EXHIBIT 3

US007725740B2

(12) **United States Patent**
Kudelski et al.

(10) **Patent No.: US 7,725,740 B2**
(45) **Date of Patent: May 25, 2010**

(54) **GENERATING A ROOT KEY FOR DECRYPTION OF A TRANSMISSION KEY ALLOWING SECURE COMMUNICATIONS**

(75) Inventors: **Henri Kudelski**, Grandvaux (CH); **Serge Gaumain**, Yverdon (CH)

(73) Assignee: **Nagravision S.A.**, Cheseaux-sur-Lausanne (CH)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1022 days.

(21) Appl. No.: **10/848,014**

(22) Filed: **May 19, 2004**

(65) **Prior Publication Data**

US 2004/0236959 A1 Nov. 25, 2004

(30) **Foreign Application Priority Data**

May 28, 2003 (CH) 0953/03

(51) **Int. Cl.**
G06F 11/30 (2006.01)
G06F 12/14 (2006.01)

(52) **U.S. Cl.** **713/194**; 726/4; 380/44

(58) **Field of Classification Search** 713/194; 726/9; 380/44
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,786,790	A	11/1988	Kruse et al.	
5,067,156	A	11/1991	Martin	
5,177,790	A *	1/1993	Hazard	380/28
5,191,608	A	3/1993	Geronimi	
5,201,000	A *	4/1993	Matyas et al.	380/30
5,774,058	A *	6/1998	Henry et al.	340/5.5
5,944,821	A	8/1999	Angelo	
6,141,756	A *	10/2000	Bright et al.	726/22
6,327,652	B1 *	12/2001	England et al.	713/2
6,415,371	B1 *	7/2002	Nakamura et al.	711/164
6,625,729	B1 *	9/2003	Angelo et al.	713/2
6,684,326	B1 *	1/2004	Cromer et al.	713/2
6,907,522	B2 *	6/2005	Morais et al.	713/2
6,920,566	B2 *	7/2005	Lewis	713/194
6,938,164	B1 *	8/2005	England et al.	713/193
6,986,052	B1 *	1/2006	Mittal	713/190
7,013,384	B2 *	3/2006	Challener et al.	713/2
7,036,023	B2 *	4/2006	Fries et al.	726/21
7,069,442	B2 *	6/2006	Sutton et al.	713/179

(Continued)

FOREIGN PATENT DOCUMENTS

EP	0 280 035	B1	8/1988

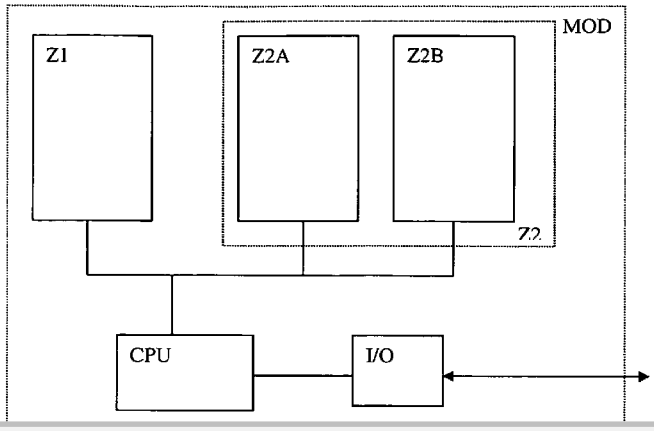
(Continued)

Primary Examiner—Edan Orgad
Assistant Examiner—James Turchen
(74) *Attorney, Agent, or Firm*—Harness, Dickey & Pierce, P.L.C.

(57) **ABSTRACT**

A method is used to restore the security of a secure assembly such as a chip card, after the contents of its second memory zone have been read by a third party. The method is for generating a security key implemented by a secure module comprising a central unit, a first conditional access memory zone and at least one second memory zone containing all or part of the user program. The method includes reading of all or part of the second memory zone, and generation of at least one root key based on all or part of the second zone data and on at least one item of secret information stored in the first memory zone.

