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 26 February 2014

Case Number: T 1330/12 - 3.5.04

Application Number: 04015158.1

Publication Number: 1492106

IPC: G11B20/00, G06F1/00

Language of the proceedings: EN

Title of invention:
A method to authenticate a data processing apparatus having a recording device and apparatuses therefor

Applicant:
SEAGATE TECHNOLOGY INTERNATIONAL

Headword:

Relevant legal provisions:
EPC 1973 Art. 56, 84

Keyword:
Inventive step - (no)
Claims - clarity - auxiliary request (no)

Decisions cited:

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 1330/12 - 3.5.04

DECISION
of Technical Board of Appeal 3.5.04
of 26 February 2014

Appellant:
(Applicant)

SEAGATE TECHNOLOGY INTERNATIONAL
P.O. Box 309
Georgetown
Grand Cayman Island (KY)

Representative:

Miller Sturt Kenyon
9 John Street
London WC1N 2ES (GB)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted on 20 December 2011 refusing European patent application No. 04015158.1 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman: F. Edlinger
Members: R. Gerdes
T. Karamanli

Summary of Facts and Submissions

I. The appeal is directed against the decision to refuse European patent application No. 04 015 158.1, published as EP 1 492 106 A2.

II. The patent application was refused by the examining division on the grounds that the claims of the main request and of the first to third auxiliary requests did not comply with Article 84 EPC.

III. The applicant appealed against this decision and with the statement of grounds of appeal submitted claims of a main request and of first to ninth auxiliary requests. The appellant requested oral proceedings as an auxiliary measure.

The appellant stated that the main request corresponded to the main request underlying the decision under appeal and that the claims of the first to ninth auxiliary requests had been amended to address, individually or in combination, the lack of clarity objections in the decision under appeal.

Considering D1 as the closest prior art, one advantage of the present invention was that no keys had to be transferred from the host to the recording device and vice versa. Consequently, the invention reduced the complexity of the used protocol for mutual authentication. Thus, the objective technical problem could be regarded as how to reduce the complexity of the authentication protocol.

IV. The independent claims of the main request read as follows:

Claim 1: "An authentication method comprising the following host-side steps to authenticate a recording device of a data processing apparatus having a host:
generating (S602) a first random number via the host;
encrypting (S604) the first random number using a host key to generate a first encrypted value;
transmitting (S606) the first random number and the first encrypted value to the recording device;
receiving (S610) a second random number and a second encrypted value from the recording device, wherein the second encrypted value was encrypted using a recording device key;
decrypting (S612) the second encrypted value using the host key to generate a first decrypted value; and
authenticating (S516) the recording device upon determining that the second random number provided from the recording device is the same as the first decrypted value."

Claim 14: "A host-side authentication apparatus to authenticate a recording device of a data processing apparatus having a host to process data and the recording device to store and reproduce data processed or to be processed by the host, the host authentication apparatus comprising:
a first encrypt module (704) to encrypt a first random number using a host key (706) allocated to the host to generate a first encrypted value;
a first decrypt module (708) to decrypt a second encrypted value provided by the recording device using the host key allocated to the host to generate a first decrypted value, the second encrypted value being a value encrypted with a recording device key (806); and
a host authentication controller (710) to provide the first random number and the first encrypted value to the recording device and to receive a second random

number and the second encrypted value provided by the recording device,
wherein the host authentication controller is adapted to:
receive a response to authenticate the host as an authorized host from the recording device receiving the first random number and the first encrypted value; and
provide a response to authenticate the recording device as an authorized recording device to the recording device, upon determining a condition that the second random number provided by the recording device is the same as the first decrypted value is satisfied."

V. Claim 14 of the third auxiliary request is identical to claim 14 of the main request.

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

"An authentication method to authenticate a host and a recording device of a data processing apparatus, the method comprising:
generating (S602) a first random number via the host;
encrypting (S604), by the host, the first random number using a host key to generate a first encrypted value;
transmitting (S606), by the host, the first random number and the first encrypted value to the recording device;
receiving (S622) the first random number and the first encrypted value by the recording device,
decrypting (S624), by the recording device, the first encrypted value using a recording device key to generate a second decrypted value;
upon determining, by the recording device, that the second decrypted value and the first random number are

identical, authenticating, by the recording device, the host as an authorized host;
once the host is authenticated, transmitting (S628), by the recording device, a response message indicating that the host is authenticated to the host;
generating (S630), by the recording device, a second random number;
encrypting (S632), by the recording device, the second random number using the recording device key to generate a second encrypted value;
transmitting (S634), by the recording device, the second random number and the second encrypted value to the host;
receiving (S608), by the host, the response message indicating that the host is authenticated from the recording device;
upon determining, by the host, that the authentication of the host is successful, receiving (S610), by the host, the second random number and the second encrypted value from the recording device;
decrypting (S612), by the host, the second encrypted value using the host key to generate a first decrypted value;
authenticating (S516), by the host, the recording device upon determining that the second random number provided from the recording device is the same as the first decrypted value; and
upon determining that the recording device is authenticated, transmitting, by the host, a response message indicating that the recording device is authenticated to the recording device."

