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) [ ] No distribution

DECISION
of 3 December 2003

Case Number:	T 0582/00 - 3.4.1
Application Number:	93918853.8
Publication Number:	0674795
IPC:	G07F 19/00
Language of the proceedings:	EN

Title of invention:
Combination pin pad and terminal

Patentee:
INTERNATIONAL VERIFACT INC.

Opponent:
Giesecke & Devrient GmbH

Headword:
-

Relevant legal provisions:
EPC Art. 100(a), 52(1), 56

Keyword:
"Inventive step (yes)"

Decisions cited:
-

Catchword:
-

Case Number: T 0582/00 - 3.4.1

DECISION
of the Technical Board of Appeal 3.4.1
of 3 December 2003

Appellant:
(Opponent)

Giesecke & Devrient GmbH
Prinzregentenstrasse 159
D-81667 München (DE)

Representative: -

Respondent:
(Proprietor of the patent)

INTERNATIONAL VERIFACT INC.
79 Torbarrie Road
Toronto,
Ontario M3L 1G5 (CA)

Representative:

Brooks, Nigel Samuel
Hill Hampton,
East Meon
Petersfield,
Hampshire GU32 1QN (GB)

Decision under appeal: **Decision of the Opposition Division of the European Patent Office posted 23 March 2000 rejecting the opposition filed against European patent No. 0674795 pursuant to Article 102(2) EPC.**

Composition of the Board:

Chairman: H. K. Wolfrum
Members: R. Q. Bekkering
J. H. P. Willems

Summary of Facts and Submissions

I. The appellant (opponent) lodged an appeal against the decision of the opposition division, dispatched on 23 March 2000, rejecting the opposition against European patent No. 0 674 795. The notice of appeal was received on 15 May 2000, the appeal fee being paid on the same day, and the statement setting out the grounds of appeal was received on 25 July 2000.

II. Opposition had been filed against the patent as a whole, based on Article 100(a) EPC on the grounds of lack of inventive step (Articles 52(1), 56 EPC).

III. In the appeal proceedings reference was made to the following documents:

D1: EP-A-0 186 981

D2: US-A-4 183 085

D3: EP-A-0 456 548

D4: US-A-4 900 903

D5: A. Beutelspacher ea, "Chipkarten als Sicherheitswerkzeug", Springer Verlag Berlin, 1991, page 136

IV. Oral proceedings were held on 3 December 2003.

V. The appellant requested that the decision under appeal be set aside and the patent revoked.

VI. The respondent requested that the appeal be dismissed.

VII. Independent claims 1 and 10 of the patent as granted read as follows:

"1. A debit terminal (2) comprising a secure module(8), a display (6), a keyboard (4) and a non-secured portion (10), characterized in that said secure module (8) controls communication of data and prompts between said keyboard (4), said display (6), and said non-secured portion (10) of said terminal (2) in either clear text mode or secure text mode, said keyboard (4) allowing the entry of either clear text or secure text, said non secured portion (10) of said terminal (2) having a predetermined group of paired prompts and authentication parameters that are authorized for clear text mode, said secure module (8) having confirmation means to independently confirm the prompt of a prompt pair received from said non-secured portion (10) is a proper prompt for clear text mode prior to communication of said prompt to said display (6)."

"10. A point of purchase terminal (2) comprising a display (6), a secure module (8), a keypad (4), a non secure module (10), and a communication port (12) for communicating with an outside source, characterized in that said terminal (2) operates in either a clear text mode where data is transmitted in a non coded manner or in a secure text mode where data is transferred in a coded manner, said secure module (8) including means for receiving prompts to be used in clear text mode and means for generating an authentication parameter for each prompt and means for transmitting and storing each paired prompt and authentication parameter in said non

secure module (10), said non secure module (10) including means for instructing said secure module (8) to operate in clear text mode and to provide pairs of prompts and authentication parameters to said secure module (8) in clear text mode, said secure module (8) when operating in clear text mode including means for confirming each prompt by regenerating the authentication parameter for the prompt and only transmitting the prompt to said display terminal (2) if the regenerated authentication parameter matches the authentication parameter provided with the pair."

