

**Internal distribution code:**

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

**Datasheet for the decision  
of 24 November 2023**

**Case Number:** T 2117/21 - 3.5.05

**Application Number:** 13714061.2

**Publication Number:** 2826201

**IPC:** H04L9/32

**Language of the proceedings:** EN

**Title of invention:**  
METHOD FOR SECURING MESSAGES

**Patent Proprietor:**  
BlackBerry Limited

**Opponent:**  
Infineon Technologies AG

**Headword:**  
Signed broadcast warning message/BLACKBERRY

**Relevant legal provisions:**  
EPC Art. 56  
RPBA 2020 Art. 12(6)

**Keyword:**  
Inventive step - (no)  
Late-filed facts - admitted in first-instance proceedings (no)



**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 2117/21 - 3.5.05

**D E C I S I O N**  
**of Technical Board of Appeal 3.5.05**  
**of 24 November 2023**

**Appellant:** Infineon Technologies AG  
(Opponent) Am Campeon 1-12  
85579 Neubiberg (DE)

**Representative:** K&L Gates LLP  
Karolinen Karree  
Karlstraße 12  
80333 München (DE)

**Respondent:** BlackBerry Limited  
(Patent Proprietor) 2200 University Avenue East  
Waterloo, ON N2K 0A7 (CA)

**Representative:** Murgitroyd & Company  
Murgitroyd House  
165-169 Scotland Street  
Glasgow G5 8PL (GB)

**Decision under appeal:** **Decision of the Opposition Division of the  
European Patent Office posted on 30 September  
2021 rejecting the opposition filed against  
European patent No. 2826201 pursuant to Article  
101(2) EPC.**

**Composition of the Board:**

**Chair** E. Konak  
**Members:** P. Cretaine  
E. Mille

## **Summary of Facts and Submissions**

I. This appeal is against the decision of the opposition division, dispatched on 30 September 2021, rejecting the opposition against the European patent No. 2 826 201. The opposition was based on the grounds of Article 100(a) EPC.

The opponent submitted documents D1 to D13 (see the impugned decision, I.3 and I.6), of which only D6, D8 and D10 were admitted into the opposition proceedings. The opponent based its objection of lack of inventive step on D10 as closest prior art, alone or in combination with D6, D8 or D11. The patentee submitted first to third auxiliary requests. The opposition division found that the claims as granted (main request) met the requirements of Article 56 EPC having regard to the disclosure of D10.

II. With the statement setting out the grounds of appeal received on 4 February 2022, the appellant (opponent) requested that D1 to D5, D7, D9 and D11 to D13 be admitted into the appeal proceedings and that the patent be revoked on the grounds of Article 100(a) EPC. Oral proceedings were requested on an auxiliary basis.

III. By letter received on 17 June 2022, the respondent (patentee) re-filed first to third auxiliary requests filed on 25 June 2020 in the first instance proceedings. The respondent requested not to admit D1 to D5, D7, D9 and D11 to D13 into the appeal proceedings, that the appeal be dismissed and that the patent be maintained as granted or in amended form based on one of first to third auxiliary requests.

IV. A summons to oral proceedings was issued on 24 January 2023. In a communication pursuant to Article 15(1) RPBA 2020 sent 18 October 2023, the board listed the points to be discussed during the oral proceedings. The board further indicated the reasons why it was minded not to admit D1 to D5, D7, D9 and D11 to D13 into the appeal proceedings.

V. Oral proceedings were held on 24 November 2023. The appellant requested that the decision under appeal be set aside and that the patent be revoked. The respondent requested that the appeal be dismissed (main request) or alternatively if the decision under appeal were set aside, that the patent be maintained in an amended form on the basis of the set of claims of any of first to third auxiliary requests filed with the letter dated 25 June 2020. At the end of the oral proceedings, the decision of the board was announced.

