Internal distribution code:

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

Datasheet for the decision of 21 January 2015

Case Number:	T 0840/11 - 3.5.03
Application Number:	04012304.4
Publication Number:	1455503
IPC:	H04L29/06
Language of the proceedings:	EN

Title of invention:
Data certification method and apparatus

Patent Proprietor:
Cryptomathic A/S

Opponent:
DanID A/S

Headword:
Data certification/CRYPTOMATHIC

Relevant legal provisions:
EPC Art. 83, 108
EPC R. 99(2), 101(1)
RPBA Art. 13(1), 12(4)

Keyword:
Admissibility of appeal - (yes)
Sufficiency of disclosure - (no)
Admissibility of requests filed before oral proceedings - (yes)
Admissibility of requests filed during oral proceedings - (no)

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

Decisions cited:
T 0144/09, T 2532/11

Catchword:

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

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 0840/11 - 3.5.03

DECISION
# of Technical Board of Appeal 3.5.03
of 21 January 2015

Appellant:
(Patent Proprietor)

Cryptomathic A/S
Jaegergardsgade 118
8000 Aarhus (DK)

Representative:

Martin, Philip John
Marks & Clerk LLP
62-68 Hills Road
Cambridge
CB2 1LA (GB)

Respondent:
(Opponent)

DanID A/S
Lautrupbjerg 10
2750 Ballerup (DK)

Representative:

Inspicos A/S
Kogle Allé 2
P.O. Box 45
2970 Hørsholm (DK)

Decision under appeal:

Decision of the Opposition Division of the European Patent Office posted on 1 March 2011 revoking European patent No. 1455503 pursuant to Article 101(3)(b) EPC.

Composition of the Board:

Chairman F. van der Voort
Members: A. Madenach
R. Cramer

Summary of Facts and Submissions

I. The present appeal arises from the decision of the opposition division posted on 1 March 2011 revoking European patent No. 1 455 503.

II. The opposition was based on the grounds of Article 100(a) EPC in conjunction with Article 52(1), (2)(c) and (3), Article 54 EPC and Article 56 EPC, Article 100(b) EPC in conjunction with Article 83 EPC, and Article 100(c) in conjunction with Articles 123(2) and 76(1) EPC.

The opposition division came *inter alia* to the conclusion that the subject-matter of the claims as granted was disclosed in a manner sufficiently clear for it to be carried out by a person skilled in the art (Article 83 EPC), but that the independent claims as granted did not meet the requirements of Articles 100(c) and 123(2) EPC. Further, it held that the independent claims of one auxiliary request contained subject-matter which extended beyond the content of the application as filed (Articles 100(c) and 123(2) EPC). A second auxiliary request was not admitted due to its late filing (Article 114(2) EPC).

III. Notice of appeal was filed against this decision by the patent proprietor (appellant), the appropriate fee was paid and a statement of grounds of appeal was subsequently filed. The appellant requested that the opposition division's decision be set aside and that the patent be maintained in amended form on the basis of claims of a main request or, in the alternative, on the basis of claims of one of first to fifth auxiliary requests, all filed with the statement of grounds of appeal. It further requested oral proceedings as an auxiliary measure.

IV. The respondent submitted a reply and requested that the appeal be dismissed or, in the alternative, that the case be remitted to the department of first instance. Oral proceedings were requested as an auxiliary measure.

V. In a communication accompanying a summons to oral proceedings the board gave its preliminary opinion.

VI. Referring to the summons, the appellant with a letter dated 22 December 2014 submitted amended claims of the main request and first to fifth auxiliary requests and further submitted claims of sixth to twelfth auxiliary requests. By letter of 16 January 2015, the appellant withdrew the main request and the first to fifth and eleventh auxiliary requests.

VII. The respondent, in its reply to the summons, further requested a different apportionment of costs in case the board decided to remit the case to the department of first instance.

VIII. During the oral proceedings before the board, the appellant submitted claims of a new main request and a further auxiliary request.

