



- (51) **International Patent Classification:**
H04L 9/08 (2006.01) *H04L 9/00* (2006.01)
- (21) **International Application Number:**
PCT/EP2016/068448
- (22) **International Filing Date:**
2 August 2016 (02.08.2016)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
201511023157.7 31 December 2015 (31.12.2015) CN
- (71) **Applicant:** GEMALTO SA [FR/FR]; 6, Rue de la Verrerie, 92190 Meudon (FR).
- (72) **Inventors:** BOURSIER, Carine; Gemalto Sa, Intellectual Property Department, 6 rue de la Verrerie, 92190 Meudon (FR). MILLET, François; Gemalto Sa, Intellectual Property Department, 6 rue de la Verrerie, 92190 Meudon (FR). YANTO, Rudy; Gemalto Sa, Intellectual Property Department, 6 rue de la Verrerie, 92190 Meudon (FR).
- (74) **Agent:** LOTAUT, Yacine; Gemalto Sa, Intellectual Property Department, 6 Rue de la Verrerie, 92190 Meudon (FR).
- (81) **Designated States** (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) **Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

[Continued on next page]

(54) **Title:** METHOD FOR PROTECTING THE USE OF A CRYPTOGRAPHIC KEY IN TWO DIFFERENT CRYPTOGRAPHIC ENVIRONMENTS

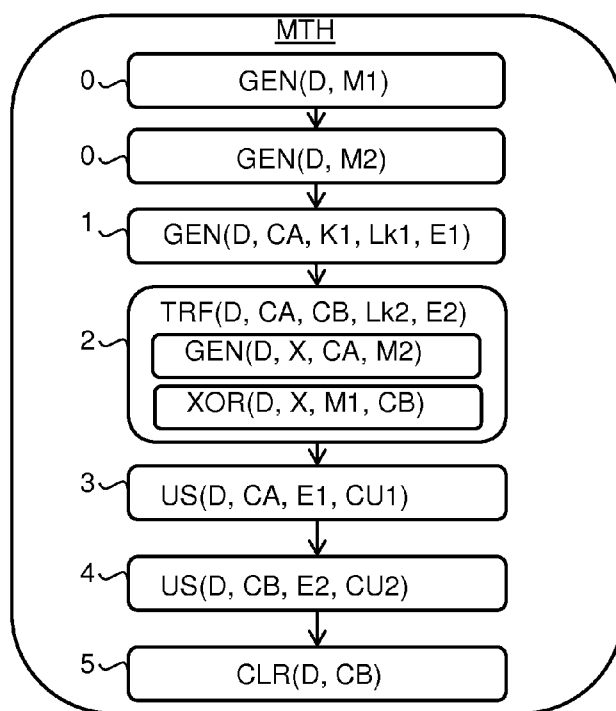


Fig. 1

(57) **Abstract:** The present invention relates to a method (MTH) for protecting a cryptographic key (K1) within a first cryptographic environment (E1) of an electronic device (D) with a first security level (L1) and within a second cryptographic environment (E2) of said electronic device (D) with a second security level (L2), wherein: • said electronic device being operated to derive a first cryptographic data (CA) from the cryptographic key (K1) in order to obtain a first key adapted to the security level (Lk1) of said first cryptographic environment (E1), said first cryptographic data (CA) being paired with said first cryptographic environment (E1); • using said first cryptographic data (CA) within said first cryptographic environment (E1); • said electronic device being operated to apply a transformation operation to said first cryptographic data (CA) to provide a second cryptographic data (CB) in order to obtain a second key adapted to the security level (Lk2) of said second cryptographic environment (E1), said second key adapted to the security level (Lk2) being different from the first key adapted to the security level (Lk1), and said second cryptographic data (CB) being paired with said second cryptographic environment (E2), said operation transformation being configured so that the provided second cryptographic data is derived from the cryptographic key (K1); • using said second cryptographic data (CB) within said second cryptographic environment (E2).

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*

METHOD FOR PROTECTING THE USE OF A CRYPTOGRAPHIC KEY IN TWO DIFFERENT CRYPTOGRAPHIC ENVIRONMENTS

TECHNICAL FIELD

5 The present invention relates to a method for protecting the use of a cryptographic key into two different cryptographic environment having respectively different security level.

Particularity, the present invention relates to the transformation of the cryptographic key into cryptographic data in order to use said cryptographic
10 key within a first cryptographic environment of an electronic device with a first security level and within a second cryptographic environment of an electronic device with a second security level.

The invention also relates to an associated electronic device.

15 BACKGROUND OF THE INVENTION

A method for transforming at least one cryptographic key into a cryptographic data in order to use said cryptographic key within a first cryptographic environment of an electronic device with a first security level and within a second cryptographic environment of an electronic device with a
20 second security level, well-known by the man skilled in the art, comprises a step of applying a mask on said cryptographic key to obtain a cryptographic data in order to make the cryptographic key confidential. The cryptographic data is used within any cryptographic environment in the electronic device which needs the use of said cryptographic key, such as the first and the
25 second cryptographic environments.

A first cryptographic environment comprises a first security level which is different from a second security level of the second cryptographic environment. In a non-limitative example, the first security level may be
30 protections against Differential Power Analysis (known as DPA), whereas the second security level may be without protections against DPA.

One problem of this prior art is that when using a masked key which is highly secure for the first cryptographic environment with also the second environment, this leads to an implementation which is costly in terms of
35 resources as the same security level is to be applied for the first and second

2

cryptographic environments, although the second cryptographic environment doesn't need a security level as secure as the first cryptographic environment's one.

5 **SUMMARY OF THE INVENTION**

The following summary of the invention is provided in order to provide a basic understanding of some aspects and features of the invention. This summary is not an extensive overview of the invention and as such it is not intended to particularly identify key or critical elements of the invention or to
10 delineate the scope of the invention. Its sole purpose is to present some concepts of the invention in a simplified form as a prelude to the more detailed description that is presented below.

It is an object of the invention to provide a method for transforming at least one cryptographic key into a cryptographic data in order to use said
15 cryptographic key within a first cryptographic environment of an electronic device with a first security level and within a second cryptographic environment of said electronic device with a second security level, said cryptographic key comprising first and second conditions of use respectively for said first cryptographic environment and for said second cryptographic
20 environment, which resolves the above-mentioned problem.

To this end, there is provided a method for transforming at least one cryptographic key into a cryptographic data in order to use said cryptographic key within a first cryptographic environment of an electronic device with a first security level and within a second cryptographic environment of said
25 electronic device with a second security level, said cryptographic key comprising first and second conditions of use respectively within said first cryptographic environment and said second cryptographic environment, wherein said method comprises:

- generating a first cryptographic data from the cryptographic key
30 without exposing said cryptographic key in order to obtain a first key adapted to the security level of said first cryptographic environment, said first cryptographic data being paired with said first cryptographic environment;
- transforming said first cryptographic data into a second cryptographic data without exposing said cryptographic key in order to obtain
35 a second key adapted to the security level of said second cryptographic

3

environment, said second key adapted to the security level being different from the first key adapted to the security level, and said second cryptographic data being paired with said second cryptographic environment;

• using said first cryptographic data within said first cryptographic environment with respect to said first conditions of use of said cryptographic key; and

• using said second cryptographic data within said second cryptographic environment with respect to said second conditions of use of said cryptographic key.

