US 20040083380A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2004/0083380 A1

Janke (43) Pub. Date: Apr. 29, 2004

(54) SECURITY MODULE WITH VOLATILE MEMORY FOR STORING AN ALGORITHM CODE

(76) Inventor: **Marcus Janke**, Munchen (DE)

Correspondence Address:
LERNER AND GREENBERG, P.A.
POST OFFICE BOX 2480
HOLLYWOOD, FL 33022-2480 (US)

(21) Appl. No.: **10/620,108**

(22) Filed: **Jul. 15, 2003**

Related U.S. Application Data

(63) Continuation of application No. PCT/EP02/00733, filed on Jan. 24, 2002.

(30) **Foreign Application Priority Data**

Feb. 16, 2001 (DE)..... 101 07 373.9

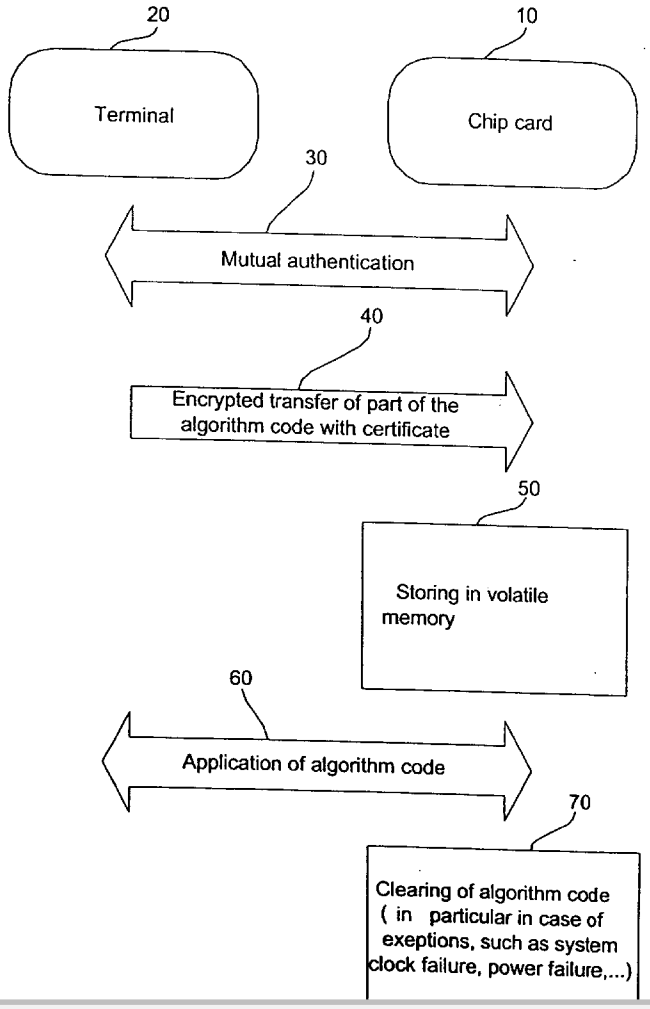
Publication Classification

(51) **Int. Cl.**[7] **H04L 9/00**

(52) **U.S. Cl.** **713/194**; 713/175

(57) **ABSTRACT**

A security module for use with a terminal comprises a data interface adapted to be coupled to a terminal, for receiving at least part of an algorithm code or the complete algorithm code from the terminal, as well as an energy interface for receiving supply energy. A volatile memory coupled to the energy interface in order to have energy supplied thereto stores the part of the algorithm code or the complete algorithm code received via the data interface, with a processor performing the algorithm code in order to obtain an algorithm code result that can be delivered to the terminal. Due to the storing of at least part of an algorithm code in the volatile memory of the security module, according to the invention, the algorithm code of the security module is effectively protected against spying out by a potential attacker.