VIII. The appellant argued that the subject-matter of claim 1 was rendered obvious by the teaching of document D3 in combination with the teachings of documents D4 and D5. In particular, the subject-matter of claim 1 only differed from the terminal known from document D3 in that predetermined pairs of prompts and authentication parameters with corresponding confirmation means were provided. The transmission and display of prompts, as well as the processing of the entered data in either clear or secure text mode, were common in the terminals at issue, as demonstrated by documents D4 (cf column 9, second and third paragraph) and D5 (page 136, lines 14 to 16). Furthermore, the authentication parameter as defined in claim 1 could be nothing more than a flag-like parameter associated with the prompt, defining whether the secured portion of the terminal should operate in the clear or secure text mode. As such it was therefore obvious to provide this parameter paired with the prompt.

IX. The respondent submitted that although it was not disputed that prompts were known and commonly used, the provision of prompts associated with an authentication code was not suggested in any of the available prior art documents. In particular having regard to the teaching of document D3, the terminal of claim 1 did not require a burdensome checking of the entire program in order to attain confidence that it operated in the proper mode when the user entered data. Document D5 merely confirmed the, uncontested, fact that both prompts and the display of stars when entering a PIN were well known. Finally, the authentication parameter defined in claim 1 was unique to a given prompt and confirmed the authenticity of the prompt as a proper prompt for clear text mode. Thus it could not be taken for some flag-like parameter merely defining the mode of operation of the secure portion of the terminal.

Reasons for the Decision

1. The appeal complies with the requirements of Articles 106 to 108 and Rule 64 EPC and is therefore admissible.

2. *Inventive step*

2.1 Having regard to claim 1, the closest prior art is provided by document D3 (cf figure 3 and corresponding description), which discloses, using the terminology of claim 1 of the patent in suit, a debit terminal comprising:
a secure module (UTA), a display (LCD), a keyboard (CL) and a non secured portion (UTP),

the secure module controlling the communication of data between said keyboard, said display, and said non secured portion of said terminal in either clear text mode or secure text mode,
the keyboard allowing the entry of either clear text or secure text.

In the terminal of D3 (cf column 8, line 33 to column 9, line 7) a quasi-randomly selected partition of the transaction algorithm of the terminal stored in the memories (MV1, MV2, MM) of the non-secured portion of the terminal is transferred to the secure module. The authenticity of the transferred partition of the algorithm is verified by calculating, using an encryption algorithm, the corresponding signature in the secure module and comparing it with the respective signature stored in memories (DA, TA) of the secure module. According to D3 (cf column 1, lines 18 to 27), in the same terminal both secret data (eg a secret code) and non-secret data (eg the amount to be paid) are entered and the terminal authorises the fetching of the secret code (cf column 7, lines 55 to 58). There is however no explicit mention of the communication of a corresponding prompt to the display or of the verification of the authenticity of those partitions of the transaction algorithm specifically relating to any prompts by means of a corresponding authentication parameter.

Thus, the subject-matter of claim 1 differs from the terminal known from document D3 in that prompts are communicated and in that the non-secured portion of the terminal has a predetermined group of paired prompts and authentication parameters that are authorized for clear text mode. Furthermore, the secure module has confirmation means to independently confirm the prompt of a prompt pair received from the non secured portion is a proper prompt for clear text mode prior to communication of the prompt to the display.

2.2 This provides additional security for confidential data, such as a PIN, entered into the terminal. Accordingly, the objective problem to be solved by the patent in suit may be seen as providing improved security measures protecting the terminal from fraudulent attacks for retrieving confidential data.

