BESCHWERDEKAMMERN	**BOARDS OF APPEAL OF**	**CHAMBRES DE RECOURS**
DES EUROPÄISCHEN	**THE EUROPEAN PATENT**	**DE L'OFFICE EUROPÉEN**
PATENTAMTS	**OFFICE**	**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 29 September 2015

Case Number:	T 0108/12 - 3.5.05
Application Number:	07000020.3
Publication Number:	1768300
IPC:	H04L9/08
Language of the proceedings:	EN

Title of invention:
Key agreement and transport protocol with implicit signatures

Patent Proprietor:
Certicom Corp.

Opponent:
Müller, Christoph

Headword:
Key agreement and transport protocol with implicit signatures/ CERTICOM

Relevant legal provisions:
EPC Art. 100(c), 123(2), 76(1), 123(3)

Keyword:
Grounds for opposition - added subject-matter (yes)
Grounds for opposition - extension of subject-matter (yes)
Amendments - intermediate generalisation -
deletion of features (yes) - broadening of claim (yes) -
relationship between Art. 123(2) and Art. 123(3) -
inescapable trap (yes)

Decisions cited:
G 0001/93, T 0461/05

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Catchword:
See reasons, point 7, in particular point 7.4

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 0108/12 - 3.5.05

DECISION
of Technical Board of Appeal 3.5.05
of 29 September 2015

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 24 November 2011 concerning maintenance of the European Patent No. 1768300 in amended form.**

Composition of the Board:

Chair	A. Ritzka
Members:	M. Höhn
	F. Blumer

Summary of Facts and Submissions

I. This appeal is against the interlocutory decision of the Opposition Division of the European Patent Office posted on 24 November 2011, maintaining the European patent No. 1768300 in amended form.

II. The notice of appeal of the proprietor (appellant 1) was received on 1 February 2012. The appeal fee was paid on the same day. The statement setting out the grounds of appeal was received on 4 April 2012. The proprietor (appellant 1) submitted 1st to 6th auxiliary requests with the statement of grounds of appeal.

The notice of appeal of the opponent (appellant 2) was received on 20 January 2012. The appeal fee was paid on the same day. The statement setting out the grounds of appeal was received on 23 March 2012.

The proprietor (appellant 1) submitted 7th to 13th auxiliary requests with a letter of reply dated 22 August 2012.

By letters of 20 August 2012 and 7 January 2013, the opponent (appellant 2) commented on the requests of the proprietor (appellant 1).

The proprietor (appellant 1) requested that the appealed interlocutory decision be set aside and that the patent be maintained
a) as granted (main request),
b) according to the 1st to 6th auxiliary requests,
c) the patent be maintained based on any one set of amended claims formed by combining any two amendments of the 1st auxiliary request and the 2nd through 6th auxiliary requests,

d) according to the 7th to 12th auxiliary requests,
e) the patent be maintained based on any one set of amended claims formed by combining any amendment of the 7th through 12th auxiliary request with any one or any two amendments of the 1st auxiliary request and the 2nd through 6th auxiliary requests,
f) according to the 13th auxiliary request,
g) the patent be maintained based on any one set of amended claims formed by combining any amendment of the 13th auxiliary request with any one or any two amendments of the 1st auxiliary request and the 7th through 12th auxiliary requests.
h) Oral proceedings were requested as an auxiliary measure.

The opponent (appellant 2) requested that the appealed interlocutory decision be set aside and that the patent be revoked.

III. With a communication dated 29 April 2015 the board summoned the appellants to oral proceedings scheduled for 29 and 30 September 2015. In an annex to the summons the board expressed its preliminary opinion that all the proprietor's requests appeared to add subject-matter to the original disclosure (Article 123(2) EPC) of the earlier application, contrary to the requirement of Article 100 (c) EPC.

IV. By letter dated 28 August 2015 the proprietor (appellant 1) withdrew all existing auxiliary requests and submitted an unchanged main request and amended auxiliary requests 1 to 16 supported by arguments in favour of an antecedent basis.