The appellant requested that the decision under appeal be set aside and that the patent be maintained in amended form on the basis of the claims of the main request, i.e. the amended new main request as filed during the oral proceedings, or, in the alternative, on the basis of the claims of one of six auxiliary requests, i.e. the sixth, seventh, eighth, ninth, tenth or twelfth auxiliary request, all as filed with the letter dated 22 December 2014, or on the basis of the claims of a further auxiliary request filed during the oral proceedings.

The respondent requested, *inter alia*, that the appeal be rejected as inadmissible (main request), that the appeal be dismissed on the ground that the appellant had not presented an admissible request (first auxiliary request) or that the appeal be dismissed on the ground that none of the requests met the requirements of Articles 83, 84, 76(1) and 123(2) EPC (second auxiliary request). In view of the board's decision it is not necessary to list the respondent's further requests.

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

IX. In view of the board's decision, claim 1 or its relevant features of the sixth to tenth and twelfth auxiliary request are quoted before claim 1 or its relevant features of the main and further auxiliary request.

X. Claim 1 of the sixth auxiliary request reads as follows:

"A method of certifying electronic data supplied by a user, the method comprising:

receiving the data to be certified at a signature server of a certifying apparatus from a source device, wherein the certifying apparatus further comprises an authentication server;

sending a request for user authentication to an authentication server via a secure tunnel (150) from tamper resistant hardware of said certifying apparatus to tamper resistant hardware of said authentication server, wherein the authentication server is separate to the signature server, and wherein said secure tunnel comprises an encrypted and authenticated communication link;

sending a user identification data request in the form of a challenge from the authentication server to said user;

receiving a response to the user identification data request from said user at said certifying apparatus, said response being a one-time password which is an encryption of said challenge with an individual key held on a secure token, wherein said secure token shares said individual key with said authentication server and wherein said secure token is possessed by said user;

receiving a derived version of said one-time password from said authentication server via the secure tunnel (150) at said certifying apparatus to validate said user;

validating the user by comparing the one-time password which is the response to the user identification data request with the derived version of said one-time password;

certifying the electronic data supplied by the user at the certifying apparatus with one or more elements of information secure to the certifying apparatus, said elements being unique to the user; and outputting the data so certified from the certifying apparatus, for passing to a recipient device;

wherein the elements of secure information certify that the supplier of the data is the user."

The respective claims 1 of the seventh to tenth and twelfth auxiliary requests contain the same validating step, i.e.:

"validating the user by comparing the one-time password which is the response to the user identification data request with the derived version of said one-time password;".

In view of this decision, it is not necessary to quote the remaining features of each of claims 1 of the seventh to tenth and twelfth auxiliary requests.

Claim 1 of the pending main request differs from claim 1 of the sixth auxiliary request in that the fifth to seventh paragraphs read as follows:

"receiving a response to the user identification data request from said user at said certifying apparatus, said response being an encryption of said challenge with an individual key held on a secure token, wherein said secure token shares said individual key with said authentication server and wherein said secure token is possessed by said user;

receiving a version of said individual key from said authentication server via a secure tunnel (150) at said certifying apparatus to validate said user;

validating the user by comparing the response to the user identification data request with the version of said individual key;".

Claim 1 of the further auxiliary request reads:

"A method of certifying electronic data supplied by a user, the method comprising:

receiving the data to be certified at a signature server from a workstation;

sending a request for user authentication to an authentication server via a secure tunnel (150) from tamper resistant hardware of said signature server to tamper resistant hardware of said authentication server, wherein the authentication server is separate to the signature server, and wherein said secure tunnel comprises an encrypted and authenticated communication link;

sending a user identification data request in the form of a challenge from the authentication server to said workstation;

receiving a response to the user identification data request from said workstation at said signature server, wherein said response is generated by the user keying said challenge on a secure token which is a device possessed by said user and which shares an individual key with said authentication server whereby said response is an encryption of said challenge with the key held on the secure token, wherein said response is keyed in at the workstation as the one-time password and said workstation sends a derived version of said one-time password;

receiving a derived version of said one-time password from said authentication server via the secure tunnel (150) at said signature server to validate said user, wherein the process used to derive the version of the password is the same in the authentication server and workstation;

validating the user by comparing the one-time password which is the response to the user identification data request with the derived version of said one-time password;

certifying the electronic data supplied by the user at the signature server with one or more elements of information secure to the signature server, said elements being unique to the user; and

outputting the data so certified from the signature server, for passing to a recipient device;

wherein the elements of secure information certify that the supplier of the data is the user."