12 Claims, 1 Drawing Sheet



U.S. PATENT DOCUMENTS

7,069,445	B2 *	6/2006	Cheston et al.	713/187
7,117,376	B2 *	10/2006	Grawrock	380/277
2002/0087877	A1 *	7/2002	Grawrock	713/200

FOREIGN PATENT DOCUMENTS

EP	0 434 551	B1	6/1991
EP	0 475 837	B1	3/1992
FR	2 829 645		3/2003
WO	WO 01/86601	A1	11/2001

* cited by examiner

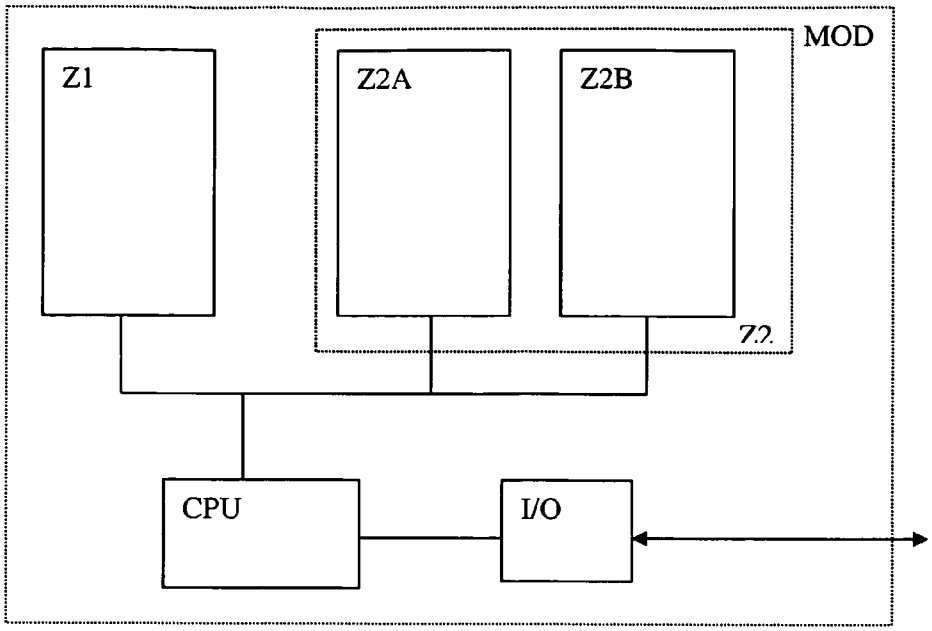


Fig. 1

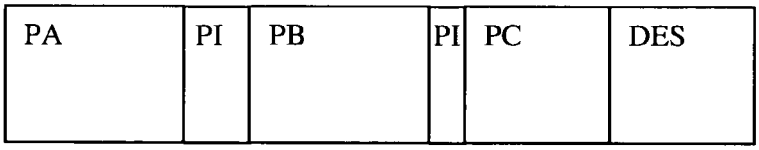


Fig. 2

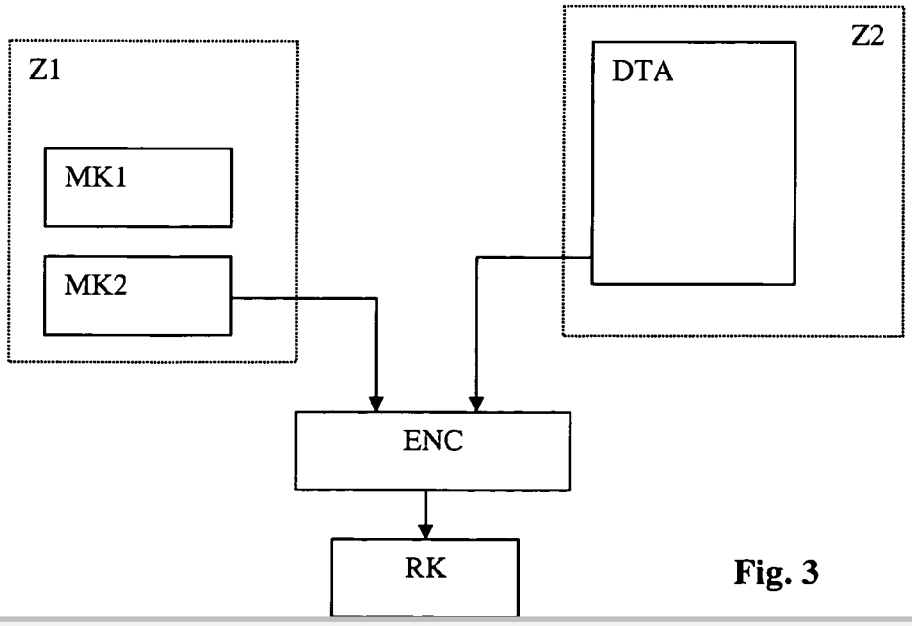


Fig. 3

GENERATING A ROOT KEY FOR DECRYPTION OF A TRANSMISSION KEY ALLOWING SECURE COMMUNICATIONS

The present application hereby claims priority under 35 U.S.C. §119 on Swiss patent application number CH 0953/03 filed May 28, 2003, the entire contents of which are hereby incorporated herein by reference.