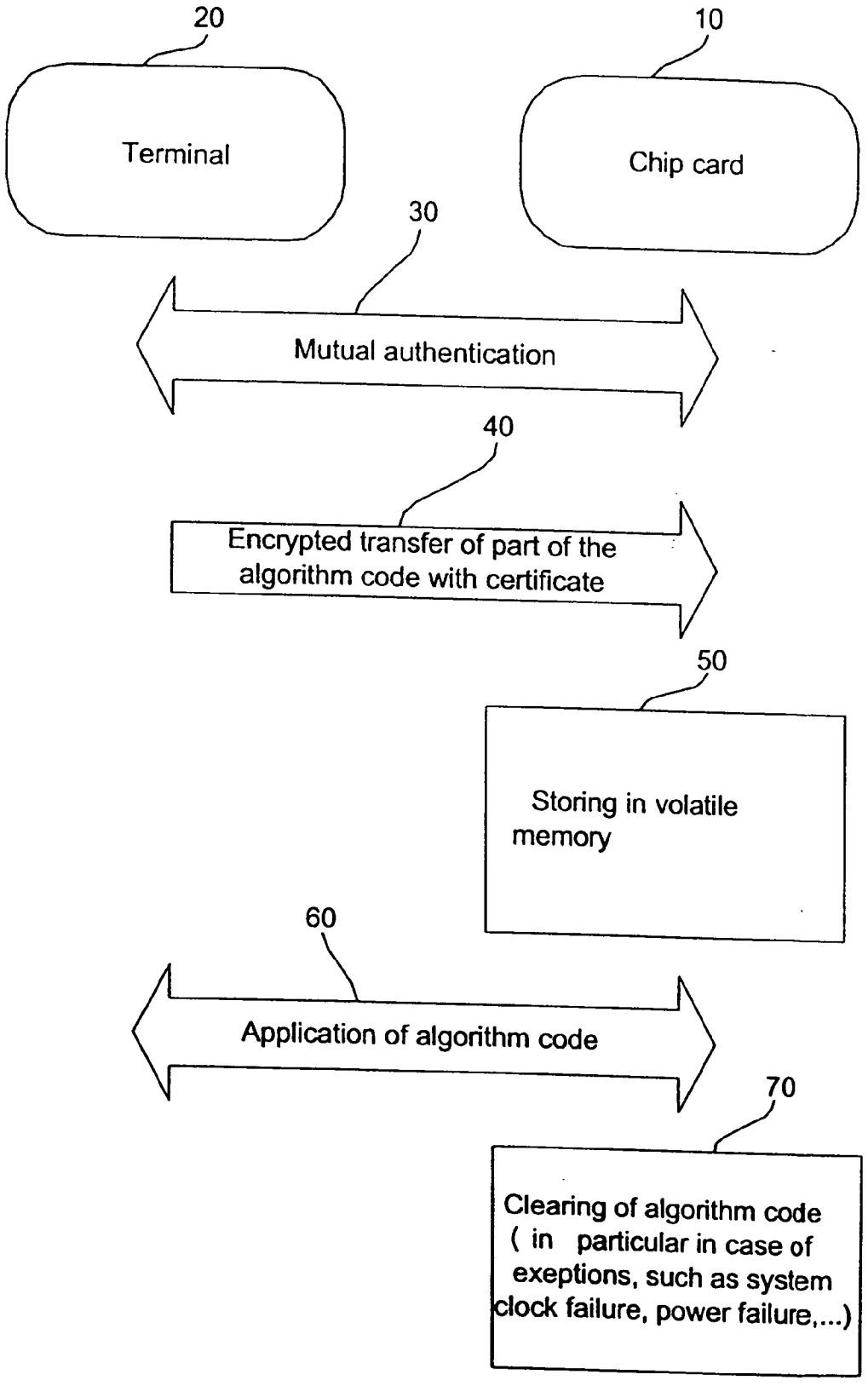


FIG 1

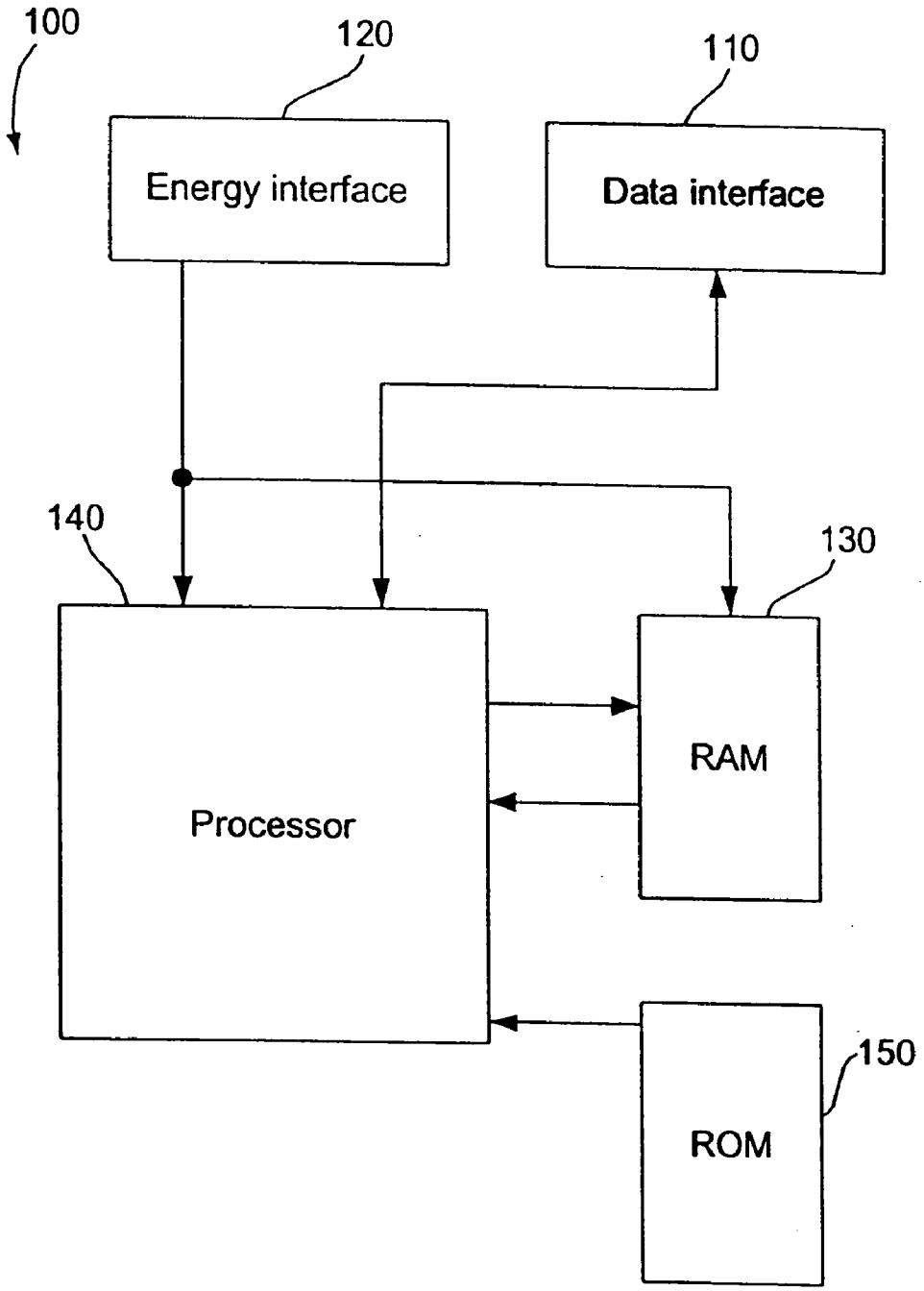


FIG 2

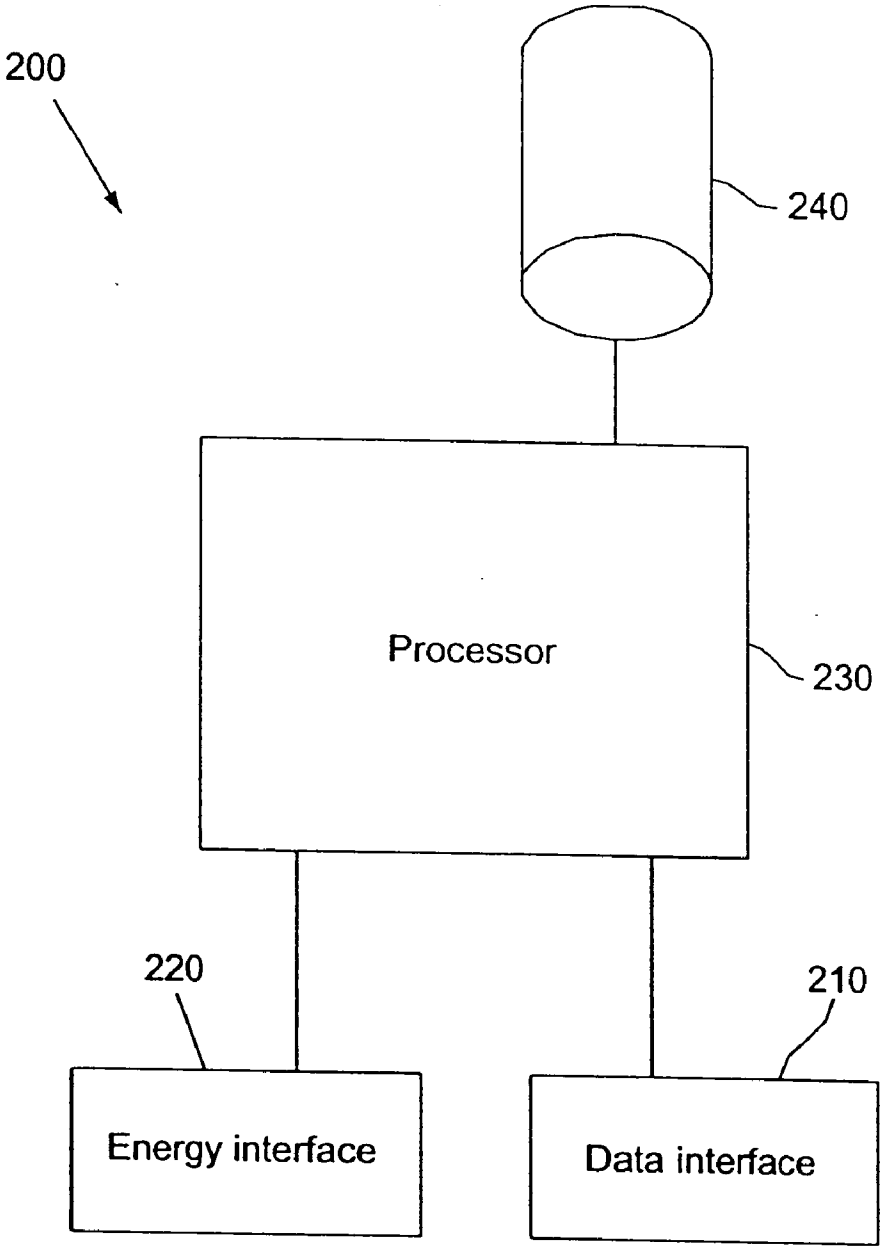


FIG 3

SECURITY MODULE WITH VOLATILE MEMORY FOR STORING AN ALGORITHM CODE

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application is a continuation of copending International Application No. PCT/EP02/00733, filed Jan. 24, 2002, which designated the United States and was not published in English.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The present invention relates to security modules, as employed for example for pay TV applications, credit cards, telephone cards or as TPM plug-in cards, and refers in particular to securing the algorithm code that is employed for the communication between security module and terminal against external attacks.

[0004] 2. Description of the Related Art

[0005] With the increasing advent of cashless payment traffic and the increasing information-technological networking as far as into individual households, such as e.g. in case of pay TV applications, there is an increasing demand for cryptographic algorithms in order to be able to perform digital signatures, authentications and encryption tasks. Known cryptographic algorithms comprise asymmetric encryption algorithms, such as e.g. the RSA algorithm, symmetric encryption processes, such as e.g. the DSE process, as well as processes based on elliptic curves.

