BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN 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 20 June 2007

Case Number: T 0419/03 - 3.5.04

Application Number: 97916402.7

Publication Number: 0891670

IPC: H04N 7/16

Language of the proceedings: EN

Title of invention:
Method for providing a secure communication between two devices and application of this method

Patentee:
Irdeto Access B.V.

Opponent:
CANAL + TECHNOLOGIES SOCIETE ANONYME

Headword:
-

Relevant legal provisions:
EPC Art. 56

Keyword:
"Inventive step (yes)"

Decisions cited:
-

Catchword:
-

Case Number: T 0419/03 - 3.5.04

D E C I S I O N
of the Technical Board of Appeal 3.5.04
of 20 June 2007

Appellant:
(Patent Proprietor)

Irdeto Access B.V.
Jupiterstraat 42
NL-2132 HD Hoofddorp (NL)

Representative:

de Vries, Johannes Hendrik Fokke
de Vries & Metman
Overschiestraat 180
NL-1062 XK Amsterdam (NL)

Respondent:
(Opponent)

CANAL + TECHNOLOGIES SOCIETE ANONYME
34 PLACE RAOUL DAUTRY
F-75516 PARIS CEDEX 15 (FR)

Representative:

Weihs, Bruno Konrad
Osha Liang
121, Avenue des Champs Elysées
F-75008 Paris (FR)

Decision under appeal:

Decision of the Opposition Division of the European Patent Office posted 16 January 2003 revoking European patent No. 0891670 pursuant to Article 102(1) EPC.

Composition of the Board:

Chairman: F. Edlinger
Members: M. Paci
T. Karamanli

Summary of Facts and Submissions

I. The appellant (patent proprietor) lodged an appeal against the decision of the opposition division revoking European patent No. 0 891 670.

II. Opposition had been filed against the patent as a whole under Article 100(a) EPC for lack of novelty and inventive step and under Article 100(b) EPC for insufficiency of the disclosure.

III. The following prior art documents cited in the opposition proceedings have been discussed in appeal proceedings:

D1: Chapters 2 and 3 of "Applied Cryptography" by Schneier, second edition, published by John Wiley and Sons Inc., 18 October 1995, pages 21 to 74

D3: "Issues in the Design of a Key Distribution Centre" by Price and Davies, NPL Report DNACS 43/81, April 1981

D6: US 5 111 504 A.

IV. In the decision under appeal the opposition division concluded that the subject-matter of amended claim 1 according to the main request did not involve an inventive step in view of D3 and D6. The subject-matter of claim 1 according to the auxiliary request was held to lack an inventive step having regard to D3, D6 and prior art acknowledged in the patent specification. However the requirement of sufficiency of disclosure was found to be met.

V. With the statement of grounds of appeal the appellant filed a new set of claims 1 to 4 and new columns 1 and 2 of the description.

VI. In a communication accompanying the summons to oral proceedings the board drew attention to D1 (cited in the notice of opposition), a reference textbook on applied cryptography published shortly before the priority date of the patent, as evidence of common general knowledge.

VII. Oral proceedings before the board were held on 20 June 2007. During the oral proceedings the appellant (patent proprietor) filed a new set of claims 1 to 4 replacing all previous claims and new columns 1 and 2 of the description. The respondent (opponent) did not argue against maintaining the patent.

VIII. The appellant (patent proprietor) requested that the decision under appeal be set aside and that the patent be maintained in amended form on the basis of claims 1 to 4 of the sole request.

IX. The respondent (opponent) withdrew the previous request that the appeal should be dismissed and explicitly declared that he agreed that a patent should be granted on the basis of the patent proprietor's request. He confirmed that this was not a withdrawal of the opposition.

X. Independent claims 1 to 4 read as follows.

"1. Method for providing a secure communication between a conditional access module (4) and a smart card (5) in a decoder for a pay TV System, wherein the conditional access module (4) generates a random key (Ci) and a random number (A), and transfers said key (Ci) together with said random number (A) to the smart card (5) in a first message encrypted using a public key, wherein said smart card decrypts the first encrypted message by means of a corresponding secret key to obtain said random key (Ci) and said random number (A), and returns said random key (Ci) in a second encrypted message containing said random number (A) as authentication, wherein said second message is obtained by encrypting said random number (A) and said random key (Ci), wherein said random key (Ci) is used by the smart card (5) to encrypt and by the conditional access module (4) to decrypt subsequent transmissions from the smart card to the conditional access module."

"2. Method for providing a secure communication between a decoder and a conditional access module (4) in a pay TV System, wherein the decoder generates a random key (Ci) and a random number (A), and transfers said key (Ci) together with said random number (A) to the conditional access module (4) in a first message encrypted using a public key, wherein said conditional access module decrypts the first encrypted message by means of a corresponding secret key to obtain said random key (Ci) and said random number (A), and returns said random key (Ci) in a second encrypted message containing said random number (A) as authentication, wherein said second message is obtained by encrypting said random number (A) under said random key (Ci), wherein said random key (Ci) is used by the conditional access module (4) to encrypt and by the decoder to decrypt subsequent transmissions from the conditional access module to the decoder."

"3. Decoder for a pay TV system, comprising a conditional access module (4) and a smart card (5), said conditional access module comprising means (8) for generating a random key (Ci) and a random number (A), means (8) for encrypting said key (Ci) and said random number (A) in a first encrypted message using a public key encryption method, means (8) for transferring said first encrypted message to the smart card, said smart card (5) comprising means (10) for receiving and decrypting said first encrypted message to obtain said random key (Ci) and said random number (A) by means of a corresponding secret key, means (10) for returning to the conditional access module a second encrypted message containing said random number (A) as authentication, wherein said second message is obtained by encrypting said random number (A) under said random key (Ci) and means (10) for encrypting subsequent transmissions to the conditional access module under said random key, wherein the conditional access module (4) has means to decrypt the encrypted subsequent transmissions received from the smart card by means of said random key."

"4. Decoder for a pay TV system, comprising a conditional access module (4) and a smart card (5), said decoder comprising means (6) for generating a random key (Ci) and a random number (A), means for encrypting said key (Ci) and said random number (A) in a first encrypted message using a public key encryption method, means (6) for transferring said first encrypted message to the conditional access module (4), said conditional access module comprising means (8) for receiving and decrypting said first encrypted message to obtain said random key (Ci) and said random number (A) by means of a corresponding secret key, means (8) for returning to the decoder a second encrypted message with said random number (A) as authentication, wherein said second message is obtained by encrypting said random number (A) under said random key (Ci), and means (8) for encrypting subsequent transmissions to the decoder under said random key, wherein the decoder has means (6) to decrypt the encrypted subsequent transmissions received from the conditional access module by means of said random key."

XI. The reasons in the decision under appeal, in so far as they apply to present claims 1 to 4, can be summarised as follows.

D3 is considered to represent the closest prior art because it has the greatest number of technical features in common with claim 1 and relates to the same general concept. It discloses a method for providing a secure communication between two devices using public key cryptography in order to exchange a random key which is used for encrypting subsequent transmissions between the two devices.

The subject-matter of claim 1 differs from the method of D3 firstly in that the method is applied to communications between two devices in a decoder for a pay TV system, said decoder comprising a conditional access module (CAM) and a smart card.

However this first difference is rendered obvious by the teaching of D6 which discloses the idea of applying encryption methods for providing secure communication between a CAM and a smart card in a decoder for a pay TV system.

A second difference to D3 resides in the authentication using an encrypted random number. According to claim 1, the first device generates a random number in addition to the random key and transfers the two together to the second device. The second device then decrypts the message and returns the random number encrypted under the random key to the first device as authentication.

