

METHOD FOR PRODUCING AN ELECTRONIC DEVICE WITH A DISABLED
SENSITIVE MODE, AND METHOD FOR TRANSFORMING SUCH AN
ELECTRONIC DEVICE TO RE-ACTIVATE ITS SENSITIVE MODE

5

Technical field

The present invention relates to secure electronic devices or products having a sensitive mode (or functionality) that is disabled after production.

10

Background of the invention

As it is known by the man skilled in the art, some secure electronic devices, such as some smart cards, have a sensitive mode (such as a test mode) that is used during their production and then disabled to avoid attackers to use it to access to all their resources and thus to control them.

15

When such an electronic device has a working problem, it may be modified to activate its test mode again in order to determine the cause of this problem. But this modification is not only kept secret by the chip manufacturer who has developed this electronic device, but also complex, costly and not reliable (because it requires a focused ion beam (or FIB) manipulation), in order to be performed only by this chip manufacturer.

20

Summary of the invention

So, an objective of the invention is to allow authorized persons, and notably persons different from the chip manufacturer, to activate again the sensitive mode of a secure electronic device in an easy and secure manner, and at low cost (compared to existing solution).

25

More precisely, the invention provides notably a first method, intended for transforming a secure electronic device, associated to a first identifier and having a sensitive mode (or functionality) disabled after production, for a new sensitive use, and comprising the steps of:

30

- (i) externally computing a cipher of the first identifier with a predetermined function fed with the first identifier and a predetermined secret key,

- (ii) transforming an accessible metal layer of this electronic device to form an activation pattern representing this externally computed cipher of the first identifier,
- (iii) getting a value representative of the activation pattern into the electronic device, and
- (iv) computing a second identifier with the transformed electronic device by feeding a reverse function of the predetermined function with the value and the secret key, to trigger a comeback to the sensitive mode if this second identifier is equal to the first identifier.

The invention proposes to use a dedicated zone of the electronic device with a pattern that provides a value per default when no transformation is realized on it. A right transformation of the deactivation pattern triggers the comeback to the sensitive mode. The right transformation is only accessible if a specific calculation using a predetermined function, the first identifier of the electronic device and a secret key can be realized. If one does not know one or several of these three elements, one is not able to recover the sensitive mode. The invention renders possible to reenter the sensitive mode through an easy material modification while insuring a right protection of the sensitive mode.

The first transformation method according to the invention may include additional characteristics considered separately or combined, and notably:

- in step (iii) the value of the activation pattern may be a binary value or an analog value; adapted deactivation pattern and adapted transformation of the adapted activation pattern would correspond to these embodiments that enable the invention to be implemented in various situations;
- in step (ii) one may define the activation pattern by means of a cutting technique that is intended to remove metallic parts into locations of the metallic layer that are defined by the computed cipher of the first identifier; this embodiment enables a very simple operation of transformation of the pattern;
 - the computed cipher of the first identifier may be defined by N bits that are respectively associated to N continuous lines of the metallic layer that belong to a security electronic circuit of the electronic device. In this case,

an untransformed continuous line may represent a bit of the computed cipher of the first identifier that is equal to zero, while a continuous line transformed into an interrupted line may represent a bit of the computed cipher of the first identifier that is equal to one; this embodiment is a particularly simple and easy way of implementing the invention on classical integrated circuit device;

- N may be greater than one;
- the cutting technique may be chosen from a group comprising at least a laser cutting and a focused ion beam cutting;
- the predetermined function may be a cryptographic function;
- the cryptographic function may be chosen from a group comprising at least a simple Data Encryption Standard algorithm (DES), a triple Data Encryption Standard algorithm (TDES), an Advanced Encryption Standard algorithm (AES), a RSA algorithm, and other secret algorithms.

The use of a cryptographic function insures a secure transformation algorithm as well as an efficient protection of the sensitive mode.