FIELD OF THE INVENTION

This invention generally concerns the domain of security modules, preferably those including at least one central unit and two memory areas.

BACKGROUND OF THE INVENTION

Units are used in operations implementing cryptographic systems and are given in monolithic form. They are either produced on the same silicon chip or they are assembled on a support and embedded in a resin or protected by a sheet covering the different elements and acting as a fuse in the case of an attempted intrusion.

These security processors have a first memory zone called a bootstrap that is executed during the activation of the processor or at each resetting to zero. This memory is of the ROM type, namely that it is Read Only Memory.

During the execution of the start-up program, this program verifies the second memory zone that is of the rewritable type, usually of the EEPROM, NVRAM or Flash type. This verification is important as it serves to ensure that the data in this second zone is valid, namely that it is definitely a program (at least in part). This verification can be carried out in various ways such as the calculation of an imprint (CRC, Hash) and the comparison of this imprint with a value stored in the same zone.

Once the master program that has been initially started completes its verification, it connects with the second zone and begins the execution of the user program at a conventional address.

The particularity of this type of processor is that at the time of the execution of the program in the second zone, it does not have free access to the memory of the first zone. This access is either definitively prohibited or is subject to a verification mechanism (password for example).

This offers important security because the verification means, as well as the start-up data, are not accessible to the user program. All the data contained in the first zone is thus protected from any intrusion.

It is possible that this first bootstrap zone, in addition to having a part in read-only memory (ROM), includes a rewritable part of memory that is subjected to the same security conditions.

When the first zone is of a very limited size, the execution of the verification program can be carried out from the second zone. The latter is divided into a verification part and a user part.

Therefore, the verification of the user program is carried out on the basis of the data of the first zone. Namely, it is carried out on the basis of a first key that is generally stored in the first zone and which allows the verification of the data imprint of the second zone.

The second zone contains data constituting the program and a signature that is encrypted by this first key.

The verification program that can either be in the first zone,

To verify that the data is correctly validated, the second zone contains the imprint encrypted by a key that is initially stored in the first zone. This key is used to decrypt the encrypted imprint and the result obtained is compared with the calculated imprint.

This key can be in the first zone either in a definitive form (ROM) or in the programmed form (EEPROM or Flash for example). In this second case, programming is carried out in a machine or in an authorized centre for example. The program of the first zone accepts this program as long as no other key is already found in this memory location.

This key can be of the symmetrical type and thus secret or it can be of the asymmetrical type. In this second variant, this key can be found in a memory zone other than the first zone because even if a third party discovered this key, the third party would not be able to identify a modified data set because he must have the corresponding private key to identify the data. Obviously, this key is not issued from the management centre that is responsible for preparing the updating of the data.

The data of the second memory zone can represent either one or several programs, either important data such as rights or decryption keys, or a combination of both.

One of the known types of attacks used to discover the contents of the second zone is to search a security defect such as a memory overflow that allows control to be taken of the processor. Once control has successfully been taken, a third party transfers the contents of the second zone towards the exterior and is able to analyse the security mechanism and the keys used.

Using the knowledge of the contents of the second memory zone, the third party has the keys serving to manage the different rights and access to services that control this processor.

Therefore, if a change of keys takes place, managed by the management centre, this change command will be encrypted by a key present in the second memory zone. The third party, who has knowledge of this key, can decrypt this message and also update the contents of this new key.

Therefore, it is apparent that while a secure mechanism has been used to verify the contents of the program zone (second zone), once security has been violated, none of the changes initiated by the management centre have an effect on security because the changing means (new transmission key for example) use keys that the third party already has in his possession. He can thus decipher the updating message and also change its transmission key. The breach cannot be stopped even if the security breach has been corrected in the application.

SUMMARY OF THE INVENTION

An object of an embodiment of this invention is to propose a method to restore the security of this type of security assembly once the contents of the second memory zone have been read by a third party.

This aim may be achieved using a method for generating a security key carried out by a security module including a central unit, a first conditional access memory zone and at least one second memory zone containing all or part of the user program, wherein it includes the following steps:

reading all or part of the second memory zone,

generation of at least one root key based on all or part of the

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.