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 24 January 2012

Case Number: T 0250/08 - 3.4.01

Application Number: 02795655.6

Publication Number: 1446759

IPC: G06K 1/00

Language of the proceedings: EN

Title of invention:
Transaction card system having security against unauthorized usage

Applicant:
Burchette, Robert, L., Jr.

Opponent:
-

Headword:
-

Relevant legal provisions:
EPC Art. 123(2), 54(1)(2), 56

Relevant legal provisions (EPC 1973):
-

Keyword:
-

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 0250/08 - 3.4.01

D E C I S I O N
of the Technical Board of Appeal 3.4.01
of 24 January 2012

Appellant: Burchette, Robert, L., Jr.
198 Burchette Road
Chesnee, SC 29323 (US)

Representative: Gray, James
Withers & Rogers LLP
Goldings House
2 Hays Lane
London SE1 2HW (GB)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 6 August 2007 refusing European patent application No. 02795655.6 pursuant to Article 97(1) EPC 1973.**

Composition of the Board:

Chairman: B. Schachenmann
Members: G. Assi
F. Neumann

Summary of Facts and Submissions

I. The European patent application No. 02795655.6 (publication number 1 446 759; International publication number WO 03/044721) was refused by the examining division which held that the sets of claims then on file did not meet the requirements of Articles 123(2) or 56 EPC 1973.

The examining division considered the following prior art documents inter alia:

(D1) US-A-6,016,476;
(D3) US-A-5,748,737;
(D4) US-B1-6,315,195;
(D5) EP-A-1 083 527.

II. The applicant (appellant) lodged an appeal, received on 4 October 2007, against the decision of the examining division. The appeal fee was paid on the same day. The statement setting out the grounds of appeal was received on 5 December 2007.

With summons of 9 August 2010 the appellant was summoned to oral proceedings scheduled to take place on 19 November 2010. A Board's communication was then issued on 24 August 2010.

After receipt of the appellant's letter of 19 October 2010 the oral proceedings took place on 19 November 2010 as scheduled. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of claims 1 and 2 filed at the oral proceedings with dependent claims and a

description to be adapted. After deliberation by the Board, the Chairman announced that the proceedings would be continued in writing.

With a communication of 25 November 2010 the Board invited the appellant to submit a complete set of claims, the dependent claims being adapted to claims 1 and 2 filed at the oral proceedings, and an adapted description.

With a letter of 15 February 2011 the appellant filed amended claims and description pages.

With a communication of 21 August 2011 the Board drew attention to some deficiencies of the application documents then on file.

With a letter of 30 November 2011 the appellant filed a new set of claims 1-39 and amended description pages 1a, 3 and 20. The appellant requested re-consideration of the application.

III. The application documents underlying the present decision are as follows:

- Claims 1-39 filed with the letter of 30 November 2011;
- Description page 1 filed with a letter of 6 February 2006;
- Description pages 1a, 3 and 20 filed with the letter of 30 November 2011;
- Description page 2 filed with the letter of 15 February 2011;

- Description page 4 filed with the statement setting out the grounds of appeal of 4 December 2007;
- Description pages 5-19 and 21 of the published application;
- Description page 22 filed with a letter of 25 April 2007; and
- Drawing sheets 1/7-7/7 of the published application.

IV. The wording of claim 1 reads as follows:

"*1. A transaction card system, said system comprising:*

a host (10);

a drone card (100) having a power source (160);

said host (10) having:

a host memory (82) configured to store account information regarding at least one transaction card;

an interface (70);

a user input device (40,50,60) configured to select a transaction card stored in said host memory (82); and

a processor (80) operatively coupled to said host memory (82), interface (70) and user input device (40,50,60), so that in response to input received from said user input device (40,50,60), said interface (70) transfers card data corresponding to a transaction card stored in said host memory (82) and a security code to said drone card (100) for generation of a readable identifier (130) by the drone card (100); and

the host (10) further comprises an authentication sensor (20) operatively coupled to said processor (80), wherein said authentication sensor (20) limits access to account information stored in said memory (82) based

upon input received by said authentication sensor (20), wherein

the security code is different for each transaction and is either generated based upon an algorithm residing on the host (10) or is selected from multiple security codes stored in the memory (82) of the host (10), said security code being capable of being transmitted by a reader to a central computer synchronized to expect said security code to authenticate a transaction, and said host (10) has a slot (14) to receive said drone card (100) during the data transfer operation from said host (10) to said drone card (100)."

