Internal distribution code:

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

Datasheet for the decision of 22 November 2017

Case Number: T 2145/12 - 3.5.03

Application Number: 02793731.7

Publication Number: 1530885

IPC: H04W8/22

Language of the proceedings: EN

Title of invention:
Robust and flexible digital rights management involving a tamper-resistant identity module

Patent Proprietor:
Telefonaktiebolaget LM Ericsson (publ)

Opponent:
Giesecke+Devrient Mobile Security GmbH

Headword:
Digital rights management/ERICSSON

Relevant legal provisions:
EPC Art. 123(2)
RPBA Art. 13(1)

Keyword:

Admissibility - new main request (no)
Added subject-matter - auxiliary requests I-V (yes)

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 2145/12 - 3.5.03

D E C I S I O N
of Technical Board of Appeal 3.5.03
of 22 November 2017

Appellant 2: (Patent Proprietor)	Telefonaktiebolaget LM Ericsson (publ) 164 83 Stockholm (SE)
Representative:	Röthinger, Rainer Wuesthoff & Wuesthoff Patentanwälte PartG mbB Schweigerstrasse 2 81541 München (DE)
Appellant 1: (Opponent)	Giesecke+Devrient Mobile Security GmbH Prinzregentenstraße 159 81677 München (DE)
Representative:	Klunker IP Patentanwälte PartG mbB Destouchesstraße 68 80796 München (DE)
Decision under appeal:	**Interlocutory decision of the Opposition Division of the European Patent Office posted on 7 August 2012 concerning maintenance of the European Patent No. 1530885 in amended form.**

Composition of the Board:

Chairman	F. van der Voort
Members:	A. Madenach
	P. Guntz

Summary of Facts and Submissions

I. The present appeals arise from the decision of the opposition division posted on 7 August 2012 concerning the maintenance of European patent No. 1 530 885 in amended form.

In the decision under appeal, the opposition division found that the first auxiliary request as filed during the oral proceedings (which was based on a previous third auxiliary request filed on 12 June 2012) to meet the requirements of the EPC. More specifically, the opposition division held that the subject-matter of claim 1 of this request involved an inventive step (Article 56 EPC).

With respect to the main request, the opposition division came to the conclusion that claim 1 met the requirement of Article 123(2) EPC and that its subject-matter was new but lacked an inventive step (Article 52(1), 54 and 56 EPC).

II. A first notice of appeal against this decision was filed by the opponent (appellant 1). Appellant 1 requested that the decision be set aside and that the patent be revoked in its entirety. As an auxiliary measure, oral proceedings were requested.

III. A further notice of appeal against this decision was filed by the patent proprietor (appellant 2). It requested that the decision be set aside and that the patent be maintained on the basis of the claims of the main request underlying the interlocutory decision. Oral proceedings were requested as an auxiliary measure.

With its reply dated 13 May 2013 to the appeal of appellant 1, appellant 2 confirmed its previous request (the claims of the main request having been resubmitted) and submitted claims of auxiliary requests I to V, the claims of auxiliary request II corresponding to those of the first auxiliary request which the opposition division found to meet the requirements of the EPC.

IV. In a communication pursuant to Article 15(1) RPBA accompanying a summons to oral proceedings, the board gave its preliminary opinion and indicated topics for discussion during the scheduled oral proceedings, including *inter alia* the question of whether or not the feature "means for performing at least part of an authentication and key agreement procedure with the network thereby producing security information" was originally disclosed.

V. With a letter dated 20 October 2017, appellant 1 requested a transfer of opponent status. With a further letter of the same date, appellant 1 confirmed its previous requests and submitted further arguments.

VI. With a letter dated 23 October 2017, appellant 2 requested that the patent be maintained as granted (main request) or, in the alternative, that the patent be maintained on the basis of any one of main requests A, B and C as submitted with this letter or on the basis of auxiliary requests I to V, auxiliary requests I and II having been submitted with this letter, the new auxiliary request I being identical to the previous auxiliary request II, and auxiliary requests III to V having been submitted with a letter dated 13 May 2013.

VII. During the oral proceedings before the board, appellant 2 (patent proprietor) requested that the decision under appeal be set aside and that the patent be maintained in amended form on the basis of the main request as filed during the oral proceedings at 12.45 hrs or, in the alternative, on the basis of one of auxiliary requests I and II, as filed with the letter dated 23 October 2017, and auxiliary requests III to V, as filed with the letter dated 13 May 2013. All other requests were withdrawn.

Appellant 1 (opponent) requested that the decision under appeal be set aside and the patent be revoked in its entirety.

After deliberation, the chairman announced the board's decision.

VIII. Claim 1 of the main request reads as follows:

"A tamper-resistant identity module (120) adapted for physical engagement with a client system (100) having means (110) for receiving digital content over a network managed by a network operator and a digital-content usage device (130), said tamper resistant identity module having means for performing at least part of an authentication and key agreement procedure with the network thereby generating security information, characterized by a DRM agent (125) for enabling usage of said digital content, said DRM agent (125) including means for performing DRM processing based on said security information from the authentication and key agreement procedure, wherein said security information is a session key (t) for extracting a content protection key."

Claim 1 of auxiliary request I reads as follows:

"A tamper-resistant identity module (120) adapted for physical engagement with a client system (100) having means (110) for receiving digital content over a network and a digital-content usage device (130), said tamper resistant identity module having means for performing at least part of an authentication and key agreement procedure with the network thereby producing security information, characterized by a DRM agent (125) for enabling usage of said digital content, said DRM agent (125) including means for performing DRM processing based on said security information from the authentication and key agreement procedure, wherein said DRM agent (125) is implemented as an application in an application environment (124) of said tamper-resistant identity module (120)."

Compared with claim 1 of auxiliary request I, claim 1 of auxiliary request II includes the following additional feature:

"and wherein the DRM agent (125) is configured to manage usage rules pertaining to usage of streamed or downloaded digital content, wherein the usage includes one of forwarding, saving, copying, printing and modifying the digital content".

Claim 1 of auxiliary request III differs from claim 1 of auxiliary request I in that the last feature, i.e. "wherein said DRM agent (125) is implemented as an application in an application environment (124) of said tamper-resistant identity module (120)", has been replaced by the following feature:

"said security information comprises key agreement information for extracting a content protection key at an application level".

Compared with claim 1 of auxiliary request III, claim 1 of auxiliary request IV includes the following additional feature:

"and wherein the content protection key is further protected at a link layer by a further key".

Claim 1 of auxiliary request V differs from claim 1 of auxiliary request I in that the last feature, i.e. "wherein said DRM agent (125) is implemented as an application in an application environment (124) of said tamper-resistant identity module (120)", has been replaced by the following feature:

"wherein said DRM agent (125) comprises means for managing usage information related to usage of said digital content, said usage information serving as a basis for charging for digital-content usage, and wherein said DRM agent (125) further comprises: means for integrity protecting said usage information based on an identity-module specific key; and means for sending said integrity protected usage information to an external party managing charging of digital-content usage".

Reasons for the Decision

1. Main request: admissibility (Article 13(1) RPBA)

1.1 The main request was filed during the oral proceedings before the board. According to Article 13(1) RPBA, any amendment to a party's case after it has filed its

grounds of appeal or reply may be admitted and considered at the Board's discretion. Following the established case law, the board exercised its discretion by considering whether the request *prima facie* overcame at least the pending objections without giving rise to new objections and whether the amendments introduced new subject-matter that could not reasonably be dealt with by the Board and the other party during the oral proceedings.

1.2 In the present case, the objection which appellant 2 intended to overcome by the late filing of the present main request was that of added subject-matter (Article 123(2) EPC) relating, *inter alia*, to the following feature in claim 1 of the previous main request as resubmitted on 13 May 2013:

"means for performing at least part of an authentication and key agreement procedure with the network thereby producing security information".

1.3 Since the question of whether or not the first part of this feature (i.e. "means for performing at least part of an authentication and key agreement procedure with the network") can be directly and unambiguously derived from the application documents as filed, is not only relevant to the present request, but is also relevant for assessing whether or not claim 1 of each of the auxiliary requests I to V complies with Article 123(2) EPC (see below), the board's considerations in this respect are given here in detail.

1.4 The first part of the feature in question derives from original claim 5, the relevant part of which reads:

"means for performing at least part of an

authentication and key agreement (AKA) procedure".

The board notes that no reference is made to a network. The only reference to a network in this context can be found in a sentence on page 18, lines 7 and 8 of the application as published (which is identical to the application as filed), which reads:

"The AKA module 122 comprises algorithms for mutual authentication between client and network, and for deriving keys.".

The board understands this sentence such that, whereas the authentication part of the AKA procedure is with the network, it is silent on whether or not the key agreement, which the board understands to lead to the derivation of keys, is with the network. On the contrary, the fact that "and for deriving keys" is separated from the authentication with the network by a comma, is understood to indicate that the key agreement may be made with a further entity. It was not disputed between the parties that the AKA procedure, including the derivation of keys, is originally disclosed as being carried out with the network operator (see Figures 1, 4, 11 and 12). A key agreement with the network operator is, however, not the same as a key agreement with the network. The network comprises more entities than the network operator, e.g. the content provider, with which a key agreement would be possible. There is, however, no original disclosure for a key agreement with other network entities including the content provider. Instead, a key agreement has only been described with the network operator (e.g. Figures 1, 4, 11 and 12). Even if the network operator were to offer content, the key agreement would still be with the network operator (page 14, lines 8 to 10). The

board notes that any key agreement related to the content provider is based on a key agreement between the client and the network operator (page 38, lines 21 to 23, and page 39, lines 27 to 29).

It follows that the feature "means for performing at least part of an authentication and key agreement procedure with the network" cannot be directly and unambiguously derived from the application documents as filed.

1.5 Appellant 2 argued that, since the claim only required that at least **a part** of the AKA procedure is with the network and since there was undoubtedly an original disclosure of the authentication part of the AKA procedure to be with the network, there was a basis for this feature in the application as filed.

The board disagrees. The formulation "at least **a part** of the AKA procedure" also includes the possibility of performing the key agreement part of the AKA procedure with the network. For this, however, there is no original disclosure, as set out in point 1.4 above.

Appellant 2 further argued that a claim with a feature where the key agreement procedure is with the network operator would not be clear, since the network operator was not a technical entity. It further argued, that a tamper-resistant identity module at a client system could not be effectively limited by features that pertain to a remote entity, like a network operator.

These arguments are, however, purely hypothetical since a claim including this feature has not been submitted.

Appellant 2 further argued that the technical implementation with a network communication unit of the client (reference numeral 110 in Figure 2A), which communicates with the network on the one hand and with the AKA module (reference numeral 122 in Figure 2B) on the other hand, provided ample support for the feature "means for performing at least part of an authentication and key agreement procedure with the network".

This argument, however, does not address the fact that the written disclosure which relates to Figures 2A and 2B, i.e. page 18, lines 1 to 13, only states that the authentication occurs between the client and the network. The derivation of keys is not said to be with the network, see point 1.4 above.

1.6 For these reasons, the board concluded that the feature "means for performing at least part of an authentication and key agreement procedure with the network" constituted added subject-matter.

1.7 The objection of added subject-matter with respect to claim 1 of the main request resubmitted on 13 May 2013 is also not overcome by any of the amendments in claim 1 of the present main request. The above-cited feature is still present in claim 1 (see point VIII above) and the only amendment potentially relevant in this respect is that the "network" is now defined as a "network managed by a network operator". This amendment does not, however, change anything to the above reasoning (points 1.4 and 1.5), since there is neither an original disclosure for a key agreement procedure with a network in general nor with a network managed by a network operator in particular.

1.8 With respect to the objection that the second part of the feature in question, i.e. "producing security information", was not originally disclosed, the board notes appellant 2's intention to overcome this objection by specifying that "said security information is a session key (t) for extracting a content protection key". This feature derives from page 21, lines 24 to 30, of the application as published. The board notes, however, that this passage, which relates to the generation of a session key, further involves a random challenge, a key "k" and/or a special DRM key "x" as input to cryptographic functions in the context of generating a session key "t" and an expected response. It thus appears, *prima facie*, that the feature relating to the security information being a session key, which does not refer to the further conditions recited in this passage, is an intermediate generalisation and as such gives rise to a further objection of added subject-matter.

