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 30 November 2018

Case Number:	T 2268/15 - 3.5.05
Application Number:	08784926.1
Publication Number:	2291946
IPC:	H04L9/08, H04W12/02
Language of the proceedings:	EN

Title of invention:
Cryptographic key generation

Patent Proprietor:
Telefonaktiebolaget LM Ericsson (publ)

Opponent:
Sony Corporation

Headword:
AKA-based security keys/ERICSSON

Relevant legal provisions:
EPC Art. 87(1), 56

Keyword:
Validity of priority claim - (yes, after amendments)
Inventive step - (yes, after amendments)

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

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 2268/15 - 3.5.05

DECISION
# of Technical Board of Appeal 3.5.05
of 30 November 2018

Appellant:
(Patent Proprietor)

Telefonaktiebolaget LM Ericsson (publ)
164 83 Stockholm (SE)

Representative:

Röthinger, Rainer
Wuesthoff & Wuesthoff
Patentanwälte PartG mbB
Schweigerstrasse 2
81541 München (DE)

Respondent:
(Opponent)

Sony Corporation
1-7-1 Konan Minato-ku
Tokyo 108-0075 (JP)

Representative:

Samson & Partner Patentanwälte mbB
Widenmayerstraße 6
80538 München (DE)

Decision under appeal:

Decision of the Opposition Division of the European Patent Office posted on 28 October 2015 revoking European patent No. 2291946 pursuant to Articles 101(2) and 101(3)(b) EPC

Composition of the Board:

Chair A. Ritzka
Members: K. Bengi-Akyuerek
F. Blumer

Summary of Facts and Submissions

I. The appeal of the patent proprietor is against the opposition division's decision to revoke the present European patent as granted. The decision was based on the finding of lack of novelty (Articles 100(a) and 54 EPC) with respect to the patent as granted (main request) as well as the first and sixth auxiliary requests, and of extension of the scope of protection with respect to the second to fifth auxiliary requests (Article 123(3) EPC). The objection of lack of novelty relied on the following documents:

D1a: 3GPP TS 33.102 V5.4.0 (2004-06), Technical Specification, Release 5, pp. 1-61, June 2004;
D2: 3GPP TS 33.401 V1.1.0 (2008-04), Technical Specification, Release 8, pp. 1-45, April 2008;
D2a: 3GPP TS 33.401 V8.0.0 (2008-06), Technical Specification, Release 8, pp. 1-45, June 2008;
D3: WO-A-2004/075584;
D5: "Additional inputs to EPS Key Derviation[sic] Function (KDF)", Change Request, 3GPP TSG-SA WG3 Meeting #52, draft S3-080700, pp. 1-2, June 2008.

As regards the assessment of the auxiliary requests on file, the opposition division admitted late-filed document D5 into the opposition proceedings and considered it to belong to the state of the art under Article 54(2) EPC on the grounds that the subject-matter claimed was not related to the "same invention" as disclosed in the following US patent application from which priority was claimed (Article 87(1) EPC):

P3: US 61/059,386.

Furthermore, the opponent introduced the following prior-art document as evidence of the UMTS standard referred to in D3:

D6: 3GPP TS 33.203 V5.3.0 (2002-09), Technical Specification, Release 5, pp. 1-37, September 2002.

By way of an *obiter dictum*, the decision under appeal further indicated that the sixth auxiliary request was considered to comply with Article 54 EPC in view of D3 but to lack an inventive step (Article 56 EPC) in view of D5, D2a and D1a.

II. With the statement setting out the grounds of appeal, the appellant filed amended claims according to eight auxiliary requests (first to eighth auxiliary requests) and requested that the decision under appeal be set aside and the patent be maintained on the basis of the claims according to the main request (patent as granted) or any of the above auxiliary requests.

III. In its letter of reply, the respondent requested that the appeal be dismissed. It challenged the novelty and inventive step of all claim requests mainly via three lines of attack: (i) D5 read with D2a, (ii) D3 alone and (iii) D2 combined with D3. Furthermore, it contended that the priority from US patent application P3 was invalidly claimed with respect to the independent claims of the patent (Article 87(1) EPC).

IV. With a letter of reply dated 29 May 2017, the appellant filed a "main request A" and "auxiliary requests 1A to 8A" and new third to sixth auxiliary requests replacing the former ones.

V. The respondent announced that it would not be attending any scheduled oral proceedings before the board.

VI. In a communication annexed to the summons to oral proceedings pursuant to Article 15(1) RPBA, the board gave its preliminary opinion on the appeal. In particular, it made observations with regard to the validity of the priority claim (Article 87(1) EPC) and to the question whether document D5 could be considered to be state of the art under Article 54(2) EPC, the matter of novelty and inventive step (Articles 54 and 56 EPC), mainly having regard to D3 and D5, and the admissibility of the auxiliary requests on file.

