Internal distribution code:

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

Datasheet for the decision of 13 October 2015

Case Number: T 0845/12 - 3.5.06

Application Number: 01944801.8

Publication Number: 1292872

IPC: G06F21/00

Language of the proceedings: EN

Title of invention:
A METHOD FOR THE APPLICATION OF IMPLICIT SIGNATURE SCHEMES

Patent Proprietor:
Certicom Corp.

Opponent:
Müller, Christoph

Headword:
Implicit signature scheme/CERTICOM

Relevant legal provisions:
EPC 1973 Art. 56, 111(1)
EPC Art. 123(2)
RPBA Art. 13(1)

Keyword:
Inventive step -
Main Request and Auxiliary Requests 0 and 0+1 - (no)
Amendments - added subject-matter (no)
Remittal to the department of first instance -
Auxiliary Request 0+4 - (yes)

Decisions cited:
G 0003/14, T 0641/00

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 0845/12 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 13 October 2015

Appellant: (Patent Proprietor)	Certicom Corp. 4701 Tahoe Boulevard Tahoe A, 6th Floor Mississauga, Ontario L4W 0B5 (CA)
Representative:	Moore, Barry Hanna Moore + Curley 13 Lower Lad Lane Dublin 2, D02 T668 (IE)
Appellant: (Opponent)	Müller, Christoph Ludwigstr. 22 79104 Freiburg im Breisgau (DE)
Representative:	Fechner, Benjamin Wendelsteinstrasse 29A 82031 Grünwald b. München (DE)
Decision under appeal:	**Interlocutory decision of the Opposition Division of the European Patent Office posted on 6 February 2012 concerning maintenance of the European Patent No. 1292872 in amended form.**

Composition of the Board:

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

Summary of Facts and Submissions

I. This is an appeal against the interlocutory decision of the opposition division, with reasons dispatched on 6 February 2012, that, account being taken of the amendments made by the patent proprietor during the opposition proceedings, European patent EP1292872, in the amended form based on what was then the first auxiliary request, and the invention to which it related met the requirements of the EPC.

II. The opposition was based on the grounds provided for in Article 100(a) and (c) EPC 1973.

III. The following document was among those mentioned during the opposition proceedings:

D1: WO 99/49612 A1

IV. In the appealed decision, claim 40 of the main request was found not to comply with Article 123(2) EPC (see decision, reasons 1) because it was impermissibly amended over original claim 44 due to the addition of the words "transaction specific" before the words "implicit signature components" in steps b and d of the claimed method and the replacement of the word "certificate" in the last step with the words "transaction specific implicit signature components". Claim 1 of the first auxiliary request, which was based on claims 1 to 39 of the main request, was found to comply with Article 123(2) EPC (decision, reasons 2.1) and with Articles 54 and 56 EPC (decision, reasons 2.2 and 2.3).

V. Notice of appeal was received from the opponent on 7 April 2012, the appeal fee being paid on the same day. The appellant-opponent (hereinafter only "oppo-

nent") requested that the decision be set aside and that the patent be revoked. The opponent's statement of grounds of appeal was received on 7 June 2012.

VI. Notice of appeal was received from the patent proprietor on 16 April 2012, the appeal fee being paid on the same day. The appellant-proprietor (hereinafter only "proprietor") requested that the decision be set aside and that the patent be maintained as granted. With its statement of grounds of appeal received on 18 June 2012, its reply to the opponent's statement of grounds of appeal received on 7 January 2013 and a further submission received on 21 October 2013, the proprietor filed claims of auxiliary requests 1 to 39.

VII. In its statement of grounds of appeal the proprietor further requested the board to speed up the processing of the appeal as far as possible, reference being made to the "Notice from the Vice-President Directorate-General 3 dated 17 March 2008 concerning accelerated processing before the boards of appeal" (OJ EPO 2008, 220).

The opponent, replying on 26 October 2012 to the proprietor's statement of grounds of appeal, requested that the proprietor's request for accelerated processing of the appeal be refused.

The board informed the appellants, with a communication dated 16 January 2013, that the proprietor had not established any specific reasons which would justify the acceleration of the present case.

VIII. With a summons to oral proceedings the board set out its preliminary opinion that claims 1 and 40 of the patent seemed not to contravene the requirements of

Article 123(2) EPC, but that the claimed invention according to all requests seemed not to establish an inventive step over D1 (Article 56 EPC 1973). The board also expressed doubts as to the admissibility under Article 12(4) RPBA of a number of auxiliary requests which seemed to be based on an auxiliary request withdrawn in the course of the opposition proceedings.

