**Internal distribution code:**

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

# Datasheet for the decision of 1 December 2020

**Case Number:** T 0676/16 - 3.5.03

**Application Number:** 13169907.6

**Publication Number:** 2635060

**IPC:** H04W12/06

**Language of the proceedings:** EN

**Title of invention:**
Mutual authentication with modified message authentication code

**Applicant:**
Qualcomm Incorporated

**Headword:**
Mutual authentication/QUALCOMM

**Relevant legal provisions:**
EPC Art. 76(1), 123(2), 84, 113(1), 116(1)
RPBA 2020 Art. 15(2)(a), 15(3)

**Keyword:**
Oral proceedings - postponement (no): request not filed as soon as possible
Right to be heard - (yes)
Added subject-matter - all requests (yes)
Clarity - all requests (no)

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 0676/16 - 3.5.03**

# D E C I S I O N
# of Technical Board of Appeal 3.5.03
# of 1 December 2020

| | |
|---|---|
| **Appellant:** (Applicant) | Qualcomm Incorporated<br>5775 Morehouse Drive, R-132 D<br>San Diego, CA 92121-1714 (US) |
| **Representative:** | Tomkins & Co<br>5 Dartmouth Road<br>Dublin 6 (IE) |
| **Decision under appeal:** | **Decision of the Examining Division of the European Patent Office posted on 30 October 2015 refusing European patent application No. 13169907.6 pursuant to Article 97(2) EPC.** |

**Composition of the Board:**

| | |
|---|---|
| **Chair** | K. Bengi-Akyürek |
| **Members:** | T. Snell |
| | N. Obrovski |

## Summary of Facts and Submissions

I. The present case concerns the appeal by the applicant (henceforth, "appellant") against the decision of the examining division refusing the present European divisional application (which has the parent application EP 05812748.1) on the ground of lack of inventive step (Articles 52(1) and 56 EPC).

II. The appellant requests that the decision under appeal be set aside and that a patent be granted on the basis of the claims of the main request or, alternatively, the claims of either the "NEW first auxiliary request" or the "NEW second auxiliary request", all claim requests as filed together with the statement of grounds of appeal. A conditional request for oral proceedings was filed in the statement of grounds of appeal.

III. In a preliminary opinion under Article 15(1) RPBA, the board, *inter alia*, raised numerous objections pursuant to Articles 76(1), 123(2) and 84 EPC with respect to claim 1 of all claim requests.

IV. Shortly before the arranged oral proceedings, the appellant submitted a request for postponement of the oral proceedings, which the board subsequently refused (see Reasons, point 1 below).

V. Oral proceedings were held in the absence of the appellant on 1 December 2020. At the end of the oral proceedings, the board's decision was announced.

VI. In this decision, the following document is referred to:

**D2**: ETSI TS 133 102 V3.6.0 (2000-10), Universal Mobile Telecommunications System (UMTS); 3G Security; Security Architecture (3GPP TS 33.102 version 3.6.0 Release 1999).

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

"A method for a cellular communications network of instructing a subscriber identity module to process authentication information, comprising:

receiving (704) authentication data at the subscriber identity module, said authentication data comprising a modified authentication management field, AMF, containing instructions to the subscriber identity module, and a message authentication code, MAC, generated using the modified AMF;

computing (706) a first expected MAC using at least a portion of said authentication data;

comparing (708) said first expected MAC to said received MAC, and when the received MAC does not equal the first expected MAC:

assuming that the received MAC is a MAC generated using a modified AMF, and computing (712) a second expected MAC;

comparing (714) said second expected MAC to said received MAC; and

characterised by:

processing (716) at least a portion of the content of the modified AMF when said second expected MAC and said received MAC are the same;

wherein the processed content of the modified AMF comprises an instruction to the subscriber identity module."

VIII. Claim 1 of the **"NEW first auxiliary request"** is the same as claim 1 of the main request except that the "receiving" step reads as follows (board's underlining):

> "receiving (704) authentication data at the subscriber identity module, said authentication data comprising a modified authentication management field, AMF, modified to contain instructions to the subscriber identity module, and a message authentication code, MAC, generated using the modified AMF;".