VI. Claim 1 of the main request (claims as granted) reads as follows:

"A method (1000) performed by a communication device (102a, 102b), said method comprising:  
receiving a transmission (1002) comprising a signature of a broadcast message, the broadcast message, and an implicit certificate;  
computing a public key using public information and the certificate; and  
verifying said signature (1004) using the public key, wherein the public key is associated with a private key used to generate the signature;  
wherein the broadcast message is a warning message."

The main request comprises further independent claims directed to a corresponding device (claim 6) and a corresponding computer program product (claim 8).

Due to the outcome of the appeal, there is no need to detail the claims of the first to third auxiliary requests.

### **Reasons for the Decision**

#### 1. Admittance of documents

In oral proceedings, both parties relied solely on their arguments provided in writing.

##### 1.1 D1 to D5, D7 and D9

These documents were not admitted into the proceedings by the opposition division for being late-filed and not referred to in any substantive argument of the opponent. The appellant provided arguments in respect of the timely filing of these documents in the proceedings before the opposition division and requested their admittance into the appeal proceedings.

However, the appellant did not base any of its substantive arguments with respect to the grounds of appeal under Article 100(a) EPC on these documents. For this reason, and irrespective of whether these documents had been late-filed or not, the board decided in oral proceedings not to admit D1 to D5, D7 and D9 into the appeal proceedings under the provisions of Article 12(6) RPBA.

1.2 D11 to D13

These documents were not admitted into the proceedings by the opposition division for being late-filed and not *prima facie* relevant.

The appellant argued that these documents should have been admitted by the opposition division because they were submitted as illustration of the common general knowledge already mentioned in the notice of opposition. Moreover, the appellant argued that D11 to D13 should be admitted into the appeal proceedings for being *prima facie* relevant for the inventive step assessment.

The board notes that D11 to D13 were late-filed since they were not submitted with or even mentioned in the notice of opposition, and since the common general knowledge they should illustrate was not exposed in the notice of opposition.

Furthermore, the board holds that D11 to D13 are not to be considered as illustration of the common general knowledge for the reason that they are not excerpts of basic or reference textbooks.

Finally, the board agrees with the decision (see sections 19 and 20) and the respondent that the late-filed documents D11 to D13 are not *prima facie* relevant documents for the assessment of inventive step. Therefore, the appellant's attacks based on late-filed documents D11 to D13 as prior art documents, provided in writing, cannot be admitted into the appeal proceedings.

For these reasons, the board decided in oral proceedings not to admit D11 to D13 into the appeal proceedings under the provisions of Article 12(6) RPBA.

2. Article 56 EPC

2.1 The labelling of features of claim 1 as granted used in the impugned decision (see Part II.8) is referred to in the following.

2.2 It was common ground in oral proceedings that D10 represented the closest prior art.

D10 discloses from page 3, line 32 to page 5, line 23 with respect to Figure 1 a method for receiving at a communication device B a message and its signature transmitted by a communication device A. The signature of the message is issued by A using A's private key received in a separate transmission from a certificate authority CA. The communication device B reconstructs A's public key by using an implicit certificate ( $I_A$ ,  $\gamma_A$ ) received from the certificate authority CA. The communication device B then verifies the signature on the message by using the reconstructed public key of A.

2.3 The board agrees with the respondent and the impugned decision that the subject-matter of claim 1 differs from the above mentioned disclosure of D10 in features V1 and V3.2, namely that the signature scheme is applied to a broadcast warning message (feature V3.2) and that the message, its signature, and the implicit certificate of the message's sender are included in a the same single transmission from the sender to the receiver (feature V1).

2.4 As to feature V3.2, the board holds that the designation of the message as a broadcast warning message does not represent a technical feature of the claimed method. Claim 1 relates to a method for receiving a broadcast message, which contrary to the generation and transmission of a broadcast message, does not involve specific technical features in the receiver with respect to the reception of a unicast message. The further feature that the message is a warning message is a feature related to the content of the message, not to its structural characteristics. Therefore, although the reception of a broadcast warning message is a distinguishing feature not disclosed in D10, the board agrees with the decision that the broadcast and warning aspects of the message may be included in the formulation of the technical problem.

