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 27 September 2007

Case Number: T 0973/05 - 3.4.03

Application Number: 92301046.6

Publication Number: 0500245

IPC: G07F 19/00

Language of the proceedings: EN

Title of invention:
Cipher communication system for transaction data

Patentee:
KABUSHIKI KAISHA TOSHIBA

Opponent:
AXALTO SA

Headword:
-

Relevant legal provisions:
EPC Art. 56

Keyword:
"Inventive step (no)"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 0973/05 - 3.4.03

D E C I S I O N
of the Technical Board of Appeal 3.4.03
of 27 September 2007

Appellant: (Patent Proprietor)
KABUSHIKI KAISHA TOSHIBA
72, Horikawa-cho
Saiwai-ku
Kawasaki-shi
Kanagawa-ken 210-8572 (JP)

Representative:
Shindler, Nigel
Brookes Batchellor LLP
102-108 Clerkenwell Road
London EC1M 5SA (GB)

Respondents: (Opponent)
AXALTO SA
36-38, rue de la Princesse - B.P.45
F-78431 Louveciennes Cedex (FR)

Representative:
Cassagne, Philippe M.J.
Propriété Intellectuelle
36-38 Rue de la Princesse
BP 45
F-78431 Louveciennes Cedex (FR)

Decision under appeal:
Decision of the Opposition Division of the European Patent Office posted 24 May 2005 revoking European patent No. 0500245 pursuant to Article 102(1) EPC.

Composition of the Board:

Chairman: R. G. O'Connell
Members: G. Eliasson
U. Tronser

Summary of Facts and Submissions

I. This is an appeal against the revocation of EP 0 500 245 for lack of inventive step having regard to the documents

E9: EP 0 422 230 A; and
E9a: WO 90 09 009 A.

Document E9 is a translation into English of document E9a published pursuant to Article 158(3) EPC, first sentence, after the priority date of the contested patent, so that document E9a alone forms part of the state of the art under Article 54(2) EPC.

The opposition appeal case was remitted for further prosecution by decision T 527/99 of Board 3.4.01.

II. In response to a communication of the present board accompanying a summons to oral proceedings, the appellant proprietor filed new claim requests with a letter dated 28 August 2007.

III. At the oral proceedings before the board, the appellant proprietor requested that the decision under appeal be set aside and the patent maintained on the basis of the main request or the auxiliary request both submitted with the letter dated 28 August 2007.

The respondent opponent requested that the appeal be dismissed or alternatively, that the case be remitted to the opposition division for further prosecution.

IV. Claim 1 of the main request reads as follows (labelling of features introduced by the board; board's emphasis marking differences over the claim which the opposition division found lacking in inventive step in the decision under appeal):

"1. A cipher communication system for communication transaction data between:

a first electronic device (1) comprising first memory means (3) for storing a key data, means (40) for generating a transaction key data which is to be used for enciphering the transaction data, means (2, 7) for enciphering the transaction key data in accordance with the key data, and means (4) for transferring the enciphered transaction key data;

and a second portable electronic device (21) comprising means (24) for receiving the enciphered transaction key data transferred from the first electronic device (1), second memory means (231) for storing the key data, means (22, 25) for deciphering the enciphered transaction key data received by the receiving means according to the key data in said second memory means (231); the second portable electronic device (21) further comprising third memory means (232) for storing the deciphered transaction key data;

and a terminal device (11) interposed between the first electronic device (1) and the second portable electronic device (21);

characterised in that

the first electronic device (1) is arranged to transmit a transaction key to the second portable electronic device (21) via the terminal device (11) before exchanging encrypted data with the terminal device (11)

and in that the second portable electronic device (21) includes data conversion means (25, 26) which is so arranged that encryption and decryption of all data received from and transmitted to the first electronic device (1) by the second portable electronic device (21) is performed by the second portable electronic device (21) itself;

f) and also in that the terminal device (11) includes means (42) for supplying power to the second portable electronic device (21) for activating the second portable electronic device (21), the second electronic device (21) including means (42a) for receiving the power supplied from the terminal device (11);

g) and also in that the third memory means (232) of the second portable electronic device (21) is a volatile memory whose memory is maintained by the power supplied from terminal device (11) but is cleared on interruption of the power supply by removal of the second portable electronic device (21) from the terminal device (11) so as to eliminate the stored transaction key data on completion of the cipher communication,

h) **and also in that the second portable electronic device (21) further includes means (22) for judging whether the key data has any abnormality, whereby the process is terminated, if there is any abnormality in the key data**."