IX. Claim 1 of the **"NEW second auxiliary request"** reads as follows (board's underlining):

"A method for a cellular communications network of instructing a subscriber identity module in a mobile station to process authentication information, comprising:

receiving (704) authentication data and an encrypted group encryption key Kg at the subscriber identity module, said authentication data comprising a modified authentication management field, AMF, containing instructions to the subscriber identity module, and a message authentication code, MAC, generated using the modified AMF;

computing (706) a first expected MAC using at least a portion of said authentication data;

generating a cipher key, CK, and an integrity key, IK, using a secret key K;

comparing (708) said first expected MAC to said received MAC, and when the received MAC docs not equal the first expected MAC:

assuming that the received MAC is a MAC generated using a modified AMF, and computing (712) a second expected MAC;

comparing (714) said second expected MAC to said received MAC; and

characterised by

when said second expected MAC and said received MAC are the same:

decrypting the encrypted group encryption key Kg using the CK;

storing the group encryption key Kg at the subscriber identity module;

deriving a broadcast group encryption key Kb from the group encryption key Kg;

processing (716) at least a portion of the content of the modified AMF and instructing the mobile station that the AMF is standardised and may be interpreted,;

wherein the processed content of the modified AMF comprises an instruction to the subscriber identity module to retain the CK and the stored group encryption key on the subscriber identity module in confidence;

and provide only the broadcast encryption key to the mobile station".

## Reasons for the Decision

1. *Request for postponement of oral proceedings*

1.1 By a submission received at the EPO on the evening of 25 November 2020, the appellant made a request under Article 15(2) RPBA 2020 for postponement of the oral proceedings scheduled for 1 December 2020. The board thus became aware of the request only the next day, i.e. three working days before the oral proceedings. The appellant, who is based in Ireland, cited as a serious reason the travel restrictions in place caused by the ongoing Covid-19 pandemic and the fact that Ireland was considered to be a risk area by the Robert Koch Institute.

1.2 By a communication sent to the appellant in advance by email dated 27 November 2020, the Board informed the appellant why it was not in a position to accede to this request. The communication included the following text (including original emphasis):

> *"The board is not in a position to accede to the appellant's request for a change of the date fixed for oral proceedings, for the following reasons:*

*Pursuant to **Article 15(2)(a) RPBA 2020**, such a "request shall be filed as soon as possible after the summons to oral proceedings has been notified and the serious reasons in question have arisen". If the requirements under this provision are not met, the board may reject the request for this reason alone (see explanatory remarks to the RPBA 2020).*

*In the present case, following the cancellation of the first summons to oral proceedings, the board's second summons to oral proceedings was dispatched on **5 June 2020**. The serious reasons relating to the Covid-19 travel restrictions and Ireland being considered an international risk area by the Robert Koch Institut in Germany have arisen at least since **the end of October 2020**. Parties are expected to consult the publicly available list of international risk areas by the Robert Koch Institut, in order to determine and inform the board in good time whether they will attend the arranged oral proceedings.*

*Nevertheless, the request to change the date fixed for oral proceedings was only submitted on **25 November 2020** (received on 26 November 2020). Either the appellant should have requested a postponement earlier, or arranged for an attorney to represent the case who is not subject to travel restrictions. By delaying the request and submitting it only shortly before the arranged oral proceeding [sic], the board has had to invest time in preparing the oral proceedings.*

*Given the difficulties and the administrative burden in finding a single date on which all three*

*members of the board and a hearing room are available in the next months, the only options to conclude these appeal proceedings in a timely manner, are to hold oral proceedings as scheduled on 1 December 2020, or to hold the oral proceedings by videoconference technology (based on Skype)* ***on the alternative date of 2 December 2020 at 9:00 hrs.***

*If the appellant does not give consent to oral proceedings via videoconference, the board intends to hold the oral proceedings as originally planned on 1 December 2020.*

*Therefore, the appellant is requested to inform the board* ***by 27 November, 15:00 hrs*** *whether they consent to hold oral proceedings via videoconference on the said date of 2 December 2020."*

1.3 The appellant responded by email on the afternoon of 27 November to the effect that they were sorry that the board had decided to refuse the request for postponement, but that they did not give consent to oral proceedings via videoconference on the proposed date of 2 December (which had been proposed by the board in view of the impossibility of arranging a video conference at such short notice to take place on 1 December). By another email received shortly after midnight on 1 December, the appellant made clear that they would not be attending the oral proceedings later that morning.

