Internal distribution code:

(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 6 September 2024

Case Number: T 1741/21 - 3.5.06

Application Number: 04748654.3

Publication Number: 1634140

IPC: G06F21/10, G06F21/73, G06Q20/02, G06Q20/38

Language of the proceedings: EN

Title of invention:
METHOD AND SYSTEM FOR PERFORMING A TRANSACTION AND FOR PERFORMING A VERIFICATION OF LEGITIMATE ACCESS TO, OR USE OF DIGITAL DATA

Patent Proprietor:
Ward Participations B.V.

Opponent:
Samsung Electronics Benelux B.V.

Headword:
Performing an electronic transaction I/WARD PARTICIPATIONS

Relevant legal provisions:
EPC Art. 100(c), 123(2)
RPBA 2020 Art. 13(1)

Keyword:
Amendments - added subject-matter (yes) - added subject-matter (no)
Amendment to appeal case - amendment detrimental to procedural economy (no)

Decisions cited:

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0

Case Number: T 1741/21 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 6 September 2024

Appellant: (Patent Proprietor)	Ward Participations B.V. Sloterweg 71 1171 CG Badhoevedorp (NL)
Representative:	DeltaPatents B.V. Fellenoord 370 5611 ZL Eindhoven (NL)
Respondent: (Opponent)	Samsung Electronics Benelux B.V. Evert van de Beekstraat 310 1118 CX Schiphol (NL)
Representative:	Kaufmann, Tobias Bardehle Pagenberg Partnerschaft mbB Patentanwälte, Rechtsanwälte Prinzregentenplatz 7 81675 München (DE)
Decision under appeal:	**Decision of the Opposition Division of the European Patent Office posted on 24 September 2021 revoking European patent No. 1634140 pursuant to Article 101(3)(b) EPC.**

Composition of the Board:

Chairman	M. Müller
Members:	A. Teale
	B. Müller

Summary of Facts and Submissions

I. The present appeal by the patent proprietor is against the decision, dispatched with reasons on 24 September 2021, to revoke European patent No. EP 1 634 140 B1 on the basis that the patent according to a main request (the patent as granted) and nine auxiliary requests contained added subject-matter, Articles 100(c) and 123(2) EPC, because, by not setting out a "BIOS", the independent claims set out a non-disclosed intermediate generalisation.

II. The patent stems from international patent application No. PCT/NL2004/000422, referred to as D2 in the decision, which was published as WO 2004/111752 A2.

III. The notice of opposition, received on 16 October 2019, relied upon the grounds for opposition under Article 100(a) (novelty and inventive step) and 100(c) EPC (added subject-matter).

IV. A notice of appeal and the appeal fee were received on 29 July 2021, shortly after the oral proceedings before the opposition division on 23 June 2021, the appellant requesting that the decision be set aside and the patent maintained as granted. The decision in writing was issued on 24 September 2021.

V. With a statement of grounds of appeal, received on 24 January 2022, the appellant refiled the main and (as auxiliary requests 1 to 4 and 10 to 14) the nine auxiliary requests treated in the decision. In addition, the appellant filed amended claims according

to new auxiliary requests 5 to 9 and made an auxiliary request for in-presence oral proceedings.

VI. In a response to the appeal, dated 7 June 2022, the respondent (opponent) requested that the appeal be dismissed, that auxiliary requests 5 to 9 not be admitted as late-filed and, as an auxiliary measure, oral proceedings.

VII. In a communication dated 30 July 2024 the board set out its provisional opinion on the appeal that the subject-matter of the independent claims of all requests seemed not to extend beyond that of the application as originally filed, Articles 100(c) and 123(2) EPC. However some dependent claims in all requests appeared to contain added subject-matter, so that the board had doubts regarding the allowability of all of the appellant's substantive requests. As the appealed decision made no finding on novelty and inventive step, the board was inclined, if the grounds of opposition under Article 100(c) EPC were overcome, to remit the case to the opposition division to consider the grounds under Article 100(a) EPC.