VII. Claim 1 of the first auxiliary request - when compared with claim 1 of the main request - claim 14 of the fourth auxiliary request - when compared with claim 14 of the main request - and claim 1 of the seventh auxiliary request - when compared with claim 1 of the sixth auxiliary request - contain the following additional feature appended to them:

"wherein the host key and the recording device key are in an inseparable relation."

VIII. Claim 1 of the second auxiliary request - when compared with claim 1 of the main request - claim 13 of the fifth auxiliary request - when compared with claim 14 of the main request - and claim 1 of the eighth auxiliary request - when compared with claim 1 of the sixth auxiliary request - contain the following additional feature appended to them:

"wherein the authentication is performed according to an open key encryption technique."

IX. Claim 13 of the ninth auxiliary request reads as follows:

"A system comprising:
an host-side authentication apparatus (700) to authenticate a recording device of a data processing apparatus having a host to process data and the recording device to store and reproduce data processed or to be processed by the host; and
a recording device-side authentication apparatus (800) to authenticate the host by the recording device of the data processing apparatus;
...
wherein when the host and the recording device are first attached, one of a pair of keys in a relation where a mutual authentication can be performed only by these keys, is allocated to the host and the other, to the recording device, the key allocated to the host

being the host key and the key allocated to the recording device being the recording device key; and wherein an open key encryption is used to authenticate the recording device and/or the host." (The central part of the claim has been omitted by the board, because its wording is not relevant for the purposes of this decision).

X. In a communication annexed to a summons to oral proceedings the board indicated *inter alia* that it tended to interpret claim 1 of the main request as a broad but not necessarily unclear claim. The board noted that the examining division had objected under Article 56 EPC to this claim in the summons to oral proceedings dated 11 July 2011. In its preliminary opinion the board agreed with that objection, in particular in view of the broad interpretation of claim 1. The subject-matter of the independent claims of all requests thus seemed to lack an inventive step (Article 56 EPC 1973) and claim 13 of the ninth auxiliary request was considered to be unclear (Article 84 EPC 1973).

The board referred to the following documents that were cited in the proceedings before the department of first instance:

D1: EP 1 124 350 A (SONY CORPORATION),
16 August 2001

D2: PATENT ABSTRACTS OF JAPAN vol. 2003, no. 01,
14 January 2003 & JP 2002281023 A, (SONY CORP),
27 September 2002

D3: US 5 590 202 A (BESTLER ET AL),
31 December 1996.

It additionally cited the following excerpt from a textbook already introduced during the examination proceedings:

D5: Menezes, A. J. et al.: Handbook of Applied Cryptography, Chapter 10: Identification and Entity Authentication, pp. 385-386, 397-403, 1997, CRC Press, Boca Raton, Fl, USA, XP002386305.

XI. With letter dated 13 January 2014 the appellant withdrew its request for oral proceedings and requested the board to take a decision based on the current state of the file.

The appellant did not provide arguments with respect to inventive step of the claimed subject-matter in view of D5. It also did not address the issue of lack of clarity of claim 13 according to the ninth auxiliary request that had been raised in the board's communication (see point X above).

Reasons for the Decision

1. The appeal is admissible.

2. The application concerns a method for performing authentication in a system consisting of a recording device such as a hard disk and a host/data processing apparatus such as a set-top box. It discloses a protocol for performing authentication of the recording device and the host involving the exchange of random numbers and corresponding encrypted values generated using a pair of keys of which one is allocated to the host and the other to the recording device. For

unilateral authentication one of the two devices generates a random number and encrypts this number using its key. The random number and the encrypted value are transmitted to the other device, which uses its key to decrypt the encrypted value. If the received random number and the decrypted value correspond, the transmitting device is considered to be authenticated. For mutual authentication the process is carried out in both directions (see paragraphs [0052] to [0063] and figures 5 and 6 of the application).

Main request

3. D5 is considered to represent the closest prior art with respect to the subject-matter of claim 1.

3.1 D5 presents a two-pass algorithm for unilateral authentication employing a random number r_B (the challenge) generated by device B to authenticate device A. In response to receiving the random number, A encrypts the random number and sends the result to B. It is also stated (see page 401 and section "10.17 Remark" on page 402) that "mutual authentication may be obtained by running any of the above unilateral authentication mechanisms twice".

3.2 Hence, the only differences between the authentication according to D5 and the subject-matter of claim 1 are the following:

(a) "A" is a host device and "B" is a recording device. However, the usage of authentication in the realm of "hosts" and "recording devices" is well-known (see D1 to D3).

(b) The random number is generated by "B" as a challenge and sent to "A". According to claim 1, the host device ("A") generates the random number itself and transmits it together with the encrypted value to the recording device ("B").