1.4 The appellant hence gave no explanation or justification for filing the request for postponement at such an unreasonably late stage, and did not

otherwise respond substantively to the board's reasons set out above. Consequently, the board had no reason to reconsider its position.

1.5 The request for postponement of the oral proceedings was therefore refused (Article 15(2)(a) RPBA 2020), and the board held oral proceedings in the absence of the appellant (Article 15(3) RPBA 2020).

*2. Right to be heard (Article 113(1) EPC)*

2.1 The board notes that the appellant, if they had so wished, could at any time have made written submissions in reply to the board's preliminary opinion sent on 12 December 2019, i.e. nearly one year before the oral proceedings took place. No substantive reply to any of the board's objections has however been made.

2.2 The board arranged oral proceedings at the appellant's request (Article 116(1) EPC). The subsequent non-attendance of the appellant in view of the Covid-19 situation was caused by the appellant's own failure to either request postponement as soon as possible, or to arrange for attendance by a representative not subject to Covid-19 travel restrictions. After the board announced that the oral proceedings would not be postponed for the reasons given above, the appellant did not provide any justification for the unreasonably late filing of the request for postponement, chose not to avail themselves of the possibility of oral proceedings by videoconference, and informed the board that they would not attend the oral proceedings either. They therefore have to be treated as relying on their written case (cf. Article 15(3) RPBA 2020).

2.3 The appellant's right to be heard pursuant to Article 113(1) EPC has therefore been respected. The board notes that the appellant has not argued otherwise.

*3. Technical context*

3.1 The present application concerns authentication in a UMTS network (although claim 1 of each claim request on file is not limited to UMTS). Essentially, a challenge-response protocol takes place between the network and the subscriber identity module (SIM) card of a user equipment. The "challenge" vector includes a "message authentication code" (MAC) and an "authentication management field" (AMF) supplied by an authentication centre (AuC) to the network.

3.2 As explained in the present application (cf. paragraphs [0017] and [0018] of the description of the application as published), the use of the AMF may be defined differently by each network operator. The aim underlying the application is to use the AMF in a standardised manner across all networks in order to communicate additional information to the SIM, e.g. instructions.

*4. Main request - claim 1 - added subject-matter (Articles 76(1) and 123(2) EPC)*

4.1 The standard test for compliance respectively with Articles 76(1) or 123(2) EPC ("gold standard") is that the application must not contain subject-matter which is not directly and unambiguously derivable from the parent application as filed or the divisional application as filed, taking account of matter which is

implicit based on the common general knowledge of the skilled person.

4.2 Claim 1 defines a method carried out at the subscriber identity module (SIM) which receives a "modified AMF". However, the features of claim 1 "receiving ... a message authentication code, MAC, generated using the modified AMF" and "assuming that the received MAC is a MAC generated using a modified AMF" have been extracted in isolation from the totality of the embodiment described in paragraphs [0048], [0050] and [0051] of the parent application as published and the divisional application as published (NB: references to the "description" in the following refer both to the parent application and the divisional application as published, as there is apparently no difference as regards the cited passages), leading to claim 1 defining an intermediate generalisation.

In this respect, the only explicit reference to "modifying" the AMF occurs in paragraph [0048] in connection with the AuC controlling whether a bootstrapping function or another network entity has the privilege to change the AMF and use it to exert control over the mobile station. The embodiment of paragraph [0051] relating to the receiver (cf. Fig. 7) discloses how modified values $AMF_0$ and $AMF^*$ are used to achieve this aim. However, this embodiment has far more steps than claim 1 of the main request.