The invention also provides a second method, intended for producing a secure electronic device associated to a first identifier and having a sensitive mode disabled after production, and comprising the steps of:

- (a) defining electronic circuits into this electronic device to perform predetermined functions, and notably a sensitive circuit intended for offering the sensitive mode,
- (b) defining a security circuit coupled to the sensitive circuit and intended for authorizing the sensitive circuit to offer the sensitive mode when it got a cipher of the first identifier, and
- (c) defining a deactivation pattern into an accessible metallic layer of the electronic device, which is arranged for inducing into the security circuit the generation of a value that is different from the cipher of the first identifier and therefore prevents the sensitive circuit to offer the sensitive mode.

The second production method according to the invention may include additional characteristics considered separately or combined, and notably:

- in step (c) one may define a deactivation pattern comprising N continuous

lines associated respectively to N bits of the cipher of the first identifier;

➤ a continuous line that is not transformed after a transformation phase may represent a bit of the computed cipher of the first identifier that is equal to zero, while a continuous line that is transformed into an interrupted line after a transformation phase may represent a bit of the computed cipher of the first identifier that is equal to one;

- the deactivation pattern may comprise eight continuous lines ($N = 8$); it could nevertheless be preferable a larger number N of thin continuous lines will be implemented (2^N possibilities). Indeed the larger would be the better but a large number of modifications will decrease significantly the reliability of the transformation as errors may occur during the transformation. If the lines are hidden within standard top metal level patterns, even a small number of lines should be sufficient. As the transformation is not instantaneous and not easily reversible, tries and fails attacks are not possible. The number N will be adapted considering the targeted resistance versus the duration of the transformation.

- the security circuit may be arranged for feeding a reverse function of a predetermined function with a predetermined secret key and the cipher of the first identifier for computing a second identifier, and for triggering a comeback of the electronic device to the sensitive mode if this second identifier is equal to the first identifier;

➤ the predetermined function may be a cryptographic function;

- the cryptographic function may be chosen from a group comprising at least a simple Data Encryption Standard algorithm, a triple Data Encryption Standard algorithm, an Advanced Encryption Standard algorithm, and a RSA algorithm;

- it may be arranged for producing a secure electronic device that defines a chip of a smart card.

The invention also relates to a secure electronic device obtained by a production method of the invention.

Said electronic device is associated to a first identifier and comprises a

sensitive mode circuit disabled after production. To enable a new sensitive use through a method of transformation of the electronic device according to one of the preceding claims, it comprises:

- 5 - an accessible metal layer of said electronic device intended to be transformed to form an activation pattern representing said externally computed cipher of the first identifier, said activation pattern;
- internal connections to get a value representative of said activation pattern into said electronic device,
- 10 - a circuit to compute a second identifier with said transformed electronic device by feeding a reverse function of said predetermined function with said value and said secret key and to trigger a comeback to said sensitive mode if said second identifier is equal to said first identifier.

15

Brief description of the figures

Other features and advantages of the invention will become apparent on examining the detailed specifications hereafter and the appended drawings, wherein:

- 20 - figure 1 schematically illustrates, in cross-section, an example of embodiment of a secure electronic device produced by means of a production method according to the invention,
- figure 2 schematically and functionally illustrates, in top view, relations between the components of the secure electronic device of figure 1 before
- 25 transformation (i.e. with a deactivation pattern),
- figure 3 schematically and functionally illustrates, in top view, relations between the components of the secure electronic device of figure 1 after transformation (i.e. with an activation pattern), and
- figure 4 schematically illustrates an example of algorithm that can be used
- 30 to implement a transformation method according to the invention.

Detailed description of the preferred embodiment

The invention aims, notably, at offering a construction method, and an associated transformation method, intended for allowing a secure electronic device CH, having a disabled sensitive mode, to be activated again in its sensitive mode after use.

