BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

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

Datasheet for the decision of 17 November 2011

Case Number: T 0399/08 - 3.5.05

Application Number: 98952478.0

Publication Number: 1033009

IPC: H04L 9/32

Language of the proceedings: EN

Title of invention:
Masked digital signatures

Applicant:
Certicom Corp.

Headword:
Masked digital signatures/CERTICOM

Relevant legal provisions:
EPC Art. 123(2)

Relevant legal provisions (EPC 1973):
EPC Art. 54(3) (4), 84

Keyword:
"Clarity and support by the description - yes, after amendment"
"Novelty - yes, after amendment"
"Remittal to the department of first instance for further prosecution"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 0399/08 - 3.5.05

D E C I S I O N
of the Technical Board of Appeal 3.5.05
of 17 November 2011

Appellant: Certicom Corp.
5520 Explorer Drive
4th Floor
Mississauga, ON L4W 5L1 (CA)

Representative: Moore, Barry
Hanna Moore & Curley
13 Lower Lad Lane
Dublin 2 (IE)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 14 September 2007 refusing European patent application No. 98952478.0 pursuant to Article 97(1) EPC 1973.**

Composition of the Board:

Chair: A. Ritzka
Members: P. Corcoran
G. Weiss

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division to refuse the European patent application No. 98 952 478.0, publication No. EP 1 033 009, originally published as international application publication No. WO 99/25092 A.

II. The decision under appeal was dispatched on 14 September 2007 and was based on a request comprising a set of claims 1 to 19 filed with the letter dated 7 March 2006

III. According to said decision, the document D1 (EP 0807908 A) constituted prior art under Article 54(3) EPC and Article 54(4) EPC 1973 for the commonly designated states DE, FR and GB and, on this basis, was found to be prejudicial to the novelty of the subject-matter of claim 1 of the aforementioned request.

IV. Notice of appeal was received at the EPO on 13 November 2007 with the appropriate fee being paid on the same date. A statement setting out the grounds of appeal was received at the EPO on 14 January 2008. With the statement setting out the grounds of appeal the appellant filed a new request comprising claims 1 to 12. An amended page 4 of the description was also filed.

V. In a communication accompanying a summons to oral proceedings to be held on 17 November 2011, the board gave its preliminary opinion that the appellant's request was not allowable. In particular, a number of objections concerning clarity and support by the

description (Article 84 EPC 1973) were raised with respect to the wording of the independent claims.

The board noted that claim 1 of the request submitted with the statement setting out the grounds of appeal had been amended with the apparent intention of distinguishing its subject-matter from the disclosure of D1. Said claim now recited steps relating to the conversion of a masked digital signature to a regular digital signature.

The board expressed the preliminary opinion that the subject-matter concerning the conversion of a masked ECDSA signature to a regular ECDSA signature as disclosed on p.6 l.20-22 of the published application was not disclosed in D1. Subject to the objections under Article 84 EPC 1973 being overcome, said subject-matter thus appeared to provide a sufficient basis for overcoming the novelty objection under Article 54(3) EPC and Article 54(4) EPC 1973.

The appellant was advised that should the aforementioned novelty objection be overcome, the board was inclined to remit the case to the department of first instance for further prosecution in view of the fact that proceedings before said department had essentially been limited to a consideration of the question of novelty in the light of a document cited as prior art under Article 54(3) EPC and Article 54(4) EPC 1973.

VI. With a letter dated 10 October 2011, the appellant filed a new set of claims 1 to 12 to replace the claims on file and also filed an amended page 6 of the description.

VII. During the oral proceedings held as scheduled on 17 November 2011, the appellant submitted a new request comprising claims 1 to 12 to replace the claims of the request filed with the letter dated 10 October 2011.

VIII. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of claims 1 to 12 submitted during the oral proceedings and the description and drawings on file, *viz.*:

Description, pages:

1, 2, 5, 8 as published;

3, 3a, 7 as filed with the letter of 7 March 2006;

4 as filed with the letter of 14 January 2008;

6 as filed with the letter of 10 October 2011.

Drawings, sheets: 1/2 to 2/2 as published.

