Internal distribution code:

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

Datasheet for the decision of 18 October 2023

Case Number: T 1489/21 - 3.5.05

Application Number: 14730967.8

Publication Number: 3008852

IPC: H04L9/06, H04L9/32, G06F21/42, H04L29/06

Language of the proceedings: EN

Title of invention:
SYSTEM AND METHOD FOR ENCRYPTION

Patent Proprietor:
Cryptomathic Ltd

Opponent:
Nets Denmark A/S

Headword:
Signature request validation/CRYPTOMATHIC

Relevant legal provisions:
EPC Art. 54, 56, 83, 123(2)

Keyword:

Novelty - (yes)
Inventive step - (yes)
Sufficiency of disclosure - (yes)
Amendments - allowable (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 1489/21 - 3.5.05

D E C I S I O N
of Technical Board of Appeal 3.5.05
of 18 October 2023

Appellant: (Patent Proprietor)	Cryptomathic Ltd Richmond House 16-20 Regent Street Cambridge CB2 1DB (GB)
Representative:	Marks & Clerk LLP 15 Fetter Lane London EC4A 1BW (GB)
Appellant: (Opponent)	Nets Denmark A/S Lautrupbjerg 10 P.O. Box 500 2750 Ballerup (DK)
Representative:	Inspicos P/S Agern Allé 24 2970 Hørsholm (DK)
Decision under appeal:	**Interlocutory decision of the Opposition Division of the European Patent Office posted on 30 June 2021 concerning maintenance of the European Patent No. 3008852 in amended form.**

Composition of the Board:

Chair	A. Ritzka
Members:	P. Cretaine
	K. Kerber-Zubrzycka

Summary of Facts and Submissions

I. This appeal is against the opposition division's interlocutory decision, issued on 30 June 2021, to maintain European patent No. 3 008 852 in amended form according to claims 1 to 8 of auxiliary request 2a filed during the oral proceedings before the opposition division.

The opposition was based on the grounds of Article 100(a), (b) and (c) EPC. In the impugned interlocutory decision, the opposition division found that claim 1 as granted met the requirements of Articles 83 and 123(2) EPC but did not meet the requirements of Article 54 EPC over the disclosure of:

D1: US 2011/0213711.

The opposition division found that auxiliary requests 1, 1a and 1b, filed with letter of 25 February 2021, were not allowable for lack of novelty of their claim 1 over the disclosure of D1. The opposition division decided not to admit auxiliary request 1c, filed by letter of 22 April 2021, into the opposition proceedings. Further, the opposition division found that auxiliary request 2, filed by letter of 25 February 2021 was not allowable for lack of novelty of its independent claims 2 and 11 over the disclosure of D1.

The following document was also cited in the decision:

D8: WO 03/015370.

II. The opponent's notice of appeal was received on 9 September 2021 and the appeal fee was paid on the same day. In its statement dated 10 November 2021 setting out the grounds of appeal, the opponent requested that the decision be set aside and the patent revoked in its entirety on the grounds of Article 100(a), (b) and (c) EPC. In particular, an objection under Article 54 EPC was based on D1 and objections under Article 56 EPC were based on D1 and D8 as closest prior art. Further, the opponent objected that the patent as maintained in amended form did not meet the requirements of Articles 83 and 84 EPC. In the alternative, oral proceedings were requested.

III. The proprietor's notice of appeal was received on 10 September 2021 and the appeal fee was paid on the same day. In its statement dated 10 November 2021 setting out the grounds of appeal, the proprietor requested that the decision be set aside and the patent maintained on the basis of the main request (claims as granted) or on the basis of auxiliary requests 1, 1a, 1b, 1c, 2 or 2a, or on the basis of auxiliary requests 3 to 6 filed by letter of 25 February 2021. In the alternative, oral proceedings were requested.

IV. By letter dated 25 March 2022, the proprietor responded to the statement setting out the opponent's grounds of appeal and submitted further auxiliary requests 2b, 2c and 2d. The proprietor requested that the patent be maintained on the basis of the main request or auxiliary requests 1, 1a, 1b, 1c, 2, 2a, 2b, 2c and 3 to 6, in that order.

V. By letter dated 25 March 2022, the opponent responded to the statement setting out the proprietor's grounds of appeal and submitted a new document:

D9: Directive 1999/93/EC of the European Parliament.

The opponent requested that auxiliary requests 1c and 3 to 6 not be admitted into the appeal proceedings.

VI. A summons to oral proceedings was issued on 5 December 2022.

VII. By letter dated 6 December 2022, the opponent responded to the proprietor and requested that auxiliary requests 2b, 2c and 2d not be admitted into the appeal proceedings.

VIII. By letter dated 23 December 2022, the proprietor formally expressed its disagreement with the opponent in respect of auxiliary requests 2b, 2c and 2d.

IX. In a communication pursuant to Article 15(1) RPBA sent on 11 August 2023, the board indicated the points which would be discussed during the oral proceedings in respect of each of the main request and auxiliary requests 1, 1a, 1b, 1c, 2, 2a, 2b, 2c, 2d and 3 to 6. Further, the board expressed in particular the preliminary opinion that the main request met the requirements of Articles 123(2) and 83 EPC, that the subject-matter of claim 1 of the main request was novel over D1 (Article 54 EPC), and that auxiliary requests 1c, 2b, 2c, 2d and 3 to 6 should not be admitted into the appeal proceedings (Article 12 RPBA).

X. By letter dated 2 October 2023, the proprietor responded to the board's communication.

XI. By letter dated 4 October 2023, the opponent responded to the board's communication.

XII. Oral proceedings were held before the board on 18 October 2023 in the form of a video conference. The appellant (patent proprietor) requested that the decision under appeal be set aside and the patent be maintained as granted (main request) or in amended form based on one of auxiliary requests 1, 1a, 1b, 1c, 2, 2a, 2b, 2c, 2d or 3 to 6. The appellant (opponent) requested that the decision under appeal be set aside and that the patent be revoked. At the end of the oral proceedings, the board's decision was pronounced.

XIII. Claim 1 of the main request (claims as granted) reads as follows:

"A method of generating a signature on behalf of a user having a first and second user device, the method comprising
receiving a request from said first user device to create a signature for a first message M;
generating a validation challenge using a second message M' which is based on the first message M and a first secret shared with said user, wherein said validation challenge is generated by encrypting said second message M’ using said first shared secret;
sending said validation challenge to said user to enable said second user device to regenerate said second message M';
receiving a validation code from said second user device, said validation code confirming the request to create a signature and said validation code being generated following confirmation from the user that the second message M’ as displayed on the second user device corresponds to the first message M, wherein the second message M' displayed on the second user device

is generated by decrypting said validation challenge using said first shared secret; and
generating the signature for the user for the first message M."

The main request further comprises independent claims directed to a corresponding method of validating a signature request on the user side (claim 4) and a corresponding method of validating a signature request and generating the signature on a signature server (claim 7). The main request further comprises independent claims directed to an apparatus configured to perform the methods of claims 1, 4 and 7 (claims 9, 13, and 15 respectively). The main request also comprises an independent claim (claim 8) directed to a computer program carrier corresponding to any of the methods of claims 1, 4 and 7, and an independent claim (claim 15) directed to a system comprising the signature server, a user's initial transaction device, and a user's validation device.

Given the outcome of the appeal proceedings, there is no need to detail the claims of the auxiliary requests.

Reasons for the Decision

1. The following numbering of the features of claim 1 of the main request is used hereafter:

Feature 1A:
A method of generating a signature on behalf of a user having a first and second user device, the method comprising
Feature 1B:

receiving a request from said first user device to create a signature for a first message M;
Feature 1C: generating a validation challenge using a second message M'
Feature 1D: which is based on the first message M and a first secret shared with said user, wherein said validation challenge is generated by encrypting said second message M' using said first shared secret;
Feature 1E: sending said validation challenge to said user to enable said second user device to
Feature 1F: regenerate said second message M';
Feature 1G: receiving a validation code from said second user device, said validation code confirming the request to create a signature and said validation code being generated following confirmation from the user that the second message M' as displayed on the second user device corresponds to the first message M,
Feature 1H: wherein the second message M' displayed on the second user device is generated by decrypting said validation challenge using said first shared secret; and
Feature 1I: generating the signature for the user for the first message M.

2. Main request - Article 123(2) EPC

The opponent argued that feature 1G was not supported by the application documents as originally filed since it did not define that the validation code was user specific. According to the opponent, page 7, lines 23 to 25, page 9, lines 30 to 33, and page 17, lines 18 to 20 of the originally filed description described that the validation code must be created using information which was specific to the user, such as a second shared secret, and no other ways of generating the validation code were described anywhere in the description.

According to the opponent, the omission in claim 1 of the feature that the validation code was created using information which is specific to the user amounted to an inadmissible intermediate generalisation. The opponent further argued that claim 1 as originally filed could not be seen as a support for the omission of this feature since feature 1G of present claim 1 of the main request defined the generation of the validation code in more specific terms, namely by defining that the generation of the validation code was triggered by, or linked to, the confirmation from the user that the second message M' as displayed on the second user device corresponded to the first message M. Further, the opponent argued that, even if originally filed claims 9, 28 and 37 defined the notion of receiving confirmation that the second message M' as displayed corresponded to the first message M, these claims did not provide a basis for the causal link that the validation code was generated as a result of the user having confirmed that M' corresponded to M.

However, the board agrees with the proprietor that feature 1G is supported by the application documents as originally filed. In that respect, figure 1a, which is a flowchart of the steps performed by the devices to implement the invention (see page 12, lines 9 and 24) shows that the validation code is created by the validation device in step S118 following receipt by the validation device in step S116 of the acceptance of message M', as defined by feature 1G. Further, the sentence on page 14, lines 1 and 2, describes that step S116 of figure 1a represents approval by the user and step S118 generation of the validation code. The feature that the validation code must be created using information specific to the user is thus not present in the description of the invention according to figure

1a. Similarly, figures 2b and 2c show an implementation of the invention (see page 12, line 13) in which the validation code is generated in step S216 when the user approves M', as described in page 17, lines 7 to 9. Here too, the feature that the validation code must be created using information specific to the user is not present in the description of the invention according to figures 2b and 2c.

Therefore the board holds that claim 1 meets the requirements of Article 123(2) EPC.

3. Main request - Article 54 EPC

The opponent argued that D1 disclosed all the features of claim 1.

As to features 1A and 1B, the opponent argued in substance that in D1 the transaction confirmation code (figure 1, 142) sent from the second user unit (figure 1, 106) to the server (figure 1, 104) represented a signature on behalf of the user since it was a signature of the received transaction information (figure 1, 136) with a key (see the "seed" in paragraph [0019]) associated with the second user unit. Further, according to the opponent, this signature was created upon request from the user since it was generated in response to a transaction request sent from the user to the server. However, the board agrees with the proprietor that D1 discloses a method for verifying a transaction, e.g. a bank transaction, requested by a user from a server (see paragraph [0012]). During verification of the transaction, a signature (figure 1, 142) is generated but it is a signature to confirm the requested transaction and at the user's request. Thus, the signature 142 in figure 1 cannot be considered a

signature on behalf of the user but rather is similar to the validation code defined in feature 1G of claim 1. Therefore, the board holds that features 1A and 1B are not disclosed in D1. Since D1 does not disclose a user's request to create a signature, feature 1G is also not disclosed in D1.

