Internal distribution code:

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

Datasheet for the decision of 17 June 2021

Case Number: T 1944/17 - 3.4.03

Application Number: 02771817.0

Publication Number: 1423826

IPC: G07C9/00

Language of the proceedings: EN

Title of invention:
SECURITY SYSTEM

Patent Proprietor:
Ericsson Inc.

Opponent:
Schorr, Frank

Headword:

Relevant legal provisions:
EPC Art. 100(c)
RPBA 2020 Art. 13
EPC R. 103(1)(a)

Keyword:

Grounds for opposition - extension of subject-matter - main request and auxiliary requests 1-5 (yes)
Amendment to appeal case - auxiliary request 6 - not prima facie solving outstanding issues - not admitted
Reimbursement of appeal fee - no - appeal not allowable

Decisions cited:

Catchword:

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 1944/17 - 3.4.03

D E C I S I O N
of Technical Board of Appeal 3.4.03
of 17 June 2021

Appellant: (Patent Proprietor)	Ericsson Inc. 6300 Legacy Drive MS EVW 2-C-2 Plano, TX 75024 (US)
Representative:	Röthinger, Rainer Wuesthoff & Wuesthoff Patentanwälte PartG mbB Schweigerstrasse 2 81541 München (DE)
Respondent: (Opponent)	Schorr, Frank Erika-Mann-Strasse 9 80636 München (DE)
Representative:	Diehl & Partner Patent- und Rechtsanwaltskanzlei mbB Erika-Mann-Straße 9 80636 München (DE)
Decision under appeal:	**Decision of the Opposition Division of the European Patent Office posted on 29 June 2017 revoking European patent No. 1423826 pursuant to Article 101(3)(b) EPC.**

Composition of the Board:

Chairman	G. Eliasson
Members:	M. Papastefanou
	A. Bacchin

Summary of Facts and Submissions

I. The appeal of the patentee is against the decision of the opposition division revoking the European patent No. 1 423 826.

The opposition was based on all grounds of opposition under Article 100(a), (b) and (c) EPC 1973. In the impugned decision, the opposition division held that both the Main Request and the Auxiliary Requests 1 to 5 before it contained added subject-matter against the requirements of Article 123(2) EPC (in relation to Article 100(c) EPC).

II. The appellant-patentee ("patentee") requested that the decision under appeal be set aside and that the patent be maintained as granted (Main Request) or on the basis of one of Auxiliary Requests 1 to 6. Auxiliary Requests 1 to 5 were filed with the statement of the grounds of appeal and correspond to the respective auxiliary requests underlying the decision under appeal (see point 3 of the statement of the grounds of appeal). Auxiliary Request 6 was filed during the oral proceedings before the board.

The patentee further requested that the appeal fee be reimbursed under Rule 103(1)(a) EPC because of a substantive procedural violation allegedly committed by the opposition division (*ibid.*, point 5).

III. The respondent-opponent ("opponent") requested that the appeal be dismissed. The opponent requested also that the case be remitted to the opposition division in case the board considered that the opposition ground under Article 100(c) EPC did not prejudice the maintenance of

the patent as granted.

IV. Claim 1 of the Main Request (patent as granted) is worded as follows (the numbering of features is added by the board and corresponds to the numbering used during the opposition procedure):

A method of enabling or activating a protected function, the method comprising:
[1.1] *storing a plurality of authorization codes and associated time indications in a wireless communication device (100),* **[1.2]** *wherein the authorization codes and the associated time indications are received at the wireless communication device from a central controller (40),* **[1.3]** *each time indication indicating a time period for the corresponding authorization code during which the authorization code is valid;*
[1.4] *computing authorization codes for different time periods using a stored master code at an access control device;*
[1.5] *transmitting an access request from the wireless communication device to the access control device (20);*
[1.6] *receiving the access request from the wireless communication device at the access control device;*
[1.7] *transmitting an authentication challenge from the access control device to the wireless communication device in response to the access request;*
[1.8] *receiving the authentication challenge from the access control device at the wireless communication device in response to the access request;*
[1.9] *computing an authentication response based on the authentication challenge and the appropriate authorization code for the current time period; and*
[1.10] *transmitting the authentication response from the wireless communication device to the access control device;*

