Internal distribution code:

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

Datasheet for the decision of 16 April 2024

Case Number: T 2196/21 - 3.5.03

Application Number: 13718664.9

Publication Number: 2826268

IPC: H04L29/06, H04W4/90, H04L9/32, H04W12/10

Language of the proceedings: EN

Title of invention:
Method for securing broadcast messages

Patent Proprietor:
BlackBerry Limited

Opponent:
Infineon Technologies AG

Headword:
Securing warning messages/BLACKBERRY

Relevant legal provisions:
EPC Art. 56, 100(a)

Keyword:
Inventive step - (yes): closest prior art is teaching away

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 2196/21 - 3.5.03

D E C I S I O N
of Technical Board of Appeal 3.5.03
of 16 April 2024

Appellant: (Opponent)	Infineon Technologies AG Am Campeon 1-12 85579 Neubiberg (DE)
Representative:	K&L Gates LLP Karolinen Karree Karlstraße 12 80333 München (DE)
Respondent: (Patent Proprietor)	BlackBerry Limited 2200 University Avenue East Waterloo, ON N2K 0A7 (CA)
Representative:	Murgitroyd & Company 165-169 Scotland Street Glasgow G5 8PL (GB)
Decision under appeal:	**Decision of the Opposition Division of the European Patent Office posted on 15 October 2021 rejecting the opposition filed against European patent No. 2826268 pursuant to Article 101(2) EPC.**

Composition of the Board:

Chair	K. Bengi-Akyürek
Members:	J. Eraso Helguera
	R. Romandini

Summary of Facts and Submissions

I. This case concerns the appeal filed by the opponent against the decision of the opposition division to reject the opposition under Article 101(2) EPC.

II. This decision refers to the following prior-art documents:

D1: Rabadi, N.M.: "Revised Self-Certified Implicit Certificate Scheme for Anonymous Communications in Vehicular Networks", 2010 IEEE Vehicular Networking Conference, pp. 286-292, 2010;

D5: Research in Motion UK Ltd.: "Comments on LS replies on length of security information in PWS", S3-111112, November 2011;

D9: EP 2 117 200 A1;

D11: National Institute of Standards and Technology (NIST): "Digital Signature Standard (DSS)", FIPS PUB 186-3, June 2009;

D14: Vodafone: "Distribution of keys for protecting public warning messages", S3-110394, April 2011;

D15: Certicom's Bulletin of Security and Cryptography Code & Cipher: "Explaining Implicit Certificates", pp. 5-6, 2004;

D16: NFC Forum: "Signature Record Type Definition", Technical Specification, SIGNATURE 1.0, NFCForum-TS-Signature_RTD-1.0, 18 November 2010.

III. Oral proceedings before the board were held on 16 April 2024. The final requests of the parties were:

- The appellant (opponent) requested that the decision under appeal be set aside and that the patent be revoked.

- The respondent (proprietor) requested, as a **main request**, that the appeal be dismissed, i.e. that the opposition be rejected and the patent maintained as granted, or, in the alternative, that the patent be maintained in amended form on the basis of the claims of either of **two auxiliary requests** filed during opposition proceedings and re-submitted with the written reply to the appeal.

At the end of those oral proceedings, the board announced its decision.

IV. **Claim 1 as granted** reads as follows:

"A method for use at a server (106), said method comprising:

sending a certificate request to the certificate authority server (104) of a Certification Authority, CA;

receiving a certificate from the certificate authority server (104), the certificate including an identity of the server (106) that owns a private key, a public key associated with the private key and a CA's signature that binds the identity and the public key;

obtaining (1062) a broadcast message, wherein the broadcast message is a warning message;

computing (1064) a signature for said broadcast message using the private key associated with the certificate; and

sending (1066) a single transmission to a communication device (102), said single transmission comprising said signature, said broadcast message and the certificate, wherein the certificate includes the public key associated with

the private key, wherein the public key can be used in verification of said signature;
wherein the server is operated by an Emergency Operations Center; and
the certificate is signed with an Elliptic Curve Digital Signature Algorithm."

