Memory carrier, authorisation method, reader, network and access control system

Memory carrier 1 for access control, comprising a unique, read-only serial code 2; a plurality of 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 comprise an authentication code 4a,6a; and 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 serial code 2 and at least part said memory carrier identification record 4, and 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 a code containing information from said serial code 2, such as said memory carrier security code, and at least part of said contract identification record 6. The invention also comprises an authorisation method using such a memory carrier 1, a reader 12 for performing said authorisation method, a network 13 of several such readers 12 and an access control system 11 comprising at least one memory carrier 1 and a reader 12 and/or a network 13.

Fig. 1
The present invention relates to the technical field of memory carriers for access control systems. 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.

It is therefore the object of the invention to provide comprehensive security in memory carriers for access control systems. The invention solves this problem with the features of the characterising part of claim 1.

The authentication code of the memory carrier identification record ensures 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.

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.

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.

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.

The invention also provides a 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, 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 said code containing information from said serial code, such as 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.

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.

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

[0013] 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.

[0014] 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.

[0015] Preferably, the operations associated with the at least one contract identification record comprise logical access to an information system.

[0016] 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.

[0017] Preferably, the operations associated with the at least one contract identification record comprise monetary transactions.

[0018] Preferably, the operations associated with the at least one contract identification record comprise access to services comprising, for example, transportation or telecommunication services.

[0019] 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.

[0020] 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.

[0021] The invention also provides an access control system comprising at least one such memory carrier and one such reader and/or network.

[0022] 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.

[0023] 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.

[0024] 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.

[0025] 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.

[0026] 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.

[0027] 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.

[0028] 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.

[0029] 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.

[0030] 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.

[0031] To illustrate an authorisation method using such a memory carrier 1, we will now refer to Figs. 2 to 4.

[0032] The first step 10 of the method consists in reading the serial code 2 of the memory carrier 1.

Example: Serial code=235

[0033] 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.

[0034] 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.

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

[0035] 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:

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.

[0036] Example: Combined value =235917
Key offset code=2+3+5+9+1 +7=27

[0037] 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.

Example:

Table 1: Example of security key table

<table>
<thead>
<tr>
<th>Key offset code</th>
<th>Security key</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td></td>
</tr>
</tbody>
</table>
With key offset code=27, security key=142035

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.

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.

Example: Memory carrier security code=925137

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

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. After this, in step 200 the result of this combination is encrypted 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.

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.

[0048] Finally, to illustrate an example of an access control system according to this invention, we will turn to Fig. 6.

[0049] 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.

[0050] 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.

[0051] 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 serial code (2);
   - a plurality of records, comprising a memory carrier identification record (4) and at least one contract identification record (6);

and characterised in that:

   - each one of the memory carrier identification record (4) and at least one contract identification record (6) comprises an authentication code (4a, 6a); wherein
   - 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 serial code (2) and at least part said memory carrier identification record (4), and
   - 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 a code containing information from said serial code (2), such as 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 records.

3. A memory carrier (1) according to claim 2, wherein said record allocation table (3) is dynamic, so that each 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 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 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 (6), 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 a code containing information from said serial code (2), such as 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 authorisation 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 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 and at least part of the memory carrier identification record 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 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.
Fig. 2
**DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document with indication, where appropriate, of relevant passages</th>
<th>Relevant to claim</th>
<th>CLASSIFICATION OF THE APPLICATION (IPC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 5 721 781 A (DEO VINAY [US] ET AL) 24 February 1998 (1998-02-24) * abstract * * column 5, line 57 - column 6, line 14 * * column 7, line 52 - line 63 *</td>
<td>1-9, 13-20</td>
<td>INV. G07F7/10 G07C9/00</td>
</tr>
<tr>
<td>A</td>
<td>WO 02/05482 A (DREXLER TECH [US]) 17 January 2002 (2002-01-17) * page 1, line 13 - page 2, line 5 *</td>
<td>1-20</td>
<td></td>
</tr>
</tbody>
</table>

**TECHNICAL FIELDS SEARCHED (IPC)**

G07F G07C G06K E05B

The present search report has been drawn up for all claims.

Place of search: Munich
Date of completion of the search: 25 October 2006
Examiner: Stenger, Michael

**CATEGORY OF CITED DOCUMENTS**

- **X**: particularly relevant if taken alone
- **Y**: particularly relevant if combined with another document of the same category
- **A**: technological background
- **O**: non-written disclosure
- **P**: intermediate document
- **T**: theory or principle underlying the invention
- **E**: earlier patent document, but published on, or after the filing date
- **D**: document cited in the application
- **L**: document cited for other reasons
- **&**: member of the same patent family, corresponding document
This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EPO file on The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

25-10-2006

<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>US 5721781 A</td>
<td>24-02-1998</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>US 4816653 A</td>
<td>28-03-1989</td>
<td>CA 1287919 C</td>
<td>20-08-1991</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 8033912 B</td>
<td>29-03-1996</td>
</tr>
<tr>
<td></td>
<td></td>
<td>W0 8707061 A1</td>
<td>19-11-1987</td>
</tr>
<tr>
<td>WO 0205482 A</td>
<td>17-01-2002</td>
<td>AU 1880202 A</td>
<td>21-01-2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2410568 A1</td>
<td>17-01-2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2005160277 A1</td>
<td>21-07-2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 6871278 B1</td>
<td>22-03-2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 2931795 A</td>
<td>16-02-1996</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2171626 A1</td>
<td>01-02-1996</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 69507278 D1</td>
<td>25-02-1999</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 69507278 T2</td>
<td>10-06-1999</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 0719438 A1</td>
<td>03-07-1996</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ES 2128749 T3</td>
<td>16-05-1999</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FR 2722596 A1</td>
<td>19-01-1996</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 9602899 A1</td>
<td>01-02-1996</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 9503089 T</td>
<td>25-03-1997</td>
</tr>
</tbody>
</table>

For more details about this annex: see Official Journal of the European Patent Office, No. 12/82