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 February 2018

Case Number: T 0248/17 - 3.5.06

Application Number: 04748654.3

Publication Number: 1634140

IPC: G06F1/00

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

Applicant:
Ward Participations B.V.

Headword:
Secure on-line transaction/WARD

Relevant legal provisions:
EPC 1973 Art. 56

Keyword:
Inventive step - after amendment and over the only document cited in the decision (yes)
Remittal to the department of first instance (yes)

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
Fax +49 (0)89 2399-4465

Case Number: T 0248/17 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 6 February 2018

Appellant: (Applicant)	Ward Participations B.V. 31, Zuidlaan 2111 GB Aerdenhout (NL)
Representative:	DeltaPatents B.V. Fellenoord 370 5611 ZL Eindhoven (NL)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 11 October 2016 refusing European patent application No. 04748654.3 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Sekretaruk
Members:	M. Müller
	G. Zucka

Summary of Facts and Submissions

I. The appeal is against the decision of the examining division, with reasons dated 11 October 2016, to refuse European patent application No. 04748654.3 for lack of novelty over the document

D12: US 2002/0023215 A1

(main and first auxiliary request) and non-compliance with Article 123(2) EPC (renamed second auxiliary request). A further request was not admitted according to Rule 137(3) EPC. Apart from D12, several other documents were mentioned in the decision but not relied upon in the reasons.

II. Notice of appeal was filed on 14 December 2016, the appeal fee being paid on the same day. A statement of grounds of appeal was filed on 5 January 2017. The appellant requested that the decision be set aside and that a patent be granted on the basis of claims 1-37 according to a main request or an auxiliary request as filed with the grounds of appeal.

III. The appellant also requested that the appeal procedure be expedited in view of the "limited remaining duration of a patent to be granted" (see the grounds of appeal, point 1.1) and, with reference to the EPO official notice concerning accelerated processing before the boards of appeal (OJ EPO 2008, 220), because infringement proceedings were envisaged (see the appellant's letter of 29 June 2017). In view of the envisaged infringement proceedings which are specifically mentioned in the official notice, the

board, in exercising its discretion, took this appeal out of turn.

IV. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that claim 1 of the two pending requests lacked novelty or inventive step. A number of terminological issues were also addressed.

V. In response to the summons, by letter dated 30 November 2017, the appellant filed amended claims 1-33 according to new second and third auxiliary requests.

VI. During the oral proceedings, which took place on 6 February 2018, the appellant withdrew all pending requests and filed an amended claim 1 as a new request. It further reserved the right to adapt the claims previously on file and the description.

VII. Claim 1 reads as follows:

"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 electronic device having a Basic In Out System and an operating system creating a run-time environment for user applications, the electronic device having a memory comprising storage locations, part of the memory being accessible to the memory of the operating system, part of the memory being a secure area of the Basic In Out System, storage locations of which are not reported to the operating system by the Basic In Out System, the method comprising:

providing authentication data in the secure area of said electronic device which authentication data are inaccessible to a user of said electronic device, wherein said memory is inaccessible to said operating system of said electronic device, thereby rendering the authentication data inaccessible to said user;

providing authentication software in said electronic device, the authentication data being accessible to said authentication software, wherein the authentication software is stored in the secure area inaccessible to said operating system;

activating the authentication software to generate a digital signature from the authentication data, wherein the authentication software is run in a secure processing environment inaccessible to said operating system;

providing the digital signature to the second transaction party."

VIII. At the end of the oral proceedings, the chairman announced the board's decision.

Reasons for the Decision

The invention

1. The application is concerned with secure electronic transactions between two transaction parties, for instance the transmission of a copyright protected digital file to a requesting user (see e.g. page 3, penultimate paragraph, and page 20, lines 20-30; all references to the description hereinbelow referring to the description as originally filed).

1.1 In this context, the application is specifically concerned with the electronic device operated by the first transaction party (see figure 3). This device comprises an operating system and a BIOS (a "Basic In Out System" as the application calls it, see the paragraph bridging pages 5 and 6). The BIOS controls the hardware components and, thereby, in particular the memory access by user applications via the operating system (see page 13, lines 8-9, 23-24 and 30-32).