Reasons for the Decision

1. MAIN REQUEST (PATENT AS GRANTED)

Claim 1 as granted comprises the following limiting features (outline used in the appealed decision):

A method for use at a server, said method comprising:

(V.1) sending a certificate request to the certificate authority server of a CA;
(V.2) receiving a certificate from the certificate authority server,
(V.2.1) the certificate including an identity of the server that owns a private key,
(V.2.2) a public key associated with the private key and
(V.2.3) a CA's signature that binds the identity and the public key;
(V.3) obtaining a broadcast message,
(V.3.1) the broadcast message is a warning message;
(V.4) computing a signature for said broadcast message using the private key associated with the certificate;
(V.5) sending a single transmission to a communication device,

(V.5.1) said single transmission comprising said signature, said broadcast message and the certificate,
(V.6) the certificate includes the public key associated with the private key,
(V.6.1) the public key can be used in verification of said signature;
(V.7) the server is operated by an Emergency Operations Center (EOC);
(V.8) the certificate is signed with an Elliptic Curve Digital Signature Algorithm (ECDSA).

1.1 Claim 1 - inventive step starting from D9 (Articles 100(a) and 56 EPC)

Starting point

1.1.1 Document **D9** concerns a method for authenticating a broadcast message in an Earthquake and Tsunami Warning System (ETWS) and serves as an appropriate starting point for the assessment of inventive step, as agreed by the respondent. In the language of claim 1, document D9 discloses a method for use at a server, said method *inter alia* comprising:

(V.3) obtaining a broadcast message ("primary notification"),
(V.3.1) the broadcast message is a warning message (Fig. 1: "First notification of UE"; [0037]: "primary notification");
(V.4) computing a signature for said broadcast message ~~using the private key associated with the certificate~~ ([0039]: "For signing, the authority which sends the warning message ... uses a regularly updated shared secret ...");

(V.5) sending a single transmission (Fig. 2: "Paging Message") to a communication device,

(V.5.1) said single transmission comprising said signature (Fig. 2: "30 bits - Reserved for signing"), said broadcast message (Fig. 2: "~20 bits - Including 1 bit ETWS identifier") ~~and the certificate~~,

(V.7) the server is operated by an EOC ([0039]: "the warning notification provider"; [0048]: "Notification Provider NP").

Distinguishing features

1.1.2 In agreement with Reasons 13 of the decision under appeal, the subject-matter of claim 1 differs from the method of **D9** in the following features:

(a) the use of an *asymmetric* signature scheme for the broadcast message as opposed to the *symmetric* signature scheme of D9 (**features (V2.1), (V2.2), (V2.3), (V4), (V6) and (V6.1)**),

(b) the inclusion of a public-key certificate signed with an ECDSA in the single warning transmission (**features (V5.1) and (V8)**) and

(c) requesting and receiving a certificate from a certificate authority server (**features (V1) and (V2)**).

1.1.3 The appellant submitted that the "Security Data" depicted in Fig. 1 of D9 fully disclosed feature (V5.1) and that paragraph [0057] of D9 partially disclosed features (V1) and (V2).

1.1.4 These arguments do not sway the board. Firstly, the "security data" of Fig. 1 is not directly and unambiguously disclosed to be a "broadcast message" like the "first notification". Secondly, the appellant does not dispute that what is requested and received in paragraph [0057] of D9 is not a "certificate" but a "key VK_i".

Technical effect and objective technical problem

1.1.5 On the basis of these differences, the opposition division defined the objective technical problem as "[how] to provide an alternative authentication method for the warning message [of D9]" (cf. appealed decision, Reasons 17 and 18).

1.1.6 The appellant argued that each of the differences (a), (b) and (c) identified by the opposition division and by the board helped to increase the security of the method of D9. Moreover, there was no particular synergy among them, in particular:

- asymmetric-cryptography schemes were known to be more secure because the private key was never distributed,
- ECDSA was known to provide a higher security than other encryption algorithms and
- the request and the receipt of the certificate from a CA server in response to a corresponding request offered the possibility to check the authenticity of the source.

Those advantages were in fact independent from each other.

1.1.7 The respondent submitted that the objective problem formulated by the opposition division was a valid one. Further, both document D9 (cf. paragraph [0038]) and the opposed patent (cf. paragraph [0025]) secured the warning message. However, the opposed patent achieved this purpose without requiring a repeated distribution of a shared secret. Rather, a *single* transmission [packet] contained all the elements required to maintain trust and verify the message in the underlying system.

1.1.8 From the arguments of the parties, the board understands that the claimed method would make possible at the receiving communication device the verification of the warning messages sent by the server with a reduced bandwidth use. Firstly, the public key of the claimed method does not require continuous updates. Secondly, the use of ECDSA reduces the number of bits required for a given cryptographic strength compared with e.g. RSA. This, together with the incorporation of consolidated information into a *single* transmission [packet], further decreases the overall number of transmissions and the overhead associated therewith. Thus, the board frames the objective technical problem as follows: "how to enable a reliable verification of the warning messages of D9 at the receiving device in a bandwidth-efficient way".