VII. By letter of reply, the appellant filed new main requests a, b and c and new auxiliary requests 1a to 8a, 1b to 8b and 1c to 8c and advanced arguments on the board's communication under Article 15(1) RPBA.

VIII. Oral proceedings were held on 30 November 2018 in the absence of the respondent, during which the appellant withdrew all the claim requests on file except for "main request A".

- The appellant's final request was that the decision under appeal be set aside and that the patent be maintained on the basis of the claims according to "main request A".

- It was established from the file that the respondent's final request was that the appeal be dismissed.

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

IX. Claim 1 of **main request A** reads as follows:

"A method for generating a cryptographic key (120) for protecting mobile communication between two entities (202, 204), wherein the method is carried out by the first entity (202, 302) as part of an Authentication and Key Agreement (AKA) procedure based on an UMTS AKA protocol initiated by the second entity (204, 304), the method being characterized by the steps of:

- providing (306) at least two parameters (106, 108), wherein the first parameter (106) comprises or is derived from a set of cryptographic keys (110, 112) having been computed by the first entity (202) by running the AKA procedure and the second parameter comprises or is derived from a token (116) having a different value each time the AKA procedure is initiated by the second entity (204, 304) for the first entity (202, 302); and
- applying (308) a key derivation function to generate a cryptographic key (120) based on the provided parameters (106, 108);

wherein the token (116) is a concatenation of the exclusive OR of a sequence number <SQN> and an Anonymity Key <AK>, an Authentication and Key Management Field <AMF>, and a Message Authentication Code <MAC>,

wherein the SQN indicates the number of times the AKA procedure has been initiated by the second entity (204, 304) for the first entity (202, 302), and

wherein the AK is a cryptographic key produced by a key generation function f5 using a random challenge pursuant to the UMTS AKA protocol."

The further independent claim 12 of "main request A" is directed to a corresponding device.

Reasons for the Decision

1. *The invention*

The present invention relates to the generation of a cryptographic security key, K_{ASME}, to be used as shared key between a mobile terminal (UE) and an access network (Access Security Management Entity, ASME) in the framework of the 3GPP-based authentication and key agreement (AKA) protocol. The above key is to be generated by means of a key derivation function (KDF) using a first input parameter (corresponding to the concatenation of a cipher key, CK, and an integrity key, IK, as "CK‖IK") and a second input parameter (corresponding to an authentication token, AUTN, made up of an exclusive OR, xOR, of a sequence number, SQN, and an anonymity key, concatenated with an authentication and key management field, AMF, and a message authentication code, MAC, as "(SQN xOR AK)‖AMF‖MAC"). This type of key generation is intended to ensure the "uniqueness" of the inputs to the KDF and thus to avoid a collision between different UEs using the same key K_{ASME} (see e.g. page 2, lines 30-33 and page 18, lines 29-31 of the present application as filed).

2. *Allowability of MAIN REQUEST A*

Claim 1 of "main request A" comprises the following features (as labelled by the parties; the amendments compared with claim 1 as granted being highlighted):

(a) A method for generating a cryptographic key for protecting mobile communication between two entities,

(b) wherein the method is carried out by the first entity as part of an AKA procedure based on a UMTS AKA protocol,

(c) initiated by the second entity and comprises the steps of

(d) providing at least two parameters,

(e) wherein the first parameter comprises or is derived from a set of cryptographic keys having been computed by the first entity by running the AKA procedure,

(f) wherein the second parameter comprises or is derived from a token having a different value each time the AKA procedure is initiated by the second entity for the first entity,

(g) wherein the token ~~comprises an~~ is a concatenation of the exclusive OR of a sequence number <SQN> and an Anonymity Key <AK>, an Authentication and Key Management Field <AMF> and a Message Authentication Code <MAC>,

(h) wherein the SQN indicates the number of times the AKA procedure has been initiated by the second entity for the first entity,

(i) wherein the AK is a cryptographic key produced by a key generation function f5 using a random challenge pursuant to the UMTS AKA protocol;

(j) applying a key derivation function to generate a cryptographic key,

(k) based on the provided parameters.

The further independent apparatus **claim 12** of "main request A" corresponds to that of present claim 1.

2.1 *Validity of priority claim (Article 87(1) EPC)*

2.1.1 As to feature (g) of present claim 1, the respondent argued that the then pending claim 1 was not supported by priority application **P3** since the latter taught that the authentication token comprised not only an exclusive OR ("xOR") of SQN and AK but also the concatenation of an Authentication and Key Management Field (AMF) and a Message Authentication Code (MAC).

