Internal distribution code:

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

Datasheet for the decision of 7 March 2018

Case Number: T 0832/14 - 3.5.05

Application Number: 96201322.3

Publication Number: 0743774

IPC: H04L9/08, H04L9/32

Language of the proceedings: EN

Title of invention:
Strengthened public key protocol

Patent Proprietor:
Certicom Corp.

Opponent:
Müller, Christoph

Headword:
Public key checking/CERTICOM

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

Keyword:
Grounds for opposition - lack of patentability (no) - fresh ground for opposition (yes)

Decisions cited:
G 0001/95, G 0007/95, G 0009/91

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 0832/14 - 3.5.05

D E C I S I O N
of Technical Board of Appeal 3.5.05
of 7 March 2018

Appellant: (Patent Proprietor)	Certicom Corp. 4701 Tahoe Boulevard Tahoe A, 6th Floor Mississauga, Ontario L4W 0B5 (CA)
Representative:	Ahmad, Sheikh Shakeel Keltie LLP No.1 London Bridge London SE1 9BA (GB)
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 11 February 2014 concerning maintenance of European patent No. 0743774 in amended form**

Composition of the Board:

Chair	A. Ritzka
Members:	P. Cretaine
	D. Prietzel-Funk

Summary of Facts and Submissions

I. This appeal is against the interlocutory decision of the opposition division, despatched on 11 February 2014, to maintain European patent No. 0 743 774 in amended form according to claims 1 and 2 of a second auxiliary request filed during the oral proceedings on 19 December 2013.

The opposition was based on the grounds of Article 100(a), (b) and (c) EPC. The opposition division found that the subject-matter of claim 1 of a main request, filed with a letter dated 19 November 2013, was not new over the disclosure of

D6: "Elliptic Curve Public Key Cryptosystems", A. Menezes, 1993, pages v to vii, ix to xii and 1 to 14.

A first auxiliary request filed during the oral proceedings on 18 December 2013 was not admitted by the opposition division because it did not prima facie meet the requirements of Articles 84 and 123(2) EPC.

The opposition division decided that claim 1 of the second auxiliary request met the requirements of Articles 83, 84 and 123(2) EPC and that its subject-matter was new (Article 54 EPC) over the disclosure of

D5: FIPS PUB 186 "Digital Signature Standard (DSS)", 1994, pages 1 to 20

and involved an inventive step (Article 56 EPC), having regard to **D5** alone or in combination with the disclosure of

D1: EP 0 535 863.

The opposition division further decided that claim 2 of the second auxiliary request met the requirements of Article 83 EPC and that its subject-matter involved an inventive step having regard to the disclosure of

D2: C. P. Schnorr: "Efficient Signature Generation by Smart Cards", Journal of Cryptology, vol. 4, 1991, pages 161 to 174

in combination with

D7: N. Koblitz: "Primality of the number of points on an elliptic curve over a finite field", Pacific Journal of Mathematics, Vol. 131, No. 1988.

II. Both parties appealed against this decision (for ease of understanding, the two appellants will henceforth be referred to as "opponent" and "patent proprietor"). The opponent's notice of appeal was received on 8 April 2014, and the appeal fee was paid on the same day. The statement setting out the grounds of appeal was received on 11 June 2014. The opponent requested that the decision be set aside and that the patent be revoked. In support of its argumentation it filed additional pages 15 to 34 and 83 to 100 of document **D6** and submitted a new document

D8: N. Koblitz: "A Course in Number Theory and Cryptography", Second Edition, 1994, pages 167 to 199.

The opponent argued that the claims of the second auxiliary request did not meet the following requirements of the EPC:

- claims 1 and 2 lacked clarity (Article 84 EPC)
- claim 1 did not meet the requirements of Article 123(2) EPC
- claim 1 lacked novelty over **D6** (Article 54 EPC)
- claim 2 lacked an inventive step over **D6** in combination with the common knowledge of the skilled person as exemplified by **D8**.

The appellant further referred to its submissions with respect to D2 and D5 in opposition proceedings.

Oral proceedings were requested on an auxiliary basis.