The wording of independent claim 2 reads as follows:

"*2. A transaction card system, said system comprising:*

a host (10);

a drone card (100);

said host (10) having:

a host memory (82) configured to store account information regarding at least one transaction card;

an output circuit;

a user input device (40,50,60) configured to select a transaction card stored in said host memory (82); and

a processor (80) operatively coupled to said host memory (82), output circuit and user input device (40,50,60), so that in response to input received from said user input device (40,50,60), said output circuit writes card data corresponding to a transaction card stored in said host memory (82) and a security code to said drone card (100) in the form of a readable identifier (130); and

the host (10) further comprises an authentication sensor (20) operatively coupled to said processor (82), wherein said authentication sensor (20) limits access to account information stored in said memory based upon input received by said authentication sensor (20), wherein

the security code is different for each transaction and is either generated based upon an algorithm residing on the host (10) or is selected from multiple security codes stored in the memory (82) of the host (10), said security code being capable of being transmitted by a reader to a central computer synchronized to expect said security code to authenticate a transaction, and said host (10) has a slot (14) to receive said drone card (100) during the writing operation from said host (10) to said drone card (100)."

Claims 3-39 are dependent claims.

Reasons for the Decision

1. The revised version of the European Patent Convention ("*EPC 2000*") entered into force on 13 December 2007. In the present decision, reference is made to "*EPC 1973*" for the EPC valid until that time or to "*EPC*" for the EPC 2000 (EPC, 13th Edition, Citation Practice, pages 4-6) depending on the version to be applied according to Article 7(1), second sentence, of the Revision Act dated 29 November 2000 (Special Edition No. 1, OJ EPO 2007, 196) and the decisions of the Administrative Council dated 28 June 2001 (Special

Edition No. 1, OJ EPO 2007, 197) and 7 December 2006 (Special Edition No. 1, OJ EPO 2007, 89).

2. The appeal is admissible.

3. Amendments

3.1 The subject-matter of claim 1 results from the disclosure of the first embodiment according to Figures 1A to 4 of the published application.

This embodiment concerns a transaction card system comprising a host 10 and a drone card 100 (Figure 1A, 1B), the drone card having a power source 160 (Figure 4; page 14, lines 7-9).

The host 10 comprises:

- A memory 82 configured to store account information regarding at least one transaction card (Figure 2; page 8, lines 20-23; page 7, line 30 to page 8, line 3);
- An interface 70 (Figure 2);
- A user input device 40, 50, 60 configured to select a transaction card stored in the memory (Figure 2; page 7, lines 11-27);
- A processor 80 operatively coupled to the memory, interface and user input device, so that in response to input received from the user input device, the interface transfers card data corresponding to a transaction card stored in the memory and a security code to the drone card for generation of a readable identifier 130 by the drone card (Figure 2; page 8, lines 18-20;

Figure 6; page 11, lines 1-15; Figure 3B and 4A; page 13, lines 8-14; page 14, lines 21-23);

- An authentication sensor 20 operatively coupled to the processor, wherein the authentication sensor limits access to account information stored in the memory based upon input received by the authentication sensor (Figure 2; page 10, lines 1-12); and
- A slot 14 for receiving the drone card during the data transfer operation from the host to the drone card (Figures 1A, 1B, 1C; page 5, lines 25 and 26).

Moreover, the security code is different for each transaction (page 11, lines 18-23) and is either generated based upon an algorithm residing on the host (page 12, lines 1-3) or is selected from multiple security codes stored in the host memory (page 12, lines 10-12). The security code is capable of being transmitted by a reader to a central computer synchronized to expect said security code to authenticate a transaction (page 12, lines 12-18).

3.2 The subject-matter of independent claim 2 results from the disclosure of the further embodiment mentioned from page 16, line 22 to page 17, line 3 of the published application.

This further embodiment relates to a transaction card system comprising a host, which has an output circuit (rather than an interface), and a drone card. The drone card has a readable identifier which does not require continuous power to remain readable. Moreover, the output circuit writes card data corresponding to a

transaction card and a security code to the drone card in the form of a readable identifier.

Apart from said disclosed difference, it results from the published application that the transaction card system according to the further embodiment (claim 2) corresponds to that according to the first embodiment (claim 1).

3.3 Dependent claims 3-39 can also be inferred from the published application. Attention is drawn to the claims concordance table produced by the appellant in the letter of 30 November 2011, with which the Board agrees.

3.4 The description has been brought into conformity with the amended claims. The Board has no remarks in this respect.

3.5 Therefore, the present application has not been amended in such a way that it contains subject-matter which extends beyond the content of the application as filed (Article 123(2) EPC).

4. Novelty

4.1 Documents D1, D3, D4 and D5 concern transaction card systems comprising a host and a drone card.

However, the Board has no reason to depart from the examining division's view to consider D1 as the closest prior art for assessing novelty and inventive step. The appellant agreed with this view.

4.2 Using the terminology of present claims 1 and 2 as well as that of D1 (between brackets), D1 (Figure 1 with the corresponding description; claims 1 and 11) discloses a transaction card system comprising a host (PDA device 10) and a drone card (universal card 26).

The universal card 26 known from D1 is, for example, a magnetic card, an IC card and/or an EAROM card (D1, column 5, lines 25-29). Thus, the expression "*universal card 26*" means a card that may or may not have a power source.

With regard to the PDA device 10 known from D1, it comprises:

- A host memory (memory module 14) configured to store account information regarding at least one transaction card;
- An interface (smartcard reader/writer 30);
- A user input device (user interface/display 34) configured to select a transaction card stored in the host memory;
- A processor (CPU 12) operatively coupled to said host memory, interface and user input device, so that in response to input received from the user input device, the interface transfers card data corresponding to a transaction card stored in the host memory to the drone card;
- An authentication sensor (biometric sensor 40) operatively coupled to the processor, wherein the authentication sensor limits access to account information stored in the host memory based upon input received by the authentication sensor;

- A slot for receiving the drone card during the data transfer operation from the host to the drone card.

Moreover, the smartcard reader/writer 30 of the known PDA device 10 is for reading and writing information to and from various cards, e.g. magnetic cards, IC cards and/or EAROM cards, using known standards and techniques (D1, column 5, lines 25-29). In view of the writing function, it appears that the smartcard reader/writer 30 may be equated to the host "*output circuit*" that "*writes*" card data to the drone card, as recited in present claim 2. However, it may also be equated to the host "*interface*" that simply "*transfers*" card data to the drone card, as recited in present claim 1, because the function of reading and writing information implies the transfer of said information.

4.3 Therefore, the subject-matter of present claim 1 is novel over document D1 (Article 54(1),(2) EPC 1973) in view of the following features:

- The interface transfers, besides card data corresponding to a transaction card stored in the host memory, "*a security code*" to the drone card "*for generation of a readable identifier by the drone card*"; and
- "*the security code is different for each transaction and is either generated based upon an algorithm residing on the host or is selected from multiple security codes stored in the memory of the host, said security code being capable of being transmitted by a reader to a central*

computer synchronized to expect said security code to authenticate a transaction".

4.4 The subject-matter of present claim 2 is novel over document D1 (Article 54(1),(2) EPC 1973) in view of the following features:

- The output circuit writes, besides card data corresponding to a transaction card stored in the host memory, "*a security code*" to the drone card "*for generation of a readable identifier by the drone card*"; and
- "*the security code is different for each transaction and is either generated based upon an algorithm residing on the host or is selected from multiple security codes stored in the memory of the host, said security code being capable of being transmitted by a reader to a central computer synchronized to expect said security code to authenticate a transaction*".

5. Inventive step

5.1 The appellant considered the following two features of claims 1 and 2 as being essential:

(a) The security code is different for each transaction;
(b) The security code is generated within the host itself.

The former feature increased security of a transaction, whereas the latter one avoided the disadvantage of a

cumbersome process of connecting to a remote computer during the transaction.