In the following description it will be considered that the (secure) electronic device CH is a chip of a smart card ED. For instance, this smart card ED may be a credit card or an electronic identity card or else an electronic passport. But the invention is not limited to this type of electronic device. It concerns any type of electronic device having a sensitive mode that is disabled after production, and notably chips of Set-Top boxes, embedded secure elements, mobile phone application processors with embedded security, and complete handset devices.

Moreover in the following description it will be considered that the sensitive mode is a test mode.

In the example illustrated in figures 1 to 3 the chip CH is attached fixedly to a support PS, for instance in plastic material. As mentioned above, in this example the support PS and the chip CH constitute a smart card ED (or secure electronic device).

This chip CH is a secure electronic device that is produced by means of a production method according to the invention.

Such a production method comprises three steps (a), (b) and (c).

The first step (a) consists in defining electronic circuits EC, SC and TC into the chip CH in order it could perform predetermined functions. One of these electronic circuits is a sensitive circuit TC that is intended for offering a sensitive mode. So, in the described example, the sensitive circuit TC is a test circuit arranged for performing internal tests in an authorized test mode.

The second step (b) consists in defining a security circuit SC coupled to the test circuit TC and to other electronic circuits EC, and intended for authorizing the test circuit TC to offer the test (or sensitive) mode when it got (or has generated internally) a value V that is a cipher CR of a first identifier I1 that is associated to the chip CH.

This security circuit SC acts as a security interface between the test

circuit TC and remaining electronic circuits EC that may be grouped into a processor (or CPU), as illustrated in figures 2 and 3, for instance.

This first identifier I1 is preferably stored in an internal memory of the chip CH that is accessible to the security circuit SC and may be part of the processor EC. This first identifier I1 may be the "signature" of the chip CH. It may be alphanumeric.

The third step (c) consists in defining a deactivation pattern DS into an accessible metallic layer ML of the chip CH, which is arranged for inducing into the security circuit SC the generation of a value V that is different from the cipher CR of the first identifier I1 and therefore prevents the test circuit TC to offer the test (or sensitive) mode.

As illustrated in figures 2 and 3, the chip CH comprises also several contact areas CA intended to be contacted by an external device to allow interactions with some of the electronic circuits EC.

The accessible metallic layer ML may be the last layer defined on the top of the chip CH. But this is not mandatory. Indeed, at least its deactivation pattern DS could be defined below a protective layer easy to remove.

The security circuit SC is preferably arranged for feeding a reverse function F^{-1} of a predetermined function F with a predetermined secret key K and the value V that it generates internally because it is connected to the deactivation pattern DS or to an activation pattern AS produced by transformation of the deactivation pattern DS as explained below. So, when the generated value V is different from the cipher CR of the first identifier I1, the feeding of the reverse function F^{-1} provides a second identifier I2 (i.e. $F^{-1}(K, V) = I2$) which differs from the first identifier I1, and therefore the security circuit SC does not authorize a comeback of the chip CH to its test mode. But, when the generated value V is equal to the cipher CR of the first identifier I1, the feeding of the reverse function F^{-1} provides a second identifier I2 (i.e. $F^{-1}(K, CR) = I2$) which is equal to the first identifier I1, and therefore the security circuit SC authorizes a comeback of the chip CH to its test mode.

The predetermined secret key K is known by the chip manufacturer.

For instance, this predetermined function F is a cryptographic or ciphering function.

This ciphering or cryptographic function F may be the so called simple Data Encryption Standard algorithm (or DES). But, it could be also a triple Data Encryption Standard algorithm (or TDES), or an Advanced Encryption Standard algorithm (or AES), or else a RSA algorithm (Rivest Shamir Adleman), for instance. It can be preferable to use a secret customized algorithm, particularly in case of onboard implementation of the invention on small embedded systems.

As illustrated in the non-limiting example of figure 2, a deactivation pattern DS may comprise N continuous lines CL associated respectively to N bits of the cipher CR of the first identifier I1. In the non-limiting example of figure 2, N is equal to eight, but this is not mandatory. Indeed N may be equal to any number greater than one.

Each continuous line CL couples at least two parts of the security circuit SC which contribute to the internal generation of the value V. These parts may be gates of integrated electronic components, such as transistors, for instance.

For instance, a continuous line CL represents a bit of the value V that is equal to zero (0) for the security circuit SC, while an interrupted line represents a bit of the value V that is equal to one (1) for the same security circuit SC. The reverse situation is also possible (a bit equal to zero is represented by an interrupted line, while a bit equal to one is represented by a continuous line).

So, when a continuous line CL couples two parts of the security circuit SC, the latter (SC) is set in a first state, and when this continuous line CL is interrupted these two parts are no more coupled and then the security circuit SC is set in a second state. The contributions of all the security circuit parts coupled by the N continuous line CL define together the value V.

As mentioned above, the invention also proposes a transformation method intended for transforming an electronic device CH, produced by means of the production method described above, in order to activate again its disabled test mode for testing purpose after use.

This transformation method comprises three steps (i), (ii) and (iii).

The first step (i) consists in externally computing a cipher CR of the

first identifier I1 with the predetermined function F fed with the first identifier I1 of the chip CH and the predetermined secret key K, described above (so, $F(K, I1) = CR$).

5 The predetermined secret key K is also known by the man who proceeds to the chip transformation.

The first identifier I1 is either known by the man who proceeds to the chip transformation, or determined into the chip CH by means of a command that is transmitted by a computer to its contact areas CA. Such a command could be "get_I1", for instance. Upon reception, this command triggers the
10 search of the first identifier I1 into the chip CH, and once it has been found this first identifier I1 is transmitted to the requesting computer through the contact areas CA.

The second step (ii) consists in transforming the accessible metal layer ML of the chip CH (and more precisely its deactivation pattern DS) to form an
15 activation pattern AS that represents the externally computed cipher CR of the first identifier I1 and that is intended to modify (or replace) the value V generated into the security circuit SC.

This activation pattern AS may be defined by means of a cutting technique that is intended to remove (or destroy) metallic parts into locations of
20 the deactivation pattern DS of the metallic layer ML that are defined by the cipher CR of the first identifier I1, externally computed during the first step (i).

Any cutting technique known by the man skilled in the art, and allowing removal (or destruction) of metallic parts into a metallic layer may be used. So, it may be a laser cutting or a focused ion beam (or FIB) cutting, for instance.

25 In the non-limiting example illustrated in figure 2, the deactivation pattern DS comprises N continuous lines CL associated respectively to N bits of the value V (and therefore of the cipher CR of the first identifier I1), with $N = 8$. It is here noted that to insure a right protection of the sensitive mode, larger number on continuous lines will be implemented in reality to enable an
30 operator to "write" the cipher on this set of continuous lines. The cipher will effectively be preferably coded on a large number of bits.

So, if each continuous line CL represents a bit of the value V that is equal to zero, then the value V, represented by the deactivation pattern DS

before transformation, is equal to 0x00 (i.e. the value 0 for a 8 bits number). Now, if each interrupted line, obtained by the transformation of a continuous line CL by means of the cutting technique, represents a bit of the cipher CR of the first identifier I1 that is equal to one, then the activation pattern AS, 5 illustrated in figure 3 and resulting from the transformation of the deactivation pattern DS of figure 2, may represent the value 0x59 of the cipher CR of the first identifier I1 (i.e. the binary number 01011001).

A lot of other activation patterns AS made of different combinations of continuous lines CL and interrupted lines (obtained by the transformation of 10 continuous lines CL by means of the cutting technique) may be used to define numerous ciphers CR of the first identifier I1 for numerous chips CH.

The third step (iii) consists in getting a value V representative of the activation pattern AS into the electronic device CH. As mentioned above, the value V is generated inside the security circuit SC because it is connected to 15 the activation pattern AS resulting from the transformation of the deactivation pattern DS.

This value V may be a binary value or an analog value. In the last case, a resistance, a capacitance or an inductance modification is obtained by trimming the deactivation pattern DS.

20 The fourth step (iv) consists in computing a second identifier I2 with the transformed chip CH (and more precisely with its security circuit SC) by feeding the reverse function F^{-1} of the predetermined function F with the generated value V (which is supposed to be the cipher CR of the first identifier I1) and the secret key K (so, $F^{-1}(K, CR) = I2$). Then, if this second identifier I2 is 25 equal to the first identifier I1 ($I2 = I1$, because $V = CR$), the security circuit SC triggers a comeback of its chip CH to the test mode. In other words, the security circuit SC authorizes the use of the test circuit TC, here for testing purpose. Now, if the second identifier I2 differs from the first identifier I1 ($I2 \neq I1$, because $V \neq CR$), the security circuit SC does not trigger a comeback of its 30 chip CH to the test mode. In other words, the security circuit SC does not authorize the use of the test circuit TC, and therefore the chip CH can just be used in its user mode which does not allow an attacker to access to its internal resources.

A non-limiting example of algorithm implementing the transformation method described above is schematically illustrated in figure 4.

This algorithm starts with a first optional step 10 consisting in transmitting a command requesting the first identifier I1 from an external computer to the chip CH.

Then the algorithm comprises a second optional step 20 consisting in searching the first identifier I1 into the chip CH, and then transmitting this first identifier I1 to the requesting computer.

Then the algorithm comprises a third step 30 consisting in externally computing a cipher CR of the first identifier I1 with the predetermined function F fed with the first identifier I1 and a predetermined secret key K ($F(K, I1) = CR$). This can be done into the requesting computer.

Then the algorithm comprises a fourth step 40 consisting in transforming the deactivation pattern DS of the chip CH to define an activation pattern AS representing the cipher CR of the first identifier I1 and that is intended to modify (or replace) the value V generated into the security circuit SC.

Then the algorithm comprises a fifth step 50 consisting in switching the chip CH on, then in getting into the security circuit SC the value V internally generated and representative of the activation pattern AS, and then in executing the reverse function F^{-1} with V (equal to CR) and K as parameters to compute a second identifier I2 ($F^{-1}(K, CR) = I2$) into the security circuit SC.

Then the algorithm comprises a sixth step 60 consisting in comparing the computed second identifier I2 with the first identifier I1 stored into the transformed chip CH. If the second identifier I2 differs from the first identifier I1 ($I2 \neq I1$), the algorithm follows with a seventh step 70 consisting in forbidding the comeback of the chip CH to the test mode. So, the chip CH can only be used in user mode. Now, if the computed second identifier I2 is equal to the first identifier I1 ($I2 = I1$), the algorithm follows with an eighth step 80 consisting in authorizing the comeback of the chip CH to the test mode.

The invention offers several advantages, and notably:

- it allows a simple way to disable a sensitive mode during chip production,
- it allows a simple but secure sensitive mode re-activation through a simple

chip transformation,

- it allows re-use of the chip after testing by a transformation of its activation pattern into the initial deactivation pattern,
- it allows a diversified transformation per chip,
- 5 - it allows having a transformation resistant to brute force attack,
- it allows having N continuous lines hidden within normal structure of the top metal level of the circuit.

The invention is not limited to the embodiments of transformation method and construction method described above, only as examples, but it
10 encompasses all alternative embodiments which may be considered by one skilled in the art within the scope of the claims hereafter.

CLAIMS

1. Method for transforming a secure electronic device (CH), associated to a first identifier and having a sensitive mode disabled after production, for a new sensitive use, characterized in that it comprises the steps of: (i) externally computing a cipher of said first identifier with a predetermined function fed with said first identifier and a predetermined secret key, (ii) transforming an accessible metal layer (ML) of said electronic device (CH) to form an activation pattern (AS) representing said externally computed cipher of the first identifier, (iii) getting a value representative of said activation pattern into said electronic device (CH), (iv) computing a second identifier with said transformed electronic device (CH) by feeding a reverse function of said predetermined function with said value and said secret key, to trigger a comeback to said sensitive mode if said second identifier is equal to said first identifier.

2. Method according to claim 1, characterized in that in step (iii) said value representative of said activation pattern is a binary value or an analog value.

3. Method according to one of claims 1 and 2, characterized in that in step (ii) one defines said activation pattern by means of a cutting technique that is intended to remove metallic parts into locations of said metallic layer (ML) that are defined by said computed cipher of said first identifier.

4. Method according to claim 3, characterized in that said computed cipher of said first identifier is defined by N bits that are respectively associated to N continuous lines (CL) of said metallic layer (ML) belonging to a security circuit (SC) of said electronic device (CH), and in that an untransformed continuous line (CL) represents a bit of said computed cipher of the first identifier that is equal to zero, while a continuous line (CL) transformed into an interrupted line represents a bit of said computed cipher of the first identifier that is equal to one.

5. Method according to claim 4, characterized in that N is greater than one.

6. Method according to one of claims 3 to 5, characterized in that said

cutting technique is chosen from a group comprising at least a laser cutting and a focused ion beam cutting.

7. Method according to one of claims 1 to 6, characterized in that said predetermined function is a cryptographic function.

8. Method according to claim 7, characterized in that said cryptographic function is chosen from a group comprising at least a simple Data Encryption Standard algorithm, a triple Data Encryption Standard algorithm, an Advanced Encryption Standard algorithm, and a RSA algorithm.

9. Method for producing a secure electronic device (CH) associated to a first identifier and having a sensitive mode disabled after production, characterized in that it comprises the steps of: (a) defining electronic circuits (EC) into said electronic device (CH) to perform predetermined functions, and notably a sensitive circuit (TC) intended for offering said sensitive mode, (b) defining a security circuit (SC) adapted to perform a reverse function using a key and a value representative of a pattern read from an accessible metallic layer, said security circuit being coupled to said sensitive circuit (TC) and intended for authorizing said sensitive circuit (TC) to offer said sensitive mode when it got a cipher of said first identifier from the reverse function, and (c) defining a deactivation pattern (DS) into the accessible metallic layer (ML) of said electronic device (CH), which is arranged for inducing into said security circuit (SC) the generation of a value by the reverse function that is different from said cipher of the first identifier and therefore prevents said sensitive circuit (TC) to offer said sensitive mode.

10. Method according to claim 9, characterized in that in step (c) one defines a deactivation pattern (DS) comprising N continuous lines (CL) associated respectively to N bits of said cipher of the first identifier.

11. Method according to claim 10, characterized in that a continuous line (CL) that is not transformed after a transformation phase represents a bit of said computed cipher of said first identifier that is equal to zero, while a continuous line (CL) that is transformed into an interrupted line after a transformation phase represents a bit of said computed cipher of the first identifier that is equal to one.

12. Method according to one of claims 9 to 11, characterized in that said

security circuit (SC) is arranged for feeding a reverse function of a predetermined function with a predetermined secret key and said cipher of the first identifier for computing a second identifier, and for triggering a comeback of said electronic device (CH) to said sensitive mode if said second identifier is equal to said first identifier.

13. Method according to claim 12, characterized in that said predetermined function is a cryptographic function.

14. Method according to claim 13, characterized in that said cryptographic function is chosen from a group comprising at least a simple Data Encryption Standard algorithm, a triple Data Encryption Standard algorithm, an Advanced Encryption Standard algorithm, and a RSA algorithm.

15. Method according to one of claims 9 to 14, characterized in that it is arranged for producing a secure electronic device (CH) defining a chip of a smart card (ED).

16. Secure electronic device (CH) obtained by a method according to one of claims 9 to 15.