III. The patent proprietor's notice of appeal was received on 16 April 2014, and the appeal fee was paid on the same day. The statement setting out the grounds of appeal was received on 23 June 2014. The patent proprietor requested that the decision be set aside and that the patent be maintained on the basis of a main request or of auxiliary requests 1 to 4, all requests as filed with the statement setting out the grounds of appeal. Auxiliary request 4 was identical to the second auxiliary request on the basis of which the opposition division had decided to maintain the patent. Oral proceedings were requested on an auxiliary basis in case the main request were not allowed. The patent proprietor argued in particular that claim 1 of the main request, which was identical to claim 1 of the main request on which the decision was based, was new over D6.

IV. By letter of 16 October 2014, the opponent responded to the patent proprietor's statement of grounds of appeal and requested that the patent proprietor's appeal be dismissed as unfounded and that the patent be revoked. The opponent argued that:

- the main request did not meet the requirements of Article 52(2)(d) EPC, and of Articles 54 and 56 EPC having regard to D6, and that
- auxiliary requests 1 to 4 did not meet the requirements of Articles 52(2)(d), 84 and 123(2) EPC, and of Article 56 EPC having regard to D6.

V. In view of both appellants' requests under Rule 84(1) EPC that the appeal proceedings be continued after the lapse of the patent, a summons to oral proceedings was issued on 22 December 2017. In an annex to the summons, the board indicated the points which would be discussed during the oral proceedings. It also expressed its preliminary opinion that the objection under Article 52(2)(d) EPC, at least against claim 1 of the main request, constituted a fresh ground for opposition in the sense of G 1/95 and G 7/95 which could as such not be introduced in the appeal proceedings without the patent proprietor's approval. The board also indicated that the admission of D8 and of the new pages of D6 should be addressed.

VI. Oral proceedings were held before the board on 7 March 2018, in the course of which the patent proprietor withdrew the main request and auxiliary requests 1 to 3. The opponent requested that the decision under appeal be set aside and that the patent be revoked.
The patent proprietor requested that the decision under appeal be set aside and that the patent be maintained according to the claims of auxiliary request 4 as submitted with the statement of grounds of appeal.
At the end of the oral proceedings, the board's decision was pronounced.

VII. Claim 1 of auxiliary request 4 (the sole request) reads as follows:

"*A method of establishing a public key of the form* α^x *for securing the exchange of data between a pair of correspondents in a public key cryptosystem comprising the steps of*
utilising a group G of order n over a finite field, Fp, wherein the group G *is* a *multiplicative group* Zp^* *where p is a prime, or an elliptic curve group,*
establishing a subgroup S of the group G having an order q,
determining an element α *of the subgroup S to generate the q elements of the subgroup S, the order q of the subgroup S being sufficiently large that a brute force approach against the public key is impractical, and*
utilising said element α *to generate a public key at one of the correspondents of the form* α^x *where x is an integer selected by the one of said correspondents as a private key,*
receiving at the other of said correspondents a message purported to be the public key α^x *,*
checking at the other of said correspondents if said message corresponds to the group identity wherein the order q is prime, or exponentiating said message to a value t where t is a divisor of the order n and
checking if a resultant value corresponds to the group identity wherein the order q is not prime, or checking if said message corresponds to a tabulated value that yields the group identity wherein the order q is not prime, and
rejecting said message or checking further if said message or resultant value corresponds to the group identity or the tabulated value".

Claim 2 of auxiliary request 4 reads as follows:

"*A method of establishing a public key of the form* α^x *for securing the exchange of data between a pair of correspondents in a public key cryptosystem comprising the steps of*
utilising an elliptic curve group G of order n over a finite field, Fp, wherein p is a prime power and said order n of said group G is a prime q,
establishing a subgroup S of the group G having an order equal to the prime q,
determining an element α *of the subgroup S to generate the q elements of the subgroup S, the order q of the subgroup S being sufficiently large that a brute force approach against the public key is impractical,*
utilising said element α *to generate a public key at one of the correspondents of the form* α^x *where x is an integer selected by the one of said correspondents as a private key,*
receiving at the other of said correspondents a message purported to be the public key α^x*, and*
checking if the message corresponds to the identity element".

Reasons for the Decision

1. Admissibility of the appeals

Both appeals comply with the provisions of Articles 106 to 108 EPC (cf. points II and III above) and are therefore admissible.