2.1.2 Following the amendments resulting in present feature (g), the board is satisfied that claim 1 is now supported by the opposed patent's priority application P3 (see e.g. page 5, last paragraph) and that the respective objection of the respondent is overcome. The board concludes that present claim 1 is thus related to the "same invention" within the meaning of Article 87(1) EPC and that therefore the priority claim is valid. As a consequence, document **D5** does not constitute state of the art under Article 54(2) EPC for the subject-matter claimed.

2.2 *Novelty and inventive step (Articles 54 and 56 EPC)*

2.2.1 The board regards prior-art document **D3** as the most suitable starting point on file for the assessment of inventive step in the present case since it - like the present invention - relates to the 3GPP-based authentication and key agreement (AKA) protocol based on the generation of an authentication token (AUTN) including an xOR operation applied to SQN and AK. The board understands that D3 discloses the following limiting features of present claim 1:

(a) A method for generating a cryptographic key (e.g. "abgeleiteter Schlüssel CK1") for protecting mobile communication between two entities *(see e.g. page 23, equation (7))*,

(b) wherein the method is carried out by the first entity ("S-CSCF 109") as part of an AKA procedure based on a UMTS AKA protocol ("IMS-AKA-Protokoll") *(see e.g. page 22, lines 32-36; Figs. 1 and 2)*,

(c) wherein the method is initiated by the second entity ("Mobilfunkgerät 103") *(see e.g. Fig. 2, "SIP-Registrierungs-Nachricht 201")* and comprises the steps of:

(d) providing two parameters ("CK|Par1" and "random") *(see page 23, equation (7))*,

(e) wherein the first parameter ("CK|Par1") comprises a ~~set of~~ cryptographic key~~s~~ ("Übertragungsschlüssel CK") having been computed by the first entity by running the AKA procedure *(see e.g. page 22, equation (3))*,

(f) wherein the second parameter ("random = RAND|AUTN|XRES") comprises a token ("AUTN") having a different value each time the AKA procedure is initiated by the second entity for the first entity *(see e.g. page 23, equation (8))*,

(g) wherein the token ("AUTN = SQN⊕AK|AMF|MAC") is a concatenation of the exclusive OR of SQN and an AK, an AMF, and a MAC *(see e.g. page 22, equation (6))*,

(h) wherein the SQN ("fortlaufende Sequenznummer SQN 302") indicates the number of times the AKA procedure has been initiated by the second entity for the first entity *(see page 20, lines 25-28, in conjunction with page 4, lines 20-22)*,

(i) wherein the AK is a cryptographic key produced by a key generation function ("f5$_K$") using a random challenge ("RAND") pursuant to the UMTS AKA protocol *(see page 22, equation (5))*;

(j) applying a key derivation function ("Schlüsselableitungsfunktion f 317") to generate a cryptographic key *(see e.g. page 22, lines 32-36; Fig. 3, "f 317")*,

(k) based on the provided parameters *(see e.g. page 22, lines 32-36)*.

2.2.2 As to features (b) and (i) of present claim 1, the appellant argued that a UMTS-based AKA protocol did not correspond to an IMS-based AKA protocol since the former protocol related to an *access* network whereas the latter one to a *service* network.

However, it is apparent to the board that D3 in fact teaches that the "IMS AKA protocol" is described in the standard document relating to the UMTS Release 5 architecture (see page 1, lines 15-19; see also **D6** referenced as "[1]" on page 1, line 25 of D3) and is used for secure user access (registration) to the IMS of the underlying UMTS system (see D3, page 1, lines 21-27). The board further holds that the skilled reader would be aware that the IMS AKA protocol is supposed to be <u>based on</u> the "UMTS AKA protocol" and that the AK is to be calculated <u>pursuant to</u> the same rules as with the "UMTS AKA protocol" as claimed (see in this respect also D6, page 11, first paragraph, emphasis added: *"The AKA-protocol is a secure protocol developed for UMTS and the <u>same</u> concept/principles will be reused for the IP Multimedia Core Network Subsystem, where it is called IMS AKA."*). Hence, the board agrees with the respondent that features (b) and (i) are considered to be anticipated by D3.

2.2.3 As to feature (h), the appellant argued that D3 disclosed merely a general sequence number SQN and not a specific sequence number indicating the number of AKA initiations.

It is evident to the board that document D3 teaches that a continuous sequence number ("fortlaufende Sequenznummer") is generated at the network entity (see page 20, lines 25-28). Furthermore, D3 (see e.g. page 4, line 20) refers to D6 which in turn references 3GPP-based standard document **D1a** as "[1]" (see e.g. D6, page 12, section 6.1, third paragraph, third sentence: *"The requirements on the handling of the counters and mechanisms for sequence number management are specified in [1]"*). Document D1a, moreover, teaches that at the start of each authentication session the network entity ("HE/AuC") generates a fresh sequence number SQN (see D1a, page 20, first two sentences: *"The HE/AuC starts with generating a fresh sequence number SQN and an unpredictable challenge RAND. For each user the HE/AuC keeps track of a counter ..."*).