IX. Claim 1 of the appellant's request reads as follows:

"A method of signing a message *m* in a public key data communication system (10), by a correspondent (12) having a long term private key *d* and a corresponding long term public key derived from said long term private key *d*, said method comprising the steps of:

in a secure computer system (18) of said correspondent (12);

selecting a first short term private key *k*;

computing a first short term public key derived from said first short term private key *k*;

computing a first signature component r by using said first short term public key;

selecting a second short term private key t;

computing a second signature component s using said second short term private key t on said message m, said long term private key d, and said first signature component r; and

computing a third signature component c using said first and second short term private keys k and t respectively, and sending by said correspondent (12) said signature components (r,s,c) as a masked digital signature of said message m to a terminal (22) associated with said correspondent;

the method further comprising

using said second and third signature components (s,c) to compute a regular signature component $\bar{s}$, wherein said terminal (22) computes said regular signature component $\bar{s}$ and sends said signature components ($\bar{s}$,r) as a regular digital signature to a receiver verifier computer system (20) to enable said receiver verifier computer system (20) to verify said regular digital signature ($\bar{s}$,r) or wherein said terminal (22) sends said signature components (r,s,c) as a masked digital signature of said message m to a receiver verifier computer system (20), to enable said receiver verifier computer system (20) to use said second and third signature components (s,c) to compute a regular signature component $\bar{s}$ to compute said regular digital signature ($\bar{s}$,r) to enable said receiver computer system (20) to verify said regular digital signature ($\bar{s}$,r)".

Claim 7 of the appellant's request reads as follows:

"A correspondent (12) comprising a processor (18) for signing a message *m* in a public key data communication system (10), said processor having access to a long term private key *d* and a corresponding long term public key derived from said long term private key *d*, said processor (18) being configured for:

selecting a first short term private key *k*;

computing a first short term public key derived from said first short term private key k;

computing a first signature component *r* by using said first short term public key;

selecting a second short term private key *t*;

computing a second signature component *s* using said second short term private key *t* on said message *m*, said long term private key *d*, and said first signature component *r*;

computing a third signature component *c* using said first and second short term private keys *k* and *t* respectively; and the correspondent (12) being configured for sending said signature components (*r,s,c*) as a masked digital signature of said message m to a terminal (22) associated with said correspondent (12) to enable said terminal to perform one of:

(i) sending said signature components (*r,s,c*) as a masked digital signature of said message *m* to a receiver verifier computer system (20) associated with said data communication system (10) to enable said receiver verifier computer system (20) to use said second and third signature components to compute a regular signature component $\bar{s}$ and verify a regular digital signature ($\bar{s}$,*r*); and

(ii) using said second and third signature components (*s,c*) to compute a regular signature

component $\bar{s}$, and sending said signature components ($\bar{s}$,r) as a regular digital signature to a receiver verifier computer system (20) to enable said receiver verifier computer system (20) to verify said regular digital signature ($\bar{s}$,r).

X. In the amended version of p.6 of the description submitted with the letter of 10 October 2011, the following sentence on l.15:

"Next a point (x_1, y_1) = kP is computed."

has been amended to read:

"Next a point (x_1, y_1) = kP is computed to derive a first short term public key."

In the letter of 10 October 2011, the appellant submitted that this amendment was based on the wording of claim 2 as originally filed and merely served to clarify the relationship between the computation of the point (x_1, y_1) and the derivation of the first short term public key. The appellant further referred in this regard to p.2 l.11-12 of the application as originally filed where the following is stated: "k is a random integer selected as a short term private or session key, and has a corresponding short term public key R = kP".

The appellant argued on the basis of the foregoing that the skilled person would have understood from the application as originally filed that the first short term public key R = kP is derived by computing the point (x_1, y_1). Thus, the aforementioned amendment on p.6 l.15 did not introduce any subject-matter extending beyond the content of the application as originally filed.

XI. At the end of the oral proceedings the chair announced the board's decision.

Reasons for the Decision

1. The appeal is admissible (cf. Facts and Submissions, item IV above).

2. *Article 84 EPC 1973*

2.1 The term "correspondent" which appears in claims 1 and 7 of the request is found in the description on p.5 l.15-20 which discloses a data communication system comprising "a pair of correspondents" respectively designated as a sender and a recipient and connected by a communication channel. According to the cited passage of the description, each of the correspondents comprises an encryption unit which enables it to process digital information and prepare it for transmission through the channel.

2.2 The board judges that the term "correspondent" is to be interpreted in the given context as denoting a node in a distributed system which "corresponds" with at least one other node by exchanging data across a communication channel. On this basis, the board finds that the use of the term "correspondent" in the wording of claim 1 is supported by the description.

2.3 Claim 1 is directed towards a method of signing a message m in a public key data communication system by a correspondent.

