Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2286851 C 2007/06/19

(11)(21) 2 286 851

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 1998/04/15
(87) Date publication PCT/PCT Publication Date: 1998/11/12
(45) Date de délivrance/Issue Date: 2007/06/19
(85) Entrée phase nationale/National Entry: 1999/10/15
(86) N° demande PCT/PCT Application No.: EP 1998/002205
(87) N° publication PCT/PCT Publication No.: 1998/050894
(30) Priorité/Priority: 1997/05/02 (DE197 18 547.9)

(51) Cl.Int./Int.Cl. *G06K 19/10* (2006.01), *G06K 1/12* (2006.01), *G06K 19/07* (2006.01), *G06K 7/00* (2006.01), *G07F 7/08* (2006.01)

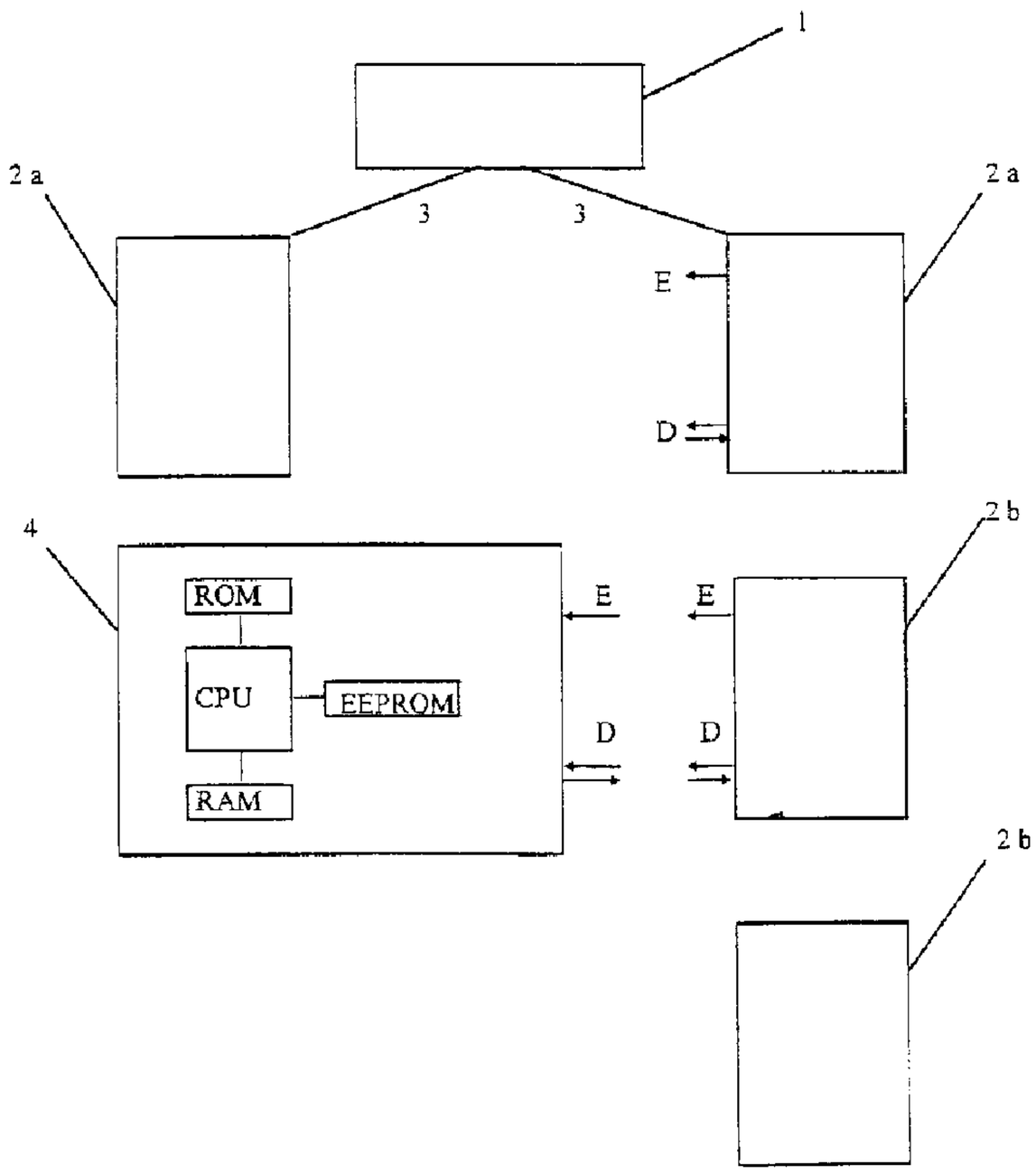
(72) Inventeur/Inventor:
SCHAEFER-LORINSER, FRANK, DE

(73) Propriétaire/Owner:
DEUTSCHE TELEKOM AG, DE

(74) Agent: FETHERSTONHAUGH & CO.

(54) Titre : SYSTEME PERMETTANT UNE LECTURE ET UN TRAITEMENT PROTEGES DE DONNEES SUR DES SUPPORTS DE DONNEES INTELLIGENTS

(54) Title: SYSTEM FOR THE SECURE READING AND EDITING OF DATA ON INTELLIGENT DATA CARRIERS



(57) Abrégé/Abstract:
The invention relates to a system for the secure reading and editing of data on intelligent data carriers (4), such as chipcards, as well as to working processes executable under said system, wherein the stored data and the therewith associated authorizations or values are especially well protected against access by unauthorized persons. This is achieved by the advantageous combination of known encryption processes. In particular, the risk involved if master keys stored in independently operating terminals (2b), such as vending machines or card telephones, became known to a criminal is eliminated or at least reduced and the misuse of the nowadays increasingly used cash-reloadable chipcards is thereby counteracted.