1.2 It is disclosed that the device contains a "secure area" which is "only accessible to the BIOS" (see page 7, lines 25-29, and page 14, lines 12-13), which comprises "applications and storage locations, which are not reported to the operating system", and which, therefore, are inaccessible to the operating system (see page 14, lines 12-34, and figure 3).

1.3 It is specifically disclosed that the BIOS manufacturer "embeds or installs authentication software" and "an encoded authentication table" in the BIOS, and that the BIOS may comprise an encryption key (see page 8, lines 24-27; page 10, lines 31-35; page 13, line 20; and page 14, lines 27-34).

1.4 When a transaction request is received by a third party, it triggers the execution of the authentication software at the requesting device (see page 20, line 36, to page 21, line 10), which then decrypts the authentication table and generates a digital signature for the transaction data (see e.g. page 12, lines 24-37, and page 21, lines 5-17; figure 6). The digital signature is forwarded to the "third party" and eventually, embedded in the requested file and returned to the requesting party (figure 7 and page 21,

lines 28-30). The signature may help detect illegal copies of the digital file.

Article 123(2) EPC

2. The Article 123(2) EPC objection raised against the second auxiliary request relates to "encryption layers" which are not presently claimed (see the decision, point 6.3 of the reasons). This objection, therefore, does not apply to present claim 1.

3. The examining division took the view (see the decision, point 7.2 of the reasons) that the term "authentication data" was not disclosed in the context of the claim considered at the time because the description disclosed that an "authentication table" was stored in the secure area, because it was not clear whether "authentication data" and "authentication table" were synonyms or not, and because the description (in particular on page 15, lines 11-14) disclosed that the authentication data was stored in a memory which was accessible (rather than inaccessible) to the operating system.

3.1 The board however notes that the claims as originally filed and the corresponding passages of the description consistently talk about "authentication data" being stored inaccessibly to the user (see, for instance, page 2, lines 2, 22, 27 and 34, and original claim 1).

3.2 The board therefore does not share the examining division's concern under Article 123(2) EPC against the claimed use of "authentication data" rather than "authentication table".

4. Also beyond that, the board is satisfied that the subject-matter of claim 1 does not extend beyond the content of the application as originally filed. The BIOS is disclosed throughout the application and the "operating system creating a run-time environment for user applications" on page 13, lines 23-24. That there is "memory being accessible to the operating system" is also disclosed, for instance, on page 15, lines 11-14. Apart from that, this feature appears to be implicit to any operating system running user applications. The "secure area of the BIOS", apparently also "part of the memory", and the fact that it is "not reported to the operating system" is disclosed on page 14, lines 12-15, lines 23-25; page 12, lines 7-12; and page 15, lines 4-5.

The prior art

5. D12 relates to electronic transaction systems, *inter alia* in the context of electronic commerce and based on Internet capable mobile phones (see paragraphs 3, 67 and 108).

5.1 D12 proposes passing the user's transaction request through a device referred to as a portable electronic authorisation device (PEAD) (see paragraph 36, and figures 2 and 4). It is also disclosed that "PEAD functionality can be embedded into" a mobile phone and even that the PEAD as a whole "can be built[]in a portable phone" or other portable device (see paragraphs 67 and 72). The PEAD will display the transaction data for approval by the user (e.g. by "activating a switch"). If users do not wish to approve a proposed transaction, it is sufficient that they do nothing (paragraph 39). When the transaction is approved, the PEAD accesses "identification data rela-

ted to the user", kept "secure within the PEAD [...] at all times" (paragraphs 40 and 51), encrypts it (with the user's private key, see paragraph 44) and transmits it back to the requesting device (paragraphs 40 to 42). This is tantamount to the PEAD creating an electronic signature (see paragraphs 51, 104 and 109).

5.2 It is disclosed that the user's private key in the PEAD cannot be accessed "directly" but only via a component referred to as the "encryption logic block" (and an optional "decryption block"), or, in a different embodiment, other "logic circuitry" (see paragraphs 50, 53, 60, 64 and 65, and figures 3, 4 and 5A), and that it may itself be "scrambled or randomized" (see paragraph 59). While the encryption logic block depicted in figure 3 appears to be hardware, the "high-level hardware implementation of PEAD" depicted in figure 5A (see also paragraphs 61 and 62) comprises program memory.

