The invention relates to a method for certifying the authenticity of a data item exchanged between two devices connected locally or remotely by a transmission line, each device comprising at least one memory and processing circuits.

The invention applies in particular to smart cards coupled remotely to an external device for bringing about certification by the card of the authenticity of a data item transmitted by the external device or for bringing about certification by the external device of the authenticity of a data item transmitted by the card.

The majority of applications which use smart cards involve conventional operations of reading and writing data in the memory of the card. The validity of these operations supposes the authenticity of the data exchanged between the card and the external device, that is, that a data item received does tally with the data item transmitted. This authenticity is not guaranteed when the card and the external device are connected remotely by a conventional transmission channel which can be observed by a criminal having the opportunity to modify the data item in the process of transmission. This problem is considerable particularly in banking applications where the data exchanged concern credits or debits of sums of money.

One solution to this problem may consist of coding the data to be transmitted, but this solution is not entirely satisfactory. In fact, the receiver decodes the data item in order to obtain a data item in plain language, but it is not certain that this data item does correspond to the one transmitted.

One method of bringing about certification, by a first device, of the authenticity of a data item contained at a given memory address of a second device is described in document FR-A-2526977. The first and second devices each calculate a result on the basis of the same algorithm, taking into account the data item to be certified, its address or position in the memory, and a secret code known

to the first and second devices. The result calculated by the second device is transmitted to the first one in order to be compared there with the result calculated by the first device. Authenticity is certified by the first device if the two results tally.

This method therefore implies that the device which carries out certification of authenticity knows in advance the memory address and the value of the data item which it is to certify. In fact, this prior art method supposes that certification of a data item received by a device is carried out, further to a dialogue between the data transmitting device and the data receiving device, by the transmitting device itself.

The invention reduces this disadvantage and makes it possible to authenticate a data item received as not only tallying with the data item transmitted, but also being transmitted by an authorised transmitting device. Thus the invention makes it possible to detect both a data item modified in the process of transmission thereof and a data item transmitted from an unauthorised transmitting device.

The invention therefore proposes a method for certifying the authenticity of a data item exchanged between two transmitting and receiving devices connected by a conventional transmission channel, each device comprising at least one memory and processing circuits, characterised in that it consists of:

- writing a coded message M at the level of the transmitting device, by implementation of a first programme which is executed by first processing circuits and which applies the function f2 of coding a reversible algorithm at least to the coding key S2 of this algorithm and to a first parameter X, so that the message M depends on at least the coding key and the first parameter, in that the coding key S2 of the algorithm being prerecorded in the memory of the transmitting device, and the first parameter X being broken down into at least one first field satisfying a predetermined condition and a second

field representative of the value of the data item, it further consists of:

- transmitting this message M to the receiving device and, by implementation of a second programme which is executed by second processing circuits, applying the function f1 of decoding said algorithm at least to this message M and to the decoding key S1 prerecorded in the memory of the receiving device, in order to obtain a second parameter X′ which therefore depends on the message M and the decoding key;
- breaking down the second parameter X′ into at least one first field and a second field,
  and verifying that the first field of the second parameter X′ verifies the same predetermined condition as the first field of the first parameter X in order to deduce therefrom that the value of the data item of the second field of the second parameter is equal to the value of the data item of the second field of the first parameter X.

According to one advantage of the invention, it is possible to write data remotely and with full security in a receiving device particularly consisting of a portable object such as a credit card.

Other advantages, characteristics and details will be apparent in the light of the explanatory description below given with reference to the attached figure which is given as an example and which shows schematically the principal components or circuits making it possible to carry out the method according to the invention.

With reference to the figure, two electronic devices (1, 2) are connected locally or remotely by a conventional transmission channel (L) of the electrical or optical type.

The device (1) comprises at least one memory (M1), processing circuits (T1) and an input/output interface (I1). All these circuits are connected together by means of a connecting bus (b1).

The device (2) comprises at least one memory (M2),

processing circuits (T2), a data input device such as a keyboard (CL) and an input/output interface (I2). All these circuits are connected together by a connecting bus (b2).

The memories (M1, M2) are for example divided into at least two storage areas (Z1, Z2). The data once recorded in the storage areas (Z1) are locked in order to be inaccessible in reading and writing from the outside. The data once recorded in the storage areas (Z2) are accessible only in reading from the outside. On the other hand, all the data recorded in the storage areas (Z1, Z2) are freely accessible internally by the processing circuits. The memories (M1, M2) generally further comprise a working area (Z3) for the storage of intermediate data during the operations performed by the processing circuits.

As an example, the device (1) consists of a portable object such as a card, while the device (2) is representative of an external device capable of interacting with a card temporarily coupled to this external device. The dialogue which will be set up between the card and the device normally makes it possible to achieve the delivery of a service or an authorisation of access by means of complementary circuits, not shown, the nature of which depends on the application envisaged.

Any dialogue necessarily implies an exchange of data, and it will be assumed that the external device (2) is caused to transmit a data item (d) to the card (1).

A first security measure consists of not transmitting in plain language the data item (d) which will be coded before transmission in such a manner that the card (1) will be capable of certifying that the decoded data item does in fact tally with the data item (d) transmitted.

The data item (d) may be a data item resulting from a calculated made by the processing circuits (T2) of the external device (2) or a data item entered on the keyboard (CL) of the external device (2) and if occasion arises preprocessed by the processing circuits (T2).

Coding of the data item (d) is obtained by a programme (P2) prerecorded in the storage area (Z1) of the memory (M2) and executed by the processing circuits (T2). This programme (P2) is the implementation of a function (f2) of coding a reversible algorithm. This function (f2) at least takes into account a coding key (S2) prerecorded in the storage area (Z1) of the memory (M2) and a parameter (X) which is linked to the data item (d).