VIII. At the oral proceedings, held in presence on 6 September 2024, the appellant withdrew auxiliary requests 1 to 4. The board stated that, in the light of page 12, lines 31 to 37, of the application as filed, the board dropped its objection of added subject-matter against *inter alia* claim 13 of auxiliary requests 5 to 9. The appellant's final requests were that the decision under appeal be set aside and that the patent be maintained as granted or, in the alternative, on the basis of the claims of auxiliary requests 5 to 9, filed with the statement of grounds of appeal, auxiliary requests 10 to 14, filed with a letter of 23 April 2021

(as 5 to 9) and refiled with the statement of grounds of appeal, and auxiliary requests 15 to 19, filed with the letter of 15 August 2024. The respondent requested that the appeal be dismissed and that auxiliary requests 5 to 9 and 15 to 19 not be admitted into the proceedings as late filed.

IX. At the end of the oral proceedings the board announced its decision.

X. The patent is thus being considered in the following form:

Description (all requests):
Columns 1 to 21.

Claims:
Main request: 1 to 25, as granted.
Auxiliary requests 5 to 9, received with the grounds of appeal: 1 to 13.
Auxiliary requests 10 to 14, received as 5 to 9 on 23 April 2021: 1 to 10.
Auxiliary requests 15 to 19, received on 15 August 2024: 1 to 9.

Drawings (all requests):
Pages 19 to 25.

XI. Claim 1 according to both the main request (the patent as granted) and auxiliary request 5, including the feature labelling used in the decision, reads as follows:

"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."

XII. Claim 12 according to the main request reads as follows:

"Method according to any of the preceding claims, wherein the authentication data are encrypted using at least two encryption layers."

XIII. Claims 5, 8, 9 and 13 according to auxiliary request 5 read as follows.

"5. Method according to claim 1, wherein the authentication software has its own unique serial number, software ID and/or private encryption key."

"8. Method according to claim 1, wherein the authentication software is installed in an application environment in the secure area such that it may obtain the authentication data without passing through an unsecured part of said electronic device."

"9. Method according to claim 1, wherein the authentication data, and the authentication software including the digital signing algorithm are locked in the secure area."

"13. Electronic device according to claim 12, wherein the electronic device is a personal computer, a cellular phone, a hand-held personal digital assistant with wireless communication capabilities, the electronic device containing a BIOS."

Reasons for the Decision

1. Admissibility of the appeal

In view of the facts set out at points I, IV and V above, the appeal fulfils the admissibility requirements under the EPC and is consequently admissible.

2. The admittance of auxiliary request 5

2.1 This request, which was filed with the grounds of appeal, corresponds, as far as the independent claims are concerned, to the main request, differing only in the deletion of several dependent claims which were dependent on claim 1.

2.2 The appellant has argued that *inter alia* auxiliary request 5 removed dependent claims from an earlier request and addressed objections raised by the opposition division. According to the respondent, this request should not be admitted into the proceedings, as it was late filed and should have been submitted during first instance proceedings.

2.3 The board notes that, as the statement of grounds of appeal was received on 24 January 2022, which was after the entry into force of RPBA 2020 on 1 January 2020, RPBA 2020 applies to the present case, Article 25(1,2) RPBA 2020. Under Article 12(2,4) RPBA 2020 auxiliary request 5 constitutes an amendment to the appellant's case, since it did not form the basis of the appealed decision, so that it is only to be admitted at the discretion of the board. While this request *could* have been filed before the opposition division, the board

does not agree that it *should* have been filed, as it would not have changed the outcome of the decision under appeal. Therefore Article 12(6) RPBA 2020 does not prevent its admittance. In the present case, the board finds that deleting dependent claims is an amendment serving procedural economy, since it simplifies the proceedings and does not give rise to new objections.

2.4 Hence the board decided to admit this request into the proceedings.

3. The admittance of auxiliary requests 6 to 19

For the purposes of this decision, it is unnecessary to decide on the admittance of these requests.

4. Summary of the invention

4.1 References in the following are to the application as originally filed (D2).

4.2 The invention relates to establishing the identity of, in other words authenticating, the parties to an electronic transaction using digital signatures. A first party to a transaction uses an electronic device to generate a digital signature which is sent to a second party to the transaction.

4.3 An aim of the invention is to avoid the user having to acquire additional authentication hardware; see page 2, lines 14 to 17. For instance, it is known to use a trusted third party to establish the identity of the parties, this approach requiring every party to have a

hardware token and reader; see page 1, line 35, to page 2, line 13.

4.4 The invention identifies a first party transferring digital data, for instance music files, to a second party by embedding the first party's digital signature in the digital data; see page 3, lines 19 to 33. The signature binds the digital data to the identity of the first party and thus permits verification of whether the second party is authorized to have the data; see page 3, line 34, to page 4, line 17. According to the invention, authentication data and an authentication algorithm are stored in the electronic device used by the first party to generate the signature.