V. Claim 1 of the auxiliary request differs from the main request in that the following passage is added at the end (labelling introduced by the board):

i) "and, when no abnormality has been found, for judging whether the data train length of the transaction key data is a multiple of 8, and if the length is not a multiple of 8, the process is terminated"

VI. The appellant proprietor presented essentially the following arguments in support of his requests:

(a) Claim 1 of the main request specified in feature h) a step of judging whether the key data has any abnormality, and if so, to terminate the cipher communication process. None of the cited prior art disclosed or suggested an IC card system in which, in addition to the security provided by an encrypted data transaction, and the clearing of the volatile memory when power is removed, the card was also protected by means for detecting an abnormal data input in this way. An unauthorised attempt to extract information from the card could be detected in this way.

(b) The distinguishing features (f) to (h) of claim 1 of the main request together contributed to

improving the protection of the stored data in the second portable device. Whereas features (f) and (g) related to the protection of data in the volatile memory of the second portable device, feature (h) improved the integrity of the system in respect of unauthorized tampering.

(c) As to the auxiliary request, feature (i) had the further effect of protecting the second portable device from tampering by terminating the process in case transaction keys of the wrong size were received.

VII. The respondent opponent presented essentially the following arguments:

(a) Claim 1 of both requests had been amended in several respects in the course of the opposition procedure in a manner which contravened Article 123(2) EPC.

(b) Features (h) and (i) introduced in the claims on appeal were not previously claimed and therefore not searched. In order to conduct a proper search on the above features, it was requested to remit the case for further prosecution.

(c) There was no synergy between features (f) and (g) on one hand and feature (h) on the other hand as they related to protecting the volatile and non-volatile memory, respectively, of the second portable device. Consequently, the added protection gained by introducing feature (h) had to be regarded as a mere aggregation. As checking

of stored data for any abnormality was commonplace in the art, there could not be any inventive merit in introducing feature (h).

(d) As to the auxiliary request, feature (i) related to protecting the second auxiliary device from tampering through feeding the device with transmission keys which were faulty, and therefore, this feature related to protecting a different aspect of the second portable device from those covered by features (f) to (h).

Reasons for the Decision

1. The appeal is admissible.

2. The respondent opponent argued that the amendments to claim 1 of both requests made in the course of the opposition procedure contravened Article 123(2) EPC (item VII(a) above). Furthermore, the case should be remitted for further prosecution, since the features introduced in the claims on appeal were not previously claimed and therefore not searched (item VII(b) above).

The board finds however that -putting the objections raised under Article 123(2) EPC to one side *arguendo*-- the subject matter of claim 1 of both requests does not involve an inventive step for the reasons below. Therefore, it is not necessary to remit the case for further prosecution.

3. *Inventive step - main request*

3.1 Document E9a was considered closest prior art in the decision under appeal and discloses a cipher communication system between a first electronic device 2, 5, 12 and a second portable device 3, 11 (see E9, Figures 1 and 2 with accompanying text). The first electronic device comprises first memory means for storing a key data km and means 15 for generating a transaction key data r1 which is to be used for enciphering the transaction data, means E1 for enciphering the transaction key data r1 in accordance with the key data km, and means for transferring the enciphered transaction key data (see in particular page 5, lines 21 to 24 and 30 to 31 of document E9). The second portable electronic device 3, 11 comprises means for receiving the enciphered transaction key data, a second memory means for storing the key data km, and means D1 for deciphering the transaction key data r1 using the key data km, a third memory means for storing the transaction key data r1 (page 5, lines 23 to 25 and 30 to 31). The transaction key data r1 is used by the encryption means E2 in the second portable electronic device 3, 11 to encrypt messages. A terminal 1 receives the second portable electronic device 3 to connect it to the first electronic device 2, 5, 12.

3.2 The subject matter of claim 1 of the main request differs from the system of document E9a in that:

f) the terminal device (11) includes means (42) for supplying power to the second portable electronic device for activating the second portable electronic device, the second portable electronic

device (21) including means (42a) for receiving the power supplied from the terminal device (11), whereas document E9a does not disclose any means for supplying power to the second portable electronic device;

g) the third memory means (232) of the second portable electronic device (21) is a volatile memory whose memory is maintained by the power supplied from the terminal device (11) but is cleared on interruption of the power supply by removal of the second portable electronic device from the terminal, so as to eliminate the stored transaction key data on completion of the communication, whereas document E9a does not disclose how the transaction key data is stored in the second portable electronic device; and in that

h) the second portable electronic device (12) includes means for judging whether if the enciphered key data has any abnormality, whereby the process is terminated, if there is any abnormality in the key data. Document E9a does not disclose any check of the key data.