[1.11] *receiving the authentication response based on the authentication challenge and the authorization code for the current time period;*
[1.12] *computing an expected authentication response based on the authentication challenge and the appropriate authorization code for the current time period;*
[1.13] *comparing the received authentication response with the expected authentication response; and*
[1.14] *generating a control signal to permit access to the protected function if the received authentication response matches the expected authentication response.*

V. Claim 1 of **Auxiliary Request 1** has the same wording as claim 1 of the Main Request whereby feature [1.4] is amended as follows (additions underlined by the board):

"computing authorization codes for different time periods using a stored master code at an access control device and storing the computed authorization codes in the access control device, wherein storing the computed authorization codes in the access control device comprises storing a plurality of authorization codes in the access control device, each authorization code being valid for a defined time period;".

VI. Claim 1 of **Auxiliary Request 2** has the same wording as claim 1 of the Main Request with the addition, in features [1.9] and [1.12] that the computing of the authentication response and the expected authentication response is done using *a non-reversible function*.

VII. Claim 1 of **Auxiliary Request 3** has the same wording as claim 1 of the Main Request whereby feature [1.4] is amended as follows (additions underlined by the board):

"computing authorization codes for different time periods using a stored master code at an access control device and a time indication supplied either by the central controller or by a clock (26) internal to the access control device;"

VIII. Claim 1 of **Auxiliary Request 4** has the same wording as claim 1 of the Main Request whereby claim [1.12] is amended as follows (additions underlined by the board):

"computing an expected authentication response based on selected portions of the authentication challenge and the appropriate authorization code for the current time period;".

IX. Claim 1 of **Auxiliary Request 5** has the same wording as claim 1 of the Main Request whereby feature [1.4] is amended as follows (additions underlined by the board):

"computing authorization codes for different time periods using a stored master code at an access control device (20) without communication between the access control device (20) and the central controller (40);".

In addition, the "and" at the end of feature [1.9] has been deleted.

X. Claim 1 of **Auxiliary Request 6** has the following wording:

A system for enabling or activating a protected function, the system comprising a wireless communication device (100) including:
memory storing a plurality of authorization codes and associated time indications in the wireless communication device (100), wherein the authorization

codes and the associated time indications are received at the wireless communication device from a central controller (40), each time indication indicating a time period for the corresponding authorization code during which the authorization code is valid;
a wireless transmitter adapted to transmit an access request and an authentication response to an access control device (20);
a wireless receiver adapted to receive an authentication challenge from the access control device responsive to the access request;
a processor adapted to compute an authentication response based on the authentication challenge and the appropriate authorization code for the current time period,
the wireless transmitted further adapted to transmit the authentication response from the wireless communication device to the access control device,
the system further comprising an access control device (20) to secure a protected function, the access control device including:
a wireless transceiver to communicate with the wireless communication device;
a processor programmed to:
compute authorization codes for different time periods using a stored master code at the access control device;
receive the access request from the wireless communication device at the access control device;
transmit the authentication challenge from the access control device to the wireless communication device in response to the access request;
receive te authentication response based on the authentication challenge and the authentication code for the current time period;
compute an expected authentication response based

on the authentication challenge and the appropriate authorization code for the current time period; compare the received authentication response with the expected authentication response; and generate a control signal to permit access to the protected function if the expected authentication response matches the received authentication response.

