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) 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, and (c) defining a deactivation pattern (DS) into an accessible metallic layer (ML) of said electronic device (CH), which is arranged for inducing into said security circuit (SC) the generation of a value 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.

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.