

CERTIFICATE OF TRANSLATION ACCURACY

I am a professional reviewer and coordinator specializing in translating major European and Asian languages to English and vice versa.

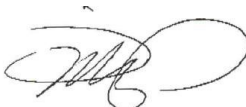
I served as Chief Examiner of the certified court interpreter test for the State of California and as a contract translator and interpreter for various federal agencies through the U.S. Department of State for more than a decade. I served as an instructor at the University of California at Berkeley and the Middlebury Institute of International Studies at Monterey (MIIS) Graduate Program in Translation.

I have more than 30 years of experience translating thousands of technical, legal, and business documents from European and Asian languages to English submitted to, among others, European and Asian judicial authorities, U.S. federal courts, the U.S. International Trade Commission (ITC), and the USPTO Patent Trial and Appeal Board (PTAB).

I certify to the best of my knowledge and ability that this is a true, correct, and complete translation of the corresponding source text, a German patent document, to the English language.

I certify under penalty of perjury that the foregoing is true and correct.

Executed this 18th day of April 2025 in Contra Costa County of the State of California.

By: 

Alex N. Jo
Member, ATA



(19) **FEDERAL REPUBLIC OF GERMANY** (12) **Unexamined Application**
 (10) **DE 102 20 629 A 1**

(51) Int. Cl.7:
G 06 F/06
 G 06 F 13/12
 G 06 F 12/14



(21) Application Number: 102 20 629.5
 (22) Filing Date: 08/05/2002
 (43) Disclosure Date: 11/27/2003

**GERMAN
 PATENT AND
 TRADEMARK OFFICE**

DE 102 20 629 A 1

(71) Applicant:

Infineon Technologies AG, 81669 Munich, DE

(74) Agent, Attorney, or Firm:

Epping Hermann Fischer,
 Patentanwalts-gesellschaft mbH, 81669 Munich

(72) Inventor:

Böker, Thorsten, Dr., 85579 Neubiberg, DE

(56) Citations:

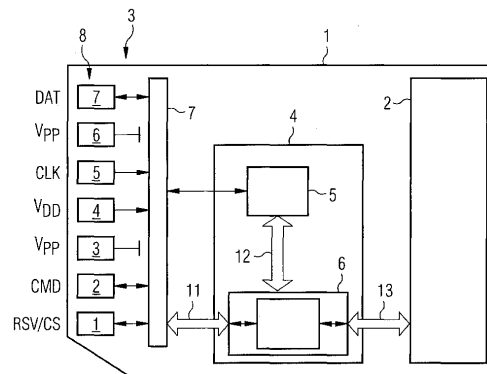
US 56 23 637 A
 SMART CARDS (online), on the Internet:
 URL: <http://www.uni-weimar-de/-schott2/sc/>;

The following information has been derived from the documents filed by the applicant

Examination request according to German Patent Act Section 44 has been filed

(54) DATA CARRIER

(57) The invention relates to a data carrier (1) comprising a non-volatile memory (2), a data interface (3) via which data can be written to and read from the non-volatile memory (2), and an interface module (4), which is connected between the data interface (3) and the memory (2) and by way of which the data can be encrypted and/or decrypted. The data carrier (1) according to the invention is characterized in that the interface module (4) comprises a control unit (5) and a logic component (6) connected thereto, the encryption and/or decryption being performed by the logic component (6) and the key to be employed being establishable by the control unit (5).



DE 102 20 629 A 1

Description

[0001] The invention relates to a data carrier comprising a non-volatile memory, a data interface via which data can be written to and read from the non-volatile memory, and an interface module which is connected between the data interface and the memory and by way of which the data can be encrypted and/or decrypted.

[0002] Such data carriers are used as memory cards, for example. Data of any kind can be stored on a small card. A host sends the data to the card via an interface. If the data is sensitive, the data is usually stored in encrypted form. In principle, two options are available for encrypting and decrypting the data. Either the host or the card itself performs this task. However, since the desired data rates are very high, the transmission including encryption or decryption must be very fast and, in the best case, at the same speed as if the data were not encrypted.

[0003] If encryption and decryption are carried out by the host, this is less problematic since sufficient processor power is usually available there. However, many memory cards are designed in such a way that almost all hosts, which may belong to different applications, can read from and write to these cards. So if a first application stores a data record that it has previously encrypted using a specific algorithm, the host of a second application that is to read the data record again must also have this algorithm, otherwise the data cannot be decrypted again.

[0004] For this reason, it is advantageous if the card itself handles the encryption and decryption, since in this case it is not necessary to know in advance which applications the memory card is to work with, and it is not necessary to ensure that these applications have the appropriate algorithms.