IX. In response to the summons, with letter dated 14 September 2015, the proprietor withdrew auxiliary requests 3, 4 and 7 to 39, but maintained the main request and auxiliary requests 1, 2, 5 and 6. It further filed claims of new auxiliary requests labelled 0, 0+1 and 0+2. As there had been no deliberation in the opposition proceedings on the inventive step of claim 40 of the patent, the proprietor suggested that, as a matter of fairness, the board should remit the case to the department of first instance for prosecution if it were to decide that claim 40 of the patent did not contravene the provisions of Article 123(2) EPC.

X. Oral proceedings were held on 13 October 2015. In the course of the oral proceedings the proprietor filed a new auxiliary request 0+4 and requested that the decision under appeal be set aside and that the patent be maintained as granted (main request), or alternatively on the basis of auxiliary requests 0 or 0+1, both filed with the letter of 14 September 2015, or of auxiliary request 0+4 filed during the oral proceedings.

XI. The claims according to the main request correspond to the claims of the patent as granted and comprise two independent claims 1 and 40, both to a method.

Claim 1 of the main request reads as follows:

"A method of verifying a transaction over a data communication system between a first and second correspondent (12, 14) through the use of a certifying authority (20), said method comprising the steps of:
a) one of said first and second correspondents (12,14) advising said certifying authority (20) that a transaction is to be validated;
b) said certifying authority (20) determining whether to validate the transaction requested by said first or second correspondent (12, 14);
c) upon agreeing to validate said transaction, said certifying authority (20) generating implicit signature components (s_i, γ_i, A_i) including transaction specific information;
d) forwarding to said first correspondent (12) at least one of said implicit signature components (s_i) for permitting said first correspondent (12) to generate an ephemeral private key;
e) forwarding to said second correspondent (14) at least one of said implicit signature components (γ_i, A_i) for permitting recovery of an ephemeral public key ($\alpha_i P$) corresponding to said ephemeral private key (α_i);
f) said first correspondent (12) signing a message (m) with said ephemeral private key and forwarding said message (m) to said second correspondent (14) and
g) said second correspondent (14) attempting to verify said signature using said ephemeral public key ($\alpha_i P$) and proceeding with said transaction upon verification."

Claim 40 of the main request reads as follows:

"A method for certifying a correspondent (12, 14) in a data communication system through the use of a certifying authority (20) having control of a

certificate's validity, said method comprising the steps of:
a) said certifying authority (20) generating a first random number (c_A);
b) generating transaction specific implicit signature components γ_A, s_A based on said first random number (c_A);
c) publishing a public key Q_c of said certifying authority (20) for use in verifying said correspondent (12, 14);
d) forwarding said transaction specific implicit signature components from said certifying authority (20) to said correspondent (12, 14);
wherein said certifying authority (20) recertifies said correspondent's (12, 14) transaction specific implicit signature components by changing said value of said first random number (c_A)"

XII. Claim 1 of auxiliary request 0 differs from claim 1 of the main request in the following additions (underlined) in steps c, d and e of the claimed method:

"c) upon agreeing to validate said transaction, said certifying authority (20) generating implicit signature components (s_i, γ_i, A_i), the component A_i including a unique distinguishing name or identity and transaction specific information for the transaction to be verified;
d) forwarding to said first correspondent (12) at least one of said implicit signature components (s_i) for permitting said first correspondent (12) to generate an ephemeral private key, α_i based on said implicit signature components ;
e) forwarding to said second correspondent (14) at least one of said implicit signature components (γ_i, A_i)

for permitting recovery of an ephemeral public key ($\alpha_i P$) corresponding to said ephemeral private key (α_i), said ephemeral public key ($\alpha_i P$) being a transaction specific public key and said ephemeral private key being a transaction specific private key, each of the transaction specific public key and transaction specific private key being computed from transaction specific information;"

Auxiliary request 0 has another independent claim 37 which is identical to claim 40 of the main request.

XIII. Claim 1 of auxiliary request 0+1 differs from claim 1 of auxiliary request 0 in the following additions (underlined) and deletions (~~struck through~~) in steps c and f of the claimed method:

"c) upon agreeing to validate said transaction, said certifying authority (20) generating implicit signature components (s_i, γ_i, A_i), the component A_i including a unique distinguishing name or identity and transaction specific information comprising a message to be signed for the transaction to be verified;
...
f) said first correspondent (12) signing ~~a~~ the message (m) with said ephemeral private key and forwarding said message (m) to said second correspondent (14) and"

Auxiliary request 0+1 has another independent claim 37 which is identical to claim 37 of auxiliary request 0.