10

To achieve those and other advantages, and in accordance with the purpose of the invention as embodied and broadly described, the invention proposes a method (MTH) for protecting a cryptographic key within a first cryptographic environment of an electronic device with a first security level and within a second cryptographic environment of said electronic device with a second security level, wherein: said electronic device being operated to:

15

• derive a first cryptographic data from the cryptographic key in order to obtain a first key adapted to the security level of said first cryptographic environment, said first cryptographic data being paired with said first cryptographic environment;

20

• using said first cryptographic data within said first cryptographic environment;

• apply a transformation operation to said first cryptographic data to provide a second cryptographic data in order to obtain a second key adapted to the security level of said second cryptographic environment, said second key adapted to the security level being different from the first key adapted to the security level, and said second cryptographic data being paired with said second cryptographic environment, said operation transformation being configured so that the provided second cryptographic data is derived from the cryptographic key,

25

30

• using said second cryptographic data within said second cryptographic environment.

According to non-limitative embodiments of the invention, the method in accordance with the invention further comprises the following

35

4

characteristics.

In a non-limitative embodiment, the first cryptographic environment and the second cryptographic environment are part of a same communication protocol.

In a non-limitative embodiment, the first security level is higher than the second security level and the first key adapted to the first security level is securely higher than the second key adapted to the second security level.

In a non-limitative embodiment, the first security level is securely lower than the second security level and the first key adapted to the first security level is securely lower than the second key adapted to the second security level.

In a non-limitative embodiment, the derivation of said first cryptographic data is a function of said cryptographic key and a first mask.

In a non-limitative embodiment, the transformation of said first cryptographic data into said second cryptographic data is function of a second mask and said first mask.

In a non-limitative embodiment, said method further comprises generating said first and said second masks associated respectively to the first and to the second cryptographic environment.

In a non-limitative embodiment, the transformation of said first cryptographic data comprises:

- generating an intermediary value which is the result of an XOR of said first cryptographic data and said second mask ; and
- XORing said intermediary value with said first mask in order to generate said second cryptographic data.

In a non-limitative embodiment, a mask is based on a master mask and on a diversifier.

5

In a non-limitative embodiment, a master mask is common to all the cryptographic keys used by said electronic device and a diversifier is different from one cryptographic key to another one.

5

In a non-limitative embodiment, said first cryptographic environment comprises a first set of cryptographic functions and said second cryptographic environment comprises a second set of cryptographic functions.

10

In a non-limitative embodiment, said first cryptographic environment comprises a first set of cryptographic functions implementing a mutual authentication between said electronic device and a remote server.

15

In a non-limitative embodiment, said second cryptographic environment comprises a second set of cryptographic functions implementing a data exchange between said electronic device and a remote server.

20

In a non-limitative embodiment, said electronic device is a secure element.

In a non-limitative embodiment, said secure element is a smart card, an embedded secure element, a micro-SD, an UICC.

25

The present invention also relates to an electronic device comprising - a processor; and a memory coupled to the processor and instructions stored into the memory that performs the method for protecting a cryptographic key within a first cryptographic environment of an electronic device with a first security level and within a second cryptographic environment of said electronic device with a second security level, wherein:

30

In addition, there is provided an electronic device adapted to transform at least one cryptographic key into a cryptographic data in order to use said cryptographic key within a first cryptographic environment of said

35

6

electronic device with a first security level and within a second cryptographic environment of said electronic device with a second security level, said cryptographic key comprising first and second conditions of use respectively within said first cryptographic environment and said second cryptographic environment, wherein said electronic device comprises an execution platform which is adapted to:

- generate a first cryptographic data from the cryptographic key without exposing said cryptographic key in order to obtain a first key adapted to the security level for said cryptographic key, said first cryptographic data being paired with said first cryptographic environment;

- transform said first cryptographic data into a second cryptographic data without exposing said cryptographic key in order to obtain a second key adapted to the security level for said cryptographic key, said second key adapted to the security level being different from the first key adapted to the security level, and said second cryptographic data being paired with said second cryptographic environment;

- use said first cryptographic data within said first cryptographic environment with respect to said first conditions of use of said cryptographic key; and

- use said second cryptographic data within said second cryptographic environment with respect to said second conditions of use of said cryptographic key.

The foregoing is a summary and thus may contain simplifications, generalizations, and omissions of detail; consequently, those skilled in the art will appreciate that the summary is illustrative only and is not intended to be in any way limiting.

For a better understanding of the embodiments, together with other and further features and advantages thereof, reference is made to the following description, taken in conjunction with the accompanying drawings. The scope of the invention will be pointed out in the appended claims.

BRIEF DESCRIPTION OF THE FIGURES

Some embodiments of methods and/or apparatus in accordance with embodiments of the present invention are now described, by way of example

only, and with reference to the accompanying drawings, in which:

- Fig.1 illustrates schematically an organization chart of a method according to a non-limitative embodiment of the invention;

5 - Fig. 2 illustrates an electronic device which is adapted to carry out the method of Fig. 1;

- Fig. 3 illustrates a first cryptographic data and a second cryptographic data which are generated by the method of Fig. 1 and which are respectively paired to two different cryptographic environments; and

10 - Fig. 4 illustrates the use of these first cryptographic data and second cryptographic data by the electronic device of Fig. 2, when said electronic device cooperates with a remote server and a local terminal.

DESCRIPTION OF EMBODIMENTS OF THE INVENTION

15 It will be readily understood that the components of the embodiments, as generally described and illustrated in the figures herein, may be arranged and designed in a wide variety of different configurations in addition to the described example embodiments. Thus, the following more detailed description of the example embodiments, as represented in the figures, is not intended to limit the scope of the embodiments, as claimed, but is merely
20 representative of example embodiments.

Reference throughout the specification to one embodiment or an embodiment means that a particular feature, structure, or characteristic described in connection with an embodiment is included in at least one embodiment of the subject matter disclosed. Thus, the appearance of the
25 phrases in one embodiment or in an embodiment in various places throughout the specification is not necessarily referring to the same embodiment. Further, the particular features, structures or characteristics may be combined in any suitable manner in one or more embodiments.

As used herein, the singular forms a, an and the are intended to
30 include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms comprises and/or comprising, when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features,
35 integers, steps, operations, elements, components, and/or groups thereof.

8

In the following description, numerous specific details are provided to give a thorough understanding of embodiments. One skilled in the relevant art will recognize, however, that the various embodiments can be practiced without one or more of the specific details, or with other methods, components, materials, et cetera. In other instances, well-known structures, materials, or operations are not shown or described in detail to avoid obfuscation.