Reasons for the Decision

1. Admissibility of the appeal (Article 108, Rules 99(2) and 101(1) EPC)

1.1 The respondent requested that the appeal be rejected as inadmissible, since the appellant's statement of grounds of appeal failed to meet the requirements set out in Rule 99(2) EPC. It indicated neither any reason for setting aside the opposition division's decision nor the extent to which it was to be amended. Instead, the appellant seemed to wholly accept the opposition division's decision and filed amended requests in response to it. The appellant had thus, according to the respondent, considered the opposition division's decision as an examination report which the appellant had accepted in its entirety and to which it had reacted by filing new requests. Hence, the appellant was attempting to use the appeal procedure as a continuation of the proceedings. Reference was made to T 2532/11 (reasons 2.2.2, 2.2.5 and 2.6.2).

1.2 The board notes that the patent was opposed *inter alia* on the ground of Article 100(c) EPC, i.e. that the subject-matter of claim 1 extended beyond the original disclosure (Article 123(2) EPC), with the argument that claim 1 as granted did not include a handheld secure token. With its communication annexed to the summons to oral proceedings, the opposition division expressed its doubts as to whether the challenge-response approach in the general way it was claimed was originally disclosed. In its response, the patent proprietor provided arguments and submitted an auxiliary request in an attempt to remove the doubts expressed by the opposition division. The filing of a second auxiliary request during the oral proceedings was not allowed by the opposition division (see point II above). With the statement of grounds of appeal, the appellant filed claims of a main request in which claim 1 specified a handheld secure token, and submitted extensive argumentation (over 5 pages) why some other features which the opposition division in its written decision considered as a necessary part of the challenge-response approach as originally disclosed did not need to be included in claim 1.

1.3 In the board's view, with the filing of the auxiliary request and the arguments in preparation for the oral proceedings before the opposition division in response to the communication annexed to the summons, the appellant made a *bona fide* effort to remove the opposition division's doubts. The subsequent filing of an appeal with new requests is understood as a response to the detailed reasons given in the opposition division's written decision. In the board's view, these requests and the arguments in their support could not be expected to have been filed in response to the rather unspecific statement of the opposition division in the communication annexed to the summons.

With respect to decision T 2532/11 cited by the respondent, the board notes that at point 2.3.3 of that decision it is held that "none of the main grounds for revocation of the patent presented in the impugned decision was addressed in the statement of grounds of appeal". This does not apply to the present case, since the statement of grounds of appeal contains a detailed discussion (cf. the section "Article 123(2) EPC - Added subject matter") of why the independent claims of the amended requests in the appellant's opinion overcome the objection of added subject-matter. Further, in T 2532/11 at point 2.4.2, it is stated that with respect to the question of whether or not newly filed requests can be seen as implicit grounds of appeal, the issue is "whether the grounds are understandable and <u>sufficiently linked</u> to the contested decision in order to form an admissible appeal" (original underlining). In the board's view, this requirement is met in the present case, considering the appellant's detailed analysis of the reasons given in the decision.

1.4 The board concludes that, since the appeal complies with Rule 99(2) EPC as well as the other requirements for an admissible appeal (which was not contested), the appeal is admissible.

2. *Admissibility of the sixth to tenth and twelfth auxiliary requests (Article 12(4) and 13(1) RPBA)*

2.1 Since the claims of the main request and the further auxiliary request were submitted after the claims of the sixth to tenth and twelfth auxiliary request and are based on the claims of the sixth and tenth auxiliary requests, respectively, the board deals with the sixth to tenth and twelfth auxiliary requests first.

2.2 The respondent requested that the board should exercise its discretion over the admission of new requests such that none of the appellant's requests filed with letter of 22 December 2014 was admitted into the appeal proceedings. Of these requests only the sixth to tenth and twelfth auxiliary requests are still pending (see points VI and VIII above).

