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 November 2013

Case Number: T 1564/08 - 3.4.03

Application Number: 98925787.8

Publication Number: 985203

IPC: G07F7/10

Language of the proceedings: EN

Title of invention:
KEY TRANSFORMATION UNIT FOR AN IC CARD

Patent Proprietor:
MONDEX INTERNATIONAL LIMITED

Opponent:
Giesecke & Devrient GmbH

Headword:

Relevant legal provisions:
EPC 1973 Art. 56, 100(a), 114(2)
RPBA Art. 12(4)

Keyword:
Inventive step - (yes)
Late submitted material - document admitted (yes) regarding documents D4 and D5 - document admitted (no) regarding document D6

Decisions cited:
T 1002/92, T 0835/00

Catchword:

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 1564/08 - 3.4.03

D E C I S I O N
of Technical Board of Appeal 3.4.03
of 21 November 2013

Appellant: (Opponent)	Giesecke & Devrient GmbH Prinzregentenstrasse 159 81677 München (DE)
Respondent: (Patent Proprietor)	MONDEX INTERNATIONAL LIMITED 47-53 Cannon Street London EC4M 5SQ (GB)
Representative:	Robson, Aidan John Reddie & Grose LLP 16 Theobalds Road London WC1X 8PL (GB)
Decision under appeal:	**Decision of the Opposition Division of the European Patent Office posted on 6 June 2008 rejecting the opposition filed against European patent No. 985203 pursuant to Article 101(2) EPC.**

Composition of the Board:

Chairman: G. Eliasson
Members: T. M. Häusser
P. Mühlens

Summary of Facts and Submissions

I. The appeal of the opponent concerns the decision of the opposition division to reject the opposition filed against the European patent No. EP-B-985203 (Article 101(2) EPC). The opposition had been filed against the patent as a whole. Ground of opposition was lack of inventive step (Articles 100(a) and 56 EPC 1973).

II. At the oral proceedings before the board the appellant (opponent) requested that the decision under appeal be set aside and that the patent be revoked. The respondent (proprietor) requested that the appeal be dismissed (main request), or, that the patent be maintained in amended form on the basis of one of the first to third auxiliary requests filed with the Opposition Division and filed again with letter dated 18 October 2013.

III. The opposition had been based *inter alia* on the following documents:

D1: WO 93/20538 A1,

D2: "Angewandte Kryptographie", B. Schneider, Addison-Wesley, 1996, Seiten 58 und 61.

Furthermore, the appellant had filed for the first time with the letter setting out the grounds of appeal the following documents:

D4: "Handbuch der Chipkarten", W. Rankl, W. Effing, 2. Auflage, Hanser, München, Wien, 1996, Seiten 152-155,

D5: DE 3833241 A1,

D6: DE 19536169 A1.

Documents D4 and D5 were admitted into the appeal proceedings and document D6 was not admitted into the appeal proceedings.

IV. The wording of independent claims 1 and 7 as granted is as follows (board's labelling (i), ..., (vii), (I), ..., (XI)):

Claim 1:

(i) "A method for loading an application onto an IC card and comprising the steps of:
(ii) providing a secret key and public key for said IC card;
(iii) encrypting at least a portion of said application using a transfer key;
(iv) encrypting said transfer key using said IC card’s public key to form a key transformation unit;
(v) transmitting said encrypted application and said key transformation unit to said IC card;
(vi) decrypting said key transformation unit using said IC card’s secret key to recover said transfer key; and
(vii) decrypting said encrypted application using said recovered transfer key."

Claim 7:

(I) "An IC card system comprising
(II) at least one IC card;
(III) an application provider for providing an application to said at least one IC card;

(IV) a communications link coupled to said at least one IC card and said application provider;

(V) a public key and secret key set generated for said IC card;

(VI) a transfer key generated for use by said application provider; and

(VII) an application, and wherein the system is configured to encrypt at least a portion of said application by said application provider using said transfer key;

(VIII) to encrypt said transfer key using said IC card's public key to form a key transformation unit;

(IX) and to transmit said encrypted application and said key transformation unit to said IC card over said communications link;

(X) to decrypt said transmitted key transformation unit using said IC card's secret key to recover said transfer key;

(XI) and to decrypt said transmitted application using said recovered transfer key to recover said application."