The present invention is not specific to any particular hardware or software implementation, and is at a conceptual level above specifics of implementation. It is to be understood that various other embodiments and variations of the invention may be produced without departing from the spirit or scope of the invention. The following is provided to assist in understanding the practical implementation of particular embodiments of the invention.

The same elements have been designated with the same referenced numerals in the different drawings. For clarity, only those elements and steps which are useful to the understanding of the present invention have been shown in the drawings and will be described.

Further, the mechanisms of data communication between the parties and their environment have not been detailed either, the present invention being here again compatible with usual mechanisms.

Furthermore, the connecting lines shown in the various figures contained herein are intended to represent exemplary functional relationships and/or physical couplings between the various elements. It should be noted that many alternatives or additional functional relationships or physical connections may be present in a practical system. Furthermore, the various entities in FIG. 1 to FIG. 4 may communicate via any suitable communication medium using any suitable communication protocol.

The present invention relates to a method MTH for transforming at least one cryptographic key K1 into a first cryptographic data CA, and a second cryptographic data CB respectively use within a first cryptographic environment E1 of an electronic device D with a first security level L1 and within a second cryptographic environment E2 of said electronic device D with a second security level L2. Said cryptographic key K1 comprises first and second conditions of use CU1, CU2 respectively within said first

9

cryptographic environment E1 and said second cryptographic environment E2.

Said method MTH is illustrated in Fig. 1 in a non-limitative
5 embodiment. It is carried out by an electronic device D illustrated in Fig. 2.

In a non-limitative embodiment, one or a plurality of cryptographic
keys K1 are used by the electronic device D within at least one cryptographic
environment E.
10

In a non-limitative embodiment, said first cryptographic environment
E1 comprises a first set of cryptographic functions F1 and said second
cryptographic environment E2 comprises a second set of cryptographic
functions F2.

15 Each cryptographic function F1, F2 uses a cryptographic key K1 and
produces a result.

Hence a cryptographic function F is always executed with a
cryptographic key K1 (in particular with the first cryptographic data CA for F1,
or with the second cryptographic data CB for F2), but said cryptographic key
20 K1 may changed from one execution to the other.

In a non-limitative example, a cryptographic function F which is a
3DES may be called with a first cryptographic key for a banking application,
and with second cryptographic key for a transport application. Said different
cryptographic keys will lead respectively to the first cryptographic data CA
25 and to the second cryptographic data CB generated from the cryptographic
key K1.

In non-limitative examples, the first set of cryptographic functions F1
implements session keys generation, a mutual authentication between said
30 electronic device D and a remote server etc.

In non-limitative examples, the second set of cryptographic function
F2 implements a DES/AES, data exchange, an encryption/decryption of
data, a MAC (Message Authentication Code) computation of data, data
integrity checking with a MAC etc.
35

10

The first security level L1 and the second security level L2 are different.

In a non-limitative embodiment, the first security level L1 is higher than the second security level L2.

5

In a non-limitative embodiment, said first security level L1 comprises high level security countermeasures. In a non-limitative example, it comprises protections against DPA ("Differential Power Analysis"), against CPA ("Correlation Power Analysis"), against DFA ("Differential Fault Attack") etc.

10

In a non-limitative embodiment, said second security level L2 comprises low level security countermeasures or none. In a non-limitative example, it doesn't comprise any protection against DPA.

15

In the non-limitative embodiment, the first cryptographic environment E1 is therefore a secure cryptographic environment, whereas the second cryptographic environment E2 is a less secure one.

20

The security level Lk of the cryptographic data generated from the cryptographic key K1 depends on the security level L associated to the cryptographic environment E which will use said cryptographic data.

In the implementation hereinafter described, the security level Lk1 of the cryptographic data CA is higher than the second security level Lk2 of the cryptographic data CB.

25

As illustrated in Fig. 3, the first cryptographic data CA will provide a first key adapted to the security level Lk1 and will be use only by the cryptographic functions F1 of the first cryptographic environment E1. The first cryptographic data CA may not be used within another cryptographic environment.

30

The second cryptographic data CB will provide a second key adapted to the security level Lk2 and will be use only by the cryptographic functions F2 of the second cryptographic environment E2. The second cryptographic data CB may not be used within another cryptographic environment.

35

The two different cryptographic environments E1, E2 with the different

11

security levels L1, L2 may be

part of a same communication protocol.

In a non-limitative embodiment illustrated in Fig. 4, the communication protocol is a Global Platform Procedure.

5 This Global Platform Procedure comprises:

- a mutual authentication phase MUT_AUTH between said electronic device D and a remote server RS, which is based on a set of session keys K11, K12 generated from a static key;
 - a secure messaging channel SM set-up for exchanging data
- 10 between said electronic device D and said remote server RS;
- a data exchange DAT_E through said secure messaging channel SM using said set of session keys, which comprises encryption/decryption ENCR/DECR of data, MAC (Message Authentication Code) computation, and checking the integrity of the data CHK_MAC.

15

After the secure messaging channel SM is set-up, data exchange may be performed between said electronic device D and said remote server RS.

20 The first conditions of use CU1 and the second conditions of use CU2 refer to how the cryptographic key K1 is used within a cryptographic function F of a cryptographic environment E.

In non-limitative examples, the first conditions of use CU1 comprise the ciphering of different messages with the cryptographic key K1 before any authentication, the number of times one may use the cryptographic key K1

25 within a cryptographic function, the variability of the input of the cryptographic function, the knowledge of the input, the knowledge of the output etc.

In non-limitative examples, the second conditions of use CU2 comprise the ciphering of different messages with the cryptographic key K1 only after an authentication, the number of times one may use the

30 cryptographic key K1 within a cryptographic function, the variability of the input of the cryptographic function, the knowledge of the input, the knowledge of the output etc.

It is to be noted that with the conditions of use CU1, CU2, one may

35 determine a set of attacks which may be applied to break a cryptographic

12

key K1. Therefore, according to these attacks, one may set-up some countermeasures that will define the security level L of the cryptographic environment E which will use the cryptographic key K1. Therefore, to one determined conditions of use CU is associated a determined security level L.

5

For example, if the variability of the input of the cryptographic function is high, this means that a possible attack to break the cryptographic key K1 may be a DPA. It is to be noted that the variability of the input means that an external entity such as a remote server, in a non-limitative example, is authorized to control and vary the input of the cryptographic function F.

10

The method MTH is described in details hereinafter in a non-limitative embodiment.

15

As illustrated in Fig. 1, the method MTH comprises:

In **step 1**) illustrated in Fig. 1 GEN(D, CA, K1, Lk1, E1), said electronic device D generates a first cryptographic data CA from the cryptographic key K1 without exposing said cryptographic key K1 in order to obtain a first key adapted to the security level Lk1 of said first cryptographic environment, said first cryptographic data CA being paired with said first cryptographic environment E1.

20

In a non-limitative embodiment, the generation of said first cryptographic data CA is function of said cryptographic key K1 and a first mask M1.