V. Independent claim 1 of the main request as filed with letter dated 28 August 2015, corresponding to the patent as granted, reads:

"A method of establishing a session key between a pair of correspondents A,B in a public key data communication system to permit exchange of information therebetween over a communication channel, each of said correspondents having a respective private key a,b and a public key p_A, p_B derived from a generator α and respective ones of said private keys a,b, said method including the steps of:
i) a first of said correspondents A selecting a first random integer x and exponentiating a first function $f(\alpha)$ including said generator to a power $g(x)$ to provide a first exponentiated function $f(\alpha)^{g(x)}$;
ii) said first correspondent A generating a first signature S_A from said random integer x said exponentiated function $f(\alpha)^{g(x)}$ and said private key a to bind said integer x and said private key a, said first correspondent A maintaining said first signature private to itself;
iii) said first correspondent A forwarding to a second correspondent B a message including said first exponentiated function $f(\alpha)^{g(x)}$;
iv) said correspondent B selecting a second random integer y and exponentiating a second function $f(\alpha)$ including said generator to a power $g(y)$ to provide a second exponentiated function $f(\alpha)^{g(y)}$ and generating a signature S_B obtained from said second integer y and said second exponentiated function $f(\alpha)^{g(y)}$ and said private key b to being [sic] said integer y and said private key b, said second correspondent B maintaining said second signature S_B private to itself;

v) said second correspondent B forwarding a message to said first correspondent A including said second exponentiated function $f(\alpha)^{g(y)}$; and
vi) each of said correspondents constructing a session key K by exponentiating information made public by the other correspondent with information that is private to themselves whereby subsequent decryption of information confirms establishment of a common key and thereby the identity of said correspondents."

Independent claim 17 of the main request, i.e. of the patent as granted, reads:

"A method of transporting a session key K between a pair of correspondents A,B in a public key data communication system to establish a common key to permit exchange of information therebetween over a communication channel, each of said correspondents having a respective private key a,b and a public key p_A, p_B derived from a generator α and respective ones of said private keys a,b, said method including the steps of:
i) a first of said correspondents A selecting a first random integer x and exponentiating a first function $f(\alpha)$ including said generator to a power $g(x)$ to provide a first exponentiated function $f(\alpha)^{g(x)}$;
ii) said first correspondent A generating a first signature S_A from said random integer x said exponentiated function $f(\alpha)^{g(x)}$ and said private key a to bind said integer x and said private key a, said first correspondent A maintaining said first signature private to itself;
iii) said first correspondent A forwarding to a second correspondent B a message including said first exponentiated function $f(\alpha)^{g(x)}$;

iv) said first correspondent computing said session key K from said public key p_B of said second correspondent B and said signature S_A;
v) said second correspondent B utilizing the public key p_A of said first correspondent and information in said message to compute a session key K' corresponding to said session key K."

VI. At the oral proceedings held on 29 September 2015 the proprietor (appellant 1) submitted a further set of claims according to auxiliary request 17.

VII. The proprietor (appellant 1) requested that the decision under appeal be set aside and the patent be maintained on the basis of the main request as filed with letter dated 28 August 2015, or, subsidiarily, on the basis of any of auxiliary requests 1 to 16 as filed with letter dated 28 August 2015, or on the basis of auxiliary request 17 as filed during oral proceedings before the board.

The opponent (appellant 2) requested that the decision under appeal be set aside and that the European patent No. 1768300 be revoked.

VIII. After due consideration of the parties' arguments the chair announced the decision.

Reasons for the Decision

1. Admissibility

Both appeals comply with Articles 106 to 108 EPC (see Facts and Submissions, point II above). They are therefore admissible.

2. Articles 100(c), 76(1) and 123(2) EPC

Since the patent in suit is based on a divisional application, according to Article 100(c) EPC the granted set of claims must find a basis in the earlier (parent) application as filed, i.e. in document WO 98/18234 A1 (Article 76(1) EPC).

References to the original disclosure or original claims, description or drawings are to be understood as referring to the disclosure of the earlier application 96944186.4 as filed, published as WO 98/18234 A1.

Proprietor's main request

3. The decision under appeal followed the opponent's (appellant 2) request and rejected the main request of the proprietor, because claim 1 added subject-matter to the content of the earlier application as filed, contrary to the provisions of Article 100 c) EPC.

