears to be disclosed (see cells 14 of Fig. 1 or cell 34 of Fog. 2 of D2) is that on request of the BIOS and/or authentication software (cells 10 or 30), the decryption key is sent by the third party to the electronic device.

The Opposition Division could not immediately identify where feature M3.4 is unambiguously disclosed. The description related to Figs. 1 and 2 refer to the use of the decrypt key by the authentication software (page 10, lines 1+ or page 10, lines 18+), but it does not appear to be disclosed that the key is inaccessible. It could be argued that claim 14 provides some kind of partial (the OS is not mentioned) basis to this feature, it is, however, not fully clear in which context this applies.

6.8 Features M4 and M4.1 to M4.3.

Feature M4 appears to have a basis in claim 1 of D2.

Feature M4.1 appears to have a basis in claims 1 and 26 of D2.

Feature M4.2 appears to have a basis in claim 1 of D2. This is confirmed by Fig. 3 which appears to show that the authentication software is stored in the secure area 62 (see also page 14, lines 31-34).

Feature M4.3 appears to have a basis in claim 27 of D2.

6.9 Feature M5.

Feature M5 appears to have a basis in claim 1 of D2.

7 Claims 23 and 24.

7.1 It appears that at least the issues mentioned above under point 6 relating to claim 1 also concern claims 23 and 24.

7.2 In addition, the Opponent has challenged the basis of feature S4.1 resp. E4.1 in relation to the reference to "a" secure memory and not "the" secure memory defined earlier in the claim.

The Patentee argues that the claims refer to "a" secure memory "location" which is mentioned for the first time, concluding that there is no added matter for that reason.

Claims 23 and 24 refer both to said memory being a secure part of the BIOS or any other secure location in the electronic device (features S3.1 resp. E3.1) and a memory location as mentioned in features S4.1 resp E4.1. The argumentation of the Opponent, that a secure memory location can be different than the

memory being a secure part of the BIOS or any other secure location, appears therefore to be valid. The wording used is different than the one used in claim 1 while it is not immediately apparent what is the basis for these differences.

8 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.

9 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. Indeed, a decryption key is already mentioned in claim 1 of the patent in suit and it is therefore not immediately apparent if the same or another key is meant. This could possibly be seen as a clarity objection, not being a ground of opposition, however, this point will have to be discussed depending on the results of the discussion concerning claim 1.

10 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 M4.1 in combination with feature M3.1. At present, the Opposition Division tends not to follow the argumentation of the Patentee as the description from which this feature was taken relates to a very specific embodiment. Furthermore, it is noted that no secure area appears to be defined in claim 1. When attempting to interpret the claim, the reader may therefore have to refer to the description which defines the secure area in a quite specific manner.

11 Claim 16.

The additional features of claim 16 appear to be based on claim 18 of D2. However, the dependencies of this claim as yet specified (claims 11 to 15) 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 11 to 15 of the patent. The Opposition Division has doubts that no new combination was thereby introduced.

12 Claim 21.

The parties appear to agree that the relevant passage for seeking a basis for this claim can be found at page 19, line 24 to page 20, line 8. The Opponent objects to claim 21 in that he argues that the specific sequence ("before...") is not explicitly disclosed in D2 and in 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 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.

13 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 encryption key, see page 3, lines 7-9. It will have to be discussed whether the new multiple dependencies find a basis in D2.

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

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

14.2 Claim 6 appears to have a basis in claim 10.

14.3 Claim 9 appears to have a basis in claim 15. However, the claimed 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.

14.4 Claims 10, 11. These claims appear to have some basis at page 17, line 32 to page 18, line 4. However, these passages refer to a second encryption layer not necessarily presently claimed as this aspect is only present starting at claim 9. Furthermore, it is not immediately apparent what is the basis for the new dependency structure.

14.5 Claim 12. This claim appears to have some basis in claim 16, apart from the newly introduced dependency.

14.6 Claim 13. This claim appears to have some basis in claim 17, apart from the newly introduced dependency.

14.7 Claim 14. This claim appears to have some basis at page 19, lines 4-5, apart from the multiple dependency.

14.8 Claim 15. Claim 15 appears to have some basis at page 26, lines 32-35 which, however, appears also to relate to an embodiment (where the memory is accessible to the user/OS) not covered by the present independent claims.