The sixth to tenth and twelfth auxiliary requests were submitted about four weeks prior to the oral proceedings and therefore at a late stage of the procedure. The board thus has to consider whether these requests can be admitted pursuant to Article 13(1) RPBA.

Further, according to Article 12(4) RPBA, without prejudice to the power of the board to hold inadmissible facts, evidence or requests which could have been presented or were not admitted in the first-instance proceedings, everything presented by the parties with the statement of grounds of appeal is to be taken into account by the board if and to the extent it relates to the case under appeal. Following T 144/09 (reasons 1.17), this discretionary power also applies to amendments made to a party's case later on during the appeal procedure.

2.3 In exercising its discretion, the board will consider whether the sixth to tenth and twelfth requests bring an entirely fresh case or whether they constitute a legitimate reaction by the appellant to the reasons for the decision under appeal and the summons.

Claim 1 of the sixth auxiliary request differs from claim 1 of the main request on which the contested decision was based *inter alia* in amendments in the steps of receiving a response and of receiving a derived version. This is also true in comparison with claim 1 of the then auxiliary request.

In the decision under appeal, the opposition division held that the step of receiving a response could only be found in the embodiment described on page 14, lines 4 to 11, of the application as filed and that the skilled person would not be directly and unambiguously led by one specifically described embodiment to conclude that not all of the described features were indispensable for the functioning of the invention.

In the board's view, the sixth auxiliary request is a serious attempt to overcome this objection by introducing the feature "secure token" and further consequential amendments which are all based on the embodiment on page 14, lines 4 to 11, of the application as filed, rather than constituting an entirely fresh case.

2.4 Further, the independent claims of all these requests differ from the independent claims of the requests submitted with the statement of grounds of appeal, which had been withdrawn, in that the data to be certified is received at "a signature server of a certifying apparatus", in that "the certifying apparatus comprises an authentication server" and in that "the authentication server is separate to the signature server".

These amendments constitute a reaction to one of the objections addressed by the board in its summons. These amendments could easily be understood and were not complex in nature.

2.5 The above considerations equally apply to the seventh to tenth and twelfth auxiliary requests, since the independent claims of these requests include further detailed features, all relating to the challenge/ response method.

2.6 In view of the above, the board exercising its discretion under Article 13(1) RPBA admitted these requests into the appeal proceedings.

3. Sixth to tenth and twelfth auxiliary requests: sufficiency of disclosure (Article 83 EPC)

3.1 Claims 1 of the sixth to tenth and twelfth auxiliary requests comprise the feature of validating "the user by comparing the one-time password which is the response to the user identification data request with the derived version of said one-time password" (see point X above).

In paragraph [0066] of the patent in suit, a "derived version" is a hash value of the one-time password (column 11, lines 52 to 54). In column 12, lines 9 to 11, it is stated that, alternatively, another type of derived version can be sent to the signature server.

The derived version of the one-time password as understood in the above sense, on the one hand, and the one-time password itself, on the other hand, are different data. It is unclear how these different data can be compared in a meaningful way. This finding was not contested by the appellant.

3.2 The appellant rather argued that the term "derived" in the independent claims of the sixth to tenth and twelfth auxiliary requests had no specific meaning other than that at the authentication server the one-time password was "derived" from the challenge using the key. The appellant thus understood the validation step as being performed with two one-time passwords as such, one obtained from the workstation and the other obtained from the authentication server.

The board cannot find any support for such an interpretation in the patent in suit. All references to a derived version of data, in particular of a password, make it clear that the data, e.g. the password, is subjected to a treatment, in the specific examples a hashing, with the result that the derived version is different from the original version.

3.3 The opposition division referred in its decision to paragraph [0066] of the patent in suit and argued that the workstation used the same hashing algorithm as the authentication server when providing the response to the signature server.