3.1 According to claim 1 of the main request a first function $f(\alpha)$ is exponentiated by the first correspondent A to provide a first exponentiated function $f(\alpha)^{g(x)}$ (step i) and the second correspondent B exponentiates a second function which is the same function $f(\alpha)$ to provide a corresponding second exponentiated function $f(\alpha)^{g(y)}$ (step iv). In original claim 1, however, the two functions and the basis in the two exponentiated functions were specified in a different way, namely $f(\alpha)$, $f'(\alpha)$ and $f(\alpha)^{g(x)}$, $f'(\alpha)^{g(y)}$, respectively.

3.2 The proprietor (appellant 1) argued that in all embodiments as well as according to original claim 7 the two functions $f(\alpha)$, $f'(\alpha)$ were indeed the same function $f(\alpha)$ and that in original claim 1 the two functions were already meant to be the same. When reading original claim 1 together with any of the protocols/embodiments, it was clear that the functions could be the same and arbitrary (see e.g. page 6, point 3 of the statement setting out the grounds of appeal dated 4 April 2012). Therefore the embodiments and original claim 7 provided a basis for claim 1 of the main request.

The proprietor further argued that the feature that the functions $f(\alpha)$ and $f'(\alpha)$ could not only be the same, but could also be equal to the identity function $f(\alpha)=\alpha$, represented a further feature which was not essential to the solution of the problem solved by the invention, namely bandwidth reduction.

3.3 The board agrees with the decision under appeal which reasoned that the specification of $f(\alpha)$ and $f'(\alpha)$ in the original application implied the use of two different functions. Even if the wording of original claim 1 was interpreted to the effect that $f(\alpha)$ and $f'(\alpha)$ can be different functions as well as comprising the special case of both functions being the same, the limitation in present claim 1 to only having the same functions is a selection for which no direct and unambiguous disclosure is found.

Claims 6 and 7 of the earlier application provide a basis for a feature that $f(\alpha)=\alpha$ and $f'(\alpha)=\alpha$. The board agrees with the opponent's argument that specifying that the two functions $f(\alpha)$ and $f'(\alpha)$ are arbitrary but the same is an intermediate generalisation between the special case that both functions are the identity function and the general case that the two functions are arbitrary and may be different. As the description does not contain any teaching as to the nature of these functions, apart from the fact that they may be the identity function, irrespective of the skilled person's knowledge of mathematics or cryptography there is no basis for an intermediate generalisation that the two functions are the same, arbitrary single function. Nor is there a basis for splitting the feature $f(\alpha)=f'(\alpha)=\alpha$ into a first feature that the functions are identical $f(\alpha)=f'(\alpha)$ and a second feature that they are the identity function $f(\alpha)=f'(\alpha)=\alpha$. This first feature without having the second feature at the same time constitutes new technical information that cannot be derived from the original application in the sense of decision T 461/05 referred to by both parties (see e.g. page 7 of the proprietor's statement setting out the grounds of appeal, and page 4 onwards of the opponent's letter dated 20 August 2012). In particular, the second feature is regarded as necessary for carrying out the invention and therefore cannot be regarded as non-essential.

3.4 In the board's judgement, there is no basis for removing the second feature as not essential. Consequently, claim 1 of the main request adds subject-matter to the original disclosure of the earlier application, contrary to Article 100 (c) EPC.

Proprietor's auxiliary requests 1 to 3

4. Since claim 1 according to these requests comprises the same feature objected to with regard to the main request (see point 3 above), claim 1 of these requests also adds subject-matter to the original disclosure of the earlier application, contrary to Article 100 (c) EPC.

Proprietor's auxiliary request 4

5. The opponent objected to claim 1 under Articles 123(2) (or 76(1), respectively) and 100(c) EPC with regard to step ii) of generating a first signature containing the additional formulation "said first correspondent A maintaining said first signature private to itself", and step iv) containing the corresponding formulation "said second correspondent B maintaining said second signature S_B private to itself".