5.3 It is also disclosed that, in some devices "there may not be a special tamper proof hardware such as a SIM [...] for the storage of the private key" (see paragraph 119) so that the private key must be "stored in the regular non-volatile memory in the portable device" (see paragraph 123). To protect that key against compromise, it is disclosed to encrypt it with a symmetric key" which, itself, may be stored on a remote server (see paragraphs 120 and 123).

5.4 The appellant referred to the two embodiments disclosed in D12 (up to paragraph 118 and from paragraph 119 onwards) as the "hardware PEAD" and the "software PEAD", respectively (see the appellant's letter of 30 November 2017, paragraph bridging pages 3 and 4 *et seq.*).

Inventive step

6. In the board's view, the most suitable starting point for assessing inventive step is the embodiment of D12 in which a "hardware PEAD" is incorporated into a portable device such as a mobile phone (see especially paragraph 72, last sentence.

6.1 In this scenario, the mobile phone as a whole qualifies as the claimed "electronic device operated by the first transaction party". The memory cell in the PEAD storing the private key constitutes a "secure area" which is "inaccessible to a user" of the electronic device, because access is possible only to the PEAD's dedicated logic circuitry, for instance the encryption and decryption logic blocks (see figures 3, 4 and 5A). The encryption circuitry of the PEAD effectively generates a digital signature from the authentication data, especially the private key, and thus carries out a function as claimed for the authentication software.

6.2 The hardware PEAD embodiment of D12 depicted in figure 3 does not disclose authentication software, but seemingly hardware. In the board's view, however, the skilled person would understand figure 5A as disclosing a software solution. At any rate, the board considers it to be well within the competence of the skilled person to replace hardware circuitry of the hardware PEAD by a corresponding software and suitable processing circuitry.

6.3 D12 does not expressly disclose the mobile device to have an operating system and does not mention a BIOS either. However, operating systems were already well-known for mobile devices before the presently claimed priority date (Symbian and PalmOS being examples in

point) and, moreover, if the skilled person were to implement the solution of D12 on a modern smartphone, an operating system and a BIOS would typically come with it.

6.4 However, the "secure area" of the PEAD in this scenario would be as inaccessible to the BIOS as it would to the operating system. In the words of claim 1, the secure area would not be one which would be for the BIOS to report (or not) to the operating system.

6.5 In the "software PEAD" of D12, the private key is stored in regular non-volatile memory (see paragraph 123) and there is no indication in D12 that this memory might be inaccessible to the operating system. The private key is secured by encryption using a key which is stored on a remote server.

6.6 In comparison with both the hardware PEAD and the software PEAD, the claimed invention provides an alternative solution for protecting the "secure area" (or its content).

6.7 As no mention at all is made in D12 of a BIOS or of the memory areas which it may or may not report to an operating system, the board takes the view that it would not have been obvious for the skilled person, on the basis of D12 alone, to modify the PEAD of D12 in such a way as to arrive at the invention.

6.8 The board thus concludes that the subject-matter of claim 1 shows an inventive step over D12 alone (Article 56 EPC 1973), by virtue of the feature that the BIOS "shields" the secure area from the operating system.

Remittal

7. The reasons of the decision relied exclusively on D12. Further documents were cited but not discussed in the decision. Two additional documents were cited in the International Search Report as very relevant when taken alone ("X"). At least some of these documents seem not to have been considered during examination.

8. The board also notes the following: During the oral proceedings before the examining division, the appellant had filed a second auxiliary request (see the minutes, page 3, lower third), which the examining division decided not to admit according to Rule 137(3) EPC because it was late filed and represented an intermediate generalisation from the description which "prima facie" did not comply with Article 123(2) EPC (see the minutes, page 4, paragraph 3 from the bottom, and the decision, point 7 of the reasons). *Inter alia*, it pointed out that "authentication data and software being unreachable and unknown to the operating system" was disclosed "only in connection with the BIOS" (see the minutes, page 5, paragraph 1, and the decision, point 7.4 of the reasons). This feature combination now being mentioned, the central reason for the non-admission decision is also overcome.

9. The board thus deems it to be appropriate to remit the case to the examining division for further prosecution.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.
2. The case is remitted to the examining division for further prosecution.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated