BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPÉEN DES BREVETS

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 February 2020

Case Number:	T 2327/17 - 3.5.05
Application Number:	10713889.3
Publication Number:	2553862
IPC:	H04L9/00
Language of the proceedings:	EN

Title of invention:
METHOD AND APPARATUS FOR AUTHENTICATED ENCRYPTION OF AUDIO

Applicant:
Robert Bosch GmbH

Headword:
Authenticated encryption of audio data/BOSCH

Relevant legal provisions:
EPC Art. 56, 84
RPBA Art. 12(4), 13(1)

Keyword:
Inventive step - main request (no) - auxiliary requests 1 and 5 (no)
Claims - clarity - auxiliary requests 3 and 4 (no)
Late-filed auxiliary request 2 - request identical to request not admitted in first instance proceedings

This datasheet is not part of the Decisior
It can be changed at any time and without notic

Decisions cited:

Catchword:

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 2327/17 - 3.5.05

DECISION
of Technical Board of Appeal 3.5.05
of 21 February 2020

Appellant:
(Applicant)

Robert Bosch GmbH
Postfach 30 02 20
70442 Stuttgart (DE)

Representative:

Robert Bosch GmbH
C/IPE41
Postfach 30 02 20
70442 Stuttgart (DE)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted on 22 May 2017 refusing European patent application No. 10713889.3 pursuant to Article 97(2) EPC.

Composition of the Board:

Chair	A. Ritzka
Members:	P. Cretaine
	D. Prietzel-Funk

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division, posted on 22 May 2017, refusing European patent application No. 10713889.3. The application was refused for lack of inventive step (Article 56 EPC) of a main request and a first auxiliary request over

D7: Alkassar A. et al: "SLC: Efficient Authenticated Encryption for Short Packets," SICHERHEIT 2006, vol. P-77, 1 January 2006, pages 270 to 278,

or

D10: Genaro R. and Rohatgi P.: "How to sign digital streams", Advances in Cryptology - CRYPTO '97, 17 August 1997, pages 180 to 197.

The following documents were also cited in the examination proceedings:

D2: Menezes A. et al.: "Chapter 9: Hash Functions and Data Integrity," Handbook of Applied Cryptography, CRC Press, pages 321 to 383, 1 October 1996,

D5: Talevski A. et al.: "Secure and Mobile VoIP," Convergence Information Technology 2007, IEEE, 21 November 2007, pages 2108 to 2113,

D6: US 4 608 455, and

D9: Palmieri F. and Fiore U.: "Providing true end-to-end security in converged voice over IP infrastructures," Computers & Security, Elsevier, vol. 28, no. 6, 2009, pages 433 to 449.

II. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the main request, the first auxiliary request, or the second auxiliary request on which the decision was based, or on the basis of the third auxiliary request or the fourth auxiliary request submitted with the statement setting out the grounds of appeal. The appellant also requested oral proceedings on an auxiliary basis.

III. A summons to oral proceedings was issued on 28 November 2019. In a communication annexed to the summons, the board gave its preliminary opinion on the case. The board raised clarity objections (Article 84 EPC) and inventive step objections (Article 56 EPC) based on D5, or D9, in combination with D7, against all requests.

IV. With a letter of response dated 21 January 2020, the appellant filed a fifth auxiliary request.

V. Oral proceedings were held on 21 February 2020. The appellant requested that the decision under appeal be set aside and a patent be granted on the basis of the claims of the main request or of the first auxiliary request, both submitted with the letter dated 6 April 2017, or of the second auxiliary request submitted with the letter dated 9 May 2017, or of the third and fourth auxiliary requests submitted with the statement setting out the grounds of appeal, or of the fifth auxiliary request submitted with the letter dated 21 January 2020. The decision of the board was announced at the end of the oral proceedings.

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

"Method of decoding audio data with low latency encrypted and authenticity protected, using an AES decryption in Cipher feedback mode removing the need for additional synchronization, detecting whether a CMAC authenticity check is successful from a single audio sample, wherein without knowing an initalisation [*sic*] vector from the encryption it takes the number of bits from a cipher-block before the correct data can be decrypted, wherein the method is performed on a sample by sample basis with a latency less than 1 µs."

Independent claim 2 of the **main request** reads as follows:

"Method of encoding audio data with ultra low latency, wherein the audio data is encrypted using AES encryption (16, 52, 116, 152) in Cipher feedback mode and authenticity protected by calculating a CMAC over the data, wherein the method is performed on a sample by sample basis with a latency less than 1 µs."

Claim 1 of the **first auxiliary request** reads as follows:

"Method of decoding audio data with low latency encrypted and authenticity protected, using an AES decryption in Cipher feedback mode removing the need for additional synchronization, detecting whether a CMAC authenticity check is successful from a single audio sample, wherein without knowing an initalisation [*sic*] vector from the encryption it takes the number of bits from a cipher-block before the correct data can be decrypted, wherein the method is performed on a sample by sample basis with a latency less than 1 µs, wherein the decrypted audio data is muted when the authenticity check fails based upon CMAC failure, wherein the encryption and the CMAC algorithm use different keys."

Claim 1 of the **second auxiliary request** differs from claim 1 of the first auxiliary request in that the wording ",wherein an additional audio receiver is connected to a running encrypted audio stream in case the additional audio receiver has proper keys" is added at the end of the claim.

Claim 1 of the **third auxiliary request** differs from claim 1 of the second auxiliary request in that the wording "an additional audio receiver is connected" is replaced with the wording "an audio receiver is connected".

Claim 1 of the **fourth auxiliary request** differs from claim 1 of the second auxiliary request in that the wording ", wherein the audio data is muted until the AES decryption in Cipher feedback mode is successful" is added at the end of the claim.

Claim 1 of the **fifth auxiliary request** differs from claim of the main request in that the wording ", wherein a current initialization vector (150) is a 24-bits encrypted audio sample (120) concatenated with 104-bits from a previous initialization vector (100)" is added after the wording "removing the need for additional synchronisation", "detecting" is replaced by "wherein it is possible to detect" and in that the wording "with a latency less than 1 µs" at the end of the claim is deleted.

Independent claim 2 of the **fifth auxiliary request** differs from claim 2 of the main request in that the wording ", wherein a current initialization vector (50) for a audio sample is a 24-bits encrypted audio sample (24) concatenated with 104-bits from a previous initialization vector (10)" is added after the wording "calculating a CMAC over a data" and in that the wording "with a latency less than 1 µs" at the end of the claim is deleted.

Reasons for the Decision

1. Main request - Article 56 EPC

D5 represents the closest prior art to the subject-matter of claim 1. D5 discloses the use of AES in Cipher feedback mode to encrypt/decrypt audio data (see page 2112, right-hand column, lines 12 to 32). It is common general knowledge that in an encryption/ decryption scheme in cipher feedback mode, the need for additional synchronisation is removed and that without knowing an initialisation vector from the encryption it takes the number of bits from a cipher-block before the correct data can be decrypted (see for instance D9, page 438, right-hand column, lines 4 to 23).

Therefore D5 discloses, using the wording of claim 1, a method of decoding audio data encrypted, using an AES decryption in Cipher feedback mode removing the need for additional synchronisation, wherein without knowing an initialisation vector from the encryption it takes the number of bits from a cipher block before the correct data can be decrypted.

The subject-matter of claim 1 differs from the disclosure of D5 in that it comprises the further step of detecting whether a CMAC authenticity check is successful from a single audio sample and that the method is performed on a sample by sample basis with a latency less than 1 µs.

With respect to the feature "with a latency less than 1 µs", the appellant argued that this feature was implied by the choice of a length of 24 bits for the audio sample which resulted in a CMAC authenticity check in less than 1 µs. The length of an audio sample being however not defined in claim 1, the board agrees with the decision under appeal (see point 7.2.8) that defining that the latency is less than 1 µs amounts to merely define a result to be achieved.

In respect of interpretation of the vague and broad feature "the method is performed on a sample by sample basis", the appellant argued that it should be interpreted as meaning that not only the CMAC authenticity check but also the AES decryption in Cipher feedback mode were performed on a sample by sample basis. In its view, obtaining a plain 24-bits audio sample, as shown by reference sign 126 in Figure 2 and described on page 5, lines 22 to 24, was an evidence that the decryption was performed on a sample by sample basis. However, the board notes that the decryption of a 24-bits audio sample at stage n + 1 depends on the decryption of the previous sample at stage n, as shown in Figure 2 and as implied by the use of a Cipher feedback mode. The board thus agrees with the decision under appeal (see point 7) that the decryption in AES Cipher feedback mode cannot be interpreted as being performed on a sample by sample basis so that the feature "the method is performed on a sample by sample basis" has to be interpreted as applying CMAC authenticity check on a sample by sample basis.

The technical effect of the above-mentioned distinguishing features is that invalid audio samples are detected without having to wait for the large number of audio samples, such as the whole audio data, to be received and decrypted. The objective technical problem can thus be formulated as how to increase the cryptographic security of the audio data stream.

The person skilled in cryptography, trying to improve the reliability of a received encrypted audio stream, would obviously consider to use an authentication scheme to add security to the encryption scheme. The skilled person would consider D7 which discloses to split a Voice over IP stream, i.e. an audio stream, into short packets, or chunks, to encrypt them using a conventional encryption scheme, to accompany each chunk with a Message Authentication Code MAC, and to compare the transmitted MAC with a recalculated MAC at reception (see the paragraph bridging pages 274 and 275). It was moreover well known at the priority date of the present application to use block-cipher-based MAC, i.e. CMAC, as MAC. By applying the teaching of D7 to the disclosure of D5 the skilled person would thus arrive at the subject-matter of claim 1 without the exercise of inventive skills.

For these reasons, the board holds that claim 1 does not meet the requirements of Article 56 EPC, having regard to D5 in combination with D7.

2. First auxiliary request - Article 56 EPC

Claim 1 of the first auxiliary request adds to claim 1 of the main request the features that the decrypted audio data is muted when the authenticity check fails based upon CMAC failure and that the encryption and the CMAC algorithm use different keys.

The board agrees with the decision under appeal (see point 7.9.1) that using different keys for encryption and MAC authentication belongs to the common general knowledge, as illustrated by section 9.87 in page 367 of D2, which is an excerpt of a technical textbook.

The board further holds that the feature defining that the decrypted audio data is muted when the authenticity check fails based upon CMAC failure is not clear (Article 84 EPC). Indeed, the claim relates to the decoding of encrypted and authenticity protected audio data, and not to the rendering of this audio data through a sound device with a muting function. This feature can thus not justify an inventive step.

For these reasons, claim 1 does not meet the requirements of Article 56 EPC, having regard to D5 in combination with D7.

3. Second auxiliary request- Article 12(4) RPBA 2007

This request has not been admitted in the first instance proceedings for being late filed and prima facie not clear. The board agrees with the clarity objections raised in the decision under appeal in points 9.1.1 and 9.1.2 and thus holds that the examining division has correctly applied the provisions of Rule 137(3) EPC.

Moreover, the board maintains that the feature defining that the decrypted audio data is muted when the authenticity check fails based upon CMAC failure is not clear (see point 3 above).

Therefore, the board decides under Article 12(4) RPBA 2007 not to admit the second auxiliary request into the proceedings.

4. Third auxiliary request - Article 84 EPC

This request has been filed with the statement setting out the grounds of appeal. Claim 1 differs from claim 1 of the second auxiliary request only by the deletion of the first occurrence of the word "additional".

The board maintains that the feature defining that the decrypted audio data is muted when the authenticity check fails based upon CMAC failure is not clear (see point 3 above). In that respect, appellant argued that this feature is made clear by the disclosure of D6, column 6, lines 26 to 28. The board is not convinced by this argument since the passage quoted in D6 relates to an apparatus comprising means for muting a recovered speech signal whereas claim 1 relates to a method for decoding audio data.

Further, the wording "in case the additional receiver has proper keys" is unclear since there is no antecedent definition of this receiver in the claim.

For these reasons, the board holds that claim 1 is not clear (Article 84 EPC).

5. Fourth auxiliary request - Article 84 EPC

This request has been filed with the statement setting out the grounds of appeal. Claim 1 adds to claim 1 of the second auxiliary request the feature that the audio data is muted until the AES decryption in Cipher feedback mode is successful.

The board maintains that the feature defining that the decrypted audio data is muted when the authenticity check fails based upon CMAC failure is not clear (see point 3 above). For the same reason, the feature defining that the audio data is muted until the AES decryption in Cipher feedback mode is successful is not clear.

Further the meaning of the wording "additional audio receiver" is unclear since no audio receiver is defined previously in the claim.

For these reasons, the board holds that claim 1 is not clear (Article 84 EPC).

6. Fifth auxiliary request - Article 56 EPC

This request has been filed in response to the communication annexed to the summons. Claim 1 differs from claim 1 of the main request by deleting the wording "with a latency less than 1 µs" and by adding the feature that the current initialization vector for a audio sample is a 24-bits encrypted audio sample concatenated with 104-bits from a previous initialization vector.

The appellant argued that these amendments were an attempt to overcome the clarity objections raised by the board in the communication annexed to the summons The board has thus decided in oral proceedings to admit the fifth auxiliary request into the proceedings under Article 13(1) RPBA 2007.

However, the board holds that the feature defining the current initialisation vector represents an obvious measure for the skilled person in cryptography. Indeed, the skilled person is aware that in an AES encryption/ decryption scheme in Cipher feedback mode, a different nonce or random initialisation vector is needed for every encryption/decryption AES message block. It may be the previous encrypted message or a new initialisation vector. The skilled person would thus choose a concatenation of the previous encrypted audio-sample with a portion of the previous initialisation vector as an obvious alternative. The appellant did not provide any convincing argument in respect of the technical advantage implied by such a choice.

For these reasons, the board holds that the subject-matter of claim 1 does not involve an inventive step (Article 56 EPC) having regard to D5 in combination with D7.

7. Conclusion

The main request, the first auxiliary request and the fifth auxiliary request are not allowable under Article 56 EPC.
The second auxiliary request is not admitted into the proceedings (Article 12(4) RPBA 2007).
The third and fourth auxiliary requests are not allowable under Article 84 EPC.
There being no allowable requests, the appeal has to be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chair:

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

A. Chavinier-Tomsic A. Ritzka

Decision electronically authenticated