This argument would in the board's view imply that the skilled person would interpret the one-time password, which is a response to the user identification data request, as a derived version of the password rather than the password itself. The interpretation of the one-time password as a derived version of the password is however not suggested by the wording of the claim. Further, there is no basis in the patent which would support such an interpretation. More specifically, in paragraph [0063] of the patent, which describes in detail the so-called challenge/response embodiment on which all auxiliary requests in question are based, it is stated that "the response which basically is an encryption of the challenge with the key held on the token 190, is keyed in at the workstation 101 as the one-time password. The signature server 110 may verify that the response is indeed an encryption of the challenge as it receives a derived version of the one time password from the authentication server 120" (column 10, lines 50 to 58). This passage therefore clearly states that the signature server receives the one-time password, which is identical to the response, from the workstation. There is no room for an interpretation that a deriving or hashing process is performed at the workstation.

The passage the opposition division referred to, i.e. paragraph [0066] of the patent in suit, is specifically directed to an alternative of the challenge/response embodiment, namely to an embodiment in which the workstation receives a one-time password directly from the authentication server via SMS (column 11, lines 48-50) instead of a user identification request in the form of a challenge. In that embodiment, the workstation does indeed perform hashing on the one-time password (column 12, lines 5-9). However, there is no indication that the same should apply to the challenge/ response embodiment.

3.4 The independent claims of the sixth to tenth and twelfth auxiliary requests comprise the feature of validating "the user by comparing the one-time password which is the response to the user identification data request with the derived version of said one-time password". Since for the above reasons the person skilled in the art would not be able to carry out the claimed comparison, the invention is not disclosed in a manner sufficiently clear and complete to be carried out by a person skilled in the art (Article 83 EPC). It follows that none of these requests is allowable.

4. Main request and further auxiliary request: admissibility (Article 13(1) RPBA)

4.1 A new main request and a further auxiliary request were submitted during the oral proceedings before the board. Their admissibility to the proceedings is subject to Article 13(1) RPBA. According to the established case law, one requirement for admitting late-filed requests during appeal proceedings is that they *prima facie* overcome the objections raised in connection with the previous requests.

4.2 In claim 1 of the pending main request, the validating step which gave rise to an objection under Article 83 EPC in respect of the sixth to tenth and twelfth auxiliary requests is amended to read "validating the user by comparing the response to the user identification data request with the version of said individual key" (see point X above).

Claim 1 further specifies that the certifying apparatus receives the version of the individual key from the authentication server and that it receives the response to the user identification data request from the user, in which the response is "an encryption of said challenge with an individual key held on a secure token, wherein said secure token shares said individual key with said authentication server".

Hence, the response is the result of an encryption process on a challenge using the individual key. It is therefore an entity different from the individual key, and hence it remains unclear how a meaningful comparison can be made between the response and the key.

4.3 Consequently, irrespective of any possible further objections, claim 1 of the pending main request does not *prima facie* overcome the objection under Article 83 EPC raised with respect to the sixth to tenth and twelfth auxiliary requests. The request is therefore not admitted.

4.4 According to claim 1 of the further auxiliary request (see point X above), a derived version of the one-time password is sent from the workstation. The claim does not, however, define to which entity this derived version of the one-time password is sent. Further, the validating step is identical to the validating step of claims 1 of the sixth to tenth and twelfth auxiliary requests, i.e. "validating the user by comparing the one-time password which is the response to the user identification data request with the derived version of said one-time password". Hence, there is a clear teaching that the one-time password is compared with a derived version, as is the case in claims 1 of the sixth to tenth and twelfth auxiliary requests. Therefore, the same objection under Article 83 EPC (see point 3 above) applies.

4.5 Hence, irrespective of any possible further objections, claim 1 of the further auxiliary request does not *prima facie* overcome the objection under Article 83 EPC raised with respect to the sixth to tenth and twelfth auxiliary requests. The further auxiliary request is therefore not admitted.

5. Since none of the appellant's admissible requests is allowable, the appeal is to be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

Beschwerdekammern des Europäischen Patentamts ✦ Boards of Appeal of the European Patent Office ✦ Chambres de recours de l'Office européen des brevets ✦

G. Rauh F. van der Voort

Decision electronically authenticated