XIV. Claims 1 to 5 of auxiliary request 0+4 are based on claims 40 to 46 of the main request, i.e. as granted, whereby claim 1 of auxiliary request 0+4 combines claims 40, 43 and 44 of the main request and reads as follows:

"A method for certifying a correspondent (12, 14) in a data communication system through the use of a certifying authority (20) having control of a certificate's validity, said method comprising the steps of:
a) said certifying authority (20) generating a first random number (c_A);
b) generating transaction specific implicit signature components γ_A, s_A based on said first random number (c_A);
c) publishing a public key Q_c of said certifying authority (20) for use in verifying said correspondent (12, 14);
d) forwarding said transaction specific implicit signature components from said certifying authority (20) to said correspondent (12, 14);
wherein said certifying authority (20) recertifies said correspondent's (12, 14) transaction specific implicit signature components by changing said value of said first random number (c_A);
wherein said first random number (c_A) has said value for one certification period, said value being changed for other of said certifications periods[;]
wherein k_i is said first random number generated by said certifying authority (20) for an ith certification period and said transaction specific implicit signature components include:
c) i, where i is a current certification period;
d) s_A, where $s_{Ai} = r_i c + k_i + c_A \pmod n$, n is a large prime number, c is a long term private key of said certifying authority (20), c_A is a second random number, and $r_i = h(\gamma_A \| A_i \| cP \| k_i P \| i)$, where A_i includes at least one distinguishing feature of said correspondent (12, 14) and transaction specific information, P is a

point on a curve, and h indicates a secure hash function;
wherein γ_A = aP+ c_AP, and where aP is a long term public key of said correspondent (12, 14) and γ_A has previously been determined by said certifying authority (20) and forwarded to said correspondent (12, 14)."

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

Reasons for the Decision

The invention

1. The invention relates to a certification authority (CA in figure 1) certifying keys for use in message exchange between two correspondents (A and B in figure 1) by distributing so-called implicitly certified key components. Explicit keys are not transmitted as explicitly signed public key certificates, but are to be reconstructed by the recipient from the implicit certificate components (see paragraph [0009] of the patent).

1.1 Such a certification protocol is already known and is acknowledged by the patent to be contained in a Canadian patent application 2,232,936 (paragraphs [0009] and [0014]). The patent aims to address certain problems in prior art implicit certification schemes encountered in verifying the validity of a certificate. Several solutions to this problem such as revocation lists or issuance of certificates with a certain expiry date are acknowledged to be known in the relevant art (paragraphs [0016], [0017] and [0019]).

1.2 The patent proposes an alternative in which the certificates are "transaction specific". When two correspondents want to exchange a message such as a "transaction record" (paragraph [0028]), the CA is requested to issue certificates. The certificates have components at least some of which are transaction-specific, as "a timestamp, a message, or similar transaction specific information" is used in their calculation (paragraph [0029], last sentence, to paragraph [0033]). Upon receipt of the certificate components the correspondents compute private and public keys for subsequent message exchange (paragraphs [0035] and [0036]).

Main request, auxiliary requests 0 and 0+1

2. It is common ground between the opposition division and both appellants, and the board agrees, that inventive step should be assessed starting from document D1.

2.1 D1 discloses a certification authority (CA in figure 1) generating an implicit certificate for a correspondent involved in message exchange with other correspondents (A and B in figure 1) using its identity. Based on the components of a correspondent's implicit certificate, third parties can reconstruct its public key (page 3, line 32 to page 4, line 28).

2.2 In the decision under appeal the opposition division identified three distinguishing features of claim 1 of the patent over D1, the central one being that the implicit signature components are transaction-specific (see point 2.2.2 of the reasons), and formulated the objective technical problem solved by these features as "the necessity to frequently verify the status of a public key to ensure that it has not been revoked by the certifying authority". The opposition division

stated that it had derived this problem from column 3, lines 4 to 6, of the patent. As such a passage cannot be found in column 3 but in column 4, the board understands this as referring to column 4, lines 4 to 6. The opposition division did not expound which technical effect the distinguishing feature of the invention has or how the invention solved this revocation problem, but found it to be inventive as there was no hint in D1 towards binding an implicit certificate to a transaction (see reasons 2.3.2).