The technical effect of feature V1 is that the message, the signature and the implicit certificate are received at the same time from the same transmission unit.

The advantage provided by this distinguishing feature is that the received message may be verified for authenticity by using the implicit certificate as soon as it is received and without having to wait for another transmission, which is a crucial issue for a warning message.

The objective technical problem may thus be formulated as how to adapt the system of D10 for the reception of broadcast warning messages.

2.5 As argued by the respondent, D10 is already adapted to receive broadcast warning messages and thus teaches an alternative solution for the problem, involving two

communication pathways, one from the device A to the device B and one from the CA to the device B for the transmission of the implicit certificate, a kind of certificate which enables a fast verification of the signature. The skilled person would find no motivation in D10 to suppress the involvement of the certificate authority in the sending of the implicit certificate in a separate transmission.

The two other prior art documents D6 and D8 admitted in the proceedings do either not disclose the transmission of an implicit certificate to a recipient of a signed message (D6) or do not disclose the transmission of an implicit certificate together with a signed message in a single transmission (D8). A combination of D10 with either one of D6 or D8 would thus, if even considered, not lead to the subject-matter of claim 1.

3. Appellant's arguments with respect to inventive step

3.1 The appellant first challenged that feature V1 was not disclosed in D1 when taking into account the whole disclosure of this document.

Firstly, according to the appellant, the fact that B got A's public data including A's implicit certificate ( $I_A, \gamma_A$ ), as disclosed in page 5, line 13, and that a communication channel is provided between A and B, as disclosed in page 4, lines 1 to 3, implies that B gets A's implicit certificate directly from A. The board is not convinced by this argument since the above mentioned passages refer to Figure 1 (see page 3, line 32) which clearly shows that the implicit certificate ( $I_A, \gamma_A$ ) is transmitted from the certificate authority CA to the device B in a different transmission through

a different communication channel than the message and its signature.

Secondly, the appellant made reference in oral proceedings for the first time to Figure 2 which, according to it, would be considered by the skilled person as being a part of Figure 1, and which showed that the implicit certificate ( $I_A, \gamma_A$ ) was transmitted from A to B. However, the board notes that Figure 2 is defined as being a representation of a second system configuration whereas Figure 1 relates to a first system configuration (see page 3, lines 22 to 27) so that it is difficult to conceive the scheme of Figure 2 as being included in the scheme of Figure 1. Further, the appellant did not provide any detailed explanations how the skilled person could combine the teachings of Figures 1 and 2 so as to arrive at a scheme according to claim 1.

- 3.2 In a second line of argument, the appellant suggested that, even if it were acknowledged that feature V1 was not disclosed in D1, the skilled person would be motivated by D1 itself to implement a single transmission of the message, the signature, and the implicit certificate from A to B. In this respect, the appellant referred to page 9, line 9, page 23, line 22 and page 24, line 10 of D10. According to the appellant, these passages showed that reducing the bandwidth was seen as a goal to be reached in D10 and that the skilled person would, to this aim, obviously consider sending the implicit certificate from A to B together with the message and its signature in a single transmission. The board is not convinced by this argument since D10, although mentioning in the above-mentioned passages that saving bandwidth is desired, does not suggest using a single transmission for the

message, its signature, and the implicit certificate. Rather, D10 proposes other solutions (see "Scheme 14" in page 10, "Scheme 4.c" in pages 23 and 24, "Scheme 5.c" in page 24) not relying on the direct transmission of the implicit certificate from A to B in the same transmission as the message and its signature. The board thus considers that the argumentation of the appellant is based on hindsight.

4. For these reasons, the board holds that the subject-matter of claim 1 and of corresponding independent claims 6 and 8 involves an inventive step (Article 56 EPC), having regard to the prior art on file. Claims 2 to 5 and 7 are dependent claims and as such also meet the requirements of Article 56 EPC.

## Order

### **For these reasons it is decided that:**

The appeal is dismissed.

The Registrar:

The Chair:



B. Brückner

E. Konak

Decision electronically authenticated