2. Article 52(2) EPC

The opponent had in writing raised an objection under Article 52(2)(d) EPC against auxiliary request 4 for

lack of technicality of all the features of claims 1 and 2. Since most of the features which were objected to were already present in the set of granted claims and since this objection had not been raised by the opponent in its notice of opposition, the board considered it to be a fresh ground for opposition in the sense defined by G 1/95 and G 7/95. According to G 9/91 (see Reasons 18), such a ground may be considered in appeal proceedings only with the patent proprietor's approval. The board also pointed out in its communication of 22 December 2017 that, in its view, the subject-matter of the claims did not relate to presentations of information (Article 52(2)(d) EPC) as such, or even to mathematical methods (Article 52(2)(a) EPC) as such. In that respect, the board had indicated that, according to the case law of the boards of appeal (see for instance T 1326/06 and T 27/97), methods in the field of cryptography which clearly aimed at increasing the security of data communication between entities had to be regarded as inventions within the meaning of Article 52 EPC.

During the oral proceedings before the board, the patent proprietor, when asked, did not give its consent to dealing with this fresh ground for opposition. Thereupon, the board decided not to introduce the ground under Article 100(a) in conjunction with Article 52(2) EPC in the appeal proceedings.

3. Admission of D8 and the new pages of D6

These documents were submitted by the opponent with its statement of grounds of appeal. The opponent argued that they were submitted in response to the amendments introduced by the claims of auxiliary request 4 filed during the second day of the oral proceedings before

the opposition division, in particular the features related to the checking of the public key when group G was an elliptic curve group. It pointed out that the new pages of D6 dealt with elliptic curve cryptography and that D8 was cited in D6. The patent proprietor held that these documents did not in any way address the checking of the public key, which was the gist of the features introduced by auxiliary request 4 with respect to the claims as granted.

Taking into account the arguments of both parties, the board decided to admit both documents into the appeal proceedings, in accordance with Article 12(4) RPBA. In particular, it considered that D6 was a textbook and that the additional pages of D6 addressed the technology in more detail rather than alternative embodiments. D8 was explicitly referred to in D6 and would have been considered by the skilled person in this context. The question whether these documents actually relate to checking of the public key must be assessed in the context of novelty and/or inventive step.

4. Article 84 EPC

Claim 1 comprises several alternatives in respect of the kind of group G used (multiplicative group or elliptic curve group), of the kind of checking performed on the message purported to be the public key, and of the further action decided in response to this checking. The opponent argued that the number of alternatives in claim 1 amounted to 24, such that the Article 84 EPC requirements for conciseness and clarity were not met. The board however considers that the skilled person can easily distinguish the alternatives

in claim 1 from one another and can thus comprehend the claimed subject-matter without any difficulty.

The opponent further argued that claim 1 lacked the essential feature that subgroup S had to be cyclic in order to determine a generating element α of it. The board however holds that, as pointed out by the patent proprietor, group G being of order n is a cyclic group itself and every subgroup of G is a cyclic group. Therefore, it is implicit in claim 1 that S is also a cyclic group.

A further objection of the opponent was that claim 2 lacked the essential feature of defining further steps after the checking of the message purported to be the public key. In the board's judgement, claim 2 comprises all the steps necessary for the definition of the claimed invention, namely the establishment of a public key for securing the exchange between two correspondents. Any steps after the checking of the received public key, be it for instance a rejection or an acceptance of the generated public key, is not necessary for this definition.

For these reasons, the board judges that the claims meet the requirements of Article 84 EPC.

5. Article 123(2) EPC

The opponent objected that claim 1 did not meet the requirements of Article 123(2) EPC.

The opponent first argued that claim 1 did not define the transmission of the generated public key from one correspondent to the other, contrary to the teaching of the originally filed description on page 7,

lines 6 to 10 (corresponding to column 4, lines 52 to 56, of the published application). The board however holds that the feature of "receiving at the other of said correspondents a message purported to be the public key" present in claim 1 implies a transmission to the "other" correspondent from the "one of the correspondents" which is previously defined in the claim and which has generated the public key in question.