5.1 In the decision under appeal the basis for this amendment was found in protocols 1', 2', 1'', and 1''' of the original description, where it was argued that the signatures were in fact not transmitted, as well as in the passages "the signatures need not be transmitted" (page 8, lines 24-25), "the transmission of S_A and S_B is avoided" (page 9, line 5), "avoiding the need to transmit the signature" (page 10, lines 4-5), and "not necessary to send the signature components" (page 13, lines 13-14). Moreover, the last step of original claim 1 already referred to private information which corresponded to the signatures in protocols 1', 2', 1'', and 1'''.

5.2 The opponent essentially argued (see e.g. point I. 4 of the statement setting out the grounds of appeal and point II.2 onwards of letter dated 7 January 2013, repeated during oral proceedings) that in the original section "disclosure of the invention" on pages 4 and 5 of the original application the signature was explicitly transmitted to the correspondent, which was in contrast to the present set of claims. Private information was disclosed to be accessible to both correspondents A and B (see original claim 1, last line "information that is private to themselves" - emphasis added). The signature was not disclosed as private information, only the random number was to be held private (see original application, page 5, lines 1 to 3). With regard to the signature there were disclosed embodiments either with its transmission or without its transmission. Furthermore, the act of keeping something private would imply measures to keep the information secret, whereas not transmitting would merely avoid such an activity without further measures regarding secrecy.

5.3 The board concurs with the opponent's arguments, in particular that the information alleged to be private is rather the random integer than the signature itself (see original application, page 5, lines 1 to 3). Maintaining something private, i.e. secret, involves more than merely not transmitting such information. While there are several passages relating to different protocols directly and unambiguously disclosing that a transmission of the respective signatures S_A and S_B can be avoided (see e.g. "the signatures [...] need not be transmitted" on original page 8, lines 24-25; "the transmission of S_A and S_B is avoided" on original page 9, line 5; "avoiding the need to transmit the signature" on original page 10, lines 4-5 and "not necessary to send the signature components" on original page 13, lines 13-14), there is hence no direct and unambiguous disclosure for signatures S_A and S_B to be maintained private.

5.4 Therefore the original (earlier) application documents do not provide a direct and unambiguous disclosure for claim 1, step ii) of generating a first signature containing the additional formulation "said first correspondent A maintaining said first signature private to itself", and step iv) containing the corresponding formulation "said second correspondent B maintaining said second signature S_B private to itself".

5.5 Independent claim 12 contains the same feature "maintaining the first signature private to itself" and therefore suffers from the same deficiency.

5.6 Claims 1 and 12 according to this request therefore do not fulfil the requirements of Article 100(c) and Article 76(1) EPC.

Proprietor's auxiliary requests 5 to 11

6. Since claim 1 according to these requests comprises the same features objected to with regard to auxiliary request 4 (see point 5 above), claim 1 of these requests also adds subject-matter to the original disclosure of the earlier application, contrary to Article 100 (c) EPC.

Proprietor's auxiliary request 12

7. In claim 1 of this request, step ii) of generating a first signature in claim 1 as granted containing the formulation "said first correspondent A maintaining said first signature private to itself" has been replaced by "said first correspondent A avoiding transmission of said first signature". Likewise, step iv) of claim 1 containing the corresponding formulation "said second correspondent B maintaining said second signature SB private to itself" has been replaced by "said second correspondent B avoiding transmission of said second signature".

7.1 The opponent (appellant 2) objected to this amendment, on the ground that it constituted an undue broadening of the subject-matter of claim 1 as granted in contrast to the requirements of Article 123(3) EPC.

7.2 The proprietor (appellant 1) argued that the amendment was merely a redefinition of a term in language closer to that of the original application, and in which the skilled person would not see a different teaching. No inappropriate advantage was achieved in the light of the criteria mentioned in decision G 1/93 (EPO OJ 1994, 541).

7.3 The proprietor further argued that the objection was surprising, since it was raised for the first time during oral proceedings. The board did not agree in this regard, since the opponent had already referred to G 1/93 in the written proceedings (see e.g. grounds of appeal dated 23 March 2012, section 3.1 on pages 13 and 14) and the issue of a conflict between Articles 123(2) and 123(3) EPC therefore had already been raised before the summons for oral proceedings. The proprietor therefore had to be prepared to discuss this issue.