V. The parties argued essentially as follows:

a) Admission of documents D4, D5, and D6 into the appeal proceedings

According to the opinion of the appellant (opponent) the documents were relevant and should therefore be admitted into the proceedings. Since in claim 1 reference was made to "at least a portion of said application" it was initially considered that the corresponding features were disclosed in document D1, in which an application key was described. Only in the

course of the proceedings before the first instance had it become clear that it had to be shown that the concept of loading an entire application onto an IC card was known to the skilled person.

The respondent (proprietor) was of the opinion that the documents should not be admitted into the proceedings. In particular, the respondent argued that according to the decision T 1002/92 a document should only be admitted into the proceedings at such a late stage if it was *prima facie* highly relevant. Since in particular the documents D4 and D5 were not relevant they should not be admitted into the proceedings. By arguing that the documents were not relevant, their admission into the appeal proceedings was implicitly objected to. Furthermore, from claim 1 as granted it emerged clearly that it was a feature of that claim that an entire application was loaded onto an IC card. Documents D4 and D5, which were intended to show such loading of an application, should therefore have been filed earlier.

b) Inventive step in relation to the granted claims

The appellant regarded document D1 as the closest state of the art from which the subject-matter of granted claim 1 differed in that it was an application that was loaded onto the IC card and in the protocol relating to the encryption, decryption and data transfer. These two points were independent of each other as evidenced by the fact that it was possible without any further changes to replace the word "application" by the word "data" in the opposed patent. The corresponding partial objective technical problems were to increase the lifetime of the IC card and to render the data transfer more comfortable, respectively. Document D4 was an excerpt from a textbook in the relevant art and would

therefore be considered by the skilled person. In particular, document D4 described in the second paragraph of section 5.10 that executable code, for example an encryption algorithm of an application provider, could be loaded onto a chip card after it had been personalized. Such a code could be regarded as an application within the meaning of that term in claim 1. Moreover, it was known from document D5 to load new applications onto a chip card in order to avoid manufacturing a new chip card whenever an application was changed. It would therefore be obvious for the skilled person to load an application onto the IC card instead of data in general as described in claim 1 of document D1. Furthermore, the claimed transfer protocol was described on page 61 of document D2. In particular, "M" corresponded to the application to be encrypted, "K" to the transfer key and steps (1), (2), (3), (4), (5), and (6) corresponded to claimed steps (iii), (ii), (iv), (v), (vi), and (vii), respectively. For the skilled person it would therefore be obvious to use that transfer protocol instead of that used in D1, which was incidentally described on page 58 of document D2, especially as these two protocols were the only possible alternatives. Consequently, the subject-matter of claim 1 did not involve an inventive step.

The respondent was of the opinion that it was impossible to formulate a relevant technical problem when starting from document D1 and referred in particular to the last paragraph of section I.D.3.3. of the book "Case Law of the Boards of Appeal of the EPO", 5th edition, December 2006. There was no logical chain of considerations leading from document D1 to the claimed invention. Furthermore, formulating two partial problems was inappropriate because the corresponding features were functionally related: firstly, it was the

application which was encrypted and loaded; furthermore, the combination allowed different application providers to securely load applications and the applications to be encrypted using a computationally less expensive encryption scheme, e.g. a symmetric encryption scheme. Rather, the invention allowed to load the application under the control of the user without involving the card issuer. The object of D1 was to avoid that a secret key had to be put on the card by the card manufacturer since it would then have at its disposal all the information necessary to decipher communications with the card as described in particular on page 1, lines 19-24 of document D1. The transfer algorithm described on page 62 of D2 was therefore contrary to the teaching of D1 as it would require a secret key to be put on the smart card. Furthermore, D1 described a one-time-only transmission of the application key: the routines C1 to C3 were to be deleted after transmission. Moreover, the executable code described in D4 could not be considered to be an application within the meaning of the term as used in the patent and could therefore not extend the lifetime of the card, either; rather, an application performed a function for a user, e.g. that of an electronic purse (see the patent, column 1, line 20). In addition, the teaching of D4 in fact discouraged the loading of programs onto a chip card. It would therefore not be obvious for the skilled person to arrive at the claimed subject-matter.

Reasons for the Decision

1. Admissibility

The appeal is admissible.

2. Admission of documents D4, D5, and D6 into the appeal proceedings

2.1 Documents D4, D5, and D6 were cited for the first time by the appellant in its letter setting out the grounds of appeal. Article 12(4) RPBA is therefore of particular relevance.

According to Article 12(4) RPBA, everything presented by the parties under Article 12(1) RPBA, in particular the statement of the grounds of appeal (Article 12(1)(a) RPBA), shall be taken into account by the board if and to the extent it relates to the case under appeal and meets the requirements of Article 12(2) RPBA, the board having the power to hold inadmissible facts, evidence or requests which could have been presented or were not admitted in the first instance proceedings.

2.2 In particular, the documents D4, D5, and D6 were cited in relation to the assessment of inventive step of the subject-matter of claim 1 as granted. The objection as to lack of inventive step had already been raised by the appellant in its notice of opposition. The documents could therefore have been presented during the first instance proceedings. Consequently, the board has the power not to admit documents D4, D5, and D6 under Article 12(4) RPBA.

2.3 The respondent raised for the first time during the oral proceedings before the board the objection that documents D4 and D5 should not be admitted into the appeal proceedings. Previously, in his reply to the letter setting out the grounds of appeal the respondent had merely argued in relation to inventive step of the granted claims and in particular that the skilled

person would not have combined document D1 with the teaching of documents D4 or D5 in the manner alleged by the appellant.

The respondent's argument that he had implicitly objected to the admission of the documents D4 and D5 by arguing that they were not relevant, is not convincing. In fact, in the annex to the summons to oral proceedings issued to the parties under Article 15(1) RPBA the board explicitly pointed out that the respondent appeared not to have objected to the admission of documents D4 and D5 into the proceedings and that the board was of the provisional opinion that these documents should be admitted into the appeal proceedings. If it was the respondent's intention to raise the objection against the admission of these documents, he should have done so at least in reply to the board's summons. However, even in the letter filed subsequently to the summons to oral proceedings, the respondent did not raise the objection against the admission of documents D4 and D5. Rather, the respondent put forward arguments concerning inventive step of claim 1 as granted and filed first, second and third auxiliary requests.

Under these circumstances, in the board's judgment it would be contrary to procedural fairness not to admit documents D4 and D5.

2.4 Referring to the decision T 1002/92 of the Boards of Appeal, the respondent argued that documents D4 and D5 should not be admitted into the appeal proceedings because they were not relevant. In exercising the power not to admit documents, the board can indeed make the admission of the documents dependent upon whether they are *prima facie* (highly) relevant. However, the board

is not required to do so because otherwise an opponent could always file a (highly) relevant document for the first time e.g. with the letter setting out the grounds of appeal and rely on its admission into the appeal proceedings because of its relevance. This would in effect undermine the nine-month opposition period.

In the present case the board decided to leave the question as to the relevance of the documents D4 and D5 open at this stage, because - having regard to the procedural considerations mentioned above under point 2.3 - the board did not find it justified not to admit documents D4 and D5 into the appeal proceedings.

2.5 Document D6 was merely cited by the appellant in his letter setting out the grounds of appeal. However, neither during the written stage of the appeal proceedings nor during the oral proceedings before the board, the appellant provided any indication as to why that document was cited. Consequently, the board sees no reason why document D6 should be admitted to the proceedings.

2.6 In view of the above documents D4 and D5 were admitted into the appeal proceedings and document D6 was not admitted into the appeal proceedings.

3. Inventive step in relation to the granted claims

3.1 Closest state of the art

The appellant regarded document D1 as the closest state of the art. Indeed, like the invention document D1 is conceived for transferring data onto an IC card and has relevant technical features in common with it. Therefore, the board sees no reason to differ from the

appellant's opinion regarding document D1 as the closest state of the art.

3.2 Distinguishing features

3.2.1 It is common ground between the parties that the subject-matter of claim 1 as granted differed from the method disclosed in document D1 in that it was an application that was loaded onto the IC card and in the protocol relating to the encryption, decryption and data transfer.

3.2.2 Indeed, document D1 discloses (see page 4, last paragraph - page 8, first paragraph; Figure 1) a communications system 2 including a key generation center (KGC) 4 and a smart card 6. The KGC 4 may be implemented by a personal computer 9 which is adapted to be connected to the smart card 6 by a public switched telecommunications network 12 on a telecommunications line 14. The smart card 6 includes a microprocessor 16, a memory 18, a random number generator 19 and a communications interface 20 for connection to the line 14 or to a smart card reader 21. The computer 9 includes software to compute a Mont_power(a, b, m) function, which is a variation of the RSA algorithm. The computer 9 also includes software to generate from the product of two primes p and q a large number m, which is difficult to factorize, and a decryption key d.