Could would approach

1.1.9 The appellant submitted that ECDSA was known to be more compact and it required the use of public-key cryptography. The skilled person would have easily recognised that the use of a shared secret in the system of D9 led to an inefficient use of bandwidth and would have replaced it by the more efficient ECDSA. In

doing so, the skilled person would have also discarded the use of different channels because this practice was inherently riskier.

1.1.10 The respondent contended that the use of multiple, separate messages was essential to the method of D9. In order to arrive at the claimed invention, the skilled person would have had to dismiss the explicit teaching of this document and make impermissible use of hindsight.

1.1.11 The board agrees with the respondent. In document D9, the amount of bits available for the signature is very limited, i.e. about 30 bits according to Fig. 2 and paragraphs [0041] and [0042]. This indeed teaches away from the claimed invention, because accommodating a public key and a certificate within few bits would be insufficient to provide a level of security at least at the level of the frequently-updated shared secret key. Alternatively, increasing the number of bits to be used in a single paging message in the scheme of D9 would require a re-design of the underlying network and cannot considered a straightforward endeavour. Rather, the skilled person would have maintained the signature in the "paging message" while reducing the update frequency of the shared secret key to an acceptable minimum or introduced ECDSA in the "Security Data" sent on the higher-bandwidth channel to reduce its size, yet keeping the "first notification".

1.1.12 It follows that the subject-matter of claim 1 does involve an inventive step starting from D9.

1.2 Claim 1 - inventive step starting from D1 (Articles 100(a) and 56 EPC)

1.2.1 In Reasons 21 of the decision under appeal, the opposition division stated the following:

> "It appears that at least in view of these amendments the examining division was of the opinion that the claims are new and involve an inventive step. The opposition division arrives at the same conclusion."

1.2.2 The appellant argued that document **D1** disclosed those features of claim 1 that are associated with a technical effect, referring to the written opinion of the International Search Authority and to the examination proceedings before the EPO.

1.2.3 The respondent acknowledged that D1 had been cited in the examination proceedings. However, the relevance of D1 had also been addressed by the response filed on 10 May 2017, and in the opposition proceedings (cf. Reasons 21 of the decision under appeal). There were no comments on the register, or filed by the opponent, or made in the decision, that D1 adversely affected the patentability of the granted claims. The opponent simply asserted – without foundation – that any feature that distinguished the method of claim 1 from D1 lacked a technical contribution. This premise was simply wrong. The lack of inventive step allegation over D1 was not fully substantiated and was thus incomplete.

1.2.4 The board concurs with the opposition division and with the respondent that the inventive-step attack using D1 as starting point is not fully substantiated and therefore not convincing. Furthermore, D1 proposes the use of an anonymous self-certified public-key "implicit certificate" scheme which fundamentally relies on the construction of the transmitter's public key on the

basis of the implicit certificate, thus teaching away from the inclusion of the public key itself in the broadcast message.

1.2.5 Hence, the subject-matter of claim 1 likewise involves an inventive step starting from D1.

2. As to the cited documents **D5** and **D11**, document D5 discloses, at most, feature V8 and makes a general reference to document D11. In that regard, the appellant's argumentation does not convincingly show how the skilled person starting from D9 would have indeed arrived at the introduction of all the distinguishing features into the system of D9 through a combination with D5. In that regard, the appellant did not advance further arguments during the oral proceedings before the board.

3. As to the late-filed documents **D14 to D16**, the board notes that the opposed patent itself explicitly acknowledges both "implicit certificates" (cf. paragraphs [0046] and [0047]) and "emergency warning systems" in general (cf. paragraph [0003]) as forming part of the known prior art. Furthermore, the appellant agreed during the oral proceedings before the board that they are merely intended to evidence that the use of "implicit certificates" belonged to the skilled person's common general knowledge at the patent's priority date. However, neither the board nor the respondent contested this. Consequently, there was no need to decide on their admittance in these appeal proceedings.

4. In conclusion, the ground for opposition under Article 100(a) EPC in conjunction with Article 56 EPC

does not prejudice the maintenance of the granted patent.

5. Since there are no other grounds for opposition invoked by the appellant that could prejudice the maintenance of the granted patent, the appeal must be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chair:

B. Brückner K. Bengi-Akyürek

Decision electronically authenticated