4.5 Figure 1 illustrates the steps taken by various "actors", namely a random-table supplier, a trusted third party (TTP), a BIOS manufacturer, a BIOS and authentication software (the latter two actors being software embedded in the device), to install software on a new electronic device, "new" meaning that it has not yet been delivered to an end-user. The device can be a computer, a PDA (personal digital assistant), a mobile telephone, a server or a printer; see sentence bridging pages 5 and 6. The device comprises a BIOS (Basic Input/Output System) with a secure storage/ memory location. The result is an electronic device having a BIOS comprising authentication software and a bit string, which can be sold to a customer; see page 9, lines 20 to 23.

4.6 Figure 2 relates to a second embodiment involving an "existing" electronic device which has already been delivered to the user. The BIOS in the device is immutable, being stored in ROM (read-only memory); see page 13, lines 10 to 13. In this embodiment

authentication software and authentication data are transferred via a communications link to the electronic device which is then caused to reboot (28). Once rebooted, the device stores the authentication software and authentication data in a secure memory location outside the BIOS, referred to in the description as the "secure part of the BIOS". The secure memory location can, for instance, be a separate part of a hard drive of a computer which is not "reported" to the operating system; see page 10, lines 22 to 28. In this context, memory resources are "reported" to the operating system (OS) when the system boots up, so that the OS "knows" of their existence and can subsequently access them.

4.7 According to page 6, lines 5 to 8, the BIOS "is only referred to as a system for accessing a memory location in a memory that is directly or indirectly connected to the electronic device". As shown in figure 3 (see page 13, line 5, to page 15, line 10), the device has a user application (30), a BIOS (44) containing an encryption key (46) and an OS (48) having a run-time environment. The device also comprises memory having a secure area (62) containing authentication software (54), in particular a digital signature algorithm (see page 15, lines 4 to 10) and authentication data (the authentication table) which is inaccessible to the OS but is accessible to the authentication software.

4.8 The authentication software runs in a secure processing environment on a piece of software termed a "console" (52)(see page 14, lines 1 to 11), the environment being inaccessible to the OS; see page 14, lines 27 to 34. The authentication software is activated to generate a digital signature from the

authentication data, the signature being provided to the second party.

4.9 In contrast, in the third embodiment, illustrated in figures 4, 5A and 5B, there is no secure memory area (see page 18, lines 17 to 21), and the authentication table is stored in encrypted form in a memory which can be accessed by the OS. This embodiment is excluded by the independent claims of all requests, since they set out *inter alia* the secure area being inaccessible to the OS.

4.10 Figure 6 illustrates a method of generating a digital signature. The authentication software first collects data (64) which is then used to generate a hash (66). The BIOS then decrypts the authentication table (68). The authentication software takes a series of random numbers from the authentication table, and the BIOS encrypts the authentication table again. The collected data together with its signature is transferred to the requesting application (74).

5. The board's understanding of the invention according to granted claim 1 (main request)

5.1 A first party having an electronic device performs an electronic transaction with a second party. The electronic device has an operating system (OS) which creates a run-time environment and a separate operating environment which is independent from, and inaccessible to, the OS. User applications run in the run-time environment, whilst authentication software runs in the operating environment.

5.2 Part of the memory of the electronic device is accessible to the OS. The storage locations of another

part of said memory are not reported to the OS at boot-up, thus constituting a secure area inaccessible to the OS and consequently the user. The secure area contains authentication software and authentication data. The authentication software has access to the authentication data and generates a digital signature from it, the signature being provided to the second party.

6. Added subject-matter, Articles 100(c) and 123(2) EPC

6.1 The original disclosure

6.1.1 The term "BIOS" occurs over 60 times in the original description and appears in original figures 1 to 3, 5a and 6 to 9. In contrast, the claims as originally filed only use the expression "BIOS" once, namely in claim 13 which sets out that "the authentication data are provided in a Basic Input-Output System (BIOS) of the electronic device."

6.1.2 Taken at face value, the board understands a "BIOS" to be a "Basic Input Output System" or, as the description puts it (see page 5, line 35), a "Basic In Out System", typically meaning software on a dedicated ROM chip on the motherboard (the "main board" in the application) of a personal computer; see page 13, lines 10 to 14.