The number m is provided to the card manufacturer which stores it in the memory 18 of the smart card 6. The smart card 6 is also loaded with executable code to include the routines C1, C2 and C3 for respectively generating a random number r using the random number generator 19, calculating x = Mont_power(r, b, m) with

b selected to be equal to 3, and for exclusive-ORing 512 bits of data with r.

When the smart card 6 is connected to a point of sale terminal 21, the routine C1 generates a random number r, which is then encrypted using the routine C2 to generate x. The latter is provided on the line 14 to the KGC 4 where it is decrypted using r = Mont_power(x, d, m). The KGC 4 then produces an application key K_i which is encrypted on the basis of the random number r to obtain ciphertext X, which is subsequently transmitted to the smart card 6. The card 6 is able to decrypt X to obtain K_i using the random number r and the routine C3. The application key K_i can then be used in applications which are loaded on the smart card 6 and as a basis for generation of session keys for subsequent communications.

3.2.3 The subject-matter of claim 1 differs therefore from the method of D1 in that the method comprises

(i)' loading an application onto an IC card,

(iii)' encrypting at least a portion of said application;

(v) transmitting said encrypted application and said key transformation unit to said IC card;

(vii) decrypting said encrypted application using said recovered transfer key.

3.3 Objective technical problem

3.3.1 In the decision under appeal the opposition division was of the opinion that the problem to be solved consisted in improving the lifetime of the card by securely loading an additional application after the

issuance of the card. Indeed, it had already been described in the specification of the opposed patent (see paragraph [0006]) that the capability of adding applications onto the IC card subsequent to issuance was necessary to the longevity of the IC card; otherwise the IC card would become useless once an application became outdated. The distinguishing feature (i)' is therefore considered to improve the lifetime of the IC card, when "lifetime" is understood within the above meaning.

However, in order to avoid an *ex post facto* view being taken of the inventive activity, the objective technical problem must be so formulated as not to contain any pointer to the technical solution of the problem. There should thus be no reference to loading an application in the formulation of the technical problem.

3.3.2 The appellant argued that increasing the lifetime of the IC card was merely a partial technical problem corresponding to the distinguishing feature of loading an application onto the IC card. A second partial problem corresponding to the transfer protocol consisted in rendering the data transfer more comfortable.

Such a formulation of partial technical problems may be appropriate in the case where there is a mere aggregation of features and there is no functional interaction between the features. However, in the present case the distinguishing features are related to loading an application onto the IC card (distinguishing feature (i)') and to the transfer protocol, which involves encrypting at least a portion of that application and transmitting and decrypting the

encrypted application (distinguishing features (iii)', (v), and (vii)). Hence, all these features concern the application and the distinguishing features are functionally interrelated. In the present case it is therefore appropriate to formulate one single objective technical problem.

The advantage of the claimed transfer protocol is to obviate the need of sending the encrypted transfer key to the application provider before transmitting the encrypted application to the IC card, while still ensuring a secure transmission. Rather, the encrypted application is transmitted to the IC card together with the encrypted transfer key. In this sense the claimed data transfer is indeed "comfortable" and still secure.

3.3.3 The respondent argued that it was impossible to formulate a relevant technical problem when starting from document D1 as the closest state of the art; the skilled person would have no hint of the problem(s) solved by the invention. Reference was made in particular to the last paragraph of section I.D.3.3 in the book "Case Law of the Boards of Appeal of the EPO", 5th edition, December 2006.

3.3.4 That paragraph appears essentially unchanged in the same section of the current 7th edition of the above book and provides a summary of the decision T 0835/00.

First of all, the above paragraph does not appear in the context of defining the relevant objective technical problem but in the context of deciding whether a document can be considered as constituting the closest state of the art.

Furthermore, in the case of T 0835/00 a technical problem had been created which was unrelated to the actual disclosure of the proposed closest prior art document. The board in T 0835/00 thus held that it was a fatal defect that a prior art disclosure from which no relevant technical problem could be formulated without inappropriate hindsight had been chosen as a starting point for the application of the problem and solution approach.