3.3 In the decision under appeal, the opposition division was of the opinion that the skilled person would arrive at features (f) and (g) without exercising inventive skills for the reason that the second portable device would have to be supplied with electric power and the standard way of supplying power to an IC card was by means of the terminal receiving the card (feature (f)). Furthermore, there was no reason for the skilled person to store the transaction key data in any other type of

memory than in a volatile memory, which in any case had to be present in the second portable device of document D9a, as the transaction key is discarded on completion of the communication (feature (g)). The appellant proprietor did not contest this finding nor does the board consider that the opposition division erred.

3.4 Feature (h) has the technical effect of ensuring that the key data stored in a non-volatile memory in the second portable electronic device has not been corrupted, which can be the result of an attempt by an intruder to read out the key data (see item VI(a) above). Thus, feature (h) contributes to improving protection of the *key data* which has to be stored in a non-volatile memory, since it is kept permanently in the second portable electronic device. Features (f) and (g) on the other hand, contribute to improving the protection of the *transaction key data* by storing it in the *volatile* memory of the second portable electronic device.

3.5 Although the combination of the features (f) to (h) all contribute to improving the overall security of the second portable electronic device, it follows from the above that they aim at protecting different aspects, namely the integrity of the transaction key data and the key data, respectively. Therefore, the board cannot accept the appellant proprietor's contention that there would be any synergy arising from the combination of features (f) to (h) in the sense that there would arise a further technical effect beyond that resulting from the aggregation of the above features (see item VI(b) and VII(c) above).

Therefore, since feature (h) relates to solving a different technical problem from those solved by features (f) and (g), feature (h) can be treated independently from features (f) and (g) in the assessment of inventive step.

3.6 The board considers the introduction of a step of checking for any abnormality in the key data, and to terminate the communication process if any abnormality would be found, to be a measure the skilled person as a matter of routine would consider to take in order to prevent tampering with the second portable electronic device. As mentioned above, unlike the transaction key data r1 which in the method of document E9a is discarded after each communication session, the key data km is permanently stored in the second portable electronic device (see E9, page 5, lines 21 to 31). Therefore the security of the cipher communication system hinges on keeping the key data secret. Furthermore, it would also make sense to check that the key data has not been altered as a result of an error when storing the key data, since alteration of the key data would inevitably prevent any encrypted communication.

3.7 Hence, the skilled person would modify the system document E9a to include features (f) to (h) without employing inventive skills in the sense that he would choose any or all of these measures as a non-inventive selection from a number of such measures which are notorious in the cryptographic art. Therefore, in the board's judgement, the subject matter of claim 1 of the main request does not involve an inventive step within the meaning of Article 56 EPC.

4. *Inventive step - Auxiliary request*

4.1 In addition to features (f) to (h) mentioned above, the method of claim 1 of the auxiliary request is further distinguished from that of document E9a in that means are included for judging whether the enciphered transaction key data has a data train length which is a multiple of 8, and for terminating the cipher communication when the transaction key data does not have a length which is a multiple of 8 (feature (i)).

4.2 Feature (i) has the effect of detecting whether the encrypted transaction key data has been corrupted either because of errors in transmission or because of an attempt by an intruder to conduct cryptanalysis on the cipher communication system implemented in the second portable electronic device. Thus, feature (i) relates to a different aspect of enhancing the security of the second portable electronic device from those addressed by features (f) to (h). Therefore, feature (i) can be treated separately in the assessment of inventive step.

4.3 As discussed under item 3 above, the skilled person would consider modifying the system of document E9a to include features (f) to (h) without employing inventive skills.

4.4 As to feature (i), a check of the data train length of the enciphered transaction key data, the board likewise finds that the skilled person would as a matter of routine introduce - as a non-inventive selection amongst many notorious measures in the art - means for

checking the data train length of incoming data, in particular for the encrypted transmission key data, since as mentioned above, any errors in the encryption key would render the communication impossible. Furthermore, since data almost invariably is transmitted in form of an integer number of bytes, thereby making the data length automatically to be a multiple of eight, it would be natural to check whether the complete bytes have been received. Finally, it is a known strategy of launching cryptographic attacks in form of transmitting intentionally faulty data and monitoring the response of the cryptosystem. Therefore, the skilled person would also as a matter of mere routine choose to terminate the process whenever faulty data is received, in particular when the data relates to the transmission key data.

4.5 For the above reasons, in the board's judgement, the subject matter of claim 1 of the auxiliary request does not involve an inventive step within the meaning of Article 56 EPC.

Order

For these reasons it is decided that:

The appeal is dismissed.

Registrar | Chair

S. Sánchez Chiquero | R. G. O'Connell