2.3 The communication of prompts to the display indicating which data should be entered as such is common in the terminals at issue (see D4, column 9, lines 11 to 13 and 34 to 39). Accordingly, it would be obvious to the skilled person to include this feature in the terminal of D3 for requesting the entry of eg the PIN. However, document D3 verifies the authenticity of the transaction algorithm in general by checking randomly selected partitions of the algorithm for a match with their corresponding signatures. Although this verification, depending on the size of the partitions, need not be more time-consuming than the verification of a prompt, it does not specifically focus on any part of the algorithm particularly prone to fraudulent manipulation for retrieving eg the PIN.

2.4 Document D4 (cf column 9, lines 11 to 17) discloses a transaction system with a terminal and a card, each having a secure microprocessor (MPU). The terminal MPU causes a prompt to appear on the display requesting that the user enters a PIN. The PIN entered by the user is sent by the terminal MPU to the card MPU where it is checked against the PIN stored in the secret zone of the card's memory. If the number matches, the card MPU notifies the terminal MPU to proceed. Prompts requesting the input of non-confidential information are also provided (cf column 9, lines 33 to 40), whereby the information is displayed in clear text for confirmation.

Security is provided in the system by on the one hand making the terminal MPU physically secure, for instance by embedding it in epoxy and to form it integrally with a value dispensing unit (eg a printer head), and on the other hand by a mutual handshake recognition procedure between the card MPU and the terminal MPU (cf column 10, lines 20 to 55). The recognition procedure involves the card encrypting eg a random number N with a first key number k1 using a first encryption algorithm E1 and sending the resulting word W1 to the terminal MPU. The terminal MPU decrypts the word W1 with the inverse encryption algorithm E1' and the first key number k1. The result is then encrypted by the terminal MPU with the key number k1 and a second encryption algorithm E2 and the resulting word W2 sent back to the card MPU. The card MPU decrypts W2 with the key number k1 and the inverse of the second encryption algorithm E2' and compares the result with the number used in the first transmission. If the numbers match the MPU's are recognized as being authorized for the transaction. There is, however, no suggestion of confirming the authenticity of the prompts.

2.5 Document D5 (cf page 136, lines 14 to 16) discloses that in case the PIN is not limited to four digits, but is of variable length, no stars or other symbols should be displayed when the PIN is entered, since this would reveal the length of the PIN and thus facilitate a possible attack. Accordingly, document D5 shows that it was common to switch the terminal to some secure text mode, thereby affecting the output to the display, when a PIN is entered. However, document D5 does not explicitly mention the communication of prompts to the display, let alone the confirmation of the authenticity of prompts by means of a corresponding authentication parameter.

2.6 The appellant argued that the authentication parameter as defined in claim 1 could be merely data associated with the prompt, much like a flag, defining whether the secured portion of the terminal should operate in the clear or secure text mode. As it was well known to switch between clear text mode and secure text mode depending on whether the terminal was prompting for clear text or secure text, it would have been obvious to provide this parameter paired with the prompt to the secure module of the terminal. In order to be distinguished from such a flag-like parameter, it should have been clearly defined in claim 1 that the authentication parameter was a unique parameter generated for each prompt by an authentication process.

This argument was not found convincing. Although the board can only agree that more explicit wording could have been used in claim 1, it is sufficiently clear that the parameter serves to confirm the authenticity of the prompt and thus is distinguished from a parameter defining the mode of operation of the secure module of the terminal.

2.7 The remaining documents D1 and D2 referred to in the appeal proceedings are less relevant.

2.8 In view of the above, in the board's opinion the cited prior art cannot be held to render the claimed solution obvious. Therefore, an inventive step has to be recognised for the subject-matter of claim 1.

2.9 The same applies to the subject-matter of claim 10, which corresponds in substance to the subject-matter of claim 1 with some further limitations. Therefore, an inventive step has to be recognised for the subject-matter of claim 10 as well.

2.10 The remaining claims 2 to 9, 11 and 12 are dependent on either claim 1 or 10 and provide further preferred features of the terminal. The subject-matter of these claims therefore also involves an inventive step.

3. In view of the above, the grounds of opposition invoked by the appellant do not prejudice the maintenance of the patent as granted.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

R. Schumacher H. Wolfrum