[0005] In the case of data carriers, today's chip card controllers are able to apply almost any encryption algorithm to any data. In terms of flexible data encryption, this is a practicable solution, but the data rates are extremely limited. They are currently around 100 kbit per second and therefore do not come close to meeting the required data rates of a memory card, which are over 10 Mbit per second. Encryption and decryption can therefore only be carried out very slowly when using conventional chip card controllers. Although more powerful controllers having sufficient processor power are feasible in principle, they usually cannot be used for cost reasons.

[0006] The object of the invention is therefore to provide a data carrier which is suitable for carrying out data encryption and/or decryption at a substantially higher speed, without requiring a particularly powerful processor.

[0007] This object is achieved by a data carrier of the type mentioned at the outset, which is characterized in that the interface module comprises a control unit and a logic component connected thereto, wherein the encryption and/or decryption are carried out by the logic component and the key to be employed can be established by the control unit.

[0008] The interface module of a data carrier according to the invention is thus divided into two parts. On the one hand, it comprises a control unit, which can be a conventional chip card controller or a part thereof, for controlling the processes and

specifying the keys to be used. On the other hand, the interface module comprises a logic component that is responsible for the encryption and/or decryption process itself and is optimized for this task. A hardware-based solution for implementing a function is always significantly faster than a software-based implementation.

[0009] The advantage of such an arrangement is that a powerful logic component is much less expensive to manufacture than a processor suitable for this task.

[0010] A particularly flexible solution for providing the logic component is to provide it by means of a function-programmable logic circuit. This allows the interface module to be adapted to changing requirements.

[0011] Further advantageous embodiments of the invention are described in the subclaims.

[0012] The invention will be described in more detail hereafter based on an exemplary embodiment. **FIG. 1** shows a schematic representation of a data carrier according to the invention.

[0013] The figure shows a data carrier **1**, in this case a memory card. The memory card comprises a non-volatile memory **2**, preferably a flash memory, which has a high capacity so that the memory card is suitable as a mass storage medium. The memory card is equipped with a data interface **3** for connecting to a host. Contact surfaces **8** are provided for contacting, to which various signals are applied during operation, such as a clock signal CLK, an operating voltage VDD, a control command CMD and, above all, a data signal DAT. An input circuit **7** is provided to receive these signals and also represents a driver level by way of which an adaptation to various hosts is carried out so that the memory card can be used flexibly with different hosts or applications. It is likewise possible to convert serial signals into parallel signals, and vice versa, at this point.

[0014] The data interface **3** is connected to an interface module **4**, which in the shown exemplary embodiment comprises a controller **5** and a logic component **6**. The logic component **6** has three interfaces. A connection to the data interface **3** is provided via a first interface **11**, a second interface **12** connects the logic component **6** to the controller **5**, and a third interface **13** connects the logic component **6** to the memory **2**.

[0015] Data to be transmitted from the data interface **3** to the memory **2** is encrypted in the logic component **6**. When reading data from the memory card, data is transmitted from the memory **2** to the data interface **3**, with decryption being performed by the logic component **6**. In both cases, the data path for encryption and decryption runs exclusively via the logic component **6**, but not via the controller **5**. The controller is only responsible for control and monitoring tasks.

[0016] The key to be employed by the logic component **6** is specified by the controller **5**. However, the controller also takes over other tasks. These are the control of the data stream, which ensures that the data is written and read correctly. Employed mechanisms are, for example, bad block management or the monitoring of "physical versus logical memory address".

[0017] In an advantageous implementation, the logic component **6**

is designed as an additional module of a chip card controller **5**. This enables a compact and cost-effective implementation.

List of reference symbols

- 1** Memory card
- 2** Non-volatile memory
- 3** Data interface
- 4** Interface module
- 5** Controller
- 6** Logic component
- 7** Input circuit
- 8** Contact surfaces
- 11, 12, 13** Interfaces of the logic component

Claims

1. A data carrier comprising:
 - a non-volatile memory (**2**);
 - a data interface (**3**) via which data can be written to and read from the non-volatile memory (**2**); and
 - an interface module (**4**), which is connected between the data interface (**3**) and the memory (**2**) and by way of which the data can be encrypted and/or decrypted,**wherein** the interface module (**4**) comprises a control unit (**5**) and a logic component (**6**) connected thereto, the encryption and/or decryption being performed by the logic component (**6**) and the key to be employed being establishable by the control unit (**5**).
2. The data carrier according to claim 1, wherein the carrier is a mass storage card.
3. The data carrier according to claim 1 or 2, wherein the control unit (**5**) is formed by a microcontroller.
4. The data carrier according to any one of claims 1 to 3, wherein the data rate of the data which can be encrypted and/or decrypted by the logic component (**6**) is greater than 10 Mbit/s.
5. The data carrier according to any one of claims 1 to 4, wherein the logic component (**6**) is a function-programmable logic circuit.

 1 page(s) of drawings