XI. The parties' arguments, as far as they are relevant for this decision, can be summarised as follows:

On added subject-matter

The **patentee** argued mainly that the passage in the paragraph bridging pages 2 and 3 of the originally filed application provided the necessary support for the claims. Moreover, feature [1.4] of claim 1 should be understood as indicating that the access control device computed multiple authorization codes over a period of time and not as a batch. Thus, in the patentee's opinion, whereas this may constitute an issue of clarity of the claim, it does not amount to added subject-matter.

According to the **opponent**, the combination of features [1.4] and [1.12] of claim 1 was not disclosed or suggested in the originally filed application. The skilled person would understand feature [1.4] to indicate that the access control device computed several authorization codes at once, and this was not part of the second embodiment of the method, which corresponded to the one of the claims.

On the admittance of Auxiliary Request 6

According to the **patentee**, the board had provided a new approach in the assessment of added subject-matter in its preliminary opinion and this constituted exceptional circumstances. Claim 1 of Auxiliary Request 6 defined a system and solved thus all the issues of lack of support the board had identified with respect to the other requests. The request should be admitted into the proceedings.

According to the **opponent**, the change of claim category was only a formal amendment, which did not modify the substance of the claimed subject-matter. The problems of added subject-matter identified with respect to the other requests persisted and the request should not be admitted.

The parties' arguments are dealt with in detail in the reasons for the decision.

Reasons for the Decision

1. The appeal is admissible.

2. The patent

2.1 The invention relates generally to security methods and systems providing security for a protected function, and in particular to such methods (and systems) that use a challenge-response protocol to control access to a protected function.

2.2 As an example the patent describes the claimed invention with respect to a hotel room door. The door is locked by an electronic door lock (access control

device). A user, who wants to enter the room, has a portable token, like a smart card (wireless communication device).

2.3 When a user checks in at the hotel, a central computer system of the hotel (central controller) generates a series of authorization codes, each associated to a specific time period (for which the code is valid) and stores them at the user's smart card.

The electronic door lock of the room is also provided with these authorization codes and the associated time periods. The authorization codes can be transmitted from the central server or can be generated locally, at the electronic door lock using a secret (master) code.

2.4 The user stands in front of the door they wish to open. The smart card sends an access request to the electronic door lock. The electronic door lock generates an authentication challenge and transmits it to the smart card. The smart card generates an authentication response based on the received challenge and the appropriate authorization code for the specific time period (stored in the smart card) and transmits it back to the electronic door lock.

2.5 The electronic door lock computes an expected authorization response based on the authorization challenge and the appropriate authorization code(stored in its memory) and compares it to the received authorization response. If they match, then the door is unlocked (see paragraphs [0011] and [0012] of the patent specification).

3. Added subject matter (Articles 100(c) EPC 1973 and 123(2) EPC)

The following points relate both to the Main Request and to the Auxiliary Requests 1 to 5, since they all comprise the features identified below, even if in slightly different wording, (see also points 17 and 18 of the decision under appeal). The patentee agreed with this approach (see last paragraph on the first page of patentee's letter of 17 May 2021).

3.1 The main contested point, which was also the ground for the revocation of the patent, relates to the following features of claim 1 (see point IV above):

computing authorization codes for different time periods using a stored master code at an access control device; (feature [1.4])
and
computing an expected authentication response based on the authentication challenge and the appropriate authorization code for the current time period; (feature [1.12]).

3.2 The application as originally filed describes two embodiments of the claimed invention. These embodiments have several features in common, but there is a clear distinction between them. In the first embodiment, the access control device is connected to a central controller and receives the authorization codes from this central controller. In the second embodiment, the access control device is a stand-alone device (i.e. with no connection to a central controller) and computes the authorization codes itself, using a master code stored in it. This distinction is made in the original application almost from the beginning (see

paragraph bridging pages 2 and 3 of the application as published).

3.3 Claim 1 of the patent (Main Request) defines a method. The features of the claim are thus to be understood as a series of operations (steps) carried out by the corresponding technical means.

3.3.1 According to claim 1, several authorization codes for different time periods are computed using a master code at an access control device (feature [1.4]). In the context of the claimed method, this feature indicates that during an initial phase of the execution of the method, before the challenge-response authentication phase takes place, a number of authorization codes are computed (generated), one for each specific time period, at the access control device.

During the subsequent challenge-response authentication phase, the expected authentication response is computed on the basis of the authentication challenge and the appropriate authorization code for the current time period (feature [1.12]). In the board's understanding, the *"appropriate authorization code for the current time period*" is selected from among the several authorization codes, which were computed (generated) at the access control device during an earlier execution phase of the method (feature [1.4]).

3.3.2 In this context, the patentee argued that claim 1 does not specify any chronological order in which the defined method steps have to be executed. According to the patentee, there was no "initial phase" of the method in which the authorization codes were computed, since this action could happen at any time during the execution of the method, even during the challenge-

response authentication process (see point 1.1 of the patentee's letter of 17 May 2021).

The board agrees with the patentee that the method steps do no have to be executed in the order they appear in the claim. It is evident, however, that when the "appropriate authorization code for the current time period" is selected, this authorization code has to have been computed before (i.e. at an earlier phase of the method). The patentee acknowledges this, as well (see last paragraph of point 1.1 of patentee's letter of 17 May 2021). In other words, it is common ground that the step of feature [1.4] must be executed before the step of feature [1.12].

3.4 The main question is whether the application as originally filed supports such a combination of method steps, or, in other words, whether the skilled person can directly and unambiguously derive from the originally filed application that the access control device computes (generates) at the same time several (more than one) authorization codes for different time periods.

3.4.1 In the board's opinion, the originally filed application does not support the claimed combination of features.

The only passage of the original description that describes the combination of the method steps related to the generation of authorization codes is on page 9, lines 3 to 24 (see application as published). The second part of page 9 (starting at line 15) relates to the second embodiment of the claimed invention, which is also the claimed embodiment, and it describes clearly that the access control device computes an

authorization code (using a master code stored in the device) when it is needed, during the challenge-response authentication process. There is no indication of a computation (generation) of several (more than one) authorization codes before the challenge-response process starts or at another point during the execution of the method.

3.4.2 Original claims 15 to 20, referred to by the parties, do not support a different interpretation. Claim 15 defines a method of enabling or activating a protected function. The definition is general and covers both the identified embodiments of the method. Claims 16 and 17, which depend on claim 15 define that the access control device stores a plurality of authorization codes, but they provide no details as to where these codes may be computed. Claim 18, which depends directly on claim 15, and is thus unrelated to the features of claims 16 and 17, defines that the authorization code is computed on the basis of a combination of a secret (master) code and a time indication. Again, this definition is general and covers both embodiments. Claim 19, which depends on claim 18, defines that the computing of the authorization code is performed by the access control device. This definition relates to the second embodiment. Claim 20, which depends on claim 18 and is unrelated to the features of claim 19, defines that the computing of the authorization code is performed by a central controller in communication with said access device. This definition relates to the first embodiment of the method.

Summarizing, claims 15 and 18 (which depends directly on claim 15) provide general definitions that cover both embodiments. Claim 19 relates clearly to the second embodiment, while claim 20 relates to the first

one. Claims 16 and 17 do not provide any indication as to which of the two embodiments they may relate.

The board finds that it is not directly and unambiguously derivable from original claims 15 to 20 that the plurality of authorization codes of claim 17 are computed by the access control device, as defined in claim 19.

3.4.3 The passages of the original description referred to by the patentee, namely the paragraph bridging pages 2 and 3 (page 2, line 21 to page 3, line 3) and the paragraph bridging pages 4 and 5 (page 4, line 22 to page 5, line 4) describe the access control device. In the board's opinion, these passages describe the capabilities and the operation of the device, as far as they relate to the claimed invention. Hence, it is described that the access control device can either receive the authorization codes from a central controller or can compute the codes itself, so that no connection to a central controller is needed. The board considers these passages to describe certain capabilities of the device but not specific operation steps of a method like the one in claim 1 of the patent. Moreover, and more importantly, these passages describe only the how the device computes or receives the authorization codes and do not disclose or suggest the combination of all the features of the method in claim 1.

3.5 The patentee argued that the board's interpretation of claim 1 and in particular of feature [1.4] was unjustifiably narrow. In the same way as in the passage of the paragraph bridging pages 2 and 3, the use of the plural ("computing authorization code**s**", emphasis added) in feature [1.4] indicated that the access control device was capable of computing all the

authorization codes it needed (in contrast to receiving them from the central controller). This was in line with the board's interpretation of the passage bridging pages 2 and 3, which was held to describe the capabilities of the device (see also point 3.4.3 above). Feature [1.4] was thus not to be understood as a single step of the method during which a batch of authorization codes were computed at the same time but rather as an indication that the access control device would compute multiple authorization codes (for multiple time periods) over a period of time.

Regarding the passage on page 9, the patentee pointed to the use of "may" (the access control device "may generate a new authorization code at a specific check-out time") and indicated that this text merely suggested an option for the implementation of the method, in which authorization codes were computed singly in real time each time a new time period is entered. The skilled person would understand from this passage that a series (multiple) authorization codes will be generated at the door lock (access control device) for a series of check-out times. This interpretation was in line with the general teachings of pages 2 and 3 of the originally filed application (see also page 5 of patentee's letter of 17 May 2021).

3.5.1 The board agrees with the patentee that there will be multiple authorization codes for multiple time periods (one code for each period). The question is, however, at which point in time these codes are computed.

According to the passage on page 9 of the originally filed application, *"[e]ach electronic door lock 20* (i.e. access control device) *may generate a new authorization code at a specified check-out time..."*

(page 9, lines 18 and 19). The board finds that this passage describes clearly when a new authorization code is computed (at a specified check-out time) and not that there is an authorization code for each specified check-out time. According to this passage, a single authorization code is computed at each check-out time.

The use of the verb "may" could indicate that this step is optional, but the application does not describe any other way of carrying out the method according to the second embodiment. The skilled person would not speculate about other possible implementations of the claimed method, when there is one described in the application. As previously explained, the board considers this passage to be the only original disclosure of the method according to the second embodiment (and claim 1).

3.5.2 Regarding the interpretation of feature [1.4] put forward by the patentee, the board considers that it is not supported by the claim as a whole.

Claim 1 of the Main Request defines a method of enabling or activating a protected function. The board understands that the features of the claim define a series of steps that have to be executed in the context of the claimed method. Although there is some freedom as to the order in which the defined steps are to be executed, the skilled person would understand that every time the method is to be run all the defined steps would have to be executed, especially since there is no indication that any of them is regarded as optional. If the patentee's interpretation were to be followed, then some of the method steps, at least the one in feature [1.4], would have to be understood outside of the context of the execution of the method

(e.g. the access control device computes several authorization codes over a period of time), while other steps of the method are to be executed in a specific order, and within a relative short period of time (the challenge-response process of features [1.5] to [1.14]). The claim does not provide any indication about such an understanding of the defined method and the board considers that the skilled person would not understand these features differently. Therefore, the patentee's interpretation of feature [1.4] cannot be followed.

3.6 The board's conclusion is, hence, that the subject-matter of claim 1 of the Main Request contains subject-matter going beyond the originally filed content of the application, contrary to the requirements of Article 123(2) EPC. The same applies, for the same reasons, to the subject-matter of claim 1 of Auxiliary Requests 1 to 5, which are found, thus, not to meet the requirements of Article 123(2) EPC, either.

The opposition ground according to Article 100(c) EPC 1973, prejudices, therefore, the maintenance of the patent as granted (Main Request) or on the basis of any one of Auxiliary Requests 1 to 5.

4. Auxiliary Request 6 - Admittance

4.1 Auxiliary Request 6 was filed during the oral proceedings before the board. It is an amendment of the appellant's case and its admittance into the proceedings is subject to the board's discretion according to Article 13(2) Rules of Procedure of the Boards of Appeal (RPBA 2020).

4.2 The patentee argued that it was the board in its preliminary opinion expressed in the communication under Article 15(1) RPBA 2020 that had made "a clear distinction" between method claims and system (device) claims for the first time, by arguing that the passages of the originally filed application referring to the access control device did not provide support for the steps of the claimed method. Such a distinction had never been made up to that point and it constituted, therefore, exceptional circumstances in the sense of Article 13(2) RPBA 2020.

The new request consisted of a single system claim, which corresponded to claim 9 of the Main Request. It did not represent new subject-matter and the board could, thus, deal with it without any undue burden. Moreover, it solved the problem of added subject-matter, since the passage in the paragraph bridging pages 2 and 3 of the originally filed application provided the necessary support. The request should, thus, be admitted into the proceedings.

4.3 According to the opponent, Auxiliary Request 6 presented a formal change of claim category and could be regarded as a reaction to the board's communication in preparation of the oral proceedings. However it did not overcome the problem of added subject-matter, since it contained the same features as the method claims of the previous requests. It was not *prima facie* allowable and, therefore should not be admitted into the proceedings.

4.4 The board acknowledges that its approach to the question of added subject-matter expressed for the first time in the communication under Article 15(1) RPBA 2020 was not exactly the same as the one of the

opposition division and accepts that this constitutes exceptional circumstances within the meaning of Article 13(2) RPBA 2020.

4.5 Nevertheless in such cases it is still within the board's discretion to admit the request into the proceedings. In particular in the exercise of the discretion under Article 13(2) RPBA 2020 the board may also take into consideration the criteria of Article 13(1) RPBA 2020 (see the Explanatory remarks on Article 13(2) in Document CA/3/19, section VI). One of the criteria used in the exercise of the board's discretion is whether the submitted amendments *prima facie* overcome the outstanding issues.

4.6 In the present case claim 1 of Auxiliary Request 6 defines a system by the functions of its various parts. These functions correspond to the steps of the method claimed in the previous requests.

4.7 The passage in the paragraph bridging pages 2 and 3 (and that of the paragraph bridging pages 4 and 5) states only that the access control device receives the authorization codes from the central controller or computes them locally, but does not provide any indication about the remaining features of the access control device or the system as a whole. As already explained (see point 3.5.1 above), the only passage in the originally filed application describing the combination of features constituting the method of the previous requests and also the functional features of the system of claim 1 of Auxiliary Request 6 is on page 9 of the originally filed application.

4.8 As explained previously, the board is of the opinion that the passage on page 9 of the original application

does not provide sufficient support for those method steps (see point 3 above). The same applies, hence, for the same reasons for the features of the system of claim 1 of Auxiliary Request.

4.9 Since Claim 1 of Auxiliary Request 6 does not prima facie overcome the objection under Article 123(2) EPC, the board, exercising its discretion under Article 13 RPBA 2020, decides not to admit it in the appeal proceedings.

5. Since none of the admitted request is allowable, the appeal must be dismissed.

6. Reimbursement of the appeal fee

6.1 The appellant requested the reimbursement of the appeal fee because of a purported substantial procedural violation committed by the opposition division (see point VII of the statement of grounds of the appeal).

6.2 Under Rule 103(1)(a) EPC a prerequisite for the board ordering the reimbursement of the appeal fee is that the board deems the appeal to be allowable.

6.3 Since the board does not deem the present appeal to be allowable, it cannot order the reimbursement of the appeal fee. The appellant's request has to be rejected at least for this reason.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

S. Sánchez Chiquero G. Eliasson

Decision electronically authenticated