7.4 The board agrees with the opponent that according to the description of the earlier application only one embodiment actually mentions not sending signatures (see protocol 2'), but no measures are disclosed to actually ensure that signatures are not transmitted.

As mentioned above (see point 5.3) and as already stated in the annex to the summons for oral proceedings, keeping something private, i.e. secret, involves more than merely not transmitting such information. Claim 1 as granted encompasses realisations where signatures are transmitted, but are maintained private, for example by transmitting signatures in a secure way. This is no longer required by amended claim 1 according to this request. On the other hand, amended claim 1 encompasses that signatures are not transmitted but are nevertheless made public, which is in contrast to claim 1 as granted.

The board therefore agrees with the opponent's argument that the features replaced by amendment not merely limit the scope of protection of claim 1, but - in contrast to the requirements set out in decision G 1/93 (see headnote 2 of the decision) - have a technical effect and contribute to the limitation of the scope of protection of claim 1. Those features therefore cannot be deleted from claim 1 without extending the scope of protection of claim 1 and thus infringing Article 123(3) EPC.

7.5 Claim 1 according to this request therefore does not fulfil the requirements of Article 123(3) EPC.

Proprietor's auxiliary requests 13 to 16

8. Since claim 1 according to these requests comprises the same feature objected to with regard to auxiliary request 12 (see point 7 above), claim 1 of these requests also does not fulfil the requirements of Article 123(3) EPC.

Proprietor's auxiliary request 17

9. During oral proceedings the proprietor (appellant 1) submitted a further auxiliary request 17 in order to address the issue of Article 123(3) EPC.

9.1 In claim 1 of this request, step ii) of generating a first signature in claim 1 reads "said first correspondent A maintaining said first signature private to itself by avoiding transmission of said first signature". Likewise, step iv) of claim 1 has the corresponding formulation "said second correspondent B maintaining said second signature private to itself by avoiding transmission of said second signature".

9.2 The opponent (appellant 2) objected to this request, that it was late-filed and raised complex new issues, and therefore requested that it should not be admitted into the appeal proceedings.

9.3 The board admitted this request, since it did not introduce new issues, but deals with subject-matter that was already present in the appeal proceedings and had been dealt with in the annex to the summons for oral proceedings (see point 6.2 referring to 6.1 and 5.3).

9.4 While the board agrees with the proprietor (appellant 1) that the amendment overcomes the objection under Article 123(3) EPC, the opponent (appellant 2) is correct that the amended features still give rise to an objection under Article 123(2) EPC.

9.5 For the reasons set out in point 5 above the board agrees with the opponent's argument that the act of keeping something private implies measures to keep the information secret, whereas not transmitting merely avoids such an activity without further measures regarding secrecy.

9.6 The board concurs with the opponent's arguments, in particular that the information alleged to be private is rather the random integer than the signature itself (see original application, page 5, lines 1 to 3). Keeping something private, i.e. secret, involves more than merely not transmitting such information. While there are several passages relating to different protocols directly and unambiguously disclosing that a transmission of the respective signatures S_A and S_B can be avoided (see point 5.3 above), there is however no direct and unambiguous disclosure for signatures S_A and S_B to be kept private.

9.7 Therefore the original application documents do not provide a direct and unambiguous disclosure for claim 1, step ii) comprising "said first correspondent A maintaining said first signature private to itself by avoiding transmission of said first signature" and step iv) with the corresponding formulation "said second correspondent B maintaining said second signature private to itself by avoiding transmission of said second signature".

9.8 Claim 1 according to this request therefore does not fulfil the requirements Article 123(2) EPC in contrast to the requirements of Article 100(c) EPC.

10. Hence, none of the proprietor's requests fulfils the requirements of the EPC.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.
2. The patent is revoked.

The Registrar: The Chair:

Beschwerdekammern des Europäischen Patentamts ✦ Boards of Appeal of the European Patent Office ✦ Chambres de recours de l'Office européen des brevets

K. Götz-Wein A. Ritzka

Decision electronically authenticated