6.1.3 The application also mentions other electronic devices, namely a server, a printer, a cellular phone and a hand-held PDA; see page 12, lines 31 to 37, and the sentence bridging pages 5 and 6. Although, in the board's understanding, not all of these devices typically comprise a BIOS, they might, and the application makes clear that an electronic device is meant to be "every device having a BIOS and capable of

communicating with external, third party applications"; see page 12, lines 31 to 32.

6.1.4 The description also states that a BIOS is "only referred to as a system for accessing a memory location in a memory that is directly or indirectly connected to the electronic device"; see page 6, lines 5 to 8.

6.1.5 In view of the last phrase, the board understands that a "BIOS" controls access by the OS and the console to memory, allowing the OS to only access certain parts of memory, but not the "secure area" (62), which can however be accessed by the console (52). For this reason, the board agrees with the finding in the decision (reasons, point 7) that the claims of all requests do not cover the third embodiment (see figures 4, 5A and 5B) in which all of memory can be accessed by the OS, and the authentication data is encrypted to render it inaccessible to the user; see page 15, lines 11 to 16.

6.1.6 Otherwise, three potential interpretations were considered during the oral proceedings before the board. (a) The phrase could be taken to *define* the term "BIOS" - and thus, deviating from the conventional understanding of the term, to actually *redefine* it - as any component "for accessing a memory location [...]". (b) It could be taken to *qualify* the type of BIOS used in the invention as one capable of "accessing a memory location [...]" and excluding others. (c) Or it could be taken to use the term "BIOS" with its conventional meaning but *stress* that the only function of relevance for the present invention is its capability of "accessing a memory location [...]".

6.1.7 The respondent dismissed option (a) and argued in favour of option (b). The board agrees that the phrase in question does not redefine the term "BIOS", and thus also dismisses option (a), but also does not accept interpretation (b) because the skilled person would have known that a basic BIOS function is to access memory, so that such a qualification would not have served any purpose. The board instead considers option (c) to be the correct one. The invention is meant to be carried out in an "existing device", having an immutable BIOS in ROM so that the authentication data and software are stored elsewhere, for instance on a hard disk; see page 17, lines 20 to 22. The phrase stresses the crucial BIOS function to be used, namely that of memory access.

6.1.8 The respondent pointed out that the passage on page 6 referred to above (point 6.14) was not contained in the priority document. The board notes, however, that the contents of the priority document have no bearing on the interpretation of the term BIOS in the context of the patent.

6.1.9 The board understands the electronic device of the invention to comprise means for controlling access to memory, said means forming an intermediate layer (see figure 3) between the device hardware (42) on the one hand and the OS (48) and the "Console" (52) - termed the "separate operating environment" in the claims - on the other.

6.2 The amendments to the granted patent (main request)

6.2.1 Claim 12 of the main request reads "Method according to any of the preceding claims, wherein the authentication

data are encrypted using at least two encryption layers."

6.2.2 According to the appealed decision (page 17, point 12.8), although based on original claim 15, this claim contained added subject-matter because it introduced a new dependency structure, relating to the third embodiment in which the memory was accessible to the user/OS; see D2, page 17, lines 20 to 22.

6.2.3 The appellant has argued that the claim dependencies of the original claims disclosed the combination of the embodiments using encryption and those using a "secure area". Moreover the original description (see page 6, lines 8 to 11) stated that the method according to the invention "may employ such a BIOS system to securely store certain digital data and/or such a BIOS system may be provided with an encryption system".

6.2.4 According to the respondent, claim 12 set out an undisclosed combination of the first and second embodiments, illustrated in figures 1 to 3, with the third embodiment, illustrated in figures 4, 5A and 5B.

6.2.5 The board notes that, whilst the first and second embodiments do disclose encryption/decryption of the authentication data (see figure 1; step 16 and figure 2; step 36), these embodiments primarily use memory access control by the BIOS to ensure that the OS and the user cannot access the authentication data. Claim 12 is however based on the passage on page 15, lines 26 to 27, of the original description relating to the third embodiment (see page 15, line 11, ff.) in which, as illustrated in figure 4, "the authentication data [...] is stored in a memory that is accessible to an operating system of the device and possibly a user of

the device". According to this original disclosure, encryption was used, and in a specific manner, as a substitute for the memory access control used in the first and second embodiments to prevent a user from accessing the authentication data. Thus claim 12 of the main request, being dependent *inter alia* on claim 1, which sets out the authentication data being inaccessible to a user of the electronic device, adds the concept that *two layers of encryption* can be used in a device also using memory access control. This is not directly and unambiguously derivable from the application as originally filed. In particular, this combination of features is not set out in the original claims, taking into account their dependencies.