This second difference is not inventive because such a concept was already used in D3 (figure 2) for the secure communication between a device A and a key distribution centre KDC (random number R in messages 1 and 2), between another device B and the KDC (random number R') and also between devices A and B (random number R''). It is true that in figure 2 of D3 the random number is not generated by the first device A, and three messages are exchanged between A and B against only two in claim 1. This difference however relates to an obvious choice which is not capable of establishing an inventive step. Indeed a skilled person would routinely consider generating and exchanging random numbers wherever and whenever required, and would consider combining the transmission of such random numbers with other information, such as a session key, as desired. Moreover, the skilled person attempting to apply the concept of D3 to secure communications between a CAM and a smart card as disclosed in D6 would immediately recognize that it is the smart card that has to be authenticated and not the CAM, since, as is apparent for example from D6, it must be checked whether or not the smart card is authorised, so that the random number has to be generated in the first device (the CAM) and returned as authentication by the second device.

Accordingly, the skilled person implementing a design based on the combined teachings of D3 and D6, and taking into account the variants of encryption and authentication that are obvious from D3, would arrive at the subject-matter of claim 1 without exercising an inventive step.

XII. The appellant (patent proprietor) argued essentially as follows.

The opposition division argued that D3 represented the closest prior art. The appellant contests this finding. D3 relates to the problems associated with the secure distribution of cryptographic keys in a data communication network wherein each user is a secure device which can communicate directly with a key distribution centre (KDC). Therefore, D3 does not relate to the same technical field as the present patent, and the technical problems disclosed in D3 differ from the problem of the present invention.

The closest prior art is D6 which relates to the same technical field as the present patent, i.e. a pay TV system, and tries to solve the same technical problem, namely protection of the interface between first and second devices of the decoder of a pay TV system.

The reasoning of the opposition division is based on hindsight because it merely shows that the teaching of D3 could have been combined with the teaching of D6, but fails to show that the skilled person would have been prompted to apply the teaching of D3 in a decoder for a pay TV system. The opposition division's extraction from D3 of the concept of using a random number as authentication is also based on hindsight and a wrong interpretation of the teachings of D3. This can be seen from the selection of elements in the different context of D3 involving a network and the KDC, and the fact that three messages are exchanged between A and B, as opposed to only two between the CAM and the smart card in claim 1. If device A alternatively generated a random key (session key Ks, as indicated in page 7, lines 31 to 34 of D3), device A would not transmit both the random number and the random key to the KDC because D3 does not teach an exchange of the random key between device A and the KDC in this situation.

Starting from D6 as the closest prior art, the subject-matter of claim 1 was not suggested by the teachings of D1 or D3. D1 is a general textbook on applied cryptography which describes various protocols using public-key cryptography. However there is no hint in D1 to attempt to have only one secret key and to start an authentication process by transferring both a random key and the random number encrypted using a public key. D3, as already explained, uses random numbers in the context of a data communication network which is very different to the direct interface between the CAM and the smart card in claim 1.

Nothing in the prior art hinted at providing secure communication between devices of a decoder where a single public key exchange is sufficient to transmit a random key which is used in the subsequent transmissions. This makes the communication simple, reduces the set-up time and complexity of calculations, requires only one secure device where a secret key is stored and nevertheless provides protection against abuse and switching between authorised and unauthorised devices. In the case of a security breach only the secure device (smart card in claim 1) has to be exchanged.

Reasons for the Decision

1. The appeal is admissible.

2. It is established jurisprudence of the boards of appeal that the purpose of the inter partes appeal procedure is mainly to give the losing party the possibility of challenging the decision of the opposition division on its merits. However amendments are to be fully examined as to their compatibility with the requirements of the EPC (see decision G 9/91, OJ EPO 1993, 408, points 18 and 19 of the reasons). The board has to examine whether the patent and the invention to which it relates meet the requirements of the EPC (Article 102(3) EPC). The fact that the respondent agreed that the patent should be granted on the basis of the patent proprietor's request (see point IX *supra*) is irrelevant in these circumstances.

Articles 84 and 123(2) and (3) EPC (amendments)

3. The board is satisfied that the amendments made by the patent proprietor do not give rise to objections under Articles 84, 123(2) and (3) EPC. The respondent has not disputed this.

Article 100(b) EPC - Sufficiency of disclosure

4. The respondent has not disputed in appeal proceedings the finding of the opposition division that the requirements of sufficiency of disclosure (ground for opposition under Article 100(b) EPC) were met. The board has no reason to question the opposition division's finding.

Novelty

5. The novelty of the subject-matter of claims 1 to 4 has not been disputed.

Inventive step

6. In the following, reference will occasionally be made to the reasoning of the opposition division in the appealed decision because the amendments to the claims made during the appeal proceedings are of such a nature that the reasoning of the opposition division remains relevant to a large extent.

7. Obviousness starting from D3

7.1 The decision under appeal started from D3 as the closest prior art, which generally deals with design issues of public key cryptosystems in a data communication network. However the board regards D3 as the wrong starting point because the choice of a suitable cryptographic protocol depends on the particular circumstances of the application. In other words, the requirements of a given application constitute determining factors for the cryptographic protocol to be used. Starting from the general issues in the design of a key distribution centre bears an increased risk of applying hindsight in the knowledge of the particular circumstances of the invention under consideration. In the board's view, D6, which relates to the same technical field as the invention, i.e. secure communications between two devices in a decoder of a pay TV system, should have been regarded as the closest prior art.

7.2 In any case, the reasoning in the decision under appeal starting from D3 does not convince the board for the following reasons.

7.3 It is true that random numbers are frequently used in encryption. However, in order to show that a particular use of a random number in a particular communication protocol was obvious, it is not sufficient to state that a random number may be used "wherever and whenever required" when particular advantages and technical effects are associated with that use.

7.4 The board is not convinced that the examples referred to in the decision under appeal suggest using a random number as claimed in the opposed patent. Messages 1 and 2 exchanged between the user device A and the key distribution centre KDC in figure 2 of D3 do not hint at using a random number (R) in combination with a random (session) key because these messages are exchanged to obtain a session key Ks from the KDC. If the random key is generated at the user device A, as in the alternative mentioned on page 7, line 31 of D3, then there is no need to exchange the random key with the KDC (indeed this should not be done to restrict the number of entities knowing the random key). In this alternative, references to the KDC could be avoided if the other's public key were known to both devices A and B. Then there would be no need for device B to call the KDC using a random number (R', as in messages 4 and 5). If device B has to call the KDC to obtain the public key of device A, device B sends a random number (R') but does not send a random key. Similarly, the random number (R'') sent in message 6 is sent in reply to the caller message 3, and there is no hint in D3 that a similar effect could be achieved by sending the random number with the caller message (see D3, page 7, paragraphs 1 and 2 and figure 2).

7.5 For the above reasons the board cannot share the reasoning in the decision under appeal as it includes *ex post facto* elements.

8. Obviousness starting from D6

8.1 The board regards D6 as the closest prior art because it relates to the same technical field as the invention, this being secure communication in a decoder (called a "descrambler" in D6) of a pay TV system between an information processor 10 (corresponding to the conditional access module in terms of the opposed patent) and a smart card 12 (D6, column 4, lines 28 to

39, and figure 1). D6 aims at avoiding piracy problems and allowing the system to be economically upgraded after a security breach (see column 2, lines 8 to 31). The smart card is used as a replaceable security element (12) cooperating with the information processor. The signal flow over the interface is protected by using a secret authentication key uniquely associated with the information processor, and preferably an additional authentication key of the smart card. The secret keys are stored in a secure RAM of the information processor and preferably also in the smart card, respectively (D6, figure 3; column 4, lines 49 to 55; column 5, lines 6 to 40; column 6, lines 11 to 19; column 7, lines 34 to 38; column 8, lines 1 to 9). During an initialisation phase, secret keys may be obtained from a trusted centre and transmitted in encrypted form to the smart card (D6, column 6, lines 26 to 59 and figure 2).

8.2 The methods and decoders of claims 1 to 4 aim at improving the security of communication between devices in a decoder for a pay TV system so that the risk of switching between authorised and unauthorised devices is reduced as far as possible (see paragraphs [0002], [0005] and [0017] of the patent specification).