2.3 In its reply to the summons and at the oral proceedings the proprietor formulated the objective technical problem solved by claim 1 of the patent as being how to extend the teaching of D1 to facilitate retrospective interrogation of message validity. The opponent argued, and the board agrees, that any public key signature scheme enables retrospective interrogation of message validity. Thus the objective technical problem over D1, as defined by the proprietor, cannot be correct.

2.4 In the board's view, the association of a certificate with one particular transaction is a mere legal declaration of the rights conferred by a certificate rather than a technical issue.

2.5 Therefore the board considers the opponent's formulation of the technical problem (see the opponent's statement of grounds of appeal, point 3.4 on page 21), i.e. how to apply the teaching of D1 to messages which concern a particular transaction (see the opponent's statement of grounds of appeal, point 3.4 on page 21), to be more appropriate than the problem defined by the opposition division. In this regard the board does not agree with the opposition division's concern that such a formulation would be an example of *ex post facto* ana-

lysis (see the decision, reasons 2.3.3). According to established jurisprudence of the boards of appeal (see especially T 641/00, OJ EPO 2003, 352), if the claim refers to an aim to be achieved in a non-technical field, this aim may legitimately appear in the formulation of the problem as part of the framework of the technical problem that is to be solved.

2.6 Given this objective technical problem, the skilled person would generate new implicit certificates using the method disclosed in D1 for each individual transaction without the need to exercise any inventive activity. The proprietor could not demonstrate any particular technical effect caused by the inclusion of the transaction-specific information in the computation of implicit signature components as compared to the computation of new implicit signature components for every new transaction without using any transaction specific information.

2.7 Thus the board concludes that the subject-matter of claim 1 of the main request does not establish an inventive step over D1 (Article 56 EPC 1973).

2.8 The additional features of claim 1 of auxiliary requests 0 and 0+1 serve to emphasise the transaction specificity of the implicit signature components and the resultant transaction specificity of the public and private keys recovered based on transaction-specific components. Thus the conclusion of lack of inventive step with regard to claim 1 of the main request remains valid for claim 1 of auxiliary request 0 and auxiliary request 0+1.

Auxiliary request 0+4

Admitting the amendment to the proprietor's case

3. Under Article 13(1) RPBA, amendments to a party's case may be admitted and considered at the board's discretion. Discretion is to be exercised in view of *inter alia* the complexity of the new subject-matter submitted, the current state of the proceedings and the need for procedural economy.

3.1 The board is of the opinion that the subject-matter of amended claim 1 raises a number of complex issues. The opponent mentioned a number of clarity issues which, to the extent that they may not be raised in view of G 3/14, may affect how the claim is to be construed in view of the description. The proprietor claimed that amended claim 1 was inventive since it improved the known methods of recertification. In the board's view, the merits of this argument require a detailed discussion.

3.2 However, since the inventive step of claim 40 of the patent had not been decided upon by the opposition division, the board considers that the proprietor is entitled to have this issue addressed now. The board also considers auxiliary request 0+4 to be a reasonable reaction to an inventive step objection which was raised during oral proceedings, based on a remark made in the board's summons to oral proceedings (see point 6.5 therein).

3.3 In the board's view, these circumstances outweigh the complexity of this case, its age and the need for procedural economy. Moreover, the opponent did not object to admitting the request. Hence, the board exercises

its discretion under Article 13(1) RPBA and admits auxiliary request 0+4 into the proceedings.

Article 123(2) EPC

4. Claim 1 of auxiliary request 0+4 is a combination of claims 40, 43 and 44 of the patent.

5. In the decision under appeal claim 40 of the patent was found not to meet the requirements of Article 123(2) EPC. The opposition division based its decision on the understanding that claim 40, based on claim 44 as originally filed, sought protection for the so-called "recertifying embodiment" disclosed on page 9, line 20, to page 12, line 10, of the description as originally filed, and concluded that the qualification of the "implicit signature components" as "transaction specific" in steps b and d of the claimed method and the replacement of the word "certificate" by "transaction specific implicit signature components" were not disclosed as part of the recertifying embodiment. In particular, according to the appealed decision (reasons 1.1-1.2), that embodiment did not even mention transactions.