2.4 More particularly, claim 1 recites steps relating to the generation of a masked digital signature, the subsequent conversion of the masked digital signature to a regular digital signature prior to verification of the signature and the use of the regular digital signature to perform the verification (cf. published application: p.6 l.3-5; p.6 l.20-28; p.7 l.8-13).

2.5 In the board's judgement, claim 1 as amended clearly defines the essential technical features of the matter for which protection is sought and in manner supported by the cited passages of the description.

2.6 In this regard, it is noted that claim 1 comprises a first embodiment according to which a regular signature component is computed by the terminal which sends the signature components ($\bar{s}$,r) as a regular digital signature to a receiver verifier computer system which verifies the regular digital signature and a second embodiment according to which the terminal sends the signature components (r,s,c) as a masked digital signature to a receiver verifier computer which computes a regular signature component $\bar{s}$ and verifies a regular digital signature ($\bar{s}$,r).

2.7 In the board's judgement, these two embodiments of claim 1 correspond to the two alternatives disclosed in the description (cf. published application: p.6 l.24-28; p.7 l.8-13). According to the description, the conversion from a masked digital signature to a regular digital signature is preferably performed outside the secure boundary protecting the private key of the sender. Either the sender performs the conversion

operation outside the secure boundary and sends the regular digital signature to the verifier or, alternatively, the sender transmits the masked signature to the verifier, and the conversion operation is performed by the verifier prior to the verification operation.

2.8 Claim 7 seeks protection for substantially the same subject-matter as claim 1 in the form of a further independent claim directed towards a "correspondent comprising a processor (18) for signing a message *m* in a public key data communication system (10)".

2.9 On the basis of the observations set forth under 2.1 and 2.2 above, the board finds that the intended meaning of the term "correspondent" as used in claim 7 is clear in the given context and that the use of this term is supported by the description.

2.10 In view of the foregoing, the board concludes that claims 1 and 7 of the appellant's request define the matter for which protection is sought in a manner which complies with the clarity and support requirements of Article 84 EPC 1973.

3. *Article 123(2) EPC*

3.1 Having regard to the fact that the passages of the description providing support for the subject-matter of claims 1 and 7 form part of the application documents as originally filed, the board concludes that the amendments to said claims also comply with the requirements of Article 123(2) EPC.

3.2 Concerning the amendment to p.6 of the description submitted with the letter of 10 October 2011, the board notes that, on the basis of the appellant's submissions pertaining thereto (cf. Facts and Submissions, item X. above), it is satisfied that said amendment represents a permissible clarification of the disclosure and does not infringe Article 123(2) EPC.

4. *Novelty*

4.1 Pursuant to Article 54(3) EPC and Article 54(4) EPC 1973 (which continues to apply in the present case, see Article 1 of the Decision of the Administrative Council of 28 June 2001 on the transitional provisions of the Act revising the EPC of 29 November 2000, Special Edition No. 1, OJ EPO 2007, 197), the document D1 (EP 0807908 A) cited in the decision under appeal constitutes prior art for the commonly designated states DE, FR and GB.

4.2 The refusal of the application in the decision under appeal was based on a finding that D1 was prejudicial to the novelty of the subject-matter of claim 1 on file when said decision was taken.

4.3 The independent claims of the appellant's present request have been amended to distinguish the claimed invention from the disclosure of D1. In particular, although D1 discloses the generation of a masked digital signature there is no identifiable disclosure in said document of the features of the present claims 1 and 7 relating to the subsequent conversion of a masked digital signature to a regular digital signature and the use of the regular digital signature to perform

a verification operation. On this basis, the board judges that D1 is not prejudicial to the novelty of the amended independent claims of the appellant's request.

5. As noted above, D1 was cited as prior art pursuant to Article 54(3) EPC and Article 54(4) EPC 1973. Therefore, having regard to Article 56 EPC 1973, second sentence, said document is not to be considered in deciding whether there has been an inventive step.

6. *Remittal*

6.1 The proceedings before the department of first instance was essentially limited to a consideration of the question of novelty in the light of a document cited as prior art under Article 54(3) EPC and Article 54(4) EPC 1973.

6.2 As the novelty objection based on D1 has now been overcome by amendment of the claims compliant with the provisions of Article 84 EPC 1973 and Article 123(2) EPC, the board judges that the most appropriate action under the given circumstances is to remit the case to the department of first instance for further prosecution on the basis of the amended claims.

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 on the basis of claims 1 to 12 submitted at the oral proceedings.

The Registrar: The Chair:

K. Götz A. Ritzka