14.9 Claims 17-20. These claims appear to have a basis in claims 19, 20, 23 and 24.

15 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 parent 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 earlier application as filed. Depending on the results of the discussion concerning the points mentioned above, it will have to be assessed whether the subject-matter of the patent extends beyond the content of the application as filed or not.

Article 100(b) EPC

16 The Opponent challenges in the notice of opposition the sufficiency of disclosure to carry out features M4.2 and M4.3 of claim 1. The Opponent mainly argues that external third party applications cannot make requests to the BIOS, as e.g. shown in Figs. 7-9.

17 The Patentee relies in its answers to E17 to E22 and argues against the view of the Opponent.

18 The Opposition Division tends to follow the view of the Patentee in that it seems that the skilled person would be able to modify the BIOS of an electronic device (used by the third party) to allow a software to use an interrupt to call a routine in the BIOS corresponding to the authentication software (thereby activating it). E17, E21 and E22 appear to be published well before the priority date of the present patent and can therefore be taken into account in this assessment. E17 discloses (page 34) that run-time functions may be optionally implemented in the BIOS. E21 appears to provide a similar information at page 2, 2nd paragraph: "But the BIOS' work isn't over. It also supplies run -time services while the computer is working". Pages 12 and 14 of E22 also appear to show that software interrupts are used to execute specific routines in the BIOS. Such modification of the BIOS appears to be within the normal knowledge of the developer of an electronic device as used in the present patent. The Opponent has also not shown why this kind of BIOS implementation would fail for technical reasons.

19 In the letter dated 10.01.2020, the Opponent further argues that feature M3.1 is also insufficiently disclosed due to the feature "or any other location". At present, the Opposition Division tends to consider that this part of feature M3.1 is going beyond the earlier application as filed (see point 6.5 above) and therefore this point will be discussed in relation with sufficiency depending on the results of the discussion concerning extension of subject-matter or not of feature M3.1.

Article 100(a) in combination with Article 54(1), (2) and Article 56 EPC

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

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

21.1 The Opponent has brought four lines of attack with regard to the priority.

21.1.1 First argumentation, concerning feature M2.

The Opposition Division refers to point 6.3 above and provisionally does not see that the presence of this feature would lead to a loss of the priority right.

21.1.2 Second argumentation, concerning feature M3.1 and the "any other secure location in said electronic device".

The Opposition Division refers to point 6.5 above. For similar reasons as stated there, a direct and unambiguous disclosure of this aspect does not appear to be present in the priority. It is, however, noted that any conclusion reached during the oral proceedings concerning this feature in relation with the earlier application as filed will most probably apply in relation to the priority.

21.1.3 Third argumentation, concerning feature M3.4.

The Opposition Division refers to point 6.7 above. Here also the objections made by the Opponent appear to be of similar nature as those concerning the extension of subject-matter compared to the earlier application. The discussion concerning this argumentation will therefore depend on the results of the one concerning extension of subject-matter.

21.1.4 Fourth 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.

21.1.5 All in all, it appears that if the objections under point 6 are dropped by the Opposition Division, the same reasons should probably be used to acknowledge the validity of the priority. If these objections are maintained the subject-matter of the claims will have to amended which might then automatically restore the priority as well. In the following, it will therefore provisionally be assumed that the priority is valid.

21.2 Similar considerations apply to independent claims 23 and 24.

22 Novelty over E1.

22.1 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) EPC, 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.

22.2 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.

22.3 The Opponent presents an argumentation against the subject-matter of claim 1 by referring to passages 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.

22.4 The general sentence (page 12, lines 23 to 25) quoted by the Opponent in its letter dated 10.01.2020 appears to be too general to provide a basis for the specific combination proposed by the Opponent. Furthermore, the further arguments brought in this letter concerning page 21, lines 14 to 18 tend not to

convince the Opposition Division: this passage of D1 does not appear to disclose directly and unambiguously the generation of a signature based on authentication data. The passage at page 6, lines 4 to 5 appears merely to state that the authentication algorithm 26 is used to authenticate the password 12 with an authentication sequence 24. From this passage, it is not immediately apparent that a signature is generated. This also does not help to understand what is meant at page 21 with the transmission of the authentication sequences to a server, as the authentication sequence appears to be a part of an algorithm i.e. a software.