[0006] In order to be able top perform the computations prescribed by the cryptographic algorithms in everyday life with an acceptable speed on the one hand and in as convenient manner for the user as possible on the other hand, chip cards, such as smart cards or signature cards, are employed comprising an individually provided cryptographic processor for implementing the cryptographic algorithm. Depending on the particular application or use, the cryptographic processor must be capable of performing authentications, signatures, certifications and encryptions or decryptions in accordance with different cryptographic algorithms. In addition to implementation of the cryptographic algorithms, the chip card contains stored, chip card-specific information, such as a secret key and, in case of a credit card, the credit card number, the account number and the balance and, in case of a pay TV smart card, a smart card ID, a customer ID and other customer-specific information. A chip card enables the user of the chip card to carry out certain transactions, such as e.g. debiting, on specifically provided terminals or other end apparatus, such as pay TV decoders, in simple and efficient manner. In this regard, the cryptographic algorithms implemented on the chip card provide for protection of the chip card traffic against criminal manipulations.

[0007] For protecting chip card terminal systems against criminal manipulations, specific protocols are employed between terminal and chip card, comprising e.g. mutual authentication as well as encryption and decryption operations making use of the cryptographic algorithms implemented in the cryptographic processor. A problem with conventional chip cards consists in that the algorithms used in stored form and thus are susceptible to being spied out by potential attackers. Spying out of cryptographic algorithms implemented in chip cards by an attacker comprises, for example, the chemical removal of the circuit structure of the cryptographic processor and the optical analysis of the exposed semiconductor structures. If an attacker, by way of the chip card in his possession, succeeds in obtaining the cryptographic algorithm implemented therein, the attacker will be in the position, due to his knowledge of the cryptographic algorithm and thus by the possibility of implementing the same, to carry out certain attacks against the chip card in order to obtain the secret data, such as the secret key or other data of crucial security of the chip card. When the underlying cryptographic algorithm is known, the attacks have a by far greater chance of success, and consequently the security chain of the chip card traffic is at risk.

[0008] With conventional chip cards, the problem of spying out is counteracted merely by specific hardware processes or technologies, such as by the hidden contact process. In case of this process, attempts are made to prevent the optical analysis of removed semiconductor structures and thus a conclusion to the underlying electronic circuit by means of hidden contacts and by the use of specific layout libraries for the underlying gates, in which different gates, such as AND gates and OR gates, differ from each other merely by different doping. These hardware concealing measures indeed increase the expenditure for finding out the underlying cryptographic algorithms for the potential attacker, but on the other hand increase also the circuitry and design expenditure, the chip area and thus the costs of the cryptographic processor and the chip card, respectively.

[0009] A chip card with increased security against foreign attacks and reduced circuit expenditure is very attractive for chip card manufacturers in particular with regard to the high market potential and the large numbers of pieces in which chip cards are produced.

SUMMARY OF THE INVENTION

[0010] It is the object of the present invention to make available a security module, a terminal and a process such that security module traffic with a higher level of security may be ensured.

[0011] In accordance with a first aspect of the invention, this aspect is achieved by a security module for use with a terminal, comprising a data interface adapted to be coupled to a terminal, for receiving at least part of an algorithm code or of the complete algorithm code from the terminal, with the algorithm code concerning a processing of secrets, an energy interface for receiving supply energy from the terminal; a volatile memory for storing the part of the algorithm code or the complete algorithm code received via the data interface, said volatile memory being coupled to the energy interface in order to have energy supplied thereto such that the same will be cleared upon an interruption of the receipt of the supply energy from the terminal; and a processor for performing the algorithm code in order to obtain an algorithm code result that can be delivered to the terminal.

[0012] In accordance with a second aspect of the invention, this aspect is achieved by a terminal for use with a security module, comprising: a data interface adapted to be

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.