25

The first mask M1 permits to obtain a first key adapted to the security level Lk1 of said first cryptographic environment.

In the non-limitative embodiment, the first mask M1 is defined in order to obtain a high secure key adapted to the security level of said first cryptographic environment.

30

The first mask M1 is defined so that it resists the attacks from an attacker who wants to recover the cryptographic key K1.

In a non-limitative embodiment (described in the following), when the first mask M1 is based on a first master mask MM1 and a first diversifier D1, in order to make the mask M1 secure, the first diversifier D1 is stored in

35

13

memory far apart from the cryptographic key K1 so that an attacker will have more difficulties to recover said first diversifier D1.

Hence, the way to compute this first mask M1 will always be used for the cryptographic key K1 which is used with a cryptographic function F1.

5

In a non-limitative embodiment, the method MTH is further adapted to generate said first mask M1 associated to said first cryptographic environment E1 (illustrated GEN(D, M1)). This step is performed previously to the first step (step 0)).

10

In a non-limitative embodiment, said first cryptographic data CA = K1 XOR M1.

The cryptographic key K1 is never exposed in clear.

15

In a non-limitative embodiment, the first mask M1 is based on a first master mask MM1 and on a first diversifier D1.

The first master mask MM1 and the first diversifier D1 permit to have a different first mask M1 for each different cryptographic key K1.

Therefore, if there is a memory dump of the cryptographic data CA corresponding to the masked cryptographic key K1, an attacker won't be able to recover another cryptographic key K1 of the electronic device D.

20

The use of a first master mask MM1 in combination with a first diversifier D1 permit to have a strong security even if the first diversifier D1 is broken by an attacker, this latter may not recover the first master mask MM1 unless he attacks at the same time the first master mask MM1, which is more difficult to do.

25

In a non-limitative variant of said embodiment, said first mask M1= MM1 XOR D1, and the first cryptographic data CA = K1 XOR (MM1XOR D1).

30

Said first cryptographic data CA is stored in memory.

In a non-limitative embodiment, when the cryptographic key K1 is a persistent key (also called static), the first cryptographic data CA may be stored in a non-volatile memory.

35

In a non-limitative embodiment, when the cryptographic key K1 is a

14

non-persistent key (also called transient key), the first cryptographic data CA may be stored in a volatile memory.

As the first mask M1 is secure, the storage of the cryptographic key K1 via the first cryptographic data CA is secure.

5 The cryptographic key K1 is stored in the electronic device D in masked value. The first cryptographic data CA is the cryptographic key K1 which is masked in a secure way.

Said masked cryptographic key CA will be manipulated within the first cryptographic environment E1 instead of the cryptographic key K1 in clear.

10 The first cryptographic data CA is paired with the first cryptographic environment E1 as it will be used by at least one cryptographic function F1 of said first cryptographic environment E1. It can only be used by said first cryptographic environment E1. In a non-limitative embodiment, the pairing is performed by storing in memory a pair CA-L1, that is to say when storing the
15 first cryptographic data CA, the associated first security level L1 is also stored.

In the non-limitative embodiment, the first cryptographic environment E1 is of a high level security L1 and the first mask M1 permits to better
20 protect the cryptographic key K1 against an attacker than the second mask M2 as said cryptographic key K1 is more exposed to attack within said first cryptographic environment E1.

Before any cryptographic function F2 which needs the cryptographic
25 key K1 is executed, said cryptographic key K1 is transferred that is to say is masked differently so that a second adapted to the security level Lk2 different from the first key adapted to the security level Lk1 is provided, and then said cryptographic key K1 is used within the second cryptographic environment E2. The said cryptographic key K1 is transferred according to
30 the following step.

In **step 2)** illustrated in Fig. 1 TRF(D, CA, CB, Lk2, E2), said electronic device D transforms said first cryptographic data CA into a second cryptographic data CB without exposing said cryptographic key K1 in order to
35 obtain a second key adapted to the security level Lk2 of said second

15

cryptographic environment, said second key adapted to the security level Lk2 being different from the first key adapted to the security level Lk1, and said second cryptographic data CB being paired with said second cryptographic environment E2.

5

In a non-limitative embodiment, when the second security level L2 of said second cryptographic environment E2 is lower than the first security level L1 of said first cryptographic environment E1, the second key adapted to the security level Lk2 is securely lower than the first key adapted to the security level Lk1.

10

The aim is to mask the cryptographic key K1 with the second mask M2 to obtain a second key adapted to the security level Lk2 securely lower than the first key adapted to the security level Lk1. If one computes directly the cryptographic key K1 with the mask M2, the cryptographic key K1 is manipulated in clear and therefore is exposed to an attacker. In order to avoid this, said first cryptographic data CA is transformed as following.

15

In a non-limitative embodiment, the transformation of said first cryptographic data CA into said second cryptographic data CB is function of a second mask M2 and said first mask M1.

20

The second mask M2 permits to obtain a second key adapted to the security level Lk2 of said second cryptographic environment.

25

In the non-limitative embodiment, the second mask M2 is defined in order to obtain a low key adapted to the security level for said cryptographic key K1.

The second mask M2 is defined so that it will less resist the attacks from an attacker who wants to recover the cryptographic key K1. But if said second mask M2 is recovered by an attacker, it won't jeopardize the security of the first cryptographic data CA which is well secure.

30

In a non-limitative embodiment, the second mask M2 is a constant.

In another non-limitative embodiment (described in the following), when the second mask M2 is based on a second master mask MM2 and a second diversifier D2, the second diversifier D2 is stored in memory next to

35

16

the cryptographic key K1.

Hence, the way to compute this second mask M2 will always be used for the cryptographic key K1 which is used with a cryptographic function F2.

5 In a non-limitative embodiment, the method MTH is further adapted to generate said second mask M2 associated to said second cryptographic environment E2 (illustrated GEN(D, M2)). This step is performed previously to the first step or just before the second step (step 0)).

10 In a non-limitative embodiment, the transformation of said first cryptographic data CA comprises:

15 - generating by means of said electronic device D an intermediary value X which is the result of an XOR of said first cryptographic data CA and said second mask M2 (sub-step illustrated in Fig. 1 GEN(D, X, CA, M2)); and

- XORing by means of said electronic device D said intermediary value X with said first mask M1 in order to generate said second cryptographic data CB (sub-step illustrated in Fig. 1 XOR(D, X, M1, CB)).

20

Hence, $X = CA \text{ XOR } M2$

$$CB = X \text{ XOR } M1$$

Hence, the electronic device D only computes CA XOR M2 resulting in X, then X XOR M1 resulting in CB. During these computations to obtain the second cryptographic data CB, the cryptographic key K1 is never exposed in clear and is never manipulated.

By applying firstly the second mask M2, then secondly the first mask M1, it permits to never manipulate the cryptographic key K1 during the computation of the second cryptographic data CB (contrary to a computation where the first mask M1 would be applied to the first cryptographic data CA, then the second mask M2 applied to the intermediate value X to obtain the second cryptographic data CB).