22.5 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 22.1 above).

23 Novelty over E2a/E2.

23.1 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.

23.2 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 23.1).

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

23.3 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 6.3 any such OS is creating a run-time environment for user applications.

M3: The Security Chip includes some memory used to store keys, see E2a, second paragraph.

M3.1, M3.5: The memory included in the security chip can be qualified as secure (second alternative of M3.1), however, the first alternative (secure part of the BIOS) does not appear to be disclosed. Furthermore, it does not appear to be unambiguously disclosed that this memory is not accessible to the OS. The snapshot (from page 14 of E2c) produced by the Opponent in its letter corresponds to a windows software, i.e. which is run by the OS. Therefore the Opposition Division tends to consider that it is not inaccessible to the user within the meaning of features M3.1 and M3.5 taken together.

M3.2: See page 1, last paragraph of E2: "encrypting and storing keys on the ... Chip".

M3.3: See again page 1, last paragraph of E2. A decryption key must be incorporated in the electronic device in order to be able to use the authentication data.

M3.4: The decryption key should be inaccessible to the user, to any user-operated software and to the OS. The Opposition Division has doubts that this feature is disclosed in E2a/E2.

M4: The Client Security Software is an authentication software. The Opponent argues based on page 3, 4th paragraph, that the functions of the security chip are an authentication software within the meaning of the claim. It is, however, not immediately apparent what is the "security policy function" which is transferred to the secure hardware. A direct and unambiguous disclosure that this environment is inaccessible to the OS does not appear to be explicitly mentioned either (feature M4.3).

M4.1: Again, the Opposition Division cannot see that the security chip or the part storing the authentication data is inaccessible to the OS.

M4.2: 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. The Opposition Division has also doubts that a strong password can be seen as a digital signature within the meaning of claim 1.

M4.3: Again, it is not clear to the Opposition Division that an authentication software is run in an environment inaccessible to the OS (see feature M4 above).

M5: 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.

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

23.5 A similar assessment applies to the subject-matter of claims 23 and 24. The feature S6 of claim 23 appears to be known from E2a, 6th paragraph.

24 Novelty over E3.

24.1 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. The passage at Col. 66, line 41 quoted by the Opponent appears to mention that the ROS includes specific software, not that this software is independent from it.

M3: 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.

M3.1, M3.5: The memory NVRAM 534b can be qualified as secure (second alternative of M3.1) as, for instance, it is a specific memory surrounded by a tamper-resistant hardware security barrier (Col. 64, lines 29-30). However, the first

alternative (secure part of the BIOS) does not appear to be disclosed. Furthermore, it does not appear to be unambiguously disclosed either that this memory is not accessible to the OS. Indeed, it is 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 memory (the NVRAM 534b) does not appear to be inaccessible to the operating system (the ROS) and therefore the Opposition Division tends to consider that it is not inaccessible to the user within the meaning of features M3.1 and M3.5 taken together.

M3.2: The Opponent refers to Col. 76, lines 19 to 20 for this feature. This corresponds to the embodiment of Fig. 9A starting at Col. 73, line 1 where the SPU is integrated within the CPU. Indeed it appears that data maybe encrypted in memory 534 (when operation in SPU mode is done). It is, however, not stated which data are encrypted, i.e. it does not appear to be disclosed directly and unambiguously in the quoted passage that authentication data are encrypted. At Col. 67, lines 47+, the SPU Encrypt/ Decrypt Engine 522 is described: here also whether the keys are themselves encrypted or not does not seem to be disclosed.

M3.3, M3.4: As it is not clear whether the authentication data (keys) are encrypted, a corresponding decryption key does not appear to be unambiguously disclosed either.

M4: 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 M4.

M4.1: 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 memory defined in feature M3.1, this area appears to be accessible to the ROS (see above features M3.1, M3.5).

M4.2: 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 M5)

M4.3: It is 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 (R)OS contrary to the requirement of feature M4.3. 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. The Opposition Division has therefore some doubts that the secure processing environment of the authentication software is inaccessible to the ROS.

M5: In view of the opinion provided above for feature M4.2, this feature does not appear to be disclosed in E3 either.