5.1 The decision further points to an alleged inconsistency between the claims and the description (see reasons 1.3), namely that according to "claims 45 and 48 the signature component s_A is calculated using A_i" whereas according to the description "only ID_A is used for that purpose". Then, "interpreting original claims 45 and 18 in the light of the description", the decision concludes "that it is not unambiguously derivable that the signature components are transaction specific". The board is not convinced by the assumption of this argument that, in case of a conflict between the claims and the description, the disclosure of the application is

determined by the description. The content of the application referred to in Article 123(2) EPC is determined by the description, claims and drawings (see e.g. Rule 137(1,2) EPC), and the board sees no legal basis for giving more weight to any of said parts when assessing the compliance of an amendment with Article 123(2) EPC, unless specific reasons present themselves for doing so. In the present case, no such reasons are apparent, given that the use of A_i for the computation of the signature components is as plausible as the use of ID_A.

5.2 As identified by the opposition division, claims 45 and 48 as originally filed specify the calculation of s_A based on a secure hash function with A_i as one of its parameters. This alternative is briefly mentioned in the "recertifying embodiment" on page 9, line 24. A_i is disclosed to have a transaction-specific and a non-transaction-specific part (page 6, lines 19 to 21, as originally filed). The opposition division and the opponent argued that there was no direct and unambiguous indication that the transaction-specific part of A_i is actually used in the calculation of s_A according to claims 45 and 48, even if it is sent to the certifying authority. This argument does not convince the board. Rather, in the board's view the skilled person would take the specification of A_i as a parameter of the function h as an indication that A_i is actually "used" in the calculation of h. *A fortiori*, this applies to the evaluation of a hash function which, as is well-known, must be such that a small modification to the input leads to a substantially different output: if Ai was an unused parameter of h, no modification of Ai whatsoever would affect the calculated hash value.

5.3 The preliminary opinion of the board to this effect was communicated to the parties in the annex to the summons to oral proceedings and the opponent did not comment.

5.4 Thus the board finds claim 40 of the patent to meet the requirements of Article 123(2) EPC.

6. Claim 43 of the patent is based on claim 47 as originally filed, amended through the addition of a reference sign and the replacement of the term "first random integer" with the term "first random number" for consistency with the obviously corresponding term in claim 44 as originally filed.

7. Claim 44 of the patent is based on claim 48 as originally filed, amended through the addition of reference signs, the replacement of "first random integer" with "first random number" as in claim 43 of the patent, the addition of the words "transaction specific" before the words "implicit signature components" as in claim 40 of the patent and the addition of the statement that A_i also includes "transaction specific information" (which, as mentioned, is disclosed on page 6, lines 29 to 30, of the description as originally filed).

8. Thus the board, being satisfied that claims 40, 43 and 44 of the patent comply with Article 123(2) EPC, concludes that their combination, and thus claim 1 of auxiliary request 0+4, also does.

Remittal to the department of first instance

9. As the decision did not contain any discussion or finding on the inventive merit of claim 40 as granted, let alone of amended claim 1, the proprietor suggested that it would be unfair for the board to come to an adverse

finding on the inventive step of claim 40 of the patent as granted (letter of 14 September 2015, page 1, 4th paragraph). Accordingly, having determined the compliance of granted claim 40 with Article 123(2) EPC, the board should remit the case to the opposition division for further prosecution (see also that letter, page 7, paragraph entitled "Claims 40-49").

10. According to Article 111(1) EPC 1973, the board has to examine the allowability of the appeal and then has discretion either to exercise any power within the competence of the department which was responsible for the decision appealed or to remit the case to that department for further prosecution.

10.1 The board agrees with the proprietor that procedures before the EPO are designed so that issues are normally decided by two instances. As follows from Article 111(1) EPC, however, and as conceded by the proprietor (see letter of 14 September 2015, page 1, 4th paragraph), this does not give the parties an absolute right to two instances.

10.2 The board considers that no purpose would be served by remitting a case for further prosecution based on a request that is clearly not allowable as it stands.

10.3 Notwithstanding the fact that the opponent raised a number of concerns it had in relation to claim 1, the board takes the view that claim 1 is not clearly unallowable. Moreover, claim 1 now specifies a considerable number of features which were not assessed in the opposition proceedings, for example as regards their potential technical effects, the technical problem they might solve and their inventive merit, and cannot readily be assessed in the present appeal proceedings.

This also applies to the proprietor's suggestion that D1 might be an inappropriate starting point for the assessment of the inventive step of the amended recertification method. The board thus concludes that a fair and proper assessment, for both parties, of whether claim 1 of auxiliary request 0+4 establishes an inventive step over the prior art necessitates the remittal of the case to the department of first instance for continuation of the opposition proceedings.

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 continuation of the opposition proceedings based on auxiliary request 0+4.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated