(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 018 632 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
16.09.2009 Bulletin 2009/38

(21) Application number: **07729015.3**

(22) Date of filing: **11.05.2007**

(51) Int Cl.:
G07F 7/10 *(2006.01)* ***G07C 9/00*** *(2006.01)*

(86) International application number:
PCT/EP2007/054563

(87) International publication number:
WO 2007/131952 (22.11.2007 Gazette 2007/47)

(54) **MEMORY CARRIER, AUTHORISATION METHOD, READER, NETWORK AND ACCESS CONTROL SYSTEM**

SPEICHERTRÄGER, AUTORISIERUNGSVERFAHREN, LESER, NETZWERK UND ZUGANGSKONTROLLSYSTEM

SUPPORT DE MÉMOIRE, PROCÉDÉ D'AUTORISATION, LECTEUR, RÉSEAU ET SYSTÈME DE CONTRÔLE D'ACCÈS

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR
Designated Extension States:
HR

(30) Priority: **12.05.2006 EP 06113897**

(43) Date of publication of application:
28.01.2009 Bulletin 2009/05

(73) Proprietor: **SERVIPARK INTERNATIONAL**
1000 Brussels (BE)

(72) Inventors:
- **DUYCK, Francis**
  9000 Gent (BE)
- **LOCATELLI, Maurizio**
  1000 Brussels (BE)
- **CLAEYS, Jean**
  9810 Nazareth (BE)

(74) Representative: **Calvo de Nó, Rodrigo et al**
Gevers & Vander Haeghen
Intellectual Property House
Holidaystraat 5
1831 Diegem (BE)

(56) References cited:
WO-A-02/05482
US-A- 4 816 653
US-A- 5 721 781
US-A- 5 768 379

EP 2 018 632 B1

Description

[0001] The present invention relates to the technical field of memory carriers for access control systems.

[0002] It has been previously known to use such memory carriers, comprising a unique, read-only serial code and a plurality of records, comprising a memory carrier identification record and at least one contract identification record, for access control. In particular, contactless cards such as CALYPSO® or MIFARE® have already been proposed as a versatile means of providing both logical and physical access control to a variety of facilities, such as public transportation, telecommunications or monetary transaction facilities. A single such card can contain information about a plurality of contracts, thus providing access to several different facilities. Although such cards already usually comprise in-built security features, they do not, by themselves, provide comprehensive security, as the structure of the contract information and the method of reading it may leave loopholes and backdoors allowing potential abuse.

[0003] United States Patent 5,721,781 disclosed a memory carrier for access control, comprising:

- a unique, read-only serial code; and
- a plurality of records, comprising a memory carrier identification record and at least one contract identification record; wherein
- each one of the memory carrier identification record and at least one contract identification record comprises an authentication code;
- the authentication code of said memory carrier identification record matches in a first check a memory carrier security code resulting from encrypting with a security key a combination of at least part of the unique, read-only serial code and at least part said memory carrier identification record.

[0004] The authentication code of the memory carrier identification record should ensure that copying the records from a valid memory carrier to a blank will not produce another valid memory carrier, since it is linked to both the memory carrier identification record, and the unique, read-only serial code of each memory carrier through an opaque encryption.

[0005] However, this measure alone cannot prevent that copying the contract identification records of one valid memory carrier to another valid memory carrier will not produce valid contract identification records in the second memory carrier, or that authorisation to proceed with operations related to a given contract can be given by a reader not having access to the specific product key associated with that contract.

[0006] Similar prior art was also disclosed in US Patent 4,816,653, International Patent Application WO 02/05482, and US Patent 5,768,379.

[0007] It is therefore the object of the invention to provide comprehensive security in memory carriers for access control systems, in particular to at least one contract identification record. The invention solves this problem with the features of the characterising part of claim 1.

[0008] The authentication code of the at least one contract identification record ensures that copying the contract identification records of one valid memory carrier to another valid memory carrier will not produce valid contract identification records in the second memory carrier, since this other authentication code is linked to both the memory carrier serial code and identification record, and to the specific contract identification record.

[0009] Moreover, the authentication code of the at least one contract identification record also ensures that no authorisation to proceed with operations related to a given contract can be given by a reader not having access to the specific product key associated with that contract.

[0010] Preferably, the memory carrier of the invention comprises a record allocation table pointing to the memory addresses of at least some of the plurality of records. Still more preferably, the record allocation table is dynamic, so that each record can be stored in the first available memory address, and said record allocation table comprises a record allocation table authentication code, so as to allow a data integrity check of said record allocation table. ,

[0011] A dynamic record allocation table enables a much faster authorisation process, a critical aspect in applications such as car parking access cards. The record allocation table authentication code ensures that this does not affect the security of the card and that the pointers to the memory addresses of the records can not be tampered with. The potential application of this secure dynamic record table is not limited to the memory carrier of the invention, and could also be applied to other memory carriers.

[0012] Preferably, the plurality of records also comprises other records, such as a life cycle record. This has the advantage of allowing further security measures against, for instance, the used of expired or stolen memory carriers.

[0013] The invention also provides a method for using said memory carrier for the authorisation of operations associated with one of the at least one contact identification record of said memory carrier, said method comprising the steps of:

- reading the unique, read-only memory carrier serial code;
- reading the memory carrier identification record;
- obtaining the security key, at least partly from a source external to the memory carrier;

- encrypting with said security key a combination of at least part of the memory carrier serial code and at least part of said memory carrier identification record, so as to obtain the memory carrier security code,
- performing a first check comparing the authentication code of the memory carrier identification record with the result of performing a first predefined calculation on the memory carrier security code;
- reading said one of the at least one contract identification records;
- obtaining the corresponding product key, at least partly from a source external to the memory carrier;
- encrypting with said product key a combination of at least part of the memory carrier security code, and at least part of said one of the at least one contract identification record, so as to obtain a business security code; and
- performing a second check comparing the authentication code of said one of the at least one contract identification record with the result of performing a second predefined calculation on the business security code.

[0014] Preferably, when using a memory carrier comprising a record allocation table pointing to the memory addresses of at least some of the plurality of records, this method also comprises the step of finding in the record allocation table the memory addresses of each memory carrier record to be read. Still more preferably, when using a memory carrier comprising a dynamic record allocation table with a record allocation table authentication code, this method also comprises the step of performing said data integrity check on said dynamic record allocation table.

[0015] Preferably, when using a memory carrier comprising a life cycle record, this method also comprises the step of reading said life cycle record.

[0016] Preferably, when using a memory carrier comprising at least one record other than the memory carrier identification record and the at least one contract identification record, wherein said other record comprises a record authentication code, this method also comprises the steps of:

- encrypting with said security key a combination of at least part of a code containing information from said serial code, such as the memory security code, and at least part of said other record, so as to obtain a record security code; and
- performing said additional redundancy check comparing the result of performing an additional predefined calculation on the record security code with the authentication code of said other record.

[0017] Preferably, a product table contains a plurality of potential product keys, each one of them individually identified by a product identification code, said one of the at least one contract identification record contains a particular product identification code, and the step of obtaining the product key involves reading a product identification code contained in said contract identification record and extracting from said product table the product key identified by said particular product identification code.

[0018] Preferably, the operations associated with the at least one contract identification record comprise logical access to an information system.

[0019] Preferably, the operations associated with the at least one contract identification record comprise physical access to an enclosed space, comprising, for example, a secure building or at least one car parking space.

[0020] Preferably, the operations associated with the at least one contract identification record comprise monetary transactions.

[0021] Preferably, the operations associated with the at least one contract identification record comprise access to services comprising, for example, transportation or telecommunication services.

[0022] The invention also provides a reader for performing said method for using said memory carrier for the authorisation of operations associated with one of the at least one contract identification record of said memory carrier, wherein the reader preferably comprises local memory storage means for containing at least part of one of said security and/or product keys.

[0023] The invention also provides a network comprising at least one such reader connected to at least one other such reader and/or a remote memory storage means for containing at least part of one of said security and/or product keys.

[0024] The invention also provides an access control system comprising at least one such memory carrier and one such reader and/or network.

[0025] The invention will be described in detail and non-limitingly with reference to the accompanying figures, in which:

Fig. 1 represents a memory carrier according to the invention;

Fig. 2 is a flow diagram representing a method of using said memory carrier according to the invention;

Fig. 3 is a flow diagram representing the process of authenticating the memory carrier identification record;

Fig. 4 is a flow diagram representing the process of authenticating the life cycle record;

Fig. 5 is a flow diagram representing the process of authenticating a contract identification record; and

Fig. 6 represents an access control system according to the invention.

[0026] Referring now to Fig. 1, a memory carrier 1 is illustrated that contains a serial code 2, a record allocation table 3, comprising a record allocation table authentication code 3a, a memory carrier identification record 4, comprising a memory carrier identification record authentication code 4a, a life cycle record 5, comprising a life cycle record authentication code 5a, and at least one contract identification record 6, comprising a corresponding contract identification record authentication code 6a and a product key 6b.

[0027] The serial code 2 is unique to each memory carrier 1 and read-only, meaning that it can not be altered, erased or overwritten without destroying the memory carrier 1.

[0028] The record allocation table 3 contains the memory address of each individual record in the memory carrier 1. So, for reading and/or writing in a given record, the record allocation table 3 needs to be consulted first in order to ascertain the memory address, that is, the actual position within the memory carrier, of that particular record. The record allocation table 3 is dynamic, that is, it can reassign a given record to a different memory address than its original one. This accelerates the read/write process, which is very advantageous in time-critical applications, such as car parking access cards. To ensure, however, that this capability is not misused to tamper with its content, the record allocation table 3 also comprises a record allocation table authentication code 3a, which can be used to perform a data integrity check of the record allocation table 3 every time that it is to be consulted.

[0029] The memory carrier identification record 4 serves to identify each individual memory carrier 1. The memory carrier identification record authentication code 4a ensures that a given memory carrier 1 cannot be falsified by copying it straight onto another, blank, memory carrier.

[0030] The life cycle record 5 contains information regarding the life cycle of each individual memory carrier 1, that is for instance, when it was produced, when it was activated, whether it has been previously locked or cancelled, whether it has been unlocked or reactivated, the expiration date, etc. The life cycle record 5 also contains an authentication code 5a to ensure, for instance, that a stolen memory carrier 1 is not illegitimately reactivated.

[0031] Each contract identification record 6 contains information identifying a contract related to certain operations which the memory carrier 1 can authorize to perform. These operations may comprise logical access to an information system, physical access to an enclosed space, monetary transactions or access to services. In this way, a single memory carrier 1 can be used, for instance, to get entrance to a parking near an entertainment arena, to access the public transportation system so as to go from the parking to the arena, to get entrance to the arena, to pay for goods bought within the arena, etc. each one of these operations being actually related to a different contract with a different contractor.

[0032] Each contract identification record 6 also comprises a contract identification record authentication code 6a and a product identification code 6b, to ensure not only that spurious contract identification records cannot be added to a memory carrier 1, but also that a given contractor can only perform those operations related to its corresponding contract identification record, that is for instance, in the example given above, that the memory card reader of the arena access system cannot illegitimately charge the electronic wallet within the same memory carrier 1.

[0033] The memory carrier 1 could be a card and could also comprise data processing means and/or a contactless interface. Contactless smart cards are particularly advantageous for realising the memory carrier 1, because of their capabilities, ease of use and practicality. However, other types of memory carriers, such as telephone SIM cards, should not be excluded.

[0034] To illustrate an authorisation method using such a memory carrier 1, we will now refer to Figs. 2 to 4.

[0035] The first step 10 of the method consists in reading the serial code 2 of the memory carrier 1.

[0036] Example: Serial code=235

[0037] In the next step 20, the record allocation table 3 is read, and in step 30 its data integrity is checked using the record allocation table authentication code 3a. If this data integrity check fails, the authorisation process can be interrupted.

[0038] In the following step 40, using the memory address obtained from the record allocation table 3, the memory carrier identification record 4 is read. The memory carrier identification record authentication code 4a is contained, for example, as a two-digit trailer, in the Memory carrier identification record.

[0039] Example: Memory carrier identification record=91748
Memory carrier ID record authentication code=48

[0040] In the next step 50, the memory carrier identification record 4 has to be authenticated. This memory carrier identification record authentication step 50 in turn comprises several smaller steps, illustrated in Fig. 3:

[0041] In step 60 at least part of the serial code 2 and at least part of the memory carrier identification record 4 are combined by, for example, concatenating them. A key offset code is then calculated in step 70 using the result of this combination, by, for example, adding all digits.

[0042] Example: Combined value =235917
Key offset code=2+3+5+9+1+7=27

[0043] Using this key offset code, in step 80 a security key is extracted from a security key table containing a plurality of potential security keys, each one identified by one key offset code.

[0044] Example:

Table 1: Example of security key table

Key offset code	Security key
...	
26	523401
27	142035
28	420153
...	

[0045] With key offset code=27, security key=142035

[0046] Using this security key in a predefined encryption algorithm, it is then possible in step 90 to encrypt the above mentioned combination of at least part of the memory carrier identification record 4 and at least part of the serial code 2 to obtain a memory carrier security code.

[0047] Example: Each digit of the security key indicates at which string position the corresponding digit of the combined value needs to be stored. In this example, the second digit of the combined value thus needs to be stored at string position 4.

Table 2: Encryption example

Combined value	2	3	5	9	1	7
Security key	1	4	2	0	3	5
Position	0	1	2	3	4	5
Memory carrier security code	9	2	5	1	3	7

[0048] In step 100, the authentication code 4a of the memory carrier identification record 4 is verified by means of a check, in this case a redundancy check, in which this authentication code 4a is compared with the result of a predetermined calculation on the memory carrier security code. If that result does not match the authentication code 4a, the process of reading the memory carrier can be interrupted.

[0049] Example: Memory carrier security code=925137

925137 mod 97 = 48 = Authentication code of the memory carrier identification record

[0050] Turning back to Fig. 2, if the memory card identification record is authenticated, the next step 110 will be to read the life cycle record 5. Authenticating the life cycle record in step 120 will comprise a number of smaller steps, illustrated in turn in Fig. 4:

[0051] In step 130, at least part of a code comprising information from the memory carrier serial code, such as the memory carrier security code, and at least part of the life cycle record 5 are combined in a similar combination process as that of step 50. After this, in step 140 the result of this combination is encrypted using an additional predefined encryption algorithm with the security key obtained in step 70. In step 150, an additional check, in this case also a redundancy check, will compare the authentication code 5a contained in said life cycle record 5 with the result of an additional predefined calculation on the result of encryption step 140. If that result does not match the authentication code 5a, the process of reading the memory carrier can be interrupted.

[0052] Turning back to Fig. 2, if the life cycle record 5 is authenticated, and the memory carrier 1 is confirmed as active by the life cycle record 5 in step 160, the next step 170 will be to read a contract identification record 6, followed by the step 180 of authenticating said contract identification record 6. The contract identification record authentication step 180 in turn comprises several smaller steps, illustrated in Fig. 5:

In step 190, at least part of a code comprising information from the memory carrier serial code, such as the memory carrier security code and at least part of the contract identification record 6 are combined in a similar combination process as that of step 50. In step 200, which can be performed simultaneously to step 190, a product key is extracted using a product identification code 6b contained in the contract identification record 6 from a product table containing

a plurality of potential product keys, each one identified by one product identification code 6b.

[0053] After this, the product key can be used in step 210 to encrypt the result of step 190 with yet another encryption algorithm to produce a business security code. To authenticate the contract identification record 6, this business security code will then be compared in yet another check 220, in the form of a redundancy check, using yet another predefined calculation, with the authentication code 6a of said contract identification record 6. If this check 220 failed, the process could also be interrupted, but if the contract identification record 6 is authenticated, then the operations related to said contract could be authorised.

[0054] Finally, to illustrate an example of an access control system according to this invention, we will turn to Fig. 6.

[0055] An access control system 11 comprises several memory carriers 1 as illustrated in Fig. 1, in this case in the form of contactless smart cards. The access control system 11 also comprises several readers 12, each one of them capable of performing the method illustrated in Figs. 2-5 using the memory carriers 1. Some of these readers 12 can be autonomous and contain the security key and product tables in local memory storage means, whereas some other of these readers 12 can be integrated in a network 13 connecting them to each other and to a remote memory storage means 14, and the security key and product key tables can be contained in the remote memory storage means 14 or distributed throughout the network 13. The network 13 can be a local network in turn connected to a remote network (not illustrated) connected to several such local networks.

[0056] Each reader 12 can have access to product tables containing different selections of product keys, therefore enabling them to authorise operations related to different selections of contracts. So, some readers 12 can be associated, for example, to a parking access, other readers 12 to a payment system, whereas other readers 12 may be associated to public transportation services. When executing the above-mentioned authorisation method, a reader 12 could either read all the contract information records 6 present in a memory carrier 1, or a selection thereof, such as only those contract information records 6 for which it has access to the corresponding product keys.

[0057] Although the present invention has been described with reference to specific exemplary embodiments, it will be evident that various modifications and changes may be made to these embodiments without departing from the broader scope of the invention as set forth in the claims. Accordingly, the description and drawings are to be regarded in an illustrative sense rather than a restrictive sense.

Claims

1. Memory carrier (1) for access control, comprising:

- a unique, read-only memory carrier serial code (2);
- a plurality of memory carrier records, comprising a memory carrier identification record (4) and at least one contract identification record (6); wherein
- each one of the memory carrier identification record (4) and at least one contract identification record (6) comprises an authentication code (4a,6a);
- the authentication code (4a) of said memory carrier identification record (4) matches in a first check a memory carrier security code resulting from encrypting with a security key a combination of at least part of the unique, read-only memory carrier serial code (2) and at least part of said memory carrier identification record (4); and

characterised in that

- the authentication code (6a) of each at least one contract identification record (6) matches in a second check a business security code resulting from encrypting with a product key a combination of at least part of said memory carrier security code, and at least part of said contract identification record (6).

2. A memory carrier (1) according to claim 1, also comprising a record allocation table (3) pointing to the memory addresses of at least some of the plurality of memory carrier records.

3. A memory carrier (1) according to claim 2, wherein said record allocation table (3) is dynamic, so that each memory carrier record can be stored in the first available memory address, and said record allocation table (3) comprises a record allocation table authentication code (3a), so as to allow a data integrity check of said record allocation table (3).

4. A memory carrier (1) according to any of the previous claims, wherein the plurality of memory carrier records also comprises at least one record (5) other than the memory carrier identification record (4) and the at least one contract identification record (6), such as a life cycle record.

5. A memory carrier (1) according to claim 4, wherein said at least one other record (5) comprises a record authentication code (5a) which matches in an additional check a record security code resulting from encrypting with said security key a combination of at least part of a code containing information from said memory carrier serial code (2), such as said memory carrier security code, and at least part of said other record (5).

6. Method of using a memory carrier (1) according to any of claims 1 to 5 for the authorisation of operations associated with one of the at least one contract identification record (6) of said memory carrier (1), said method comprising the steps of:

- reading (10) the unique, read-only memory carrier serial code (2);
- reading (40) the memory carrier identification record;
- obtaining (60,70,80) the security key, at least partly from a source external to the memory carrier (1);
- encrypting (90) with said security key a combination of at least part of the memory carrier serial code (2) and at least part of said memory carrier identification record (4), so as to obtain the memory carrier security code,
- performing said first check (100) comparing the authentication code (4a) of the memory carrier identification record (4) with the result of performing a first predefined calculation on the memory carrier security code;
- reading (170) said one of the at least one contract identification record (6);
- obtaining (200) the corresponding product key, at least partly from a source external to the memory carrier (1);
- encrypting (210) with said product key a combination of at least part of the memory carrier security code, and at least part of said one of the at least one contract identification record (6), so as to obtain a business security code; and
- performing said second check (220) comparing the authentication code (6a) of said one of the at least one contract identification record (6) with the result of performing a second predefined calculation on the business security code.

7. A method according to claim 6 for using a memory carrier according to claims 2 or 3, also comprising the step of finding (20) in the record allocation table (3) the memory addresses of each memory carrier record (4,5,6) to be read.

8. A method according to claim 7 for using a memory carrier according to claim 3, also comprising the step of performing a data integrity check (30) on the record allocation table (3).

9. A method according to any of claims 6 to 8 for using a memory carrier according to claim 4, also comprising the step of reading (110) said other record (5).

10. A method according to claim 9 for using a memory carrier according to claim 4, and wherein said at least one other record (5) is a life cycle record, wherein said method also comprises the step of checking (160) in the life cycle record (5) whether the memory carrier (1) is currently active.

11. A method according to claims 9 or 10 for using a memory carrier according to claim 5, also comprising the steps of:

- encrypting (140) with said security key a combination of at least part of a code containing information from said memory carrier serial code (2), such as the memory carrier security code, and at least part of said other record (5), so as to obtain a record security code; and
- performing said additional redundancy check (150) comparing the result of performing an additional predefined calculation on the record security code with the authentication code (5a) of said other record (5).

12. A method according to any of claims 6 to 11, wherein a security key table contains a plurality of potential security keys, each one of them individually identified by a key offset code, and the step of obtaining the security key comprises the steps of:

- performing (70) a further additional predefined calculation involving at least part of the memory carrier serial code (2) and at least part of the memory carrier identification record (4) to obtain one particular key offset code; and
- extracting (80) from said security key table the security key identified by that particular key offset code.

13. A method according to any of claims 6 to 12, wherein said one of the at least one contract identification record (6) contains a particular product identification code, and the step of obtaining the product key comprises the steps of:

- reading a product identification code contained in said contract identification record (6); and

- extracting (210) from a product table containing a plurality of potential product keys, each one of them individually identified by a different product identification code, the product key identified by the product identification code contained in said contract identification record (6).

14. A method according to any of claims 6 to 13, wherein the operations associated with the at least one contract identification record (6) comprise logical access to an information system.

15. A method according to any of claims 6 to 14, wherein the operations associated with the at least one contract identification record (6) comprise physical access to an enclosed space, comprising, for example, a secure building, an entertainment venue or at least one car parking space.

16. A method according to any of claims 6 to 15, wherein the operations associated with the at least one contract identification record (6) comprise monetary transactions.

17. A method according to any of claims 6 to 16, wherein the operations associated with the at least one contract identification record (6) comprise access to services comprising, for example, transportation or telecommunication services.

18. A reader (12) adapted for performing the authorisation method of at least one of claims 6 to 17, preferably comprising local memory storage means for containing at least part of one of said security and/or product keys.

19. A network (13) comprising at least one reader (12) according to claim 18 and, connected to said at least one reader (12), at least one other reader (12) according to claim 18 and/or at least one remote memory storage means (14) for containing at least part of one of said security and/or product keys.

20. An access control system (11) comprising at least one memory carrier (1) according to one of claims 1 to 5 and at least one reader (12) according to claim 18 and/or a network (13) according to claim 19.

Patentansprüche

1. Speicherträger (1) für Zugangskontrolle, umfassend:

- einen eindeutigen Nurlese-Speicherträger-Seriencode (2);
- mehrere Speicherträger-Datensätze, umfassend einen Speicherträger-Identifikationsdatensatz (4) und wenigstens einen Vertrags-Identifikationsdatensatz (6); wobei
- jeder von dem Speicherträger-Identifikationsdatensatz (4) und dem wenigstens einen Vertrags-Identifikationsdatensatz (6) einen Authentifizierungscode (4a, 6a) umfasst;
- der Authentifizierungscode (4a) des Speicherträger-Identifikationsdatensatzes (4) in einer ersten Prüfung mit einem Speicherträger-Sicherheitscode übereinstimmt, welcher aus Verschlüsseln, mit einem Sicherheitsschlüssel, einer Kombination wenigstens eines Teils des eindeutigen Nurlese-Speicherträger-Seriencodes (2) und wenigstens eines Teils des Speicherträger-Identifikationsdatensatzes (4) resultiert; und

dadurch gekennzeichnet, dass

- der Authentifizierungscode (6a) eines jeden des wenigstens einen Vertrags-Identifikationsdatensatzes (6) in einer zweiten Prüfung mit einem Geschäftssicherheitscode übereinstimmt, welcher aus Verschlüsseln, mit einem Produktschlüssel, einer Kombination wenigstens eines Teils des Speicherträger-Sicherheitscodes und wenigstens eines Teils des Vertrags-Identifikationsdatensatzes (6) resultiert.

2. Speicherträger (1) nach Anspruch 1, ferner umfassend eine Datensatz-Zuordnungstabelle (3), welche auf die Speicheradressen wenigstens einiger der mehreren Speicherträger-Datensätze zeigt.

3. Speicherträger (1) nach Anspruch 2, wobei die Datensatz-Zuordnungstabelle (3) dynamisch ist, derart, dass jeder Speicherträger-Datensatz in der ersten verfügbaren Speicheradresse gespeichert werden kann, und die Datensatz-Zuordnungstabelle (3) einen Datensatz-Zuordnungstabellen-Authentifizierungscode (3a) umfasst, um so eine Datenintegritätsprüfung der Datensatz-Zuordnungstabelle (3) zu erlauben.

4. Speicherträger (1) nach einem der vorhergehenden Ansprüche, wobei die mehreren Speicherträger-Datensätze ferner wenigstens einen Datensatz (5) umfassen, anders als der Speicherträger-Identifikationsdatensatz (4) und der wenigstens eine Vertrags-Identifikationsdatensatz (6), wie etwa einen Lebenszyklus-Datensatz.

5. Speicherträger (1) nach Anspruch 4, wobei der wenigstens eine andere Datensatz (5) einen Datensatz-Authentifizierungscode (5a) umfasst, welcher in einer zusätzlichen Prüfung mit einem Datensatz-Sicherheitscode übereinstimmt, welcher aus Verschlüsseln, mit dem Sicherheitsschlüssel, einer Kombination wenigstens eines Teils eines Codes, der Information aus dem Speicherträger-Seriencode (2) enthält, wie etwa des Speicherträger-Sicherheitscodes, und wenigstens eines Teils des anderen Datensatzes (5) resultiert.

6. Verfahren zum Verwenden eines Speicherträgers (1) nach einem der Ansprüche 1 bis 5 zur Autorisierung von Operationen, welche einem des wenigstens einen Vertrags-Identifikationsdatensatzes (6) des Speicherträgers (1) zugeordnet sind, wobei das Verfahren die Schritte umfasst:

- Lesen (10) des eindeutigen Nurlese-Speicherträger-Seriencodes (2);
- Lesen (40) des Speicherträger-Identifikationsdatensatzes;
- Erhalten (60, 70, 80) des Sicherheitsschlüssels, wenigstens teilweise aus einer Quelle außerhalb des Speicherträgers (1);
- Verschlüsseln (90), mit dem Sicherheitsschlüssel, einer Kombination wenigstens eines Teils des Speicherträger-Seriencodes (2) und wenigstens eines Teils des Speicherträger-Identifikationsdatensatzes (4), um so den Speicherträger-Sicherheitscode zu erhalten;
- Durchführen der ersten Prüfung (100) durch Vergleichen des Authentifizierungscodes (4a) des Speicherträger-Identifikationsdatensatzes (4) mit dem Ergebnis des Durchführens einer ersten vorbestimmten Rechnung an dem Speicherträger-Sicherheitscode;
- Lesen (170) des einen des wenigstens einen Vertrags-Identifikationsdatensatzes (6);
- Erhalten (200) des entsprechenden Produktschlüssels wenigstens teilweise aus einer Quelle außerhalb des Speicherträgers (1);
- Verschlüsseln (210), mit dem Produktschlüssel, einer Kombination wenigstens eines Teils des Speicherträger-Sicherheitscodes und wenigstens eines Teils des einen des wenigstens einen Vertrags-Identifikationsdatensatzes (6), um so einen Geschäftssicherheitscode zu erhalten; und
- Durchführen der zweiten Prüfung (220) durch Vergleichen des Authentifizierungscodes (6a) des einen des wenigstens einen Vertrags-Identifikationsdatensatzes (6) mit dem Ergebnis des Durchführens einer zweiten vorbestimmten Rechnung an dem Geschäftssicherheitscode.

7. Verfahren nach Anspruch 6 zum Verwenden eines Speicherträgers nach Anspruch 2 oder 3, ferner umfassend den Schritt des Auffindens (20) in der Datensatz-Zuordnungstabelle (3) der Speicheradressen jedes Speicherträger-Datensatzes (4, 5, 6), der zu lesen ist.

8. Verfahren nach Anspruch 7 zum Verwenden eines Speicherträgers nach Anspruch 3, ferner umfassend den Schritt des Durchführens einer Datenintegritätsprüfung (30) an der Datensatz-Zuordnungstabelle (3).

9. Verfahren nach einem der Ansprüche 6 bis 8 zum Verwenden eines Speicherträgers nach Anspruch 4, ferner umfassend den Schritt des Lesens (110) des anderen Datensatzes (5).

10. Verfahren nach Anspruch 9 zum Verwenden eines Speicherträgers nach Anspruch 4, und wobei der wenigstens eine andere Datensatz (5) ein Lebenszyklus-Datensatz ist, wobei das Verfahren ferner den Schritt des Prüfens (160) in dem Lebenszyklus-Datensatz (5) umfasst, ob der Speicherträger (1) aktuell aktiv ist.

11. Verfahren nach Anspruch 9 oder 10 zum Verwenden eines Speicherträgers nach Anspruch 5, ferner umfassend die Schritte:

- Verschlüsseln (140), mit dem Sicherheitsschlüssel, einer Kombination wenigstens eines Teils eines Codes, der Information aus dem Speicherträger-Seriencode (2) enthält, wie etwa des Speicherträger-Sicherheitscodes, und wenigstens eines Teils des anderen Datensatzes (5), um so einen Datensatz-Sicherheitscode zu erhalten; und
- Durchführen der zusätzlichen Redundanzprüfung (150) durch Vergleichen des Ergebnisses des Durchführens einer zusätzlichen vorbestimmten Rechnung an dem Datensatz-Sicherheitscode mit dem Authentifizierungscode (5a) des anderen Datensatzes (5).

12. Verfahren nach einem der Ansprüche 6 bis 11, wobei eine Sicherheitsschlüsseltabelle mehrere potentielle Sicherheitsschlüssel enthält, von denen jeder einzeln durch einen Schlüsseloffsetcode identifiziert ist, und der Schritt des Erhaltens des Sicherheitsschlüssels die Schritte umfasst:

- Durchführen (70) einer weiteren zusätzlichen vorbestimmten Rechnung, welche wenigstens einen Teil des Speicherträger-Seriencodes (2) und wenigstens einen Teil des Speicherträger-Identifikationsdatensatzes (4) beinhaltet, um einen konkreten Schlüsseloffsetcode zu erhalten; und
- Extrahieren (80), aus der Sicherheitsschlüsseltabelle, des Sicherheitsschlüssels, welcher durch den konkreten Schlüsseloffsetcode identifiziert ist.

13. Verfahren nach einem der Ansprüche 6 bis 12, wobei der eine des wenigstens einen Vertrags-Identifikationsdatensatzes (6) einen konkreten Produktidentifikationscode enthält, und der Schritt des Erhaltens des Produktschlüssels die Schritte umfasst:

- Lesen eines Produktidentifikationscodes, welcher in dem Vertrags-Identifikationsdatensatz (6) enthalten ist; und
- Extrahieren (210) aus einer Produkttabelle, welche mehrere potentielle Produktschlüssel enthält, von denen jeder einzeln durch einen unterschiedlichen Produktidentifikationscode identifiziert ist, des Produktschlüssels, welcher durch den Produktidentifikationscode, der in dem Vertrags-Identifikationsdatensatz (6) enthalten ist, identifiziert ist.

14. Verfahren nach einem der Ansprüche 6 bis 13, wobei die Operationen, welche dem wenigstens einen Vertrags-Identifikationsdatensatz (6) zugeordnet sind, logischen Zugang zu einem Informationssystem umfassen.

15. Verfahren nach einem der Ansprüche 6 bis 14, wobei die Operationen, welche dem wenigstens einen Vertrags-Identifikationsdatensatz (6) zugeordnet sind, physischen Zugang zu einem geschlossenen Bereich, umfassend, zum Beispiel, ein sicheres Gebäude, ein Entertainment Venue oder wenigstens einen Autoparkbereich, umfassen.

16. Verfahren nach einem der Ansprüche 6 bis 15, wobei die Operationen, welche dem wenigstens einen Vertrags-Identifikationsdatensatz (6) zugeordnet sind, Geldtransaktionen umfassen.

17. Verfahren nach einem der Ansprüche 6 bis 16, wobei die Operationen, welche dem wenigstens einen Vertrags-Identifikationsdatensatz (6) zugeordnet sind, Zugang zu Diensten, umfassend, zum Beispiel, Transport- oder Telekommunikationsdienste, umfassen.

18. Leser (12), angepasst zum Durchführen des Autorisierungsverfahrens nach wenigstens einem der Ansprüche 6 bis 17, vorzugsweise umfassend lokale Speichermittel zum Enthalten wenigstens eines Teils von einem von den Sicherheits- und/oder den Produktschlüsseln.

19. Netzwerk (13) umfassend wenigstens einen Leser (12) nach Anspruch 18 und, verbunden mit dem wenigstens einen Leser (12), wenigstens einen weiteren Leser (12) nach Anspruch 18 und/oder wenigstens ein entferntes Speichermittel (14) zum Enthalten wenigstens eines Teils von einem von den Sicherheits- und/oder den Produktschlüsseln.

20. Zugangskontrollsystem (11), umfassend wenigstens einen Speicherträger (1) nach einem der Ansprüche 1 bis 5 und wenigstens einen Leser (12) nach Anspruch 18 und/oder ein Netzwerk (13) nach Anspruch 19.

Revendications

1. Support de mémoire (1) pour contrôle d'accès, comprenant :

- un code de série unique (2) du support de mémoire, à lecture uniquement,
- une pluralité d'enregistrements du support de mémoire, comprenant un enregistrement d'identification (4) du support de mémoire et au moins un enregistrement d'identification (6) de contrat, où
- chacun de l'enregistrement (4) d'identification du support de mémoire et et du au moins un enregistrement (6) d'identification de contrat comprend un code d'authentification (4a, 6a),
- le code d'authentification (4a) de l'enregistrement (4) d'identification dudit support de mémoire correspond

dans un premier contrôle à un code de sécurité du support de mémoire résultant de l'encryptage par un code de sécurité d'une combinaison d'au moins une partie du code de série (2) unique du support de mémoire à lecture uniquement et d'au moins une partie dudit enregistrement (4) du support de mémoire, et

caractérisé en ce que

- le code d'identification (6a) de chacun des au moins un enregistrement (6) d'identification de contrat correspond dans un deuxième contrôle à un code de sécurité administratif résultant de l'encryptage avec un code produit résultant d'une combinaison d'au moins une partie dudit code de sécurité du support de mémoire et d'au moins une partie dudit enregistrement (6) d'identification de contrat.

2. Support de mémoire (1) selon la revendication 1, comprenant aussi une table d'allocation d'enregistrements pointant sur les adresses mémoire d'au moins quelques-uns de la pluralité d'enregistrements du support de mémoire.

3. Support de mémoire (1) selon la revendication 2, où ladite table d'allocation d'enregistrements (3) est dynamique, de sorte que chaque enregistrement du support de mémoire peut être stocké dans la première adresse mémoire disponible, et ladite table d'allocation d'enregistrements (3) comprend un code d'authentification (3a) de la table d'allocation d'enregistrements, de manière à permettre un contrôle d'intégrité des données de ladite table d'allocation d'enregistrements (3).

4. Support de mémoire (1) selon l'une quelconque des revendications qui précèdent, dans lequel la pluralité d'enregistrements du support de mémoire comprend aussi au moins un enregistrement (5) autre que l'enregistrement d'identification du support de mémoire (4) et le au moins un enregistrement (6) d'identification de contrat, comme un enregistrement de cycle de vie.

5. Support de mémoire (1) selon la revendication 4, dans lequel ledit au moins un autre enregistrement (5) comprend un code (5a) d'identification d'enregistrement qui correspond dans un contrôle additionnel à un code de sécurité d'enregistrement résultant de l'encryptage avec ledit code de sécurité d'une combinaison d'au moins une partie d'un code contenant une information provenant dudit code de série (2) du support de mémoire, comme ledit code de sécurité du support de mémoire, et d'au moins une partie dudit autre enregistrement (5).

6. Procédé d'utilisation d'un support de mémoire (1) selon l'une quelconque des revendications 1 à 5 pour l'autorisation d'opérations associées avec l'un du au moins un enregistrement (6) d'identification de contrat dudit support de mémoire (1), ledit procédé comprenant les étapes suivantes :

- lecture (10) de l'unique code de série (2) du support de mémoire à lecture uniquement,
- lecture (40) de l'enregistrement d'identification du support de mémoire,
- obtention (60, 70, 80) du code de sécurité, au moins en partie depuis une source extérieure au support de mémoire (1),
- encryptage (90) avec ledit code de sécurité d'une combinaison d'au moins une partie du code de série (2) du support de mémoire et d'au moins une partie dudit enregistrement (4) d'identification du support de mémoire, de manière que l'on obtienne le code de sécurité du support de mémoire,
- exécution dudit premier contrôle (100) comparant le code d'authentification (4a) de l'enregistrement (4) d'identification du support de mémoire avec le résultat de l'exécution d'un premier calcul prédéfini sur le code de sécurité du support de mémoire,
- lecture (170) dudit au moins un enregistrement (6) d'identification de contrat,
- obtention (200) du code produit correspondant, au moins en partie à partir d'une source extérieure au support de mémoire (1),
- encryptage (210) avec ledit code produit d'une combinaison d'au moins une partie du code de sécurité du support de mémoire et d'au moins une partie dudit au moins un enregistrement (6) d'identification de contrat, de manière à obtenir un code de sécurité administratif, et.
- exécution dudit deuxième contrôle (220) comparant le code d'authentification (6a) dudit un d'au moins un enregistrement d'identification de contrat (6) avec le résultat d'un deuxième calcul prédéfini sur le code de sécurité administratif.

7. Procédé suivant la revendication 6 pour l'utilisation d'un support de mémoire selon les revendications 2 ou 3, comprenant aussi les étapes consistant à trouver (20) dans la table (3) d'allocation d'enregistrements les adresses mémoire de chaque enregistrement (4,5,6) du support de mémoire devant être lu.

8. Procédé selon la revendication 7 pour l'utilisation d'un support de mémoire selon la revendication 3, comprenant aussi l'étape d'exécution d'un contrôle (30) d'intégrité des données sur la table d'allocation d'enregistrements (3).

9. Procédé selon l'une quelconque des revendications 6 à 8 pour l'utilisation d'un support de mémoire selon la revendication 4, comprenant aussi l'étape de lecture (110) dudit autre enregistrement (5).

10. Procédé selon la revendication 9 pour l'utilisation d'un support de mémoire selon la revendication 4, et dans lequel ledit au moins un autre enregistrement (5) est un enregistrement de cycle de vie, où ledit procédé comprend aussi l'étape de contrôle (160), dans l'enregistrement de cycle de vie (5), l'activité courante du support de mémoire (1).

11. Procédé selon les revendications 9 ou 10 pour l'utilisation d'un support de mémoire selon la revendication 5, comprenant aussi les étapes suivantes :

- encryptage (140) avec ledit code de sécurité d'une combinaison d'au moins une partie d'un code contenant une information provenant dudit code de série (2) du support de mémoire, comme le code de sécurité du support de mémoire, et d'au moins une partie dudit autre enregistrement (5), de manière à obtenir un code de sécurité, et
- exécution dudit contrôle de redondance (150) additionnel comparant le résultat de l'exécution d'un calcul additionnel prédéfini sur le code de sécurité d'enregistrement avec le code d'authentification (5a) dudit autre enregistrement (5).

12. Procédé selon l'une quelconque des revendications 6 à 11, dans lequel une table de codes de sécurité contient une pluralité de codes de sécurité potentiels, dont chacun est individuellement identifié par un code de décalage de clé, et l'étape d'obtention du code de sécurité comprend le étapes suivantes :

- exécution (70) d'un autre calcul additionnel prédéfini impliquant au moins une partie du code (2) de série du support de mémoire et au moins une partie de l'enregistrement (4) d'identification du support de mémoire afin d'obtenir un code particulier de décalage de clé, et
- extraction (80) de ladite table de clé de sécurité de la clé de sécurité identifiée par ce code particulier de décalage de clé

13. Procédé selon l'une quelconque des revendications 6 à 12, dans lequel ledit au moins un enregistrement d'identification de contrat (6) contient un code particulier d'identification de produit, et l'étape d'obtention du code de produit comprend les étapes suivantes :

- lecture d'un code d'identification de produit contenu dans ledit enregistrement d'identification de contrat (6), et
- extraction (210), d'une table de produits contenant une pluralité de codes de produit potentiels, dont chacun est individuellement identifié par un code d'identification de produit différent, de la clé de produit identifiée par le code d'identification de produit contenu dans ledit enregistrement d'identification de contrat (6).

14. Procédé selon l'une quelconque des revendications 6 à 13, dans lequel les opérations associées au minimum un enregistrement d'identification de contrat (6) comprennent un accès logique à un système informatique.

15. Procédé suivant l'une quelconque des revendications 6 à 14, dans lequel les opérations associées au minimum un enregistrement d'identification de contrat (6) comprennent un accès physique à un espace clos, comprenant par exemple un bâtiment sécurisé, un lie de loisirs ou au moins un emplacement de parking.

16. Procédé selon l'une quelconque des revendications 6 à 15, dans lequel les opérations associées au minimum un enregistrement d'identification de contrat (6) comprend des transactions monétaires.

17. Procédé selon l'une quelconque des revendications 6 à 16, dans lequel les opérations associées au minimum un enregistrement d'identification de contrat (6) comprend l'accès à des services, comprenant par exemple des services de transport ou de télécommunication.

18. Lecteur (12) adapté pour exécuter le procédé d'autorisation selon au l'une des revendications 6 à 17, comprenant de préférence des moyens de stockage en mémoire locale destinés à contenir au moins une partie de l'un desdits codes de sécurité et / ou de produit.

19. Réseau (13) comprenant au moins un lecteur (12) selon la revendication 18 et, connecté audit au moins un lecteur

(12), au moins un autre lecteur (12) selon la revendication 18 et / ou au moins un moyen distant de stockage en mémoire (14) destiné à contenir au moins une partie de l'un desdits codes de sécurité et / ou de produit.

20. Système de contrôle d'accès (11) comprenant au moins un support de mémoire (1) selon l'une des revendications 1 à 5 et au moins un lecteur (12) selon la revendication 18 et / ou un réseau (13) selon la revendication 19.

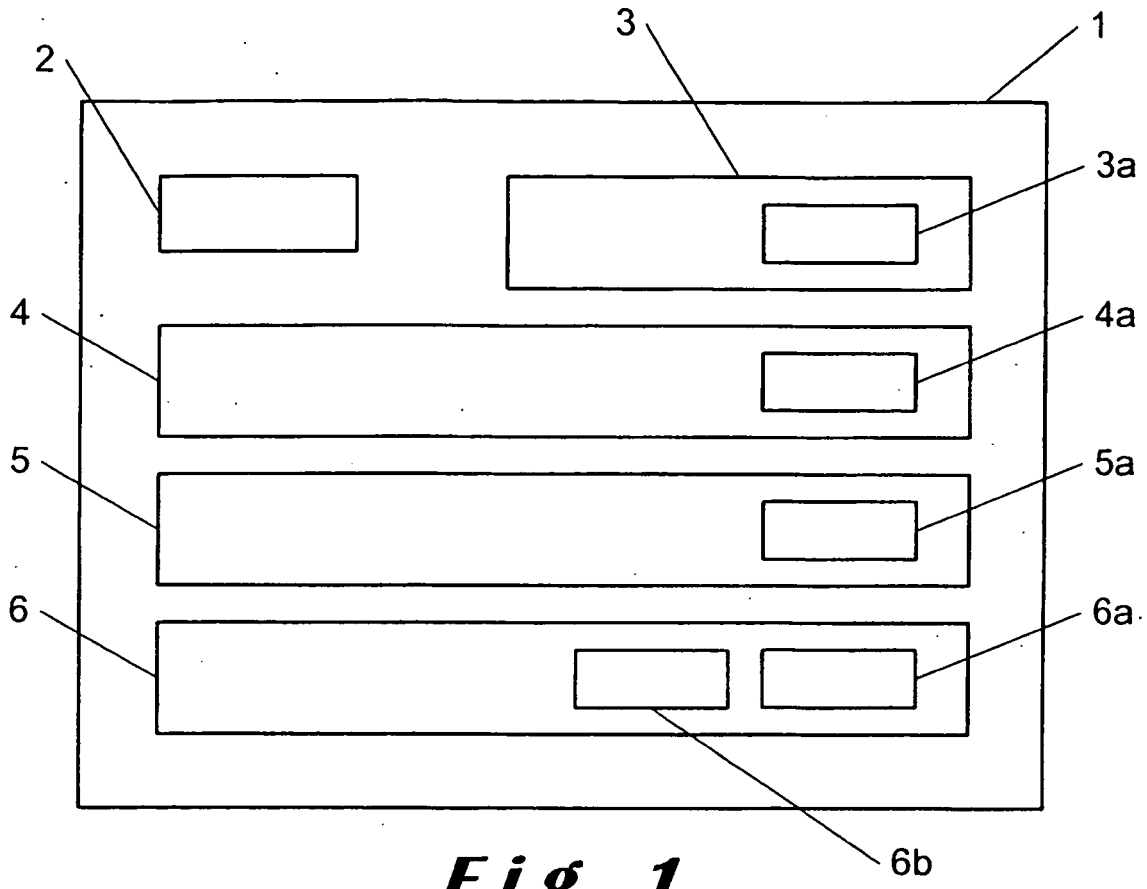

Fig. 1

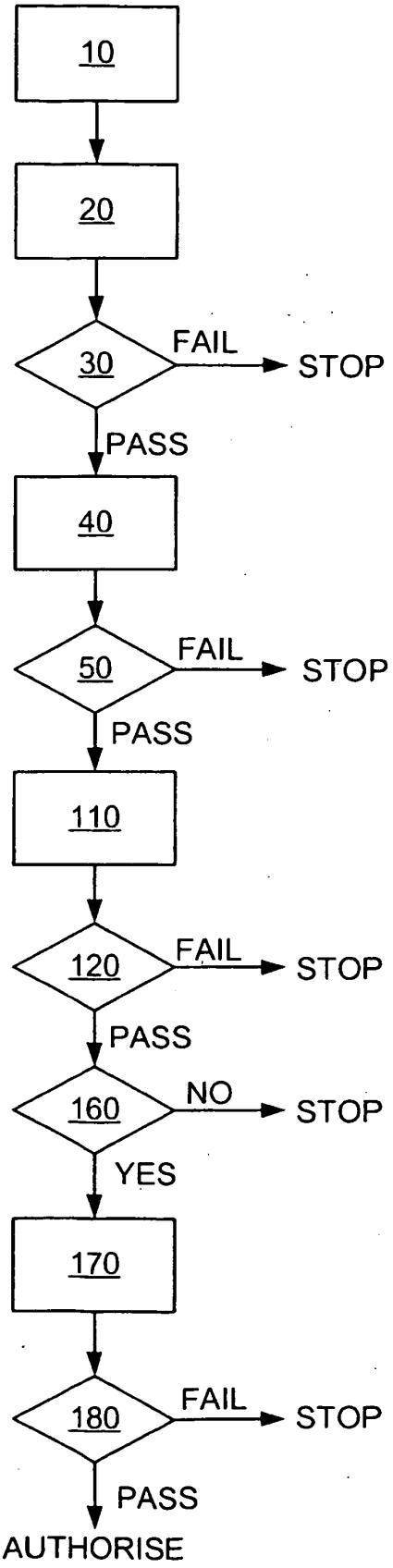
10
20
30
FAIL
STOP
PASS
40
50
FAIL
STOP
PASS
110
120
FAIL
STOP
PASS
160
NO
STOP
YES
170
180
FAIL
STOP
PASS
AUTHORISE

Fig. 2

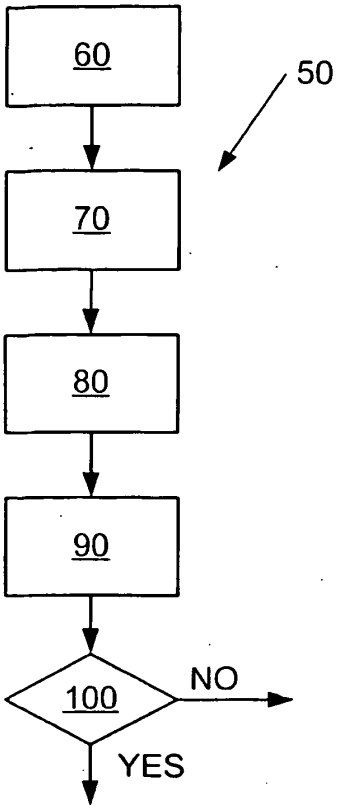

Fig. 3

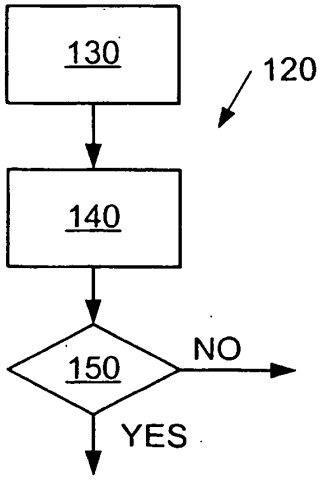

Fig. 4

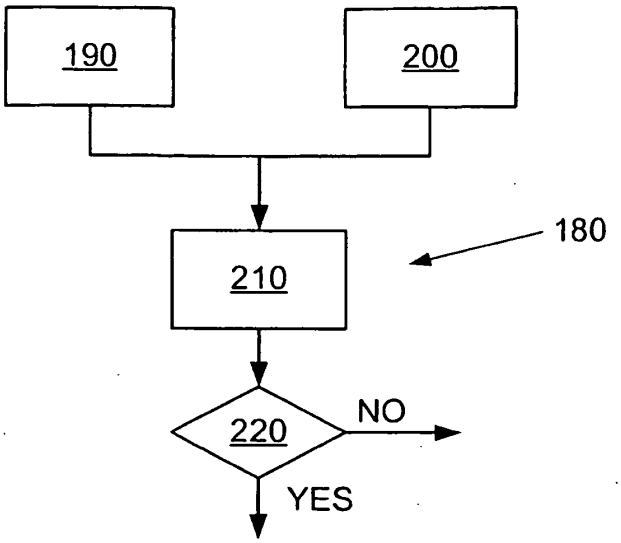

Fig. 5

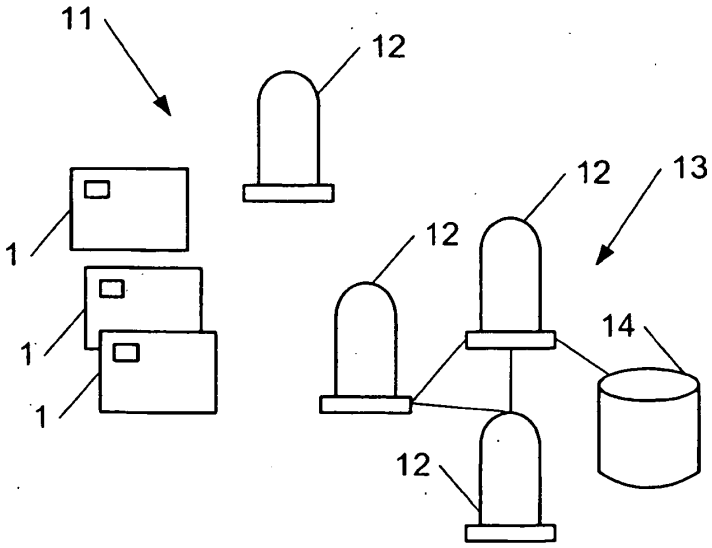

Fig. 6

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 5721781 A **[0003]**
- US 4816653 A **[0006]**
- WO 0205482 A **[0006]**
- US 5768379 A **[0006]**