BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS **BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE** **CHAMBRES DE RECOURS DE L'OFFICE EUROPÉEN 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 18 March 2021

Case Number:	T 1365/16 - 3.5.03
Application Number:	04733283.8
Publication Number:	1642437
IPC:	H04L29/06, H04L9/06
Language of the proceedings:	EN

Title of invention:
Key agreement and transport protocol

Patent Proprietor:
BlackBerry Limited

Opponent:
Infineon Technologies AG

Headword:
Key agreement protocol/BLACKBERRY

Relevant legal provisions:
EPC Art. 123(2)

This datasheet is not part of the Decisior
It can be changed at any time and without notic

Keyword:
Added subject-matter - all requests (yes): intermediate generalisation; general statements like "the invention ... may equally be utilised in ..." cannot replace a direct and unambiguous disclosure

Decisions cited:
G 0002/10, T 0331/87, T 1067/97, T 1538/12, T 1852/13

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 1365/16 - 3.5.03

DECISION
of Technical Board of Appeal 3.5.03
of 18 March 2021

Appellant I: (Opponent)	Infineon Technologies AG Am Campeon 1-12 85579 Neubiberg (DE)
Representative:	Fechner, Benjamin K&L Gates LLP Karlstraße 12 80333 München (DE)
Appellant II: (Patent Proprietor)	BlackBerry Limited 2200 University Avenue East Waterloo, ON N2K 0A7 (CA)
Representative:	Ahmad, Sheikh Shakeel Keltie LLP No.1 London Bridge London SE1 9BA (GB)
Decision under appeal:	**Interlocutory decision of the Opposition Division of the European Patent Office posted on 11 April 2016 concerning maintenance of the European Patent No. 1642437 in amended form.**

Composition of the Board:

Chair	K. Bengi-Akyürek
Members:	T. Snell
	R. Romandini

Summary of Facts and Submissions

I. The present case concerns appeals filed by the opponent (henceforth, "Appellant I") and the proprietor (henceforth, "Appellant II") against the interlocutory decision of the opposition division maintaining the patent in amended form on the basis of the "second auxiliary request".

II. Appellant I requests that the decision under appeal be set aside and that the patent be revoked.

III. Appellant II requests that the decision under appeal be set aside and that the patent be maintained in amended form in accordance with one of the following claim requests:

Main request;
Auxiliary requests 1A to 1C;
Auxiliary requests 2A to 2C;
Auxiliary requests 3A to 3C;
Auxiliary requests 2D and 3D.

The main request and auxiliary requests 1A to 1C, 2A to 2C and 3A to 3C are as filed with Appellant II's submission dated 11 July 2017. Auxiliary requests 2D and 3D are as filed with their submission dated 17 December 2020.

IV. Claim 1 of the **main request** reads as follows:

"A method of symmetric key agreement between a first correspondent (10) and a second correspondent (12) in a data communication system, each of said first correspondent (10) and said second correspondent (12) having a master key K,

said method comprising the steps of:

said first correspondent (10) generating a first value X and providing said first value X to said second correspondent (12);

said second correspondent (12) generating a second value Y and

computing a shared key k by operating a keyed cryptographic function on a combination of said first value X and said second value Y, said second correspondent (12) using said master key K as an input to said keyed cryptographic function;

said second correspondent (12) providing said second value Y to said first correspondent (10);

said first correspondent (10) computing said shared key k by operating said keyed cryptographic function on said combination of said first value X and said second value Y, said first correspondent (10) using said master key K as an input to said keyed cryptographic function."

V. Claim 1 of **auxiliary request 2C** reads as follows (i.e. the claim request allowed by the opposition division):

"A method of symmetric key agreement between a first correspondent (10) and a second correspondent (12) in a data communication system, each of said first correspondent (10) and said second correspondent (12) having a master key K,

said method comprising the steps of:

said first correspondent (10) generating a first value X and providing said first value X to said second correspondent (12);

said second correspondent (12) generating a second value Y and

computing a shared key k by operating a first keyed cryptographic hash function on a concatination *[sic]* of said first value X and said second value Y,
said second correspondent (12) using said master key K as an input to said first keyed cryptographic hash function;

said second correspondent (12) providing said second value Y to said first correspondent (10);

said first correspondent (10) computing said shared key k by operating said first keyed cryptographic hash function on said concatination *[sic]* of said first value X and said second value Y, said first correspondent (10) using said master key K as an input to said first keyed cryptographic hash function;

said second correspondent (12) applying a second keyed cryptographic hash function

to a combination of said first value X, said second value Y, and identification information of said first correspondent (10) to yield a first hash value, said second correspondent (12) using said shared key k computed by said second correspondent (12) as an input to said second keyed cryptographic hash function;

said second correspondent (12) providing said first hash value to said first correspondent (10);

said first correspondent (10) applying said second keyed cryptographic hash function to

a combination of said first value X, said second value Y, and said identification information of said first correspondent (10) to yield a second hash value,

said first correspondent (10) using said shared key k computed by said first correspondent (10) as an input to said second keyed cryptographic hash function; and

said first correspondent (10) verifying that said first hash value equals said second has *[sic]* value,

wherein said first value X is a random integer generated by said first correspondent (10) and said second value Y is a random integer generated by said second correspondent (12)."

VI. Claim 1 of **auxiliary request 2D** is the same as claim 1 of auxiliary request 2C except that the terms "first keyed" and "second keyed" are amended to "keyed", and, on the first occurrence of the term "second keyed" in the claim, the wording "a second keyed" is replaced by "said keyed".

VII. Claim 1 of **auxiliary request 3C** is the same as auxiliary request 2C except that the following wording is inserted ahead of the final feature "wherein said first value X ...":

> "said first correspondent (10) applying said second keyed cryptographic hash function to a combination of said first value X, said second value Y, and identification information of said second correspondent (12) to yield a third hash value, said first correspondent (10) using said shared key k computed by said first correspondent (10) as an input to said second keyed cryptographic hash function;
>
> said first correspondent (10) providing said third hash value to said second correspondent (12);
>
> said second correspondent (12) applying said second keyed cryptographic hash function to a combination of said first value X, said second value Y, and said identification information of said second correspondent (12) to yield a fourth hash value, said second correspondent (12) using said shared key k computed by said second correspondent (12) as an input to said second keyed cryptographic hash function; and
>
> said second correspondent (12) verifying that said third hash value equals said fourth hash value,".

VIII. Claim 1 of **auxiliary request 3D** is the same as claim 1 of auxiliary request 3C except that the terms "first keyed" and "second keyed" are amended to "keyed", and, on the first occurrence of the term "second keyed" in the claim, the wording "a second keyed" is replaced by "said keyed".

IX. For reasons of conciseness, the wording of claim 1 of **auxiliary requests 1A to 1C, 2A, 2B, 3A and 3B** is not reproduced here.

Reasons for the Decision

1. Technical context

1.1 The opposed patent relates to key agreement protocols for transfer and authentication of encryption keys between a first and a second correspondent. In the claimed key agreement protocol, both parties contribute cryptographic information (in the embodiment of Fig. 8, random values X and Y) which enables the parties to jointly establish a shared secret key k. An authentication feature provides each party with the assurance that no third party may gain knowledge of the shared secret key. In the present case (as shown in Fig. 8), authentication values ($hash_B$, $hash_A$) are computed by both parties based on a hash function, using the shared key k, of a concatenation of X, Y and the ID value of one of the correspondents. Each party verifies whether the hash value computed by itself matches that received from the other party for mutual authentication purposes.

1.2 A key agreement protocol may be based on public key cryptography, which is inherently *asymmetric*. This is the case for all but one of the detailed embodiments of the patent (cf. Figs. 2 to 7). A single embodiment however (cf. Fig. 8) concerns a *symmetric* key agreement protocol. The claims of the main request and all the auxiliary requests now on file concern such a symmetric key agreement protocol.

2. *General principles as regards Article 123(2) EPC*

2.1 The "gold standard" for assessing compliance with Article 123(2) EPC is that amendments must be *directly and unambiguously* derivable from the application documents as filed, taking account of matters implicit to the person skilled in the art (cf. G 2/10).

2.2 In the more recent, and now well-established, jurisprudence of the boards of appeal, the so-called "essentially test" (as set out in T 331/87) is no longer considered appropriate (cf. e.g. T 1852/13, Reasons, point 2.2.3 ff.).

2.3 As regards *intermediate generalisations*, it is not possible to base an amended claim on the extraction of isolated features from a set of features originally disclosed only in combination, e.g. a specific embodiment in the description or drawings of the original patent application. However, such an amendment may be justified if there is no clearly recognisable functional or structural relationship among the features of the specific combination and if the extracted feature(s) is/are thus not inextricably linked with those features (see e.g. T 1067/97, Reasons, point 2.1.3).

3. *All requests - claim 1 - Article 123(2) EPC*

3.1 The appellant argues essentially that claim 1 of each request is based on Figure 8 and the associated description on page 10, lines 16-22 as filed. The omission of certain features of Figure 8 (in particular, the randomness of the values X and Y, the several concatenation/hash computation features, and the computation and verification of hash values in the first correspondent) is justified by reference to this passage, and by the fact that the omitted features are not essential, following T 331/87 (*supra*). The skilled person would understand that Figure 8 merely discloses one possible embodiment. Starting from this embodiment, the reference on page 10 to "the invention" would lead the skilled person to consult the independent claims as filed, in particular independent claim 3. Although claim 3 is directed to a public/private key-based embodiment, it neither requires random numbers nor any concatenation. It is therefore clear and unambiguous to the skilled person that the embodiment of Fig. 8 can also be generalised by omitting these non-essential features.

3.2 The board does not agree with Appellant II's arguments for the following reasons:

3.2.1 Firstly, whether or not a feature is "essential" is not the appropriate test (cf. point 2.2 above). Instead, it is necessary to determine what is directly and unambiguously disclosed in the application as filed ("gold standard").

3.2.2 As stated, claim 1 of each request is directed to a method of *symmetric* key agreement between a first and a second correspondent in a data communication system. The only embodiment in the application as filed which concerns a symmetric key agreement is Figure 8. The previous Figures 2 to 7 disclose several embodiments of a method of key agreement which rely on public-key cryptography and which are thus *asymmetric*.

3.2.3 Whereas the several public key-based embodiments are described in a certain amount of detail, the embodiment of Figure 8, which is a flow diagram including full mathematical expressions for implementing key exchange and authentication in both directions, is referred to only briefly at the end of the description in the following terms (cf. page 10, lines 16 to 22 of the description as filed):

> "*It will be appreciated that although <u>the invention</u> has been described with reference [to] public key based agreement protocols and entity authentication protocols, <u>it may equally be utilized on symmetric key agreement protocols</u>. In such an embodiment, the computation of the shared key K may be performed using a master key K_m as one input to a keyed hash function. A concatenation of the ephemeral keys G_A, G_B, is used as the other input and the resultant output is used as the shared key K.*
>
> *Such an arrangement is shown <u>in figure 8</u>.*" (board's underlining).

3.2.4 The term "*the invention*" as used here is vague and unspecific and as such cannot be a *direct and unambiguous* basis for applying aspects of embodiments which apply to a public key-based protocol (Figures 2 to 7) to the embodiment of Figure 8, which concerns a symmetric key protocol. Building on the guidance expressly stated in the cited passage regarding the computation of the shared key ("In such an embodiment ..."), the skilled person wishing to apply the teaching of "the invention" to the embodiment of Figure 8 would have to make their own considerations as to how to make use of either the general disclosure of claim 3 or the detailed embodiments of Figures 2 to 7, including deciding which features should be included and which left out. Whether and how the skilled person would generalise the embodiment of Figure 8 is however neither inherent nor implicit from the disclosure as filed, but concerns at most matters related to obviousness. This is however not a sufficient basis to comply with Article 123(2) EPC, where generally the "disclosure test" is to be applied (see e.g. G 2/10, Reasons, point 4.5.1).

3.2.5 In particular, as stated in decision T 1538/12 (cf. Reasons, point 1.1):

> *"General statements at the end of the description (e.g. ... 'other variations and modifications of the exemplary embodiments described above may be made' or 'other embodiments will be apparent to those skilled in the art') do not constitute, and thus cannot replace, a direct and unambiguous disclosure of the particular generalisation included in claim 1 as granted. The general statements at the end of the description are furthermore open ended and attempt to burden the skilled reader with having to work out which combinations of features from the detailed embodiments might be claimed together, while the applicant is supposedly dispensed from having to present his invention in terms more general than mere detailed description of particular embodiments*."

3.2.6 The same considerations apply, *mutatis mutandis*, to the general statement that "the invention ... may equally be utilized on symmetric key agreement protocols", even if this statement is not quite as general as the two examples given in T 1538/12.

3.2.7 The board concludes that only the embodiment of Figure 8 *taken in its entirety* discloses, directly and unambiguously, a method of *symmetric* key agreement on which a claim complying with Article 123(2) EPC could be based. It follows that any features left out of this embodiment would result in an unallowable intermediate generalisation with respect to the application as filed, all the more so as there is a clearly recognisable functional or structural relationship between all the features of Figure 8 (cf. point 2.3 above).

3.2.8 As regards the claim requests on file, there is no version of claim 1 which comprises all the features of Figure 8, because no version of claim 1 includes the following features:

(i) computing a hash value by applying a keyed hash function to the *concatenation* of the variables Y, X and Id_A (cf. Fig. 8, the third block on the right-hand side: "Compute hash over string ($Y \| X \| Id_A$) using keyed hash function h_k with key k to yield string $hash_B$");

(ii) computing a hash value by applying a hash function to the *concatenation* of the variables X, Y and Id_A or Id_B as defined in the third and fifth blocks on the left-hand side and the fourth block on the right-hand side of Figure 8.

Moreover, where these hash functions are partially defined (e.g. in claim 1 of auxiliary requests 2C, 2D, 3C and 3D), the more general term "*combination*" is used instead of "*concatenation*". However, there is no basis for broadening the "concatenation" functions disclosed in Figure 8 to mere "combinations", for the reasons given above.

3.2.9 With respect to claim 1 of auxiliary requests 2C, 2D, 3C and 3D, Appellant II argued that the use of the term "combination" in claim 1 had been the result of a "transcribing error", as was evident from the file history (here, Appellant II referred to a submission dated 6 September 2010, i.e. during the examination proceedings). The correct definition was given in the dependent claims (cf. dependent claim 3 of auxiliary requests 2C and 2D, and dependent claim 2 of auxiliary requests 3C and 3D. Consequently, the term "combination" implicitly had to be understood as "concatenation" in line with the dependent claims.

3.2.10 This argument is however not convincing. The purpose of dependent claims is to define *further* embodiments in terms of additional (i.e. limiting) features (cf. Rules 43(3) and (4) EPC). They cannot be used as a basis for interpreting the independent claim as being correspondingly limited.

The alleged "transcribing error" could make no difference in this regard, especially as the term "combination" is clear and makes technical sense in the present context (cf. Article 84 EPC). In any case, the board points out that even if the applicant had during the prosecution of the file erroneously or inadvertently used the term "combination", there had been ample opportunity in the meantime to file a corresponding amendment, at the latest following the raising of this issue by Appellant I in their statement of grounds of appeal (cf. page 14, point 2).

3.3 The board concludes that claim 1 respectively of the **main request** and each of auxiliary requests **1A to 1C**,

2A to 2D and 3A to 3D does not comply with Article 123(2) EPC.

4. Conclusion

As there is no allowable set of claims, it follows that the decision under appeal is to be set aside and that the patent is to be revoked.

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

B. Brückner K. Bengi-Akyürek

Decision electronically authenticated