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) [X] To Chairmen

D E C I S I O N
of 21 January 1997

Case Number: T 0894/93 - 3.4.1

Application Number: 85901991.1

Publication Number: 0179104

IPC: G07F 7/10

Language of the proceedings: EN

Title of invention:
An apparatus communicating with data systems and a method of communicating with data systems

Patentee:
ASCOM NORDIC A/S

Opponent:
GAO Gesellschaft für Automation und Organisation mbH

Headword:
-

Relevant legal provisions:
EPC Art. 52(1) and 56

Keyword:
"Inventive step - yes"

Decisions cited:
T 0813/93

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 0894/93 - 3.4.1

D E C I S I O N
of the Technical Board of Appeal 3.4.1
of 21 January 1997

Appellant: (Opponent)
GAO Gesellschaft für Automation und Organisation mbH
Euckenstrasse 12
D-81369 München (DE)

Representative:
Klunker, Hans-Friedrich Dr.
Klunker, Schmitt-Nilson, Hirsch
Winzererstrasse 106
D-80797 München (DE)

Respondent: (Proprietor of the patent)
ASCOM NORDIC A/S
Park Allé 295
DK-2605 Brondby (DK)

Representative:
Plougmann, Ole
c/o Plougmann & Vingtoft A/S
Sankt Annae Plads 11
P.O. Box 3007
DK-1021 Copenhagen K (DK)

Decision under appeal: **Decision of the Opposition Division of the European Patent Office dated 12 August 1993 rejecting the opposition filed against European patent No. 0 179 104 pursuant to Article 102(2) EPC.**

Composition of the Board:

Chairman: G. D. Paterson
Members: U. G. O. Himmler
Y. J. F. Van Henden

Summary of Facts and Submissions

I. The Appellant had given notice of opposition to the granted European patent No. 0 179 104. By its decision of 1 July 1993 the Opposition Division rejected the opposition pursuant to Article 102(2) EPC and maintained the patent as granted.

The independent claims 1 and 15 read as follows:

"1. An apparatus (10,49) communicating with at least two different data systems (18, 40), having different secrecy and security levels, for receiving data originating from data read from a data carrying card (21, 22, 23, 24), for receiving a card identifying signal positively identifying the card (21, 22, 23, 24) as a card belonging to a first data system (40), or alternatively, as a card belonging to a second data system (18), and for transmitting the data originating from the data read from the card to said first data system (40), or alternatively, for verifying the authenticity of a person in possession of the card relative to said second data system (18), comprising:

a data input means (79) for receiving the data originating from the data read from the card (21, 22, 23, 24) and for receiving the card identifying signal,

an input means (46) for input of a personal authentication code,

a first storage means (80, 82) for storing a first encryption algorithm and a transmission protocol, a second storage means (85, 86) for storing a verification algorithm,"

an encryption means (82), controlled by the data input means (79) and the first storage means (80, 82), for encryption of the data and the code, so that, provided the card (21) is identified as a card belonging to the first data system (40), the data originating from the data read from the card and the code are encrypted by employing the first encryption algorithm stored in the first storage means (80, 82), and are output to the first data system (40) controlled by the transmission protocol stored in the first storage means, and

a comparator means (76), controlled by the data input means (79) and the second storage means (85, 86), for comparing the data originating from the data read from the card (22, 23, 24) and the code, so that, provided the card is identified as a card belonging to the second data system (18), an authenticity code is supplied to the second data system (18) in case the data originating from the data read from the card are verified in relation to the code by employing the verification algorithm stored in the second storage means, or alternatively, a non-authenticity code is supplied to the second data system in case the data originating from the data read from the card (22, 23, 24) are not verified in relation to the code by employing the verification algorithm stored in the second storage means."