6.2.6 Hence the amendment in claim 12 of the main request causes the subject-matter of the patent to extend beyond the content of the application as filed, so that the patent according to the main request does not comply with Article 100(c) EPC and cannot be maintained in this form; this follows from Article 101(2) EPC.

6.3 The amendments of the patent according to auxiliary request 5

6.3.1 Claim 1 is the same as that of the granted patent, so that the respondent's arguments regarding claim 1 of the main request apply equally to claim 1 of this request.

6.3.2 Claim 1 as originally filed set out a "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, the method comprising: providing authentication data in a memory of said electronic device which

authentication data are inaccessible to a user of said electronic device; providing authentication software in said electronic device, the authentication data being accessible to said authentication software; activating the authentication software to generate a digital signature from the authentication data; providing the digital signature to the second transaction party."

6.3.3 During grant proceedings claim 1 was restricted by adding the following features:

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

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

6.3.4 Regarding feature M3, the respondent has argued that the inclusion of the features "separate, independent and inaccessible environment" and "secure area", but not "BIOS", amounts to a non-disclosed intermediate generalisation. The board comes to a different conclusion. Although the board agrees that the description almost exclusively refers to devices with a BIOS without redefining the term "BIOS" (see above, points 6.1.1, 6.1.3 and 6.1.7), the board also considers that the description makes clear that the BIOS function relevant for the invention is only the memory access control. Moreover, this insight is reflected in the original claims, most of which do not require a BIOS. Instead, claim 1 as originally filed sets out authentication data in memory which is accessible to authentication software. It is implicit

in claim 1 as originally filed that the device comprises a system for accessing a memory location.

6.3.5 The respondent has also queried whether the "processing environment" in feature M6.3 is the same as the "operating environment" in feature M3, or whether the different expressions have different technical meanings. The board takes the view that the "processing environment" is only open to two reasonable interpretations: the operating environment (console 52) or the OS (48). However, in the light of figure 3 and feature M6.1 of claim 1, the authentication software cannot be understood to run under the OS (48); see page 7, lines 31 to 34. Hence the board finds that the expression "processing environment" must be interpreted to mean the same as the expression "operating environment". Having heard the board's conclusion, the respondent did not raise an objection of added subject-matter in this regard.

6.3.6 Turning to feature M4.2, the board finds it to be based on page 14, lines 12 to 22, of the application as originally filed.

6.3.7 The board concludes that the subject-matter of claim 1 does not extend beyond that of the application as originally filed.

6.3.8 The deletion of several dependent claims has rendered objections against them in the decision under Article 123(2) EPC moot.

6.3.9 In the oral proceedings the respondent only objected to dependent claims 5, 8, 9 and 13 under Article 123(2) EPC, arguing that, although the text of these claims could be found in the description, their features were

always intimately related to the BIOS, and the BIOS had been left out of these claims.

6.3.10 In view of the board's considerations under point 6.1.7 and 6.3.4 above, the board finds that all of these claims are properly based on the application as originally filed. Claim 5 is based on page 8, lines 28 to 29, the board seeing no functional relationship between the BIOS and the authentication software having its own serial number, software ID and private encryption key. Claim 8 is based on page 14, lines 31 to 34, the location of the authentication software in the secure area not requiring that a BIOS be present. Claim 9 is based on page 15, lines 8 to 10, the board understanding "locking" the algorithm in the secure area to mean storing it there. Claim 13 is based on the sentence bridging pages 5 and 6 and page 12, lines 31 to 37.

6.3.11 Consequently the board finds that the amendments to the patent according to auxiliary request 5 comply with Article 123(2) EPC.

7. Remittal, Article 111(1) EPC and Article 11 RPBA

As the appealed decision made no finding on novelty and inventive step, the board considers this to be a special reason for remitting the case to the opposition division to consider the grounds for opposition under Article 100(a) EPC.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.
2. The case is remitted to the department of first instance for further prosecution.

The Registrar: The Chairman:

L. Stridde M. Müller

Decision electronically authenticated