As to features 1C and 1H, the opponent held that D1 implicitly disclosed that the transaction information (figure 1, 136) was sent from the server to the second user device and (which could be considered as a validation challenge in the sense of claim 1) was encrypted with a secret shared with the user's second device. In that respect, the opponent first argued that, since D1 related to a bank transaction scheme, it was implicit that every communication between the server and the user devices had to be encrypted. However, the board notes that D1 teaches that the user requesting the bank transaction is authenticated by the server (see paragraph [0019]) and that the transaction confirmation code is cryptographically generated using a seed key provided by the server (see paragraph [0027]), but that D1 is completely silent about other cryptographic measures, although it does mention in paragraphs [0002] to [0004] that security is an important concern. The skilled person would thus not consider that the transaction information sent from the server to the second user device must be encrypted. Further, the opponent argued that D1 disclosed in paragraph [0022] that the server might send the validation challenge over a wi-fi connection to the second user device, which was *per se* an encrypted communication channel. However, the board agrees with the proprietor that a bank server is usually not directly connected to a user's wi-fi network, and that even if it were, the wi-fi password cannot be

considered a shared secret in the accepted cryptographic sense since it may be distributed to devices other than the second user device. Therefore, the board holds that the skilled person would not consider it implicit that the transaction information sent from the server to the second user device in D1 is encrypted. Features 1C and 1G are thus not disclosed in D1.

For these reasons, the board holds that claim 1 of the main request (claims as granted) is novel over the disclosure of D1 (Article 54 EPC).

4. Main request - Article 56 EPC

4.1 D1 as closest prior art

4.1.1 Claim 1

The opponent argued that the subject-matter of claim 1 was not inventive over D1.

The subject-matter of claim 1 differs from D1 at least in that the request sent from the first user to the server is a request for signature of a message M and in that the validation challenge sent from the server to the second user device is encrypted with a shared secret.

The proprietor formulated the objective technical problem as how to ensure that the transaction in D1 takes place. The opponent argued that the two above-mentioned differences were juxtaposed in the claim, so that partial problems should be formulated. However, the board agrees with the proprietor that this argument was brought forward for the first time in oral

proceedings and should not be admitted into the proceedings.

The board agrees with the proprietor that the skilled person would not get any hint from D1 to add a request for signature of a message to the process of D1. D1 is concerned with the verification of electronic business transactions (see paragraphs [0001] and [0012]) and does not mention the user requesting a signature on a message that it sends to the server. Contrary to what the opponent argued, a digital signature is not always required for a bank transaction such as the one described in D1. In D1, the transaction is secured by authenticating the user. Moreover, the process of D1 does not require encryption in the communication channel from the server to the second user device. On the contrary, paragraph [0024] explains in substance that if the non-encrypted transaction information is tampered with by a third party, the user simply cancels the transaction. Furthermore, the seed used for signing the transaction information (figure 1, 142) is not transmitted to the second user device together with the transaction information, such that encryption on the channel transmitting the transaction information is also not required to protect the seed from eavesdropping.

The board also agrees with the proprietor that the skilled person would not consider combining D1 with D8 and that even such a combination would not lead to the subject-matter of claim 1. Firstly, D1 is directed to the verification of a transaction requested by a user, whereas D8 deals with the digital signature of data upon request by a user. Secondly, D8 does not disclose several technical features of claim 1 of the present main request. In that respect, D8 discloses a method

for signing a message by a signature server upon request by a user. In a first embodiment, a physical secure token (see figure 1, 190) receives a one-time password from an authentication server (figure 1, 120), distinct from the signature server, through a secure tunnel (see page 23) and the user enters the one-time password into their workstation (figure 1, 101), for transmission to the signature server (figure 1, 110). In a second embodiment of D8, the token is replaced by a mobile phone which receives the one-time password from the authentication server by SMS (see page 14, first full paragraph, and page 15, first full paragraph), which is by definition a non-encrypted communication channel. The one-time password received by the physical token or the mobile phone may be based on a hash of the message to be signed. However, a user is not able to identify the message from its hash value (see page 16, lines 4 to 6). In a single passage in page 18, lines 4 to 9, pointed out by the opponent, D8 mentions that one possible way of achieving WYSIWYS ("What You See Is What You Sign") is to let the certifying apparatus confirm essential parts of the data supplied by the user for certification. The board agrees with the proprietor that the skilled person would realise that only a certifying apparatus in the form of a mobile phone would be adapted to display and present to the user the essential part of the message to be signed. In that case however, according to D8, the message to be signed, or the essential parts of it, would be transmitted by SMS, and thus non-encrypted, from the authentication server to the mobile device, contrary to the requirements of features 1C, 1D and 1H of claim 1. More importantly, D8 does not disclose that the mobile phone generates and sends a validation code to the signature server following confirmation from the user, as required by feature 1G of claim 1. Rather, D8

teaches in all embodiments that a validation code is keyed into the user's workstation (figure 1, 101) for transmission to the signature server (see page 14, lines 17 to 27).