3.3 The technical effect of difference (b) is that the overhead of an additional transmission from B to A can be dispensed with. Thus, the board accepts the appellant's formulation of the technical problem "how to reduce complexity of an authentication protocol" (see statement of grounds, page 3, third paragraph).

3.4 The advantages and disadvantages of this simplification are foreseeable. The disadvantage of the generation of the random number by the entity requesting authentication is that the authenticating entity does not have control over the generation of the random number itself. That means that a malevolent entity wishing to be authenticated can choose any number it wishes as the "random" number, encrypt this number and send the number and the result of the encryption to the authenticating entity. The random number could even be a number that was obtained previously together with the corresponding encrypted number by eavesdropping on the interface between recording device and host. Hence, simplification is achieved at the foreseeable expense of reduced security. In view of the foreseeable effects of the modification the board concludes that given the circumstances a skilled person would have considered implementing the proposed simplification.

3.5 As a consequence, the subject-matter of claim 1 lacks an inventive step (Article 56 EPC 1973).

3.6 Independent claims 14 and 20 specify the corresponding "host-side authentication apparatus" and "recording device-side authentication apparatus". These claims additionally specify that - as a result of authentication - a message indicating acceptance is sent to the other device. It would have been obvious for the skilled person that the result of authentication had to be communicated to the other device either explicitly as required by the claims or implicitly by accepting or denying subsequent communication requests (see also D5, page 386, chapter 10.1.1(i)). Hence, the subject-matter of these claims equally lacks an inventive step over D5.

First and second auxiliary requests

4. Claim 1 of the first auxiliary request contains the additional feature that "the host key and the recording device key are in an inseparable relation". Claim 1 of the second auxiliary request specifies in addition to the features of claim 1 of the main request that "authentication is performed according to an open key encryption technique".

4.1 The appellant argued in point 4 of the statement of grounds of appeal that a person skilled in the art of cryptography knew what was meant by "a pair of keys which are in an inseparable relation to each other" and that "those keys" were "commonly used in public key encryption techniques". Hence, the decisive question in respect of claim 1 of the first and second auxiliary requests is whether it was obvious to use an open (public) encryption technique in the context of the authentication method of the main request discussed above.

4.2 Public key encryption techniques were well-known at the effective date of the application and have been employed for authentication of recording devices and recording media (see D1, paragraphs [0002], [0010] and [0014], or D2, Abstract). Hence, the board holds that the subject-matter of claim 1 according to both requests lacks an inventive step.

Third to fifth auxiliary requests

5. Claim 14 according to the third auxiliary request is identical to claim 14 of the main request. Hence, the subject-matter of this claim lacks inventive step for the same reasons (see point 3.6 above).

6. Independent claim 14 of the fourth auxiliary request corresponds to claim 14 of the main request and contains the additional feature of claim 1 of the first auxiliary request. Claim 13 of the fifth auxiliary request includes the additional feature of claim 1 of the second auxiliary request. As set out under point 4.2 above, the use of public key encryption schemes was well-known and does not combine with the further features of the claims to result in inventive subject-matter. Hence, the subject-matter of claim 14 of the fourth auxiliary request and of claim 13 of the fifth auxiliary request lacks an inventive step.

Sixth to eighth auxiliary requests

7. Claim 1 of the sixth auxiliary request specifies the steps carried out for the authentication procedure on the host device and those for authentication on the recording device.

The resulting method effectively only consists in running the unilateral authentication of the higher-ranking requests on both devices. D5 discloses that "mutual authentication may be obtained by running any of the above unilateral authentication mechanisms twice (once in each direction)", see page 402, Remark 10.17. Hence, the subject-matter of claim 1 according to the sixth auxiliary request does not involve an inventive step.

8. The independent claims according to the seventh and eighth auxiliary requests contain the additional features of claim 1 of the first auxiliary request and the second auxiliary request, respectively. Thus the reasoning under section 4 above applies likewise.

Ninth auxiliary request

9. Under Article 84 EPC 1973, the claims shall define the matter for which protection is sought. They shall be clear and concise and be supported by the description.

9.1 Claim 13 relates to a system comprising a host-side authentication apparatus and a recording device-side authentication apparatus. It also contains the following feature: "wherein when the host and the recording device are first attached, one of a pair of keys in a relation where a mutual authentication can be performed only by these keys, is allocated to the host and the other, to the recording device, the key allocated to the host being the host key and the key allocated to the recording device being the recording device key". This feature specifies a **method step** relating to the initial preparation of the system in order to link the two apparatuses by the common pair of keys for the purpose of mutual authentication. It is unclear which structural features of the host-side authentication apparatus and the recording device-side authentication apparatus are involved in this method step by having been allocated a pair of keys when they were first attached.

9.2 Hence, claim 13 does not comply with the requirements of Article 84 EPC 1973.

Conclusion

10. It follows from the above that the decision under appeal cannot be set aside.

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

K. Boelicke F. Edlinger

Decision electronically authenticated