The opponent further stated that the definition of a "message purported to be the public key" was not present in the application documents as originally filed, in particular in the passage on page 7, lines 6 to 10, which related to the reception by one correspondent of the public key sent by the other correspondent. The board however agrees with the patent proprietor that the description clearly mentions that one correspondent (A) sends a public key to the other correspondent (B), see column 1, line 46 to 50, and that an active adversary (E) may replace this public key with a different value, see column 2, lines 27 to 30. According to these passages, correspondent B expects to receive a public key of the form α^x from correspondent A, while not being aware that E may have modified it. The formulation "a message purported to be the public key α^x" is thus fully supported by the description.

The opponent further argued that the feature of "exponentiating the message with a value t where t is a divisor of the order n and checking if a resultant value corresponds to the group identity where the order q is not prime" had no support. The opponent relied for its argumentation on the first paragraph of page 7 (corresponding to the passage from column 4, line 47,

to column 5, line 7, of the published application), which taught that the message should be exponentiated with the value t for each small divisor of (p-1), i.e for each small divisor of the order n = p-1 of group G, and not only for a divisor of the order n as defined in claim 1. In the board's view, the vague wording "small divisor of (p-1)" is not restrictive and may be seen to encompass all the divisors of n = p-1, except n itself. Further, the skilled person would understand from the above-mentioned passage that each time the message is raised to a power t, a check for the group identity is subsequently performed. Therefore, the exponentiation of the message to a value t, where t is a divisor of the order n, followed by the checking of the result of the exponentiation with the group identity, as actually defined in claim 1, is supported by the description as originally filed.

Furthermore, the opponent argued that the four termination alternatives defined in the last step of claim 1, namely rejecting the message or checking further if:
- the message corresponds to the group identity, or
- if the message corresponds to the tabulated value, or
- if the resultant value corresponds to the group identity, or
- if the resultant value corresponds to the tabulated value,
were not disclosed in the originally filed description on page 7, first paragraph (corresponding to the passage from column 4, line 47, to column 5, line 7, of the published application), which mentioned only one alternative, namely that the key exchange was terminated if the result of the checking of the exponentiated message was 1.
The board however notes that the checking step of

claim 1 defines three different alternatives:
- when the order q is prime:
  - checking the message with respect to the group identity,
- when the order q is not prime:
  - checking the resultant value with respect to the group identity, or
  - checking the message with respect to a tabulated value.

The skilled person would thus consider that the rejecting step actually comprises three alternatives corresponding to the three alternatives of the checking step. The first alternative is described in column 4, lines 28 to 36, the second is disclosed in column 4, lines 47 to 58, and the third is described in column 5, lines 10 to 13. Therefore the board holds that the last step of claim 1 is supported by the application documents as originally filed.

For these reasons, the board judges that auxiliary request 4 meets the requirements of Article 123(2) EPC.

6. Article 54 EPC

6.1 The opponent argued that the subject-matter of **claim 1** was already known from D6.

6.2 D6 on pages 10 and 11 (see the paragraph "NSIT Signature Scheme") discloses a method of establishing at a user a public key y of the form $g^x \bmod p$, utilising a multiplicative group Z_P^* of order p-1, where p is prime, and comprising the steps of:
- establishing a subgroup of the multiplicative group of order q,
- determining an element g of the subgroup to generate the q elements of the subgroup,

- utilising said element g to generate the user's public key y of the form $g^x \bmod p$, where x is an integer and the private key of the user.

D6 further discloses on page 8, lines 22 and 23, and on page 13, lines 11 to 13, that an elliptic curve over a finite field can be used to implement the NSIT signature scheme. The public key y disclosed in D6 being used in a signature scheme, it can be considered as having been established by a first correspondent ("user" on page 11, line 4) and received by a second correspondent, which verifies the signature by making use of the public key (page 11, lines 13 to 17), for securing the exchange of data with the second correspondent.

Moreover, since multiplication in a finite multiplicative group or addition in an additive group, such as an elliptic curve group, must always, according to mathematical group theory, be performed modulo the order of the group plus one, the notation α^x used in claim 1 has to be understood as $\alpha^x \bmod p$.

For these reasons, the board holds that the public key α^x of claim 1 can be read onto the public key y in D6.

