(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 August 2007 (23.08.2007)

PCT

(10) International Publication Number
WO 2007/093580 A1

(51) International Patent Classification:
G06F 21/20 (2006.01)

(21) International Application Number:
PCT/EP2007/051355

(22) International Filing Date:
12 February 2007 (12.02.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
MI2006A000284 16 February 2006 (16.02.2006) IT

(71) Applicant and
(72) Inventor: **BRUNAZZO, Mauro** [IT/IT]; Via Vittorio Veneto, 41, I-21010 Arsago Seprio Va (IT).

(74) Agent: **MITTLER, Enrico**; Mittler & C. s.r.l., Viale Lombardia, 20, I-20131 Milano (IT).

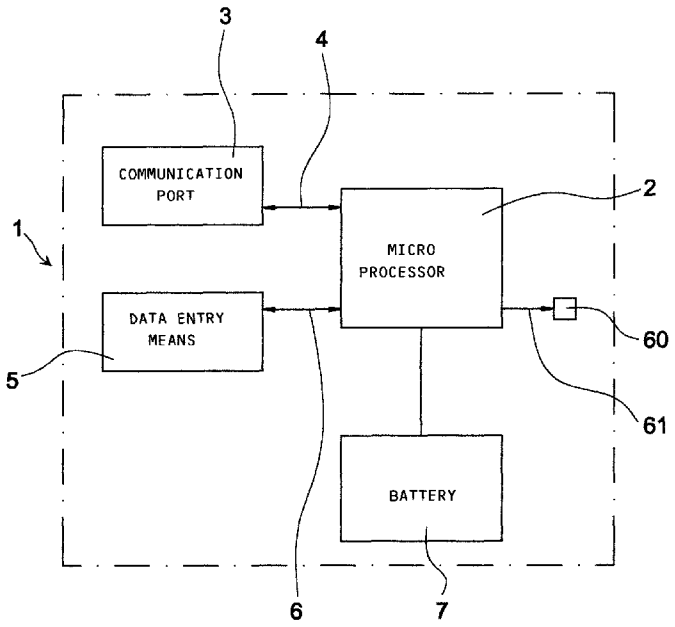
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** SMART CARD WITH IDENTITY CHECKING



(57) **Abstract:** A smart card is described, comprising a battery for electrical power supply (7), a port (3) for communication with an external reader, a microprocessor (2) with programmable access data, which normally keeps said communication port (3) in an inactive state, and data entry means (5), to allow the user of the card to input into said microprocessor (2) recognition data which can be compared with said access data; the microprocessor (2) can switch said communication port (3) into an active state suitable for communicat ion with the external reader. The data entered by the user can be secret codes or biometric data: this prevents utilisation of the card by users who are not recognised.

WO 2007/093580 A1

"Smart card with identity checking".

* * * *

The present invention concerns a smart card with identity checking.

The "intelligent card", also known as a "smart card", is an electronic card which stores information and puts it at the disposal of automatic devices, henceforth named "readers". The transmission of information occurs through a communication port, which can be of various types:

- with magnetic strip: in this case, the technique of reading/writing the data exploits variation of the magnetic field on a strip;
- with direct contact: in this case, the reader and the card are in contact to form an electrical circuit: the card is normally equipped with a microprocessor which, when powered by the reader, can transmit and receive data according to a pre-established communication protocol;
- without direct contact: in this case, the card, equipped with a microprocessor, receives energy from outside, through electromagnetic waves of suitable frequency, and exchanges data with the reader by means of radio waves.

The above types of card have become extremely widespread in recent decades. There is a continually growing number of computerised systems carrying out automatic functions for the supply of services, the distribution of goods or authorisation of access, and these systems operate even on an international scale. Operations such as the drawing of cash from Bancomat (ATM) machines, or the purchase of products from automatic vending machines, have now entered everybody's daily life. In what follows, the term "delivery of service" will be used for all these operations.

Normally, these computerised systems base their recognition of the user on the reading of a smart card, which is distributed by the issuing company, and which is to be inserted into a reader at the time of requesting the transaction or the purchase. If a higher level of security is required, the electronic card may be assigned a recognition code, generally known as a

"PIN" (from "Personal Identification Number"), which the user must enter on a keypad located in proximity to the reader: if the code entered does not match the PIN associated with the card, the system treats the user as not authorised to conclude the purchase of the goods or the transaction in progress.

However, the procedure for recognising the user can go wrong in a number of cases. The growing availability of cheap electronic equipment has allowed simple devices to be put together which are capable of fraudulently acquiring the PIN. There is a well-known proliferation of small videocameras and illicit keypad covering devices, which record the PIN as it is entered. It is also well-known that many users, in contravention of the recommendations of the issuing companies, are in the habit of keeping a written copy of their PIN in proximity to the card, for example in their wallet, or of storing it in their mobile phone. It is therefore possible, if a card is lost or stolen, for the recognition mechanism to be circumvented by unauthorised users.

In the current state of affairs, however, computerised systems based on recognition by means of an electronic card are so widespread that their replacement with more secure systems would be difficult to achieve, as well as being costly. The optimal solution should therefore bring to a higher level of security, but maintaining compatibility with existing systems, thus allowing the gradual replacement of traditional cards with others which are more secure.

The object of the present invention is to create a smart card with identity checking which enables the secure recognition of the user and is compatible with traditional recognition systems.

In accordance with the invention, this aim is achieved with a smart card comprising a battery for electrical power supply, a port for communication with an external reader, a microprocessor with programmable access data, which normally keeps this communication port in an inactive state, and data

entry means to allow the user of the card to input into said microprocessor recognition data which can be compared with said access data to enable the microprocessor to switch said communication port into an active state, suitable for communication with the external reader.

The card is thus normally inactive and capable of preventing its use by a reader until the moment when the authorised user is recognised.

Recognition of the user can occur through the entry of a numerical code on a keypad incorporated into the card, or else by means of a sensor which records a piece of biometric data, as for example the user's voice or fingerprint. The recognition code or biometric data thus entered is compared with the access data previously recorded in a permanent memory in the microprocessor at the time of issue of said card. If the recognition data coincides with the access data, the microprocessor activates the communication port to make the card usable for the operations for which it is intended; otherwise the card remains inactive.

Activation of the card can be associated with a signal, given by means of a luminous (LED, OLED) or acoustic signalling device.

In this way, the information stored in the memory associated with the microprocessor can be accessible from outside only if the card is used by an authorised user.

The effect of the authorisation can be timed and, for example, can allow the reading of the information by the reader for a preset period of time only, after which the communication port is once again deactivated by the microprocessor and, for further operations, a new recognition procedure is required.

Although it comprises various types of device, the card retains the dimensions of normal cards and is therefore totally compatible with current systems. Recognition of the user is performed inside the card. The reader has no knowledge of the existence of the recognition procedure used by the card: the said reader, therefore, does not require to be modified in any way.

It should be noted that, for the delivery of service to the user, two recognition procedures are necessary:

- the recognition procedure according to the invention, executed internally to the card, by means of which the microprocessor compares the access data with the recognition data;

- the traditional recognition procedure, executed by the computerised system through traditional operations (checking the information transmitted by the microprocessor to the communication port, possible checking of any PIN entered by the user on the keypad attached to the reader, checking of operations which may be carried out by the user).

Only in the case of recognition of the user by means of both the procedures will the user be authorised to obtain the service requested.

These and other characteristics of the present invention will be made more clearly evident from the following detailed description of some examples of practical embodiment which are illustrated without limiting effect in the attached drawings, in which:

figure 1 is a general block diagram of the smart card according to the present invention;

figure 2 shows a view of one of the two faces of an example of a card according to the invention, illustrating a communication port with magnetic strip; some devices included in the card are not shown;

figure 3 shows a view of the same card as in figure 2, illustrating the reading/writing devices on the magnetic strip;

figure 4 shows a view of one of the two faces of another example of a smart card according to the invention, illustrating a communication port with direct contact; some devices included in the card are not shown;

figure 5 shows a view of one of the two faces of a further example of a card according to the invention, illustrating a communication port without direct contact; some devices included in the card are not shown;

figure 6 shows a view of one of the two faces of a card according to the

invention, illustrating a keypad as a means of entering recognition data; some devices included in the card are not shown;

figure 7 shows a view of one of the two faces of a card according to the invention, illustrating a fingerprint sensor as a means of entering recognition data; some devices included in the card are not shown;

figure 8 shows a state diagram which exemplifies the procedure for loading the access data at a preliminary stage onto a card according to the invention;

figure 9 shows a state diagram which exemplifies the operation of a card according to the invention;

figure 10 shows a state diagram which exemplifies the operation of a traditional computerised system following the insertion into a reader of a traditional card or of a card according to the invention.

With reference to figure 1, a card 1 according to the invention is made up of a microprocessor 2, which can communicate with an external reader via a communication port 3, connected with said microprocessor 2 via a bi-directional path 4; said microprocessor 2 receives recognition data from a data entry means 5 via a unidirectional path 6. Said microprocessor 2 is powered by a battery 7. A signalling device (LED) 60 is controlled by the microprocessor 2 via the unidirectional path 61.

With reference to figure 2, an example of a card 10 according to the invention includes a communication port of the type with magnetic strip 12. In figure 2, neither the data entry means nor the battery are illustrated.

Figure 3 is an illustration of the said card 10, which shows the method by which the microprocessor 2 reads/writes to the magnetic strip 12: a plurality of reading/writing heads 13, normally not visible, each of them connected to the microprocessor, reads the data to be stored and writes it to said magnetic strip 12 in the process of writing the card. The writing having been performed, the heads 13 delete the information from the magnetic strip 12 at the moment when the card returns to the inactive state. By means of

said heads 13, the information is again written to said magnetic strip by the microprocessor 2 at the stage of activating said card 10, and re-deleted at the end of the period of activation.

With reference to figure 4, another example of a card 20 according to the invention includes a communication port of the type with direct contact 22. In figure 4, neither the data entry means nor the battery are illustrated.

With reference to figure 5, a further example of a card 30 according to the invention includes a communication port of the type without direct contact 32, which consists of an antenna. In figure 5, neither the data entry means nor the battery are illustrated.

With reference to figure 6, an example of a card 40 according to the invention comprises a keypad 42 as data entry means. In figure 6, neither the communication port nor the battery are illustrated.

With reference to figure 7, a card 50 according to the invention comprises a fingerprint sensor 52 as data entry means. In figure 7, neither the communication port nor the battery are illustrated.

It should be noted that card 1 according to the invention, in all its embodiments 10, 20, 30, 40 and 50, does not differ from traditional cards from the point of view either of bulk or of communication port, and can therefore be inserted into a traditional reader: compatibility between traditional computerised systems and the system according to the invention is therefore guaranteed.

With reference to figure 8, a state diagram is shown which represents the operations of loading the access data for the said card 1 according to the invention, at a preliminary stage. Said card is in the "virgin card" state 300, and has not yet been assigned any authorised user and is therefore not usable. The "loading access data" state 302 is reached when the authorised user enters the access data into the microprocessor for the first time, for example by making a fingerprint or typing a code into the keypad (event 301). This operation, which is carried out once only in the entire lifetime of

the card 1, is irreversible; it may be carried out by means of dedicated apparatus and by a trained operator, such as a staff member of the company providing the service; alternatively, if the data entry means is a keypad 42, it is possible for a factory code to be assigned to it, the same for all virgin cards, which is then changed by the user. At the end, the card becomes usable, and moves (event 303) to the "card inactive" state 300. At this point the card can be used in an unlimited number of operations, whenever the correct access data is entered by the user.

With reference to figure 9, a state diagram may be seen which represents the typical operation of said card 1 according to the invention, once the access data has been loaded into it by the procedure illustrated in figure 8. Normally, said card 1 is in a "card inactive" state 300. When a user enters input data, for example by making a fingerprint on a sensor 52 or typing a code into a keypad 42 ("signature entry" event 101), said card 1 changes to a "recognition" state 102, during which microprocessor 2 compares the data entered by the user with the access data stored earlier: if the comparison has a negative result, the card denies authorisation ("authorisation denied" event 103) and returns to the "card inactive" state 300. If, on the other hand, the comparison has a positive result ("authorisation" event 104), said microprocessor 2 transmits the information for the reader to said communication port 3, and said card 1 changes to "card active" state 105, during which said card 1 can be used; at the expiry of the preset time, microprocessor 2 deletes the information from the communication port 3 ("timeout" event 106), and returns to the "waiting" state 300.

With reference to figure 10, the process of recognition of the user by a traditional computerised system, into which the card 1 according to the invention is introduced, is also illustrated. The system is in the "system waiting" state 200; on the introduction of said card into a reader ("card introduction" event 201), the system changes to "recognition" state 202,

during which the said system effects the recognition of the user by checking the information obtained from said card 1 and transmitted by said communication port 3. If the recognition procedure has a negative result, the system denies authorisation to the user ("authorisation denied" event 203) and returns to "system waiting" state 200. It should be noted that for the system there is no difference between the case of the user committing an error in typing the PIN into the keypad, and the case of card 1 not being in "card active" state 105 because said card has not recognised the user. If recognition has a positive result, the system authorises the user ("authorisation of operations" event 204), leading to "service delivery" state 205, during which the system effects the delivery of the service requested by the user. At the end of the operations, when the service has been provided, the reader returns the card 1 ("end of operations" event 206), and the system goes back to "system waiting" state 200.

CLAIMS

1. Smart card comprising a battery for electrical power supply (7), a port (3) for communication with an external reader, a microprocessor (2) with programmable access data, which normally keeps said communication port (3) in an inactive state, and data entry means (5) to allow the user of the card to input into said microprocessor (2) recognition data which can be compared with said access data to allow the microprocessor (2) to switch said communication port (3) into an active state, suitable for communication with the external reader.

2. Card according to claim 1, characterised in that said communication port (3) is of the type with magnetic strip (12).

3. Card according to claim 2, characterised by comprising a plurality of heads (13) associated with said magnetic strip (12) and connected to said microprocessor (2) to enable the writing and deletion of information to the magnetic strip (12).

4. Card according to claim 1, characterised in that said communication port (3) is of the type with direct contact (22).

5. Card according to claim 1, characterised in that said communication port (3) is of the type without direct contact (32).

6. Card according to any of the preceding claims, characterised by comprising a keypad (42) as data entry means (5).

7. Card according to any of the preceding claims, characterised by comprising a fingerprint sensor (52) as data entry means (5).

8. Card according to any of the preceding claims, characterised by comprising a signalling device (60) which notifies the user that authorisation has occurred for using the card.

9. Card according to any of the preceding claims, characterised by being configurable into three states: a “card inactive” state (300), during which the microprocessor (2) keeps the communication port (3) inactive, thus preventing a reader from obtaining information; a “recognition” state

(102), during which the microprocessor (2) compares the recognition data obtained from the data entry means (5); a “card active” state (105), during which the microprocessor (2) activates the communication port (3), allowing a reader to obtain information.

10. Card according to any of the preceding claims, characterised by being able to communicate with readers of traditional type.

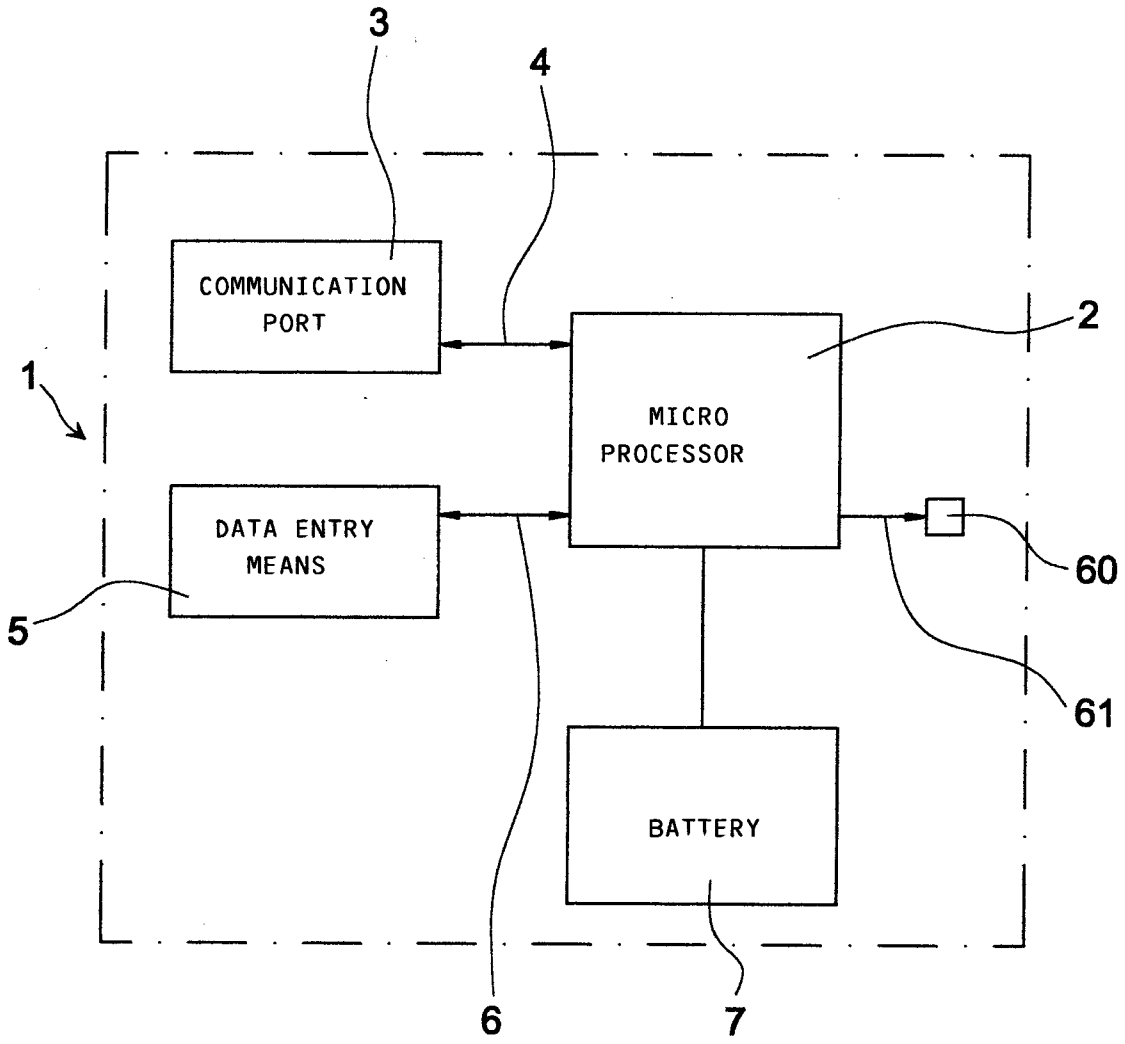

3
4
COMMUNICATION PORT
2
1
MICRO PROCESSOR
DATA ENTRY MEANS
60
5
61
BATTERY
6
7

Fig.1

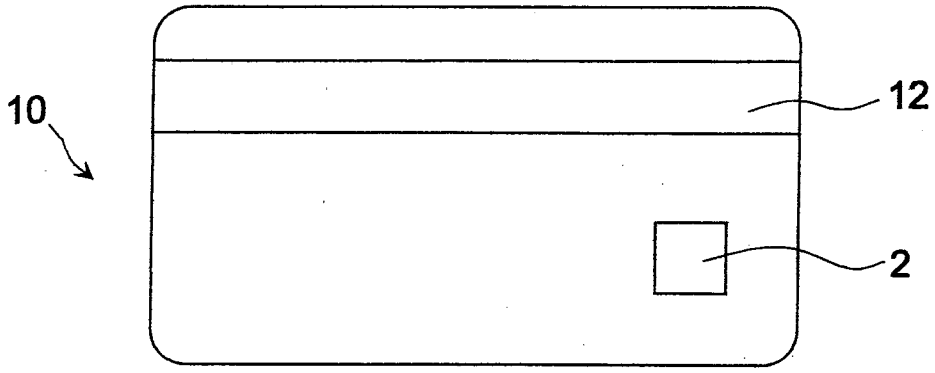


Fig.2

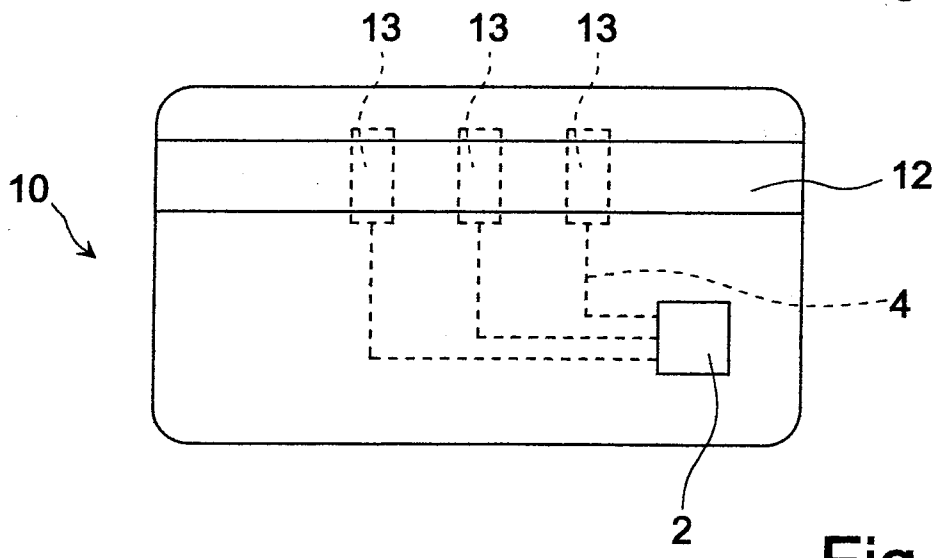


Fig.3

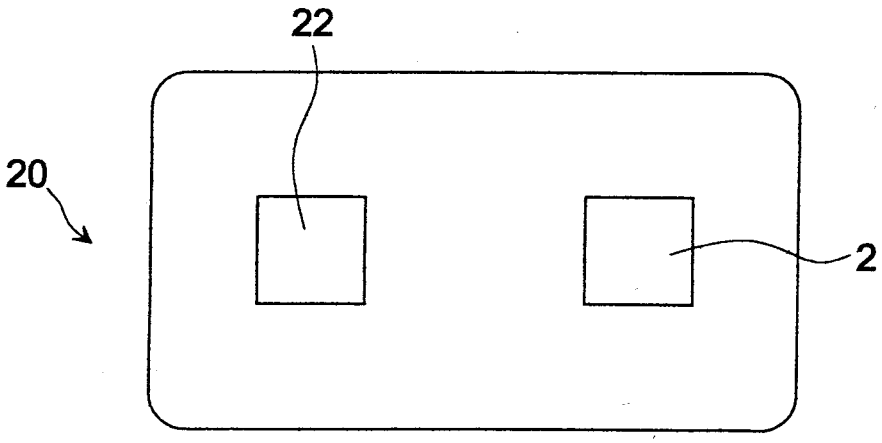


Fig.4

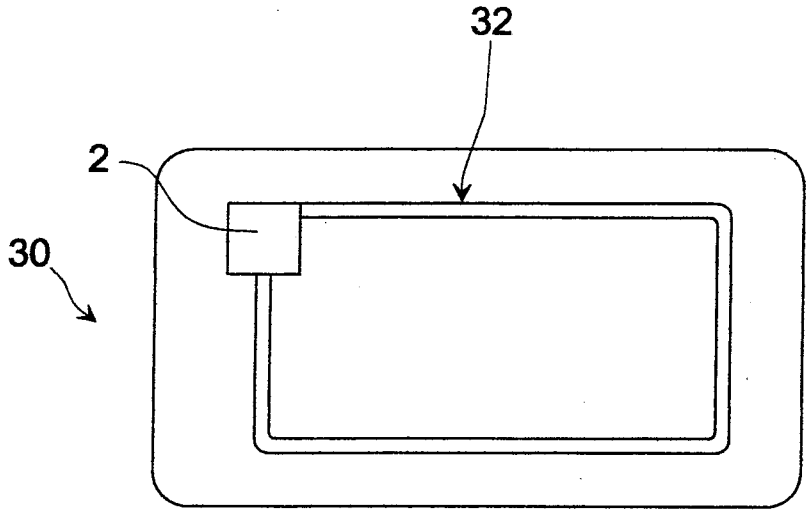


Fig.5

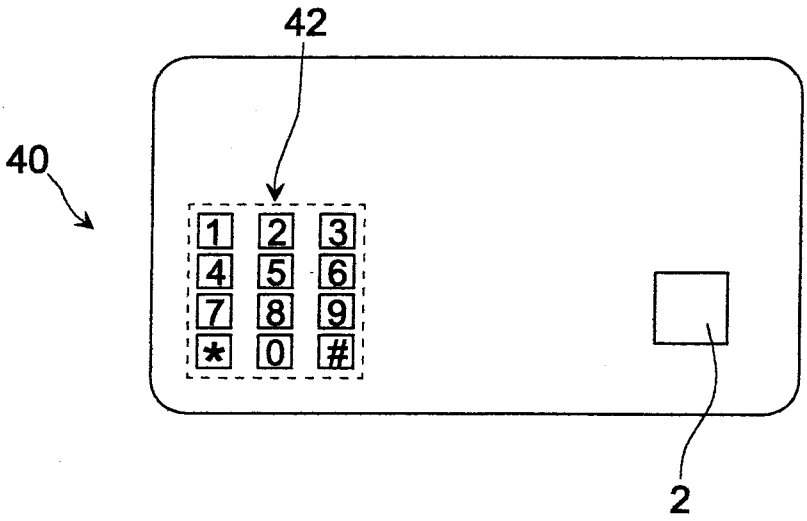


Fig.6

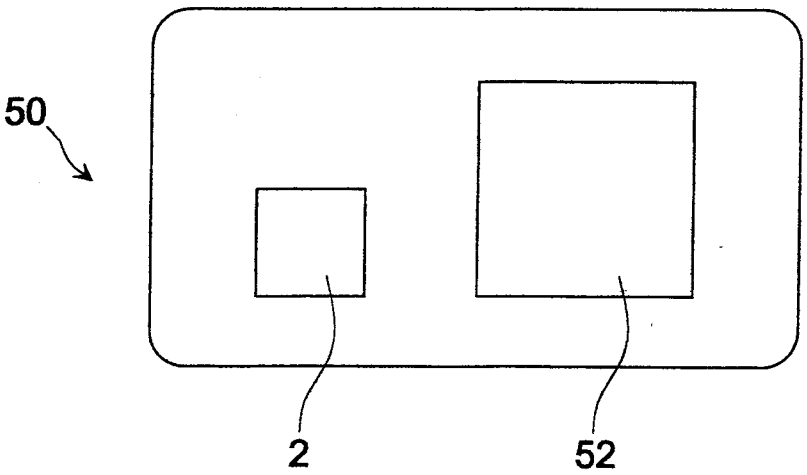


Fig.7

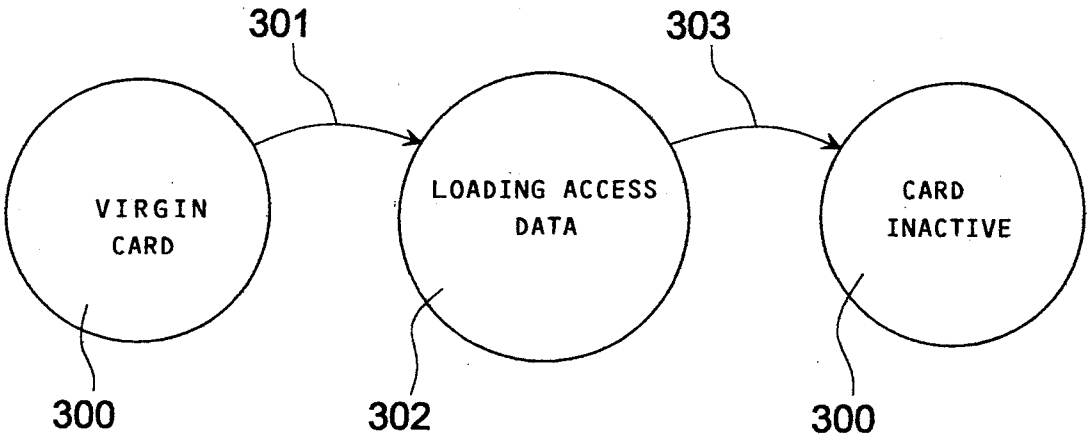