"15. A method of communicating with at least two different data systems (18, 40) having different secrecy and security levels of receiving data originating from data read from a data carrying card (21, 22, 23,24) and of transmitting the data originating from the data read from the card (21, 22,

23, 24) to a first data system (40), or alternatively, of verifying the authenticity of a person in possession of the card relative to a second data system (18), comprising:

receiving the data originating from the data read from the card (21, 22, 23, 24), received from the reading means, as a card belonging to the first data system (40), as a card belonging to the second data system (18), or as a card belonging to neither of the data systems,

inputting (46) a personal authentication code (PIN), encrypting the data originating from the data read from the card (21) and the code, provided the card (21) is identified as a card belonging to the first data system (40), the data originating from the data read from the card and the code being encrypted by employing an encryption algorithm (82), and being output to the first data system (40) controlled by a transmission protocol, and

comparing (76) the data originating from the data read from the card and the code, provided the card is identified as a card belonging to the second data system (18), an authenticity code being supplied to the second data system in case the data originating from the data read from the card are verified in relation to the code by employing a verification algorithm, or alternatively, a non-authenticity code being supplied to the second data system in case the data originating from the data read from the card are not verified in relation to the code by employing the verification algorithm."

Against this decision the Opponent lodged an appeal and requested

- to set aside the appealed decision and to revoke the patent,

- auxilliarily, oral proceedings.

II. The Appellant requested the revocation of the patent for lack of inventive step having regard to the prior art cited during the opposition procedure:

D1: DE-A- 28 15 448
D2: DE-A- 27 40 467
D4: US-A- 4 219 151

III. The grounds of appeal filed with the Appellant's letter of 14 December 1993 as well as the Appellant's arguments brought forward during the oral proceedings held on 21 January 1997 can be summarized as follows:

The subject-matter of claim 1 lacks inventive step having regard to the documents D1 as well as D4 in combination with document D2 after eliminating the redundant and functional features from the independent claim 1.

In particular, the problem of transparency is emphasised by the patentee, but does not really exist and is theoretical and hypothetical. The alleged invention is nothing but the integration of two operation modes of a data system in one housing. However, such universally usable apparatus operating in on-line or off-line mode are generally known, e.g. from document D1.

Even if it were admitted that there would be two completely different and not compatible systems, then such an apparatus is nothing but the aggregation of two independent devices each of which is known per se, in a common housing. The one device has nothing in common with the other, and at the card entrance of the housing there is a switch which enables the connection to the one or the other system.

The same reasoning applies to method claim 15 which corresponds to apparatus claim 1.

IV. The Respondent (Patentee) contested these submissions of the Appellant and gave reasons why in his opinion the subject-matter of the independent claims is not obvious having regard to the state of the art. In particular, the Respondent argued that the underlying problem of the opposed patent was not known from the documents of the state of the art and therefore a solution of this new problem could not be derived from these documents.

V. At the conclusion of the oral proceedings,

- the Appellant requested the revocation of the patent in its entirety,

- the Respondent requested to dismiss the appeal and maintain the patent as granted,
  auxiliarily to maintain the patent in an amended form.

VI. The Board announced its decision to dismiss the appeal.

Reasons for the Decision

1. *State of the art*

D1 This document is concerned with an apparatus working in an "on-line" or "off-line" mode system depending on the extent of the envisaged bank transaction. For limited transactions the system works in an "off-line" mode, for transactions surmounting a certain risk or amount the system works in the "on-line" mode only. This known system is not suitable for cards of different types or companies. The system is not capable of distinguishing between first system "on-line" cards and second system "off-line" cards.

The main concern of this document is preventing the possibility of tapping the transmission lines when the system works in the "on-line" mode and thereby obtaining knowledge of important data such as the PIN number and the related account number. For preventing such tapping or other kind of fraud the system uses an encryption means for both operational modes.

D2 The apparatus described in this document and used for cash dispensing is able to distinguish between different cards of different companies and different authorization levels. Depending on the kind of card used there are provided "on-line" and "off-line" services; see page 5, last paragraph to page 6, first paragraph; page 6, last paragraph to page 7, 2nd paragraph; page 8, 1st and 2nd paragraph.