D6 further discloses on page 10, last line, that the order q of the subgroup is between 2^{159} and 2^{160} and on page 11, last paragraph, that the security of the system is based on the difficulty of the discrete logarithm problem in the subgroup of order q of Z^*p generated by g. Since it is common knowledge that the difficulty of the discrete logarithm problem in a cyclic group increases with the order of the group, the board holds that the two above-mentioned passages clearly anticipate the broad and vague feature of

claim 1 that the order q of the subgroup S is sufficiently large that a brute force approach against the public key is impractical.

6.3 The opponent alleged that D6 further disclosed checking whether the message corresponded to the group identity, wherein the order q was prime and wherein the group G was a group of points on an elliptic curve, i.e one of the several alternatives defined by claim 1. To this end the opponent relied on passages of D6 dealing with public key generation in multiplicative groups (pages 2, 3, 5, 8, 10 and 11) and with mathematical operations on a group of points on an elliptic curve (pages 13, 17 and 18). According to the opponent, D6 teaches on page 18 to check if one of two points of the elliptic curve is the group identity before performing an addition of the two points, and the skilled person would have to apply this checking to a public key generated in an elliptic curve group when it is sent to the second correspondent. The board however considers that the passages of D6 relating to operations in an elliptic curve group do not in any way mention the generation, let alone the checking, of a public key. Therefore, in the board's judgement, the alternative of claim 1 in respect of the checking which was the only one referred to in the opponent's argumentation is not disclosed in D6.

6.4 The board thus considers that D6 discloses all features of claim 1 except for the last two steps of checking and rejecting or checking further.

Therefore, the board judges that the subject-matter of **claim 1** is novel (Article 54 EPC) having regard to the disclosure of D6.

7. Article 56 EPC

7.1 Claim 1

The opponent argued that the skilled person, being aware of the possibility of a man-in-the-middle attack on the transmitted public key, would obviously consider a check on the received public key at the second correspondent. Checking if the public key corresponds to the group identity is obvious, taking into account that D6, in particular on page 18, discloses checking each operand for the group identity before performing the operation, i.e. the additive operation modulo n in the elliptic curve group.

The patent proprietor however plausibly argued that the attack described first in column 2, lines 11 to 45, and further in column 4, lines 28 to 36, of the published application was not known at the priority date of the application. The board notes in that respect that none of the prior-art documents deal with such a substitution attack. It further agrees with the patent proprietor that, the attack not being known, the skilled person would not have been incited to check the public key for the group identity but would rather have assumed that the transmitted public key, irrespective of whether or not its value was identical to the group identity, was a valid non-substituted public key.

The board thus considers that the alternative of claim 1 involving an elliptic curve group and a checking of the public key for the group identity, which is the only alternative of claim 1 that the opponent had objected to, is not obvious having regard to the disclosure of D6. Since the opponent did not object to the other alternatives of claim 1, the board judges

that the subject-matter of claim 1 involves an inventive step (Article 56 EPC), having regard to the disclosure of D6.

7.2 Claim 2

Claim 2 relates to the alternative of claim 1 wherein the group G is an elliptic curve group and the subgroup S has a prime order, but with the omission of the last step of rejecting and checking further.

The opponent's Article 56 EPC objection in respect of claim 1 was directed only against this alternative. Further, the board considered in point 7.1 that the decisive feature for the issue of inventive step was the checking of the received public key and not a further step depending on the result of this checking (see also point 4, where the board decided that the step after checking was not an essential feature of claim 2). For these reasons, the board decides that the subject-matter of claim 2 involves an inventive step, having regard to the disclosure of D6.

8. In conclusion, the board judges that the grounds for opposition under Article 100(a) and (c) EPC pursued by the opponent in the appeal proceedings do not prejudice the maintenance of the patent as amended according to auxiliary request 4. Given that auxiliary request 4 is identical to the second auxiliary request on which the decision under appeal was based, this finding confirms the interlocutory decision of the opposition division.

Order

For these reasons it is decided that:

1. The appeal of the appellant-opponent is dismissed.
2. The decision under appeal is set aside.
3. The case is remitted to the opposition division with the order to maintain the patent on the basis of the claims of auxiliary request 4, as submitted with the statement setting out the grounds of appeal dated 23 June 2014, and of the description and drawings of the patent specification.

The Registrar: The Chair:

K. Götz-Wein A. Ritzka

Decision electronically authenticated