Fig.8

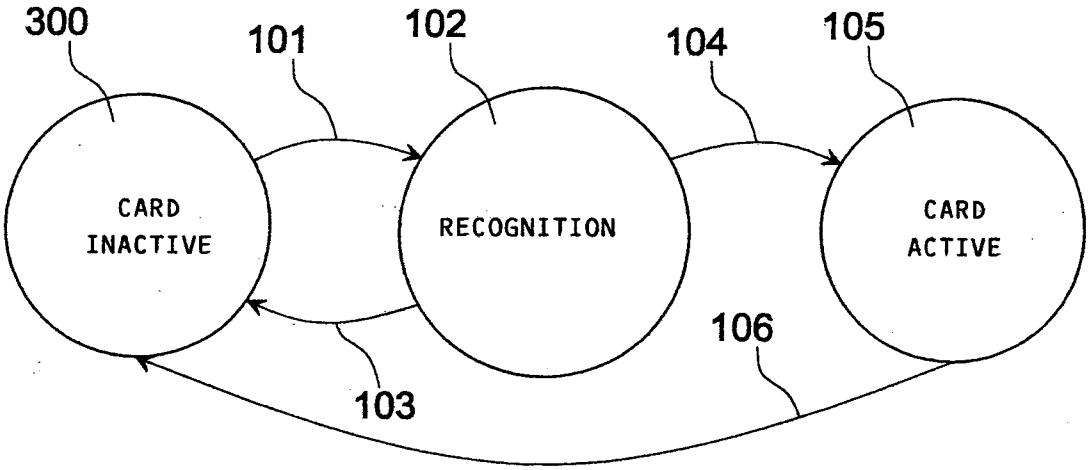


Fig.9

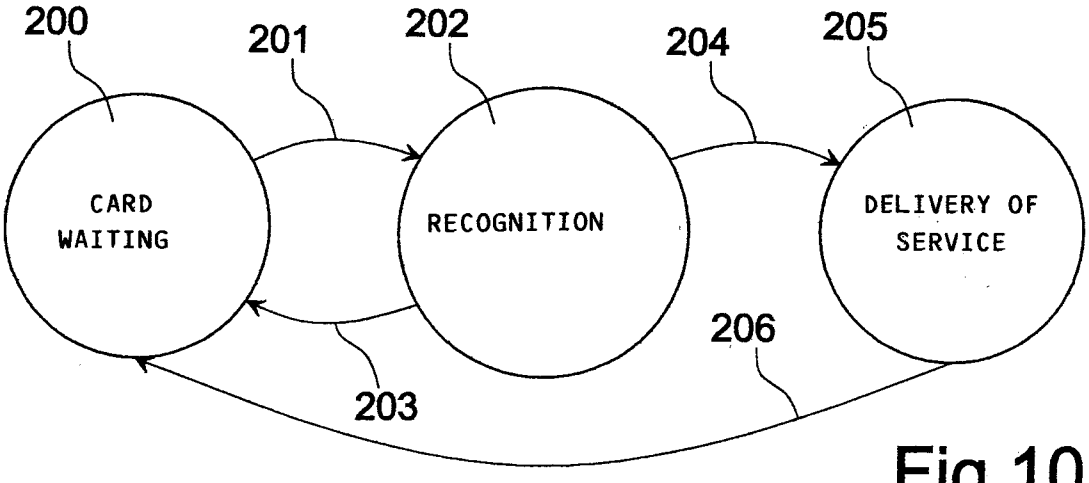


Fig.10

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2007/051355

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/20

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/177045 A1 (BROWN KERRY DENNIS [US]) 9 September 2004 (2004-09-09) the whole document	1-10
X	US 6 188 309 B1 (LEVINE RONALD M [US]) 13 February 2001 (2001-02-13) the whole document	1,2,4-6, 9,10
X	US 5 623 552 A (LANE WILLIAM F [US]) 22 April 1997 (1997-04-22) column 2, line 10 - column 6, line 26 figures 1a,1b,2	1-4,7-10
X	EP 1 074 949 A (SHEN MING SHIANG [TW] SHEN MING-SHIANG [TW]) 7 February 2001 (2001-02-07) paragraph [0001] - paragraph [0015] figure 1	1,4,5, 7-10

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 April 2007	24/04/2007

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Segura, Gustavo

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2007/051355

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01/35334 A (LI KENNETH [US]) 17 May 2001 (2001-05-17) page 4 - page 10	1,4,5, 7-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2007/051355

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004177045 A1	09-09-2004	NONE	
US 6188309 B1	13-02-2001	NONE	
US 5623552 A	22-04-1997	NONE	
EP 1074949 A	07-02-2001	AU 729157 B1	25-01-2001
WO 0135334 A	17-05-2001	AU 1767201 A	06-06-2001