4.3 In accordance with the case law of the Boards of Appeal, intermediate generalisations may be allowable only where there is no functional and/or structural relationship between the features of the claim and other features presented in the underlying description as part of the same embodiment. However, that is not

the case here, since there is a clear functional relationship linking all the steps of the embodiment of Figure 7 and paragraph [0051].

4.4 Consequently, claim 1 of the main request does not comply with either Article 76(1) or 123(2) EPC.

*5. Main request - claim 1 - clarity (Article 84 EPC)*

5.1 The term "authentication management field" is held to be unclear, since it is not considered to be a sufficiently well-defined term of the art. In this respect, although the term "AMF" arguably has a recognised meaning in the specific context of UMTS, claim 1 embraces other cellular communications networks than UMTS. Moreover, as set out in the description, there is no standardised use of the AMF (cf. paragraph [0013]), even in the context of UMTS.

5.2 Furthermore, the expression "modified authentication management field" lacks clarity as it is unclear what the reference basis is for such a "modified AMF" (cf. the comments of the examining division in the impugned decision, page 5, section II.i).1, lines 11-15).

5.3 On this latter point, the appellant argued in the statement of grounds of appeal that it was clear from claim 1 alone that the AMF was modified to contain instructions to the SIM and that "Prior art/regular AMFs do not contain instructions to the SIM".

However, the board notes that claim 1 embraces the case that the modified AMF is a modification of an AMF that is not a "prior art/regular" AMF, e.g. one which is itself a "modified" AMF. Furthermore, in the light of **D2**, page 61, a prior art/regular AMF apparently can

contain instructions to the SIM. Therefore, it is not inherent that "regular" AMFs do not contain instructions to the SIM.

5.4 The meaning of the term "assuming" in claim 1 is considered to be technically unclear since making an assumption seems rather to be a step of a cognitive nature, i.e. to be performed by a human being or belong to the field of artificial intelligence. Plausibly, however, the SIM does not actually make an assuming step, but simply, as a result of the failed comparison, computes a second MAC based on the modified AMF. It is further unclear why the claim refers here to "using a modified AMF" rather than using "the modified AMF".

5.5 Consequently, present claim 1 does not comply with Article 84 EPC.

*6. NEW first auxiliary request - claim 1*

The above points 4 and 5 with respect to claim 1 of the main request apply, *mutatis mutandis*, to claim 1 of the first auxiliary request, despite the attempted clarification of the term "modified AMF containing instructions to the SIM" to "modified AMF modified to contain instructions to the SIM". This amendment still does not make clear what the reference basis is for the "modified AMF".

*7. NEW second auxiliary request - claim 1*

7.1 Above points 4 and 5 apply, *mutatis mutandis*, to claim 1 of this auxiliary request.

7.2 The amendments with respect to claim 1 of the main request are essentially derived from paragraph [0047]

of the description concerning a "group" embodiment. This embodiment is now combined with the existing subject-matter taken from paragraphs [0050] and [0051] relating to a "modified" AMF. Paragraph [0047] on the one hand and paragraphs [0050] and [0051] on the other hand however concern different embodiments with no indication that they can be combined.

Consequently, present claim 1 is not directly and unambiguously based on either the parent application as filed or the divisional application as filed (Articles 76(1) and 123(2) EPC).

7.3 In addition, claim 1 is based on an intermediate generalisation in respect of the feature "deriving a broadcast group encryption key Kb from the group encryption key", since in paragraph [0047] this feature is presented as "deriving a broadcast encryption key Kb from the group encryption key Kg and some other data" (Articles 76(1) and 123(2) EPC).

7.4 The feature "instructing the mobile station that the AMF is standardised and may be interpreted" is of unclear scope (Article 84 EPC) and also taken out of its original context (cf. paragraph [0044] of the description) and combined with other embodiments, although neither the parent application as filed nor the divisional application as filed provide any support for such a combination (Articles 76(1) and 123(2) EPC).

*8. Conclusion*

As there is no allowable claim request, it follows that the appeal must be dismissed.

**Order**

**For these reasons it is decided that:**

The appeal is dismissed.

The Registrar: The Chair:

B. Brückner K. Bengi-Akyürek

Decision electronically authenticated