35 It is to be noted that said result X XOR M1 is equivalent to K1 XOR

17

M2, as it is equal to $= CA \text{ XOR } M2 \text{ XOR } M1 = K1 \text{ XOR } M1 \text{ XOR } M2 \text{ XOR } M1$.

5 In a non-limitative embodiment, the second mask M2 is based on a second master mask MM2 and on a second diversifier D2. In a non-limitative variant of said embodiment, said second mask $M2 = MM2 \text{ XOR } D2$.

The use of a second master mask MM2 in combination with a second diversifier D2 permits to have a strong security as if the second diversifier D2 is broken by an attacker, this latter may not recover the second master mask MM2 unless he attacks at the same time the second master mask MM2, which is more difficult to do.

15 In a non-limitative embodiment, said second cryptographic data CB is computed on the fly, each time a cryptographic function F2 of the second cryptographic environment E2 needs the cryptographic key K1 to be executed, that is to say before the execution of said cryptographic function F2. In an embodiment, the second cryptographic data CB may be stored in a volatile memory.

20 In another non-limitative embodiment, said second cryptographic data CB is stored in memory, which may be either non-volatile, or volatile, which may depend on if the cryptographic key K1 is respectively static or transient.

25 As the second mask M2 is less secure than the first mask M1, the storage of the cryptographic key K1 via the second cryptographic data CB is less secure than the storage of the cryptographic key K1 via the first cryptographic data CA.

The cryptographic key K1 is stored in the electronic device D in masked value. The second cryptographic data CB is the cryptographic key K1 which is masked in a less secure way.

30 Said masked cryptographic key CB will be manipulated within the second cryptographic environment E2 instead of the cryptographic key K1 in clear.

The second cryptographic data CB is paired with the second cryptographic environment E2 as it will be used by at least one cryptographic function F2 of said second cryptographic environment E2. It can only be

18

used by said second cryptographic environment E2.

In a non-limitative embodiment, the pairing is performed by storing in memory a pair CB-L2, that is to say when storing the second cryptographic data CB, the associated second security level L2 is also stored.

5

In the non-limitative embodiment above-described, the second cryptographic data CB is a degraded way to store the cryptographic key K1. The second key adapted to the security level Lk2 is a degraded secure level compared to the first key adapted to the security level Lk1.

10

The transformation of the first cryptographic data CA into a second cryptographic data CB permits to perform a key transfer of the cryptographic key K1 from the first cryptographic environment E1 (which is secure in the non-limitative embodiment described) to the second cryptographic environment E2 (which is less secure in the non-limitative embodiment described). The key transfer method proposed herein allows to securely modify the mask of the cryptographic key K1 in order to transform it into a key adapted to the needed security level Lk so as to bring it in line with the security level L of the cryptographic environment E which will use said cryptographic key K1.

20

The different masks M1, M2 permit to give respectively the right key adapted to the security level Lk1, Lk2 to the cryptographic key K1 according to respectively the cryptographic environments E1, E2 needs, that is to say according to respectively their security levels L1, L2.

25

In other words, the different masks M1, M2 permit to securely store the cryptographic key K1 and to give respectively a different storage security level Lk1, Lk2 depending respectively on the security level L1, L2 of the cryptographic environments E1, E2.

30

Others known protection memory can be added to reinforce the protection of the storage of the masked cryptographic key.

In **step 3)** illustrated in Fig. 1 US(D, CA, E1, CU1), said electronic device D uses said first cryptographic data CA within said first cryptographic

35

19

environment E1 with respect to said first conditions of use CU1 of said cryptographic key K1.

It is to be noted that in a non-limitative embodiment, a cryptographic
5 function F (F1 described here or F2 described in the following) is part of a command received by the electronic device D from an external entity, such as for example, a remote server. For example, when the electronic device D is a smart card, a cryptographic function F1 is part of an APDU (Application Protocol Data Unit) command.

10 For each received command, some conditions must be verified before the execution of the command. In non-limitative examples, the conditions may be as following: a challenge is sent before executing the current command, an authentication is performed before executing the current command, a previous command is sent and successfully executed before
15 the current command, a security flag is raised, an electronic device state or an application state is set to a given value etc.

The implementation of all the checks will be performed according to a communication protocol specifications and/or application specifications which specify the commands to be executed.

20 By this way, the conditions of use CU for executing a cryptographic function F are checked.

When a cryptographic function F1 is executed by the electronic device D, said electronic device D will use the first cryptographic data CA and the
25 first mask M1, as it knows which mask to use in this case.

In a non-limitative example as illustrated in Fig. 4, the first cryptographic environment E1 comprises a first set of cryptographic functions F1 implementing a mutual authentication MUT_AUTH between said
30 electronic device D and a remote server RS.

In the case of the Global Platform Procedure above-described, the cryptographic key K1 is a set of sessions key K11, K12 which is generated from a static key which can be an authentication private key. This set of sessions key K11, K12 is used for the mutual authentication, that is to say
35 before an external entity is authenticated.

20

In this case, during the mutual authentication, the cryptographic key K1 is highly exposed to attacker. Therefore, it needs a high secure key adapted to the security level, which is in a non-limitative example the first key adapted to the security level Lk1 which is provided through the first cryptographic data CA.

After the mutual authentication occurred, if it is a success, the cryptographic key K1 which will be used is less exposed to an attacker as only the authorized entity, here a remote server RS, may reach this phase. Therefore, it needs a lower secure key adapted to the security level, which is in a non-limitative example the second key adapted to the security level Lk2 which is provided through the second cryptographic data CB.

Hence, the step 4) described hereinafter is performed.

In **step 4)** illustrated in Fig. 1 US(D, CB, E2, CU2), said electronic device D uses said second cryptographic data CB within said second cryptographic environment E2 with respect to said second conditions of use CU2 of said cryptographic key K1.

When a cryptographic function F2 is executed by the electronic device D and if it needs the cryptographic key K1, said electronic device D will use the second cryptographic data CB and the second mask M2 as it knows which mask to use in this case.

It is to be noted that in a non-limitative embodiment, after the mutual authentication is processed, a secure message channel SM is set-up between the electronic device D and the remote server RS to exchange data DAT securely. The electronic device D and the remote server RS exchange data using the cryptographic key K1 which is a set of session keys K11, K12.

In a non-limitative example illustrated in Fig. 4, the second cryptographic environment E2 comprises a second set of cryptographic functions F2 implementing a data exchange DAT_E between said electronic device D and a remote server SERV.

21

Said data exchange DAT_E comprises encryption/decryption of data ENCR/DECR, MAC computation, and/or checking integrity of data CHK_MAC.

5 In the non-limitative example of the cryptographic key K1 which is a set of session keys K11, K12:

- the first session key K11 will be used to encrypt data of the electronic device D, and to decrypt incoming data from the remote server RS which has been authenticated before;

10 - the second session key K12 will be used to check integrity of the incoming data from the remote server RS which has been authenticated before, via a MAC (Message Authentication Code) in a non-limitative example.