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

24.3 A similar assessment applies to the subject-matter of claims 23 and 24. The feature S6 of claim 23 appears to be known from E3, Col. 54, lines 22-25.

25 Inventive step 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 e.g. paragraph 0125, the private key 212. Fig. 14 discloses some memory which appears to be accessible to the OS, see e.g. the HDD or the DRAM. Furthermore, the trusted module has some memory which could be considered as being secure 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 accessible to the OS.

M3.1, M3.5: The first alternative (secure part of BIOS) does not appear to be disclosed. Concerning the second alternative, it is not known if the memory is inaccessible or not to the operating system and therefore the features M3.1 and M3.5 do not appear to be directly and unambiguously disclosed.

M3.2: The Opponent acknowledges that this feature is not disclosed in E6.

M3.3, M3.4: M3.3 requires a decryption key for decrypting the authentication data. This is understood in the manner that the encryption key must be specific to encrypted authentication data which are not present in E6. Furthermore, it is required that the decryption key (stored in the trusted module) should be inaccessible to the OS which does not appear to be unambiguously disclosed (see features M3, M3.1 above).

M4: See e.g. the licensing code components 200 mentioned at paragraph 0125.

M4.1: The licensing code components are stored in the trusted module, which the Opposition Division provisionally does not consider as being inaccessible to the OS.

M4.2: See paragraph 0136, a digital signature appears to be generated by the secure executor 204 using the private key 212.

M4.3: As mentioned above, an environment inaccessible to the OS does not appear to be explicitly disclosed.

M5: Paragraph 0160 together with paragraphs 0136 and 0137 appear to disclose this feature.

25.2 The provisional opinion of the Opposition Division is that more differences are present in claim 1 compared to E5 than according to the submissions of the Opponent. It is true that it could possibly be successfully argued that encrypting/

decrypting data having some security relevance could be seen as obvious for the skilled person. However, it appears that the differences mentioned above go beyond merely this aspect. Therefore, the argumentation of the Opponent cannot be presently agreed by the Opposition Division.

25.3 A similar assessment applies to the subject-matter of claims 23 and 24. The feature S6 of claim 23 appears to be known from E6, paragraph 0160.

26 Inventive step over E5.

26.1 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: 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 being secure. However, again it could not be corroborated from the explanations of the Opponent where it is disclosed that such secure portion is not reported to the OS (directly or indirectly).

M3.1, M3.5: The data blocks 302 or 304 are not part of the BIOS (first alternative of feature M3.1) but can be considered as secure (part of the second alternative). However, a direct and unambiguous disclosure that the memory is not reported to the OS (directly or indirectly) does not appear to be present.

M3.2, M3.3, M3.4: The Opponent acknowledges that these features are not disclosed in E5.

M4: Paragraph 0074 together with e.g. paragraphs 0049-0050 may be seen as disclosing feature M4.

M4.1: As mentioned above for feature M3, the Opposition Division has doubts that the secure area of E5 can unambiguously be seen as inaccessible to the OS.

M4.2: 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".

M4.3: 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.

M5: Feature M5 refers to the digital signature defined in feature M4.2 (generated by the authentication data) 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.

26.2 The provisional opinion of the Opposition Division is that more differences are present in claim 1 compared to E5 than according to the submissions of the Opponent. As for E6, the argumentation of the Opponent starting from E5 cannot therefore be presently agreed by the Opposition Division.

26.3 A similar assessment applies to the subject-matter of claims 23 and 24. The feature S6 of claim 23 appears to be known from E5, see e.g. paragraph104.

27 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. The lines of argumentations provided at present by the Opponent do not appear to lead to the conclusion that the independent claims do not involve an inventive step.

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 **08.10.20**

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
[x] English

☐ German

☐ French.

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

if possible by

Date **08.10.20**

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 **08.10.20**

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

Date: 27.05.2020

Reference	Application No./Patent No.
S154820EPT1EIN OPPO 01	17000713.2 - 1010 / 3229099
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
+ 09.12.20

on 08.12.20 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 08.10.20.

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:
Hijazi, Ali

2nd Examiner:
Kleiber, Michael

Chairman:
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

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
27.05.2020

Reference	Application No./Patent No.
330.002 EPw2	17000713.2 - 1010 / 3229099
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
+ 09.12.2020

on 08.12.20 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 08.10.20.

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