8.3 The skilled person starting from D6 and confronted with this problem is assumed to be familiar with common general knowledge in the technical field of cryptology (as exemplified by D1). It is known therefrom that public-key cryptography can avoid the need for transmitting a secret key over an insecure channel. Two different keys, one public and the other private (secret), are used for this purpose. It is computationally hard to deduce the private key from the public key. Anyone with the public key can encrypt the message but not decrypt it. Only the person with the private key can decrypt the message. Every user has their own public key and private key. However public key algorithms are slow and vulnerable to chosen plaintext attacks (see, for instance, D1, pages 31 to 33). Therefore a hybrid cryptosystem, as presented on page 33 or on page 48 of D1, in which public-key cryptography is used to agree on a session key which is then used for symmetric encryption and decryption of subsequent transmissions, has advantages over the public-key algorithm. Other known protocols involve a trusted centre ("Trent") for obtaining a session key. In the latter protocol (D1, page 64), as in many other protocols, random numbers are also employed.

8.4 Although a great number of different protocols are described, there is no hint in D1 that it would be advantageous to start an authentication process by transferring both a random key and a random number encrypted using a public key and to rely on a single private key in certain circumstances. On an objective reading of the protocol examples in D1, a person skilled in the art would have understood that the names "Alice" and "Bob" simply stand for first and second participants (see D1, page 23, table 2.1), which are otherwise interchangeable because they are not part of a particular communication unit in a given application. Thus every participant is supposed to have a pair of public and private keys, the private key being the secret one which is stored at each participant's location, respectively, and never disclosed to anyone else (see D1, page 32, paragraph 3). This also applies to the examples which do not mention a second private key (because this is not needed in this phase of the communication; for example pages 33 and 48 of D1). Moreover, in all the examples of public-key protocols where a random number is involved, there are also two pairs of public and private keys which means that a private key has to be stored at each participant's location.

8.5 Similar considerations apply to the disclosure of D3. While it is true that three message steps (3, 6 and 7) may be sufficient if the session (random) key is generated at device A and the public keys are already known to A and B, both of these participants have their public and private keys and a random number is generated at the location of the called user device B and returned in the second message from the called user device B to device A.

8.6 The invention as specified in present claims 1 to 4 goes beyond a straightforward use of commonly known encryption protocols in secure communication between devices in a known decoder combination including a conditional access module and a smart card. It is based on the insight that it is sufficient to store only one secret key in a secure device (the smart card in claims 1 and 3, the conditional access module in claims 2 and 4). While, having knowledge of the invention, it can be easily deduced from the common general knowledge about public key encryption that a single secret key stored in a secure device and corresponding to the public key of a calling (insecure) device may be sufficient to securely exchange a session key (random key Ci) for the subsequent transmissions if the authentication and key exchange is started in the manner as claimed in the opposed patent, D1 and D3 do not provide any hints at this simple authentication procedure. In accordance with the opposed patent, the exchange of a random key (Ci) and a random number (A) make it possible to verify whether a smart card or a conditional access module are authorised. The calling conditional access module (in a decoder, claims 1 and 3) or the decoder (claims 2 and 4) therefore need not be secure devices because they do not need any secret key (in contrast to those of D6). Any breach of security can be countered by replacing only the secure part (the smart card in claims 1 and 3, or the conditional access module in claims 2 and 4). Once the secure device is authenticated, and as long as it is not removed, the subsequent transmissions are encrypted and decrypted with the random key which avoids the disadvantages of public key algorithms.

9. For the above reasons the board concludes that the subject-matter of independent claims 1 to 4 is not rendered obvious by the available prior art documents.

10. Hence the board is satisfied that, taking into consideration the amendments made by the proprietor during the opposition proceedings, the patent and the invention to which it relates meet the requirements of the EPC (Article 102(3) EPC).

Order

For these reasons it is decided that:

1. The decision is set aside.

2. The case is remitted to the first instance with the order to maintain the patent in the following version:

   Description:
   Columns 1 and 2 received during oral proceedings of 20 June 2007
   Columns 3 and 4 of the patent specification

   Claims:
   No. 1 to 4 received during oral proceedings of 20 June 2007

   Drawings:
   Figures 1 and 2 of the patent specification.

The Registrar: The Chairman:

D. Sauter F. Edlinger