In that regard, the appellant submitted at the oral proceedings before the board that D1a provided two alternatives as regards the sequence number generated, namely sequence numbers that are or are not time-based (see D1a, page 53, sections C.1.1.2 and C.1.1.3), such that the skilled person was presented with several options from which only the first alternative relied on counting the AKA initiations (see also appealed decision, page 10, second paragraph).

2.2.4 In any event, as to feature (e), the board concurs with the appellant that D3 fails to disclose that the first parameter (i.e. "CK|Par1" in equation (7) of D3) comprises or is derived from a <u>set</u> of cryptographic key<u>s</u> computed by the first entity "S-CSCF 109" since - besides the input parameter value "Par1" - only one cryptographic key, namely cipher key CK, is used as the first input parameter in D3. Hence, present claim 1 is distinguished from the disclosure of D3 at least by feature (e) and is thus novel over D3 (Article 54 EPC).

2.2.5 The board accepts that distinguishing feature (e) has the technical effect that it increases the overall security of the underlying system due to the use of *multiple* cryptographic keys for the generation of the first parameter, on the basis of which the resulting overall cryptographic key is subsequently to be generated.

2.2.6 Starting out from the teaching of D3, the skilled person would notice that - in addition to the cipher key CK - the only cryptographic key that is theoretically meaningful in that context is the integrity key ("Integritätsschlüssel IK 314"; see e.g. page 1, lines 29-34: *"Gemäß dem IMS-AKA-Protokoll authentifizieren das Mobilfunkendgerät und das Kommunikationsnetz ... sich gegenseitig und es werden zwei kryptographische Schlüssel generiert, der so genannte Integritätsschlüssel und der so genannte Übertragungsschlüssel ..."* or page 15, lines 23-26: *"Zur Sicherung der Kommunikation erzeugt der beschriebene Mechanismus Sitzungsschlüssel, die von dem ... gebildeten Integritätsschlüssel und/oder Übertragungschlüssel abgeleitet werden ..."*).

2.2.7 However, the board finds that the following teaching of D3 on page 14, lines 1-7 and page 24, line 36 to page 25, line 8 would most likely deter the skilled person from using an integrity key or any other cryptographic key in order to make the generation of the first parameter more complex and thus less vulnerable to security attacks (emphasis added by the board):

> *"Durch die Verwendung des Übertragungsschlüssels (und* ***nicht*** *des Integritätsschlüssels) als Basisschlüssel zur Schlüsselableitung wird zusätzlich vermieden, dass Unterschiede bei der Verwendung des Schlüssels zwischen verschiedenen Versionen des Standards (UMTS-3GPP Release 5 und UMTS-3GPP Release 6, usw.) entstehen, die zu höheren Standardisierungs- und Integrationsaufwänden führen würden."*

> *"Vor Weiterleiten der Authentifikations-Anforderungsnachricht 204 speichert der P-CSCF-Computer 113 den Integritätsschlüssel IK 314 sowie den ersten abgeleiteten Schlüssel CK1, entfernt diese aus der Authentifikations-Anforderungsnachricht 204 und übermittelt eine reduzierte Authentifikations-Anforderungsnachricht 205 an das Mobilfunkendgerät 103.*
>
> *Damit ist der Integritätsschlüssel IK 314 in dem P-CSCF-Computer 113 verfügbar,* ***nicht*** *aber in dem Mobilfunkendgerät 103."*

2.2.8 In view of the above, the board holds that the person skilled in the field of 3GPP-based mobile networks *could* but not *would* ignore the above teachings and apply an additional cryptographic key at the cost of overall cryptographic complexity and increased processing power needs. Hence, the skilled person would not come up with the solution according to feature (e) of present claim 1 without the benefit of hindsight analysis.

2.2.9 Given that the other prior-art documents on file do not come closer to the present invention than D3 and that they fail to disclose or render obvious in particular feature (e) in combination with the remaining features of present claim 1, the subject-matter of claim 1 is held to be new and to involve an inventive step within the meaning of Article 52(1) EPC in conjunction with Articles 54 and 56 EPC.

As, moreover, the subject-matter of independent apparatus claim 12 corresponds to that of claim 1, the above observations also apply to claim 12.

3. Since the board holds that there are no other objections to be raised as regards the present claim set, the board decides that the patent is to be maintained on the basis of "main request A".

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the opposition division with the order to maintain the patent on the basis of Main Request A (claims 1 to 17) and a description and drawings to be adapted.

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