5.2 With regard to feature (a), the appellant submitted that it was essential for avoiding the problem of skimming, in particular.

Although the published application does not explicitly address this particular problem, it mentions fraudulent use, for example through counterfeit (page 1, lines 14 and 15) and indicates that it is an object of the invention to provide a transaction card system which prevents unauthorized usage (page 1, lines 27-30).

Having regard to D1, Figure 4 shows a flow diagram illustrating a client/server mode of operation. According to this mode (column 9, line 65 to column 10, line 17), once a user is verified (step 110), a central server 60 (Figure 3) prompts the user to provide transaction limitations such as, inter alia, the period of time in which a temporary digital certificate will remain valid (step 112). The central server receives and processes the requested information so as to create the digital certificate encoded with the limitations submitted by the user (step 114). The central server then encrypts the digital certificate and downloads it into the digital certificate processing module 20 of the CPU 12 of the PDA device 10 (Figure 1) via a communication link L1 (Figure 3; Figure 4, step 116). Lastly, the digital certificate is stored in the memory 14 of the PDA device 10 (Figure 1). With a valid digital certificate, a local mode of operation can be performed.

Figure 5 of D1 shows a flow diagram illustrating an example of the local mode of operation. According to this mode (column 11, lines 15-50), once the user is verified (step 208), the digital certificate previously obtained in the client/server mode of operation is retrieved from the memory 14 of the PDA device 10 and loaded into the digital certificate processor module 20 (Figure 1). This module processes the digital certificate to determine whether the digital certificate is still valid, i.e. unexpired, and whether the use of the selected card has been prohibited or limited by the user during the client/server mode of operation (step 212). If the digital certificate is not valid, the selected card information will not be written to the universal card 26 (step 210). On the other hand, if the digital certificate is valid, the requested card information is retrieved from memory 14 and stored in the encrypter/decrypter module 24 (Figure 1). The selected card information is decrypted using an encryption key unique to the PDA device 10 (step 214). The decrypted card information is sent to the smartcard reader/writer 30 (Figure 1) where it is written to the universal card 26 (step 216). The universal card 26 is then removed from the smartcard reader/writer 30 and swept through the magnetic reading device of a transaction terminal 80 (Figure 3; Figure 5, step 218). The transaction information is thus sent to a financial institution 70 via a communication link L4 (Figure 3; Figure 5, step 220). In a more advanced transaction terminal 80, the universal card 26 may be overwritten with a receipt of the transaction (step 222).

Before carrying out a transaction with the system of D1, a user can set a short period of time in which the temporary digital certificate remains valid. In such a case, a third party, for example a waiter in a restaurant to whom the user hands over a transaction card for paying the bill, may succeed in fraudulently copying, or "*skimming*", information from the transaction card during this short period of time, in the hope of being able to make an illegal transaction later on. However, assuming that the third party indeed tries to make such an illegal transaction, this may be refused depending on whether the temporary digital certificate is still valid or not.

However, whether or not the transaction card system known from D1 already solved the skimming problem may be left open. An essential issue is rather the fact that according to feature (a), the security code which is written to the drone card is changed with each transaction. As will be shown below, this feature is neither disclosed by D1 nor may it be considered obvious.

The operational mode of D1 discussed above requires two levels of security checks before the universal card can be employed, namely the user must be verified and the digital certificate must be valid. It will be clear that this mode of operation is different to that claimed in the present application. In particular, in D1, the transaction card information will not be written to the universal card if either of these security checks fails. The PDA device of D1 does not transfer a security code to the universal card and indeed there is no need, in this scenario, to do so.

Any configuration of the PDA device enabling a security code to be transferred from the PDA device to the universal card cannot therefore be seen to be obvious.

In addition thereto, D1 (column 14, line 47 to column 15, line 25) refers to two further operational modes in which an "*authorisation number*", which may be considered as a security code, is required.