1.9 Since the amendments introduced with claim 1 of the present main request as submitted during the oral proceedings in order to overcome a previously raised objection of added subject-matter did not, *prima facie*, overcome this objection and gave rise to further objections of added subject-matter (see points 1.7 and 1.8 above), the board, exercising its discretion under Article 13(1) RPBA, did not admit the main request to the appeal proceedings.

2. Auxiliary requests I to V: added subject-matter (Article 123(2) EPC)

2.1 Claim 1 of each of the auxiliary requests I to V also includes the feature "means for performing at least

part of an authentication and key agreement procedure with the network".

2.2 For the reasons set out above in points 1.4 and 1.5, the application as filed does not provide a basis for this feature.

2.3 Further, the board notes that claim 1 of each of the auxiliary requests I to V includes the features "thereby producing security information" and "performing DRM processing based on said security information". There is no literal support for these features in the application documents as originally filed. According to claim 5 as originally filed, DRM processing is "based on information from said AKA procedure". A similar wording is used on page 4, lines 16 to 19. In the board's view, the above-cited features of claim 1 are more specific than what is originally disclosed, since "security information" is more specific than "information" and the AKA procedure "producing information" is more specific than "information from" the AKA procedure.

The latter understanding is also supported by the description, page 4, lines 19 to 22, according to which authentication information can be used for charging purposes, and key agreement information can be used for extracting a content protection key. The board understands information for charging purposes to typically include a name and an account number. This information, however, is not produced by the AKA procedure, since it pre-exists before the AKA procedure is carried out. Hence, this information is at the most merely passed on by the AKA procedure. In the application as filed, information, which is "produced" by the AKA procedure and on which DRM processing is

based, is only a key (e.g. Figure 4, page 21, lines 26-30, and page 22, line 28, to page 23, line 2).

In this respect, it is noted that it was not disputed that in all embodiments of the originally disclosed module the AKA procedure produces a key which is sent to the DRM agent (e.g. Figure 4, page 21, lines 26 to 30, and page 22, line 28, to page 23, line 2). The AKA procedure produces further information, like e.g. the expected response (page 21, lines 26 to 30), which is, however, not sent to the DRM agent. Hence, security information produced by the AKA and on which DRM processing is based is only a key.

From the above, it follows that the features "security information" and "producing" have only originally been disclosed with the "security information" being a key. The omission of this technical limitation thus amounts to an unallowable intermediate generalisation.

2.4 The board notes that in claim 1 of auxiliary requests III and IV the "security information" is further characterised in that "said security information comprises key agreement information for extracting a content protection key at an application level". This further specification of "security information" can, however, not be understood as a limitation of the "security information" to "key agreement information" or a key, since due to the term "comprises", it is not excluded that the security information on which DRM processing is based includes further information.

2.5 Appellant 2 argued, that there was no substantive technical difference between the terms "security information" and "information".

The board disagrees. "Information" may include for example, name, account information, and price information, which cannot be considered to constitute security information. Hence, the term "information" is broader than the term "security information". The point raised by appellant 2 that replacing the originally disclosed term "information" by "security information" was merely a matter of clarification (Article 84 EPC) is irrelevant, since the requirements relating to amendments (Article 123(2) EPC) and to clarity (Article 84 EPC) are different requirements of the EPC, which need to be fulfilled independently.

Appellant 2 further argued that the AKA procedure is disclosed to produce security information different from a key in the form of an authentication response RES. Hence, there was an original basis for an intermediate term like the "security information" as used in claim 1 of each of the auxiliary requests I to V.

The board does not accept this argument, since the DRM processing is not based on the authentication response RES as part of the security information as required by claim 1 of each of the auxiliary requests I to V.

2.6 Since claim 1 of each of the auxiliary requests I to V requests includes subject-matter which extends beyond the content of the application as filed, none of these requests meets the requirement of Article 123(2) EPC.

3. Since none of the admitted requests is allowable, 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 Chairman:

G. Rauh F. van der Voort

Decision electronically authenticated