For these reasons, the board holds that the subject-matter of claim 1 involves an inventive step(Article 56 EPC) having regard to the disclosure of D1 as closest prior art, alone or in combination with D8.

4.1.2 Claim 4

The opponent argued that independent claim 4 was not inventive over D1.

The board agrees with the opponent that claim 4 does not require that the signature be generated "on behalf of a user", contrary to claim 1. Therefore, the signed transaction information in D1 (figure 1, 142), which is generated in both the second user device and the server, represents a signature which is created in response to a signature request from a signature creation device, namely the server (figure 1, 104). According to the opponent, the only difference between the subject-matter of claim 1 and D1 would thus be that the validation challenge, namely the transaction information in D1, is encrypted at the server and decrypted before being displayed to the user.

However, the board agrees with the proprietor that there are other differences. In D1, the transaction information which is presented to the user on the second unit for confirmation is the data which should be signed in the server. In contrast, the validation challenge in claim 4 is created using data, namely a second message M' based on the first message M, which

is not the message M to be signed. Moreover, in D1 the signed transaction information (figure 1, 142) sent to the server is not a validation code confirming a request to create a signature, as required by claim 4, but is the requested signature itself. Furthermore, as argued by the proprietor in the written proceedings, the security of the signature in claim 4 is increased with respect to D1 since it is not generated in the validating device itself. The skilled person would not be prompted to implement the above-mentioned distinguishing features in the process of D1 relating to the creation of the signed transaction information.

For these reasons, the board holds that the subject-matter of claim 4 involves an inventive step (Article 56 EPC), having regard to D1.

4.2 D8 as closest prior art

The opponent argued that the subject-matter of claim 1 was not inventive over D8.

As stated in point 4.1.1 above, D8 does not disclose at least features 1C, 1D, 1G and 1H of claim 1, and D1 does not disclose at least features 1A, 1C and 1D of claim 1. Due to these numerous differences between D8, D1 and the subject-matter of claim 1 as detailed in point 4.1.1, the board agrees with the proprietor that the skilled person would not consider combining D8 with D1 and that, even if such a combination were contemplated, it would not lead to the subject-matter of claim 1.

Therefore, the board holds that the subject-matter of claim 1 involves an inventive step (Article 56 EPC)

having regard to the disclosure of D8 as closest prior art, alone or in combination with D1.

5. Main request - Article 83 EPC

The opponent argued that, since the validation code was not defined in claim 1 as being specific to the user, this claim covered embodiments which did not achieve the object of the invention, namely to provide a secure electronic signature at the wilful act of the user as stated in paragraph [0002] of the patent. According to the opponent, an intruder could falsify the validation code, such that the security required would not be achieved, contrary to the requirements of Article 83 EPC.

However, the board agrees in substance with the proprietor that the feature that the validation challenge is decrypted by the second user device using a secret shared with the server implies that only the user who has requested the signature receives the validation challenge. This is sufficient to attest that the signature will be generated at the wilful act of the user.

Moreover, as stated in point 18 of the impugned decision, the absence in feature 1G of encryption of the validation code which could render the validation code specific to the user does not result in insufficiency of disclosure as to how a validation code to be transmitted to the server is issued in the second user device, but simply leads to transmission which is less secure than with encryption.

The board thus holds that the requirements of Article 83 EPC are met.

6. Conclusion

The grounds of opposition under Article 100(a), (b) and (c) EPC do not prejudice maintenance of the patent as granted.

Order

For these reasons it is decided that:

The decision under appeal is set aside.

The patent is maintained as granted.

The Registrar: The Chair:

K. Götz-Wein A. Ritzka

Decision electronically authenticated