In the first case (Figure 6; column 12, line 30 to column 13, line 5), the universal card itself is not required to complete the transaction. This will be the case, for example, when a remote (for example, telephone) transaction is performed. Here, the desired transaction card information is not written to the universal card, but instead is displayed on the PDA device. An authorisation number which is a function of the unexpired digital certificate that was obtained from the central server in the client/server mode is also displayed on the PDA device. The authorisation number and the unique number identifying the universal card can be communicated to a merchant and serve to confirm that the user has been verified and that the digital certificate is still valid. Since no information is written to the universal card in this case, the operational context is very different to that of the claims of the present application. It cannot be seen to be obvious to configure the PDA device in this context to enable a security code to be transferred from the PDA device to the universal card.

In the second case (see column 14, line 47 to column 15, line 25), the PDA device may be used as a personal credit card centre whereby funds may be directly

transferred between individuals having such PDA devices via credit cards or debit cards (column 14, lines 47-51). As an example, the case is considered in which a user owes another user a certain amount of money (column 14, line 51 to column 15, line 25). In this context, to prevent fraudulent transactions, the authorisation number, which is generated upon user verification, may be used for only one transaction between the users (column 15, lines 9-15). The entire process, including user verification and subsequent generation of an authorisation number, must be subsequently repeated for each additional transaction between the users. Therefore also in this case, the authorisation number is not written to the universal card. Thus, even in the context where the universal card has some data written on to it and is used in combination with a one-time authorisation number, it cannot be seen to be obvious to configure the PDA device to transfer a security code to the universal card.

5.3 With regard to feature (b), the question arises whether the local mode of operation just discussed in accordance with Figure 6 of D1 may be understood as implying that the authorisation number is generated in the PDA device.

As described above, upon user verification, an authorisation number is generated which is used to inform a merchant that the user was properly verified (column 12, line 57 to column 13, line 5). It is not clear in D1 whether the authorisation number is generated in the PDA device without connection to a remote computer. However, in view of the fact that

feature (a) is not considered to be obvious, this question may be left open.

5.4 It results from the foregoing that the security of the transaction card system of D1 essentially relies on the operation of downloading a temporary digital certificate to the PDA device before a transaction takes place. For carrying out the transaction, if the digital certificate is valid, the selected card information is locally decrypted using an encryption key unique to the PDA device and then either transferred to the universal card or displayed on the PDA device.

Starting from the disclosure of D1, the problem as defined by the appellant would consist in providing a card transaction system that improves security of the transaction with particular regard to the skimming aspect, the system itself being, at the same time, inherently safe, simply configured and compatible with existing transaction networks and protocols.

The appellant submitted that the claimed transaction card system relied on an improved security level due to the stand-alone character of the transaction card system in generating a security code which changes for each transaction (features (a) and (b) mentioned above). These features were not suggested by D1 nor by any of the other cited documents D3, D4 and D5, which were less relevant than D1.

5.5 The Board agrees with the appellant's view.

Moreover, the Board is aware of the use of so-called one-time-passwords (OTPs) in other contexts like, for example, internet online banking systems. Leaving open whether the use of such OTPs was prior art at the priority date of the present application (Article 54(2) and 89 EPC 1973), the Board finds convincing the appellant's submission that online banking networks were not compatible with transaction networks. For this reason, the skilled person would not regard the OTPs of online banking systems as a solution to the stated problem. Rather, the skilled person, starting from the transaction card system according to D1 and wishing to improve the transaction security, would rely on known solutions like the use of PINs or signatures.

5.6 The assessment of inventive step mentioned above equally applies to claim 1 and claim 2.

5.7 Therefore, the subject-matter of independent claims 1 and 2 involves an inventive step (Article 56 EPC 1973).

6. Further requirements

The Board holds that the application also meets the remaining relevant provisions of the EPC. Detailed remarks in this respect are not necessary.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the examining division with the order to grant a patent on the basis of the following documents:

- Claims 1-39 filed with the letter of 30 November 2011;
- Description page 1 filed with the letter of 6 February 2006;
- Description pages 1a, 3 and 20 filed with the letter of 30 November 2011;
- Description pages 2 filed with letter of 15 February 2011;
- Description page 4 filed with the statement setting out the grounds of appeal of 4 December 2007;
- Description pages 5-19 and 21 of the published application;
- Description page 22 filed with a letter of 25 April 2007; and
- Drawing sheets 1/7-7/7 of the published application.

The Registrar The Chairman

R. Schumacher B. Schachenmann