However, in the present case document D1 is concerned with smart cards. It is even explicitly mentioned in document D1 that applications are loaded on the smart card 6 (D1, page 8, lines 3-5). The aim of improving the lifetime of the card - understood as indicated above - is therefore certainly related to the disclosure of document D1. Furthermore, it has been described in detail above under point 3.2.2 that data are transferred between the KGC 4 and the smart card 6. Hence, the aim of rendering the data transfer more comfortable is also related to the disclosure of document D1. Moreover, these aims do not contain any pointers to the claimed solution so that the objective technical problem can well be formulated based on these aims without inappropriate hindsight.

The respondent's arguments are therefore not convincing.

3.3.5 In view of the above, the objective technical problem is to improve, in a manner that enhances the comfort and ensures security, the lifetime of the IC card, where "lifetime" and "comfort" are understood as indicated above.

3.4 Obviousness

3.4.1 The appellant argued that it was known from documents D4 and D5 to load an application onto a chip card.

Document D5 describes (see column 1, line 3 - column 2, line 12) the programming of chip cards for several applications. The aim of document D5 is to provide a method to provide further applications to the card without deteriorating its safety arrangements. It is in particular envisaged to use the existing cryptological functions of the card to control the loading of new applications onto the chip card. The card issuer or a control entity may, when the card is first personalized, set a control flag for further applications to be loaded. The loading of the desired application is then possible. In this way the card issuer or control entity always keeps the control over loading applications onto the card.

As mentioned above, it is explicitly mentioned in document D1 that applications are *loaded* on the smart card 6 (D1, page 8, lines 3-5), without providing any details on how they had actually been transferred to the card. On the other hand it is mentioned in D5 as an inconvenience of the prior art chip cards that a new chip card has to be produced and programmed whenever the range of applications ("Anwendungsbereich") changes or expands. The board is therefore of the opinion that it would be obvious for the skilled person, when starting from D1, to load an application in order to solve the posed technical problem to improve, in a manner that enhances the comfort and ensures security, the lifetime of the IC card.

3.4.2 The appellant argued that it would be obvious for the skilled person to use the transfer protocol disclosed on page 61 of document D2 for transmitting the application in order to solve the posed technical problem, especially since there were only two alternative transfer protocols.

Apart from the two protocols described in D2 on pages 58 and 61, respectively, there are other protocols which could well be used for transmitting an application in a secure fashion to a smart card: for example, the application could be encrypted using asymmetric encryption (using a public key and a secret key set); or the application could be encrypted using a session key. The appellant's argument that there were only two alternative transfer protocols is therefore not convincing.

In fact, it is mentioned explicitly in document D1 on page 8, lines 3-5, that the application key can be used as a basis for generating session keys for subsequent communications. Since the application key is provided by the KGC 4 to the smart card 6 and is thus known to these entities, it is evident that the envisaged communication is to take place between the smart card 6 and the KGC 4. Furthermore, the application key stems from the KGC 4 and is to be used by the smart card 6 in applications loaded on the smart card 6 (*ibid.*). It can therefore be assumed that these applications are associated with the KGC 4. Accordingly, it would be natural for the skilled person, following the considerations mentioned above under point 3.4.1, to load an application onto the smart card 6 by transfer from the KGC 4 using a session key derived from the application key in order to ensure secure communication. The skilled person would therefore see

no reason to use the claimed transfer protocol for loading the application. The transfer method involving the session key would remain behind the claimed transfer protocol in terms of "comfort" as it would still involve sending the encrypted random number r to the KGC 4 before transmitting the encrypted application (using the session key) to the smart card 6.

3.4.3 Therefore, the subject-matter of claim 1 as granted involves an inventive step. Independent system claim 7 corresponds essentially to method claim 1. Claims 2 to 6 and 8 to 12 are dependent on claims 1 and 7, respectively.

Accordingly, the subject-matter of claims 1 to 21 as granted involves an inventive step (Article 52(1) EPC and Article 56 EPC 1973).

4. Conclusion

In view of the above, the appeal is to be dismissed in accordance with the respondent's main request. Under these circumstances the respondent's auxiliary requests need not be considered.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

S. Sánchez Chiquero G. Eliasson

Decision electronically authenticated