The set of session keys K11, K12 is never exposed.

15 The data exchange DAT_E is secure as it is performed via a secure message channel SM.

As the security level L2 of the second cryptographic environment E2 is less secure than the first one L1 of the first cryptographic environment E1, the cryptographic functions F2 comprise less countermeasures, and therefore less complex unit operations than the first cryptographic functions F1. Hence, the cryptographic functions F2 are faster to be executed and they use less volatile memory for their execution. Therefore, it improves the time and memory performances of the whole communication protocol.

25

In a non-limitative embodiment where the electronic device D is a secure element such as a smart card, an eSE, an UICC, a micro-SD, the data are exchanged by means of APDU (Application Protocol Data Unit).

30 In a non-limitative embodiment, after the data exchange has been processed, the second cryptographic value CB is erased from the memory of the electronic device D (**step 5**) illustrated in Fig. 1 CLR(D, CB)). It permits to save some memory.

35 Hence, with the method MTH, the same cryptographic key K1 with two

22

different keys adapted respectively to the security level Lk1, Lk2 may be used respectively within two different cryptographic environments E1, E2 with two different security levels L1, L2 without compromising and exposing the cryptographic key K1, and with respect to the different conditions of used
5 CU1, CU2 of said cryptographic key K1 with respectively the two different cryptographic environments E1, E2.

The method MTH above-described is carried out by the electronic
10 device D adapted to transform at least one cryptographic key K1 into a cryptographic data in order to use said cryptographic key K1 within a first cryptographic environment E1 of said electronic device D with a first security level L1 and within a second cryptographic environment E2 of said electronic device D with a second security level L2, said cryptographic key K1
15 comprising first and second conditions of use CU1, CU2 respectively within said first cryptographic environment E1 and said second cryptographic environment E2.

The electronic device D is described with reference to Fig. 2.
20

In a non-limitative embodiment, the electronic device D is a secure element.

A secure element is a secure component which may perform cryptographic functionalities and is adapted to store a secret key.

25 In a non-limitative variant, the electronic device D is a smart card. In non-limitative examples, the smart card is an Electronic Identity Card, is a health card, a driving license, a passport, a privacy card, a financial service card, an access card etc. It may be contact or contactless.

In other non-limitative variants, the electronic device D is an eSE
30 (embedded secure element), a micro-SD, an UICC (Universal Integrated Circuit Card). In another non-limitative embodiment, the electronic device D is a mobile phone, a smart phone, a tablet etc. Said electronic device D may comprise a secure element.

23

Said electronic device D comprises an execution platform EP which is adapted to:

- generate a first cryptographic data CA from the cryptographic key K1 without exposing said cryptographic key K1 in order to obtain a first key adapted to the security level Lk1 for said cryptographic key K1, said first cryptographic data CA being paired with said first cryptographic environment E1 (function illustrated GEN(D, CA, K1, Lk1, E1)) ;
- transform said first cryptographic data CA into a second cryptographic data CB without exposing said cryptographic key K1 in order to obtain a second key adapted to the security level Lk2 for said cryptographic key K1, said second key adapted to the security level Lk2 being different from the first key adapted to the security level Lk1, and said second cryptographic data CB being paired with said second cryptographic environment E2 (function illustrated TRF(D, CA, CB, Lk2, E2));
- use said first cryptographic data CA within said first cryptographic environment E1 with respect to said first conditions of use CU1 of said cryptographic key K1 (function illustrated US(D, CA, E1, CU1)); and
- use said second cryptographic data CB within said second cryptographic environment E2 with respect to said second conditions of use CU2 of said cryptographic key K1 (function illustrated US(D, CB, E2, CU2)).

In a non-limitative embodiment, said execution platform EP is further adapted to:

- generate the first mask M1 (function illustrate GEN(D, M1));
- generate the second mask M2 (function illustrate GEN(D, M2)).

In a non-limitative embodiment, said execution platform EP is further adapted to erase said second cryptographic value CB from the electronic device's memory (function illustrated CLR(D, CB)).

30

In a non-limitative embodiment, said execution platform EP is further adapted to:

- generate an intermediary value X which is the result of an XOR of said first cryptographic data CA and said second mask M2 (sub-function illustrated in Fig. 2 GEN(D, X, CA, M2)); and

35

24

- XORing said intermediary value X with said first mask M1 in order to generate said second cryptographic data CB (sub-function illustrated in Fig. 2 XOR(D, X, M1, CB)).

5 In a non-limitative embodiment, said execution platform EP is a processor unit or a virtual machine.

In a non-limitative embodiment, said processor unit comprises one or a plurality of processors.

10

It is to be understood that the present invention is not limited to the aforementioned embodiments.

Hence, a cryptographic key K1 may be transformed into more than two cryptographic data in order to be used respectively within more than two different cryptographic environments E with different associated security level L. Hence, in a non-limitative example, a cryptographic key K1 may be used within three cryptographic environments with three different security levels, one high security level, one medium security level, and one low security level.

20 Hence, in another non-limitative embodiment, the first security level L1 is lower than the second security level L2 and the first key adapted to the security level Lk1 is lower than the second key adapted to the security level Lk2.

25 Hence, some embodiments of the invention may comprise one or a plurality of the following advantages:

- it gains improvement on time and memory performance;
- it permits to use a same cryptographic key K1 during a same communication protocol comprising different cryptographic environments E1, E2 and to take into account its different conditions of use CU1, CU2 applied to these different cryptographic environments E1, E2;

30 as the cryptographic key K1 is securely paired to the appropriate cryptographic environment E1, E2 via the different masks M1, M2, it increases the security of the use of the cryptographic key K1;

35 as the cryptographic key K1 is kept being transferred with the

25

masks changing every time it is used, this will make the value of the cryptographic key K1 not exposed although it is used in a less secure cryptographic environment E2;

5 - it gives a secure cryptographic key management and also it sustains the ability to use a less secure cryptographic environment E2 in a safer way;

10 - it permits to have a multiple levels of security for some cryptographic functions in order to gain some speed improvement. During critical and sensitive processes, the electronic card D will use the strongest security cryptographic environment E1, and for other processes, the electronic card D will use the degraded security cryptographic environment E2;

15 - it permits to securely use the same cryptographic key K1 for different cryptographic environment E1, E2 which have different security levels without exposing the cryptographic key K1;

20 - it permits to partition the cryptographic data CA, CB used to protect the cryptographic key K1, as only the first cryptographic data CA may be used with the first cryptographic environment E1, and only the second cryptographic data CB may be used with the second cryptographic environment E2;

 - it permits to associate the cryptographic key K1 and a key adapted to the security level Lk only to one cryptographic environment according to its security level L;

25 - as an electronic device D such as a secure element comprises limited resources in term of memory, time processing etc. it permits said electronic device D to improve its performances as the right key adapted to the security level is associated according to the needs of the cryptographic environment E1, E2;

30 - it avoids using the same cryptographic key with different cryptographic environments with different security levels. In particular, it avoids using the same masked key which is used for the second cryptographic environment E2 (which in the non-limitative example given comprises a lower security level than the first cryptographic environment) within the first cryptographic environment E1, which could jeopardize the
35 mechanism to make the cryptographic key confidential as the second

26

security level is not enough secured. Hence, it avoids an attacker breaking the cryptographic key, even masked.

CLAIMS

1- Method (MTH) for protecting a cryptographic key (K1) within a first cryptographic environment (E1) of an electronic device (D) with
5 a first security level (L1) and within a second cryptographic environment (E2) of said electronic device (D) with a second security level (L2), wherein:

- said electronic device being operated to derive a first cryptographic data (CA) from the cryptographic key (K1) in order to obtain a first key adapted to the security level (Lk1) of said first cryptographic environment (E1), said first cryptographic data (CA) being paired with said
10 first cryptographic environment (E1);

- using said first cryptographic data (CA) within said first cryptographic environment (E1);

- said electronic device being operated to apply a transformation
15 operation to said first cryptographic data (CA) to provide a second cryptographic data (CB) in order to obtain a second key adapted to the security level (Lk2) of said second cryptographic environment (E1), said second key adapted to the security level (Lk2) being different from the first key adapted to the security level (Lk1), and said second cryptographic data
20 (CB) being paired with said second cryptographic environment (E2), said operation transformation being configured so that the provided second cryptographic data is derived from the cryptographic key (K1);

- using said second cryptographic data (CB) within said second cryptographic environment (E2).

2- Method (MTH) according to claim 1, wherein the first security level (L1) is respectively securely higher or lower than the second security level (L2) and the first key adapted to the first security level (Lk1) being respectively securely higher or lower than the second key adapted to
30 the second security level (Lk2).

3- Method (MTH) according to any one of the previous claims 1 to 2, wherein the derivation of said first cryptographic data (CA) is function of said cryptographic key (K1) and a first mask (M1).

28

4- Method (MTH) according to the previous claim 3, wherein the transformation of said first cryptographic data (CA) into said second cryptographic data (CB) is function of a second mask (M2) and said first mask (M1).

5

5- Method (MTH) according to the previous claim 4, wherein said method (MTH) further comprises generating said first and said second masks (M1, M2) associated respectively to the first and to the second cryptographic environment (E1, E2).

10

6- Method (MTH) according to the previous claim 5 or claim 6, wherein the transformation of said first cryptographic data (CA) comprises:

- generating an intermediary value (X) which is the result of an XOR of said first cryptographic data (CA) and said second mask (M2); and
- 15 - XORing said intermediary value (X) with said first mask (M1) in order to generate said second cryptographic data (CB).

7- Method (MTH) according to any one of the previous claims 3 to 6, wherein the generation of the mask (M1, M2) is based on a master mask (MM1, MM2) and on a diversifier (D1, D2).

20

8- Method (MTH) according to the previous claim 7, wherein the master mask (MM1, MM2) is common to all the cryptographic keys (K1) used by said electronic device (D) and a diversifier (D1, D2) is unique for each cryptographic key (K1).

25

9- Method (MTH) according to any one of the previous claims 1 to 8, wherein said first cryptographic environment (E1) comprises a first set of cryptographic functions (F1) and said second cryptographic environment (E2) comprises a second set of cryptographic functions (F2).

30

10- Method (MTH) according to any one of the previous claims 1 to 9, wherein said first cryptographic environment (E1) comprises a first set of cryptographic functions (F1) implementing a mutual authentication between said electronic device (D) and a remote server (SERV).

35

29

11- Method (MTH) according to any one of the previous
claims 1 to 10, wherein said second cryptographic environment (E2)
comprises a second set of cryptographic functions (F2) implementing a data
5 exchange between said electronic device (D) and a remote server (SERV).

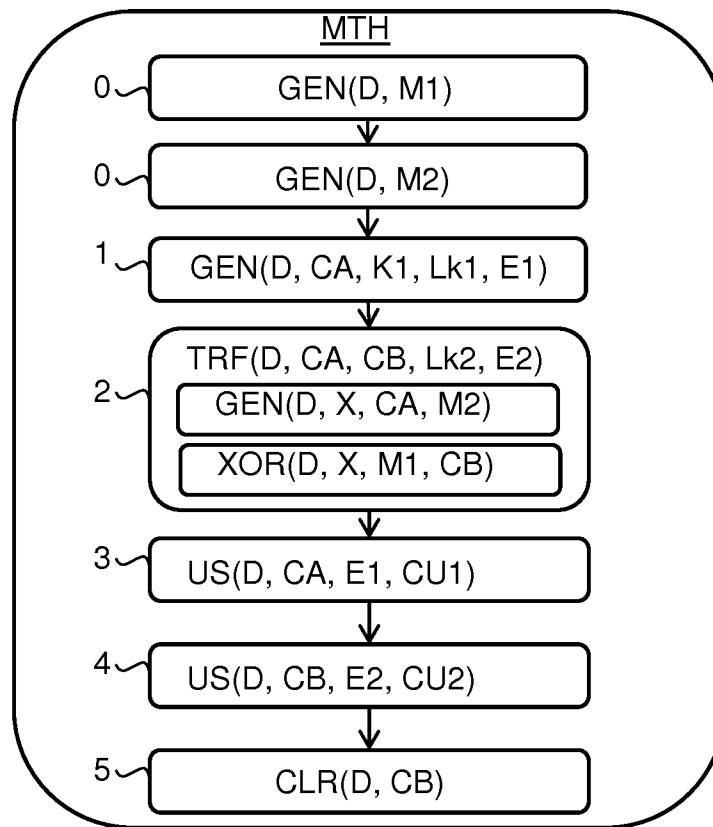
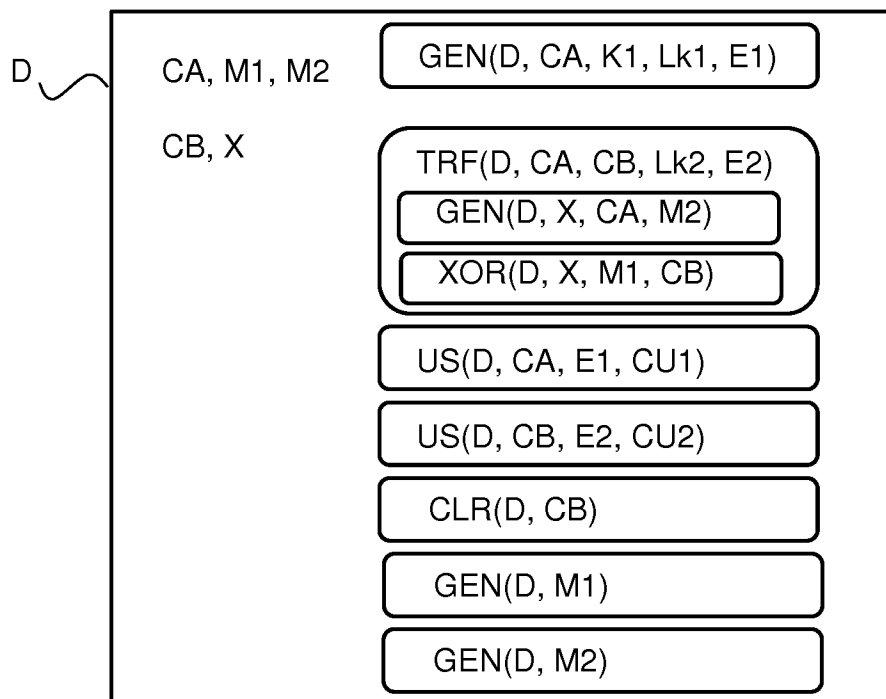
12- Method (MTH) according to any one of the previous
claims 1 to 11, wherein said electronic device (D) is a secure element.

10 13- Method (MTH) according to claim 12, wherein said
secure element is a smart card, an embedded secure element, a micro-SD,
an UICC.

14- Electronic device (D) comprising a processor and an
15 instruction memory operated to perform the method for protecting a
cryptographic key (K1) within a first cryptographic environment (E1) of an
electronic device (D) with a first security level (L1) and within a second
cryptographic environment (E2) of said electronic device (D) with a second
security level (L2) according to any previous claims.

20

1/2

Fig. 1Fig. 2

2/2

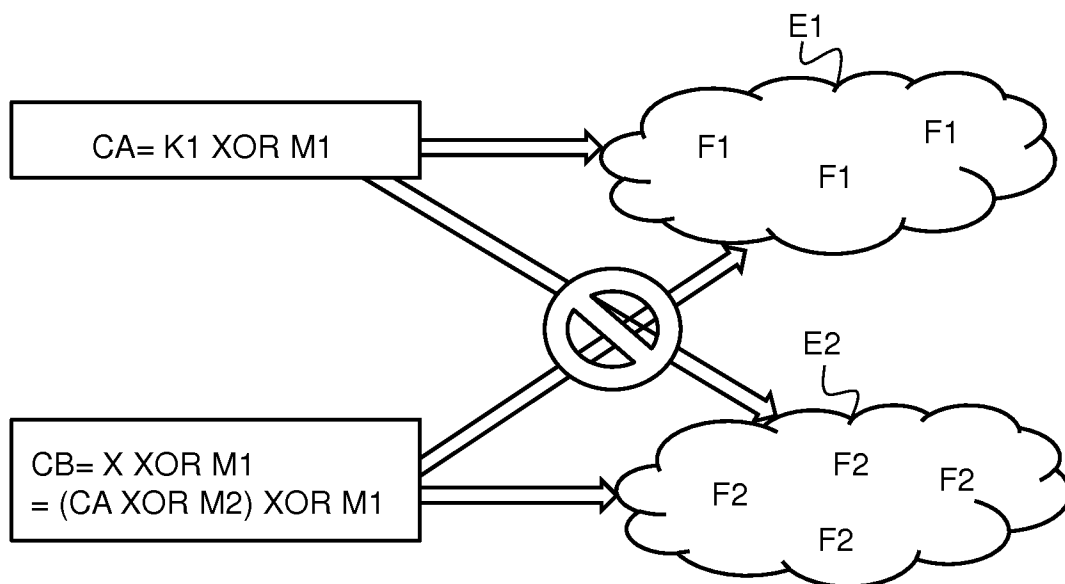


Fig. 3

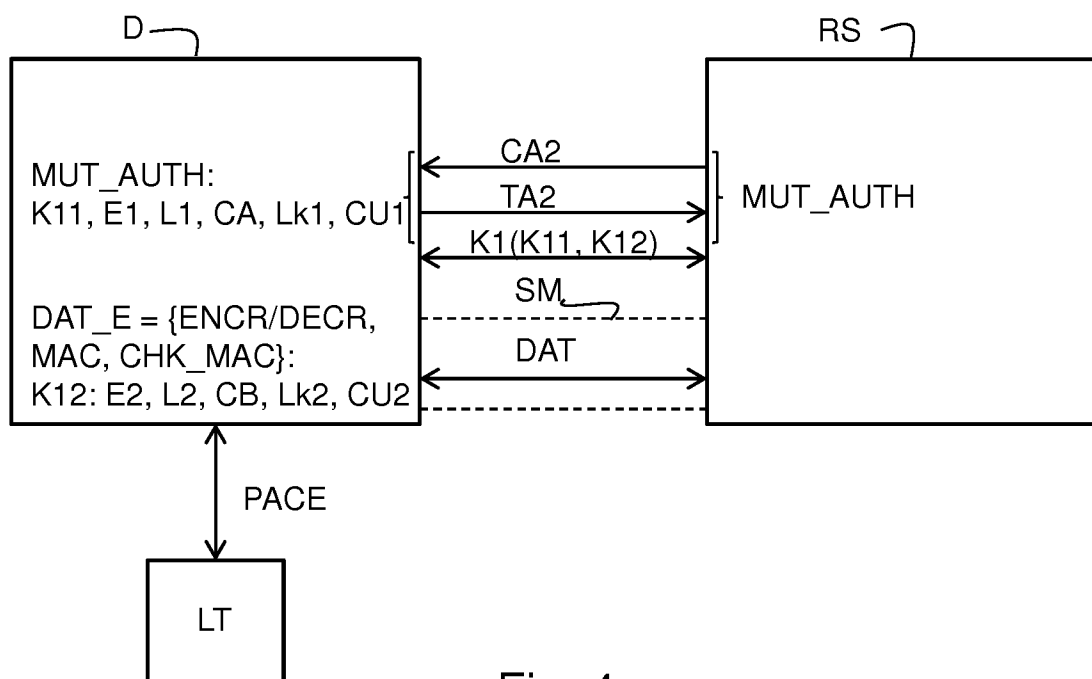


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2016/068448

A. CLASSIFICATION OF SUBJECT MATTER
 INV. H04L9/08 H04L9/00
 ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009/034724 A1 (LIARDET PIERRE-YVAN [FR] ET AL) 5 February 2009 (2009-02-05) paragraph [0007] paragraphs [0037] - [0038] paragraph [0040] - paragraph [0055] -----	1-14
A	US 2010/158246 A1 (NEUMANN HEIKE [DE] ET AL) 24 June 2010 (2010-06-24) paragraph [0057] - paragraph [0061] -----	1-14



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

13 October 2016

Date of mailing of the international search report

21/10/2016

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Authorized officer

Apostolescu, Radu

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2016/068448

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009034724 A1	05-02-2009	EP 2020773 A2	04-02-2009
		US 2009034724 A1	05-02-2009

US 2010158246 A1	24-06-2010	BR PI0811911 A2	18-11-2014
		CN 101682513 A	24-03-2010
		EP 2168303 A2	31-03-2010
		JP 2010529767 A	26-08-2010
		KR 20100020519 A	22-02-2010
		US 2010158246 A1	24-06-2010
		WO 2008152533 A2	18-12-2008