If the user is identified as an "on-line" authorized person, a PIN number has to be typed in by the user which is checked by a centralized computer. There is not provided any encryption of the PIN number or any other data when transmitted to the centralized computer.

If the user is entitled only to off-line services, a further evidence for the verification of the authorization has to be provided. The authorization is then verified by a comparison of the data on the card and the data on the further evidence.

The main relevant teaching of this document with respect to the subject-matter of the patent in suit is that the apparatus is able to distinguish between different types of cards.

D4 Document D4 relates to a cash dispensing apparatus with a card verification system which is able to switch between the on-line and the off-line operation mode. However, there is no mention, not even notionally, in document D4 that the apparatus could accept or distinguish between different types of cards and that the decision of the mode selector (16 in Figure 4) whether on-line or off-line operation is selected depends on the kind of card or the data on the card. The mode selector (16) in Figure 4 switches from one mode to the other according to business hours and availability of a transmission line, and does not depend on the data on the card; cf. column 4, line 68 to column 5, line 1 and column 7, line 25-41.

2. The only issue to be decided is that of inventive step.

3. *Underlying Problem*

The starting point of the present invention, in accordance with the description of the patent specification (cf. column 1, line 63 to column 2, line 15), is the fact that more and more card systems are being issued. This situation created a need for an apparatus which can be used by different kinds of cards and cards issued by different companies, in particular cards having different secrecy and security levels. Thus, in accordance with the established jurisprudence of the Boards of Appeal the closest prior art is document

D2 = DE-A- 27 40 467, because it is the only cited document which deals with different kinds of cards, e.g. cards attributed to different companies or different systems. It is explicitly stated in this document D2 that there are "direct" clients belonging to the same banking system and "indirect" clients belonging to other banking systems or companies. Direct and indirect clients are entitled to different services; cf. page 5, paragraph 3 and page 6, paragraph 1 of the description. The cards of the direct clients give access to the system via a personal identification number (PIN), whereas indirect clients need a further, "evidence producing" document in addition to the card in order to have access to the system.

The other cited documents D1 and D4 are not concerned with handling different kinds of cards but with operating one kind of card in two different modes, e.g. on-line and off-line mode. Therefore, choosing one of these documents as starting point of the invention would be a theoretical and artificial approach not in line with the Board of Appeal case law (see No. 3 of T 0813/93 with indication of further decisions).

Therefore, there were good reasons for a skilled person to select the content of document D2 as a basis for further development when considering the state of the art.

However, in document D2 there is no protection provided against cross-coupling of information and data from the one card system to the other card system. Both kinds of cards are checked in a first verification device (reference sign 2) for protection against faked cards, followed by a read-out station (4) for reading out the important data related to the intended operation, and only then follows a station (7) for distinguishing between the different kinds of cards. All such data, having been collected from the verification and read-out stations, is compiled and processed in the control and storing device (3), or they are sent to the comparator station (6) from where they are sent back to the control device (3) for further processing. There is no indication whatsoever to prevent cross-coupling in the control and storing device (3) or in the comparator (6) from the one card system to the other card system. Further there is no mention of any protection against tapping of the display (9) where on-line and off-line authorization is indicated or tapping of the data transmission lines (21) from and to the central main computer.

Starting from this prior art document the objective problem to be solved by the present patent is eliminating the risk of providing transparency to the first data system (or the high secrecy and high security data system) from the second data system (or the low secrecy and low security data system); see column 2, line 16 to 43 and column 4, line 15 to 19 of the patent specification corresponding to page 2, line 22 to page 3, line 6 and page 5, lines 6 to 9 of the originally filed documents.

4. *Inventive step*

The essential difference between the subject-matter of Claim 1 of the patent in suit and the apparatus described in document D2 is that according to Claim 1, immediately after identification of the system to which the card belongs, the data read out from this card is strictly attributed to the related system, and the other system remains locked for this card.