To be more precise, the parameter (X) is broken down into several fields (X1, X2, ... Xn) with at least one of these fields which must satisfy a predetermined relationship and at least one field which is representative of the binary configuration or value (v) of the data item (d).

As an example, the parameter (X) comprises three fields (X1, X2, X3) with:

- X1 = X2 = ad (d)
- X3 = v

where ad(d) is the memory address of the card (1) where the data item (d) and (v) the value of the data item (d) is to be recorded.

Thus a coded message (M) is obtained such as M = f2(x, S2).

This message (M) is transmitted to the card (1) by the transmission channel (L). The processing circuits (T1) of the card (1) will execute on the message (M) received a programme (P1) prerecorded in the storage area (Z1) of the memory (M1). This programme (P1) is the implementation of the reverse function (f1) or function of decoding the reversible algorithm used during the operation of coding by the external medium (2). The programme (P1) decodes the message (M) by means of a decoding key (S1) prerecorded in the storage area (Z1) of the memory (M1) such that:

$$f1(M, S1) = X'$$

The parameter (X') obtained in this way is, like the parameter (X), broken down into several fields (X'1, X'2, ... X'n), and the conditions or relationships which are satisfied by the fields of the parameter (X) must also be

satisfied by the corresponding fields of the parameter (X'). Repeating the example taken above, the parameter (X') is broken down into three fields (X'1, X'2, X'3).

According to the invention, if the fields (X'1, X'2) satisfy the same relationship as the fields (X1, X2), that is, the data of these fields are identical and equal to the address (ad) of the data item (d), the card considers that the field (X'3) does indeed represent the value (v) of the data item (d) transmitted by the external medium (2).

The card (1) by means of its processing circuits (T1) can then carry out writing of the data item (d) at the address (ad) of the storage area (Z2) or (Z3) of the memory (M1) of the card (1).

Otherwise, the card (1) considers that the value (v) of the data item of the field (X'3) of the parameter (X') is not equal to the value of the data item (d) transmitted. Under these conditions, the card (1) does not take the message (M) received into account, knowing that there has been:

- either an error in transmission of the message (M),
- or a modification of the message (M) during transmission thereof,
- or that the message (M) has not been transmitted by an authorised transmitting device if the coding key (S2) does not correspond to the decoding key (S1) of the card (1) which is supposed to be a good card.

In order to increase security in transmission of the data item (d), the coding programme (P2) can also take a random number (E) into account. Thus, the same data item (d) will be coded differently in order to prevent a criminal from being able to reuse a previous message (M).

The random number (E) is provided by the card itself. To be more precise, this number is taken from the storage area (Z2) or control area of which at least one bit is modified every time the card (1) has been used. The random number then consists of the word of the storage area (Z1) which contains the last bit modified. Naturally, this

number (E) is transmitted to the external medium (2) before the coding operation.

In a variant, the random number (E) may consist of the initial content of the word situated at the address (ad) of the memory where it is wished to write. As the writing of a data item in the memory is carried out word by word, the writing of a data item (d) of several words will require transmission word by word according to the method of the invention with a different random number (E) each time consisting of the content of the word at the address (ad) which is successively modified until the data item (d) is written in full.

Naturally, the invention applies in the opposite direction when the external device (2) wants to certify a data item (d) transmitted by the card (1).

The aforementioned coding programme (P2) and decoding programme (P1) may be identical, which means that the keys (S1) and (S2) are also identical. As a security measure, these keys must remain secret and it is for this reason that they are prerecorded in the storage areas (Z1) inaccessible from the outside.

In a variant, the aforementioned algorithm may be an algorithm with a public key known in the art.

Claims

1. Method for certifying the authenticity of a data item exchanged between two transmitting and receiving devices connected by a conventional transmission channel, each device comprising at least one memory and processing circuits, characterised in that it consists of:

- writing a coded message M at the level of the transmitting device (2), by implementation of a first programme (P2) which is executed by first processing circuits (T2) and which applies the function f2 of coding a reversible algorithm at least to the coding key S2 of this algorithm and to a first parameter X, so that the message M depends on at least the coding key and the first parameter, in that the coding key S2 of the algorithm being prerecorded in the memory (M2) of the transmitting device (2), and the first parameter X being broken down into at least one first field (X1) satisfying a predetermined condition and a second field (X2) representative of the value (v) of the data item (d), it further consists of:
- transmitting this message M to the receiving device (1) and, by implementation of a second programme (P1) which is executed by second processing circuits (T1), applying the function f1 of decoding said algorithm at least to this message M and to the decoding key S1 prerecorded in the memory (M1) of the receiving device (1), in order to obtain a second parameter X′ which therefore depends on the message M and the decoding key;
- breaking down the second parameter X′ into at least one first field (X′1) and a second field (X′2),
  and verifying that the first field (X′1) of the second parameter X′ verifies the same predetermined condition as the first field (X1) of the first parameter X in order to deduce therefrom that the value of the data item of the second field (X′2) of the second parameter is equal to the value of the data item (d) of the second field (X2)

* C L M S *

of the first parameter X.

2. Method according to claim 1, characterised in that it consists of having a random number (E) taken into account by the functions (f1, f2).

3. Method according to claim 2, characterised in that it consists, when the transmitting device (2) or the receiving device (1) is a portable object, of having the random number (E) managed by the portable object by taking it from a control storage area (Z2) the content of which is modified every time the portable object is used.

4. Method according to any of the preceding claims, characterised in that it consists of defining the aforementioned predetermined condition which must be satisfied by the first field (X1) of the first parameter X, from the memory address (ad) at which the data item (d) is to be written.