Contrary to the apparatus of Claim 1, the apparatus according to document D2 uses for all kinds of cards the same control unit, storage and comparator units without any protection against penetration of a first category card into the system of the second category card or vice-versa.

The subject-matter of the independent apparatus claim 1 of the patent in suit is distinguished from the apparatus known from D2 by the following features:

According to the patent in suit there is provided

- a system communicating with at least **two different** data systems,

- a first system for transmitting the data originating from the data read from the card **to said first** data system

or alternatively

- a second system for verifying the authenticity of a person in possession of the card **relative to said second** data system,

- a **first** storage means for storing a **first encryption algorithm and a transmission protocol,**

- a **second** storage means for storing a verification algorithm,

- an **encryption means**, controlled by the data input means and the first storage means, for encryption of the data and the code, so that, provided the card is identified as a card belonging to the first data system, **the data** originating from the data read from the card **and the code are encrypted** by employing the first encryption algorithm stored in the first storage means, **and are output to the first** data system controlled by the transmission protocol **stored in the first** storage means,

- provided the card is identified as a card belonging to the second data system, an authenticity code is **supplied to the second data system** in case the data originating from the data read from the card are verified in relation to the code by employing the verification algorithm **stored in the second** storage means

or alternatively

- a non-authenticity code is **supplied to the second data system** in case the data originating from the data read from the card are not verified in relation to the code by employing the verification algorithm **stored in the second** storage means.

By these features the problem of transparency from one system to the other system is eliminated and solved.

Starting from document D2 as the closest prior art, the person skilled in the art would have taken into consideration the second closest prior art document D1 because this document provides a card system having different security levels and is particularly concerned with the protection of data derived from a card, even if this system can be used by one kind of card only.

When applying the teaching of document D1 to the apparatus known from document D2 with the aim to increase the security level of the system, the person skilled in the art would have replaced in the terminal of document D2 the control and storage unit (3) by the encryption, storage and control unit (18, 19, 20 in Figure 2) of D1. However, such a measure would not have led to the subject-matter of claim 1 which chooses a different solution for the transparency problem, i.e. a complete separation of both systems immediately after the identification of the card system by locking the reading, verification, encryption, storing and control means of the other system. The implementation of document D1 into the system of document D2 would not have solved the transparency problem, which does not exist in the system of document D1, because this system is not concerned with at least two different card systems and the possibilities of their mutual cross-coupling. The system of document D1 deals with preventing the tapping of data transmission lines to either the central main computer (3) or to the local storing unit (8). In this system, which uses for one and the same card system a common terminal for carrying out transactions requiring different security levels depending on the risk of the envisaged transaction, there is no protection against the possibility of giving a card carrying out a transaction of the low security level access to the encryption function in the jointly used storing-, control- and encryption-unit (18-19-20) of the common terminal.

The Board does not accept the argument of the Appellant that the claimed subject-matter is merely an aggregation of two well known systems jointly integrated in a common housing, the entrance of which is a card identification unit followed by an electronic distributing switch which leads the data read from the card either to the one or to the other system. In the Board's view this argumentation is based upon hindsight, because the skilled person would have either provided two completely separate terminals or, if he had intended to simplify and unify the two separate terminals, he would have commonly used as many parts as possible for both systems. The outcome would have been an apparatus put together from document D2 and document D1 as set out above.

5. For the above reasons, in the Board's judgement, the subject-matter of the independent claim 1 as granted involves an inventive step within the meaning of the Article 56 EPC.

6. At the end of the oral proceedings both parties explicitly agreed, as the Appellant had already stated in his grounds of appeal (page 10, last paragraph), that the apparatus claim 1 corresponds completely with the independent method claim 15 and that therefore the same reasoning applies to method claim 15 as to apparatus claim 1.

Also the Board is of this opinion.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

M. Beer G. D. Paterson