Abstract

The invention relates to a system for the secure reading and editing of data on intelligent data carriers (4), such as chipcards, as well as to working processes executable under said system, wherein the stored data and the therewith associated authorizations or values are especially well protected against access by unauthorized persons. This is achieved by the advantageous combination of known encryption processes. In particular, the risk involved if master keys stored in independently operating terminals (2b), such as vending machines or card telephones, became known to a criminal is eliminated or at least reduced and the misuse of the nowadays increasingly used cash-reloadable chipcards is thereby counteracted.

Fig. 1

FILE, ~~PIN IN~~ THIS AMENDED
~~TEXT~~ TRANSLATION

P97047WO

System for the secure reading and editing of data on intelligent data carriers

Description

The invention relates to a system for the secure reading and editing of data on intelligent data carriers according to the preamble of claim 1 as well as to processes executable under said system.

A system according to the preamble of claim 1 is disclosed, for example, in the technical book "Kryptologie" by A. Beutelspacher, 5th edition, Chapter 4, published in 1997 by Vieweg-Verlag [Vieweg Publishing House], Braunschweig/Wiesbaden, and is assumed as known. In particular, the challenge and response process described therein in connection with Fig. 4.12 on p. 93 and Fig. 4.16 on p. 101 and based on symmetrical encryption is suitable for the authentication of intelligent data carriers vis-à-vis computers or data entry terminals thereof.

Systems are also known which employ asymmetrical key processes or a plurality of symmetrical or asymmetrical key processes in succession (see e.g. "Funkschau" 1996, No. 25, pp. 60-63). However, asymmetrical key processes, such as the RSA algorithm described in the aforementioned book on p. 122 f., have, as compared with symmetrical processes, the disadvantage that, as a result of the need to carry out arithmetic operations with very large numbers, they are relatively slow and, if used for the authentication of the individual data carriers, require many keys to be stored in each terminal or - in the case of an existing data link to a central storage - in that storage.

The intelligent data carriers used in such systems, e.g. IC cards equipped with processors and storage devices - today usually referred to as chipcards - which often contain highly sensitive data, such as access authorizations to secure areas or the permission to withdraw amounts of money from an account, are largely secure against unpermitted use, unauthorized reading and intentional falsification of the stored data thanks to the use of the aforementioned cryptographic processes. The same is true also of the nowadays increasingly used, reloadable so-called electronic purses (e.g. paycards, cashcards), from which amounts of money can be withdrawn in order to pay for goods or services, at least if the terminals at which the withdrawals are made have a link to a computer centre through which it is possible to retrieve a therein stored key required for the authentication of a data carrier or through which it is possible for a cryptogram communicated from a data carrier for authentication to be forwarded to the computer centre for verification.

The latter, however, is not always the case, because data links for public card telephones, public-transport ticket machines, carpark ticket machines or vending machines are too costly. In such cases, a key required for security-critical operations is stored usually in the terminal, inside a so-called security module. This key is normally a master key which is used to calculate the key required for the data carrier in question and matching the specific key thereof, this involving the use of a data carrier-specific item of information communicated from the data carrier, such as the chipcard number.

The fact that said master key is located in a terminal in an insecure environment compromises the security of the entire system, because, if it became known to a criminal, that criminal would then be able to make illegal duplicates of all the data carriers used in the system.

The object of the present invention is to exclude or at least reduce such a risk and thereby to increase the security of the system.

Working processes for said system are indicated, with regard to the reading of data and with regard to the editing of the data contained on the data carrier.

The storing of a second key pair on the data carrier - said second key pair satisfying an asymmetrical key algorithm - makes it possible, at the end of a data-reading or -editing operation, to confirm the operation by means of a so-called electronic signature. The calculation and verification of said electronic signature require the key pair stored on the data carrier and cannot be achieved simply by means of a key derived from the master key of a terminal and the reproduction of said key on the data carrier.

The further development of the invention makes it possible to verify that the individual data carriers belong to the system using an asymmetrical key process, without, however, there being the disadvantages of an asymmetrical key process, as would result, for example, if secret keys for all data carriers were stored at a central location. Furthermore, in this further development of the invention, the correctness of the key pair stored on the data carrier and used for generation of the electronic signature is co-certified by

the system. The secret key used for the generation of the certificate remains in the computer centre and is therefore safe against outside access.

Further embodiments, for the authentication of the data carriers vis-à-vis a terminal, permit the use of a key process employing a symmetrical key algorithm. The derivation from a master key of the keys used for the authentication of the individual data carriers dispenses with the need for the online connection of all terminals to the computer centre or for the storage of extensive key lists in the terminals. The variants described in claims 4 and 5 of the storage and/or calculation on the data carrier of the key used for authentication permit the authentication operation to be adapted to the technical possibilities (computing and storage capacity) of the data carriers used.

A further embodiment relates to the making available of a further key usable in a symmetrical key process. A further embodiment relates to measures aimed at better supervision of withdrawal operations in data carriers used as electronic purses.

Hereinbelow, example embodiments of the system according to the invention and of processes executed under said system for the reading and editing of the data stored on data carriers are to be described with reference to the drawings, in which:

Fig. 1 shows schematically the essential hardware of a system according to the invention; and

Fig. 2 shows a flow chart relating to the secure modification of the data on a data carrier of a system in the form of that according to claim 7.

Fig. 1 shows a computer centre 1 which is connected by data lines to terminals 2a of a first type. Terminals 2b of a second type do not have a permanent connection to the computer centre, but are able, like the terminals of the first type, to communicate with data carriers 4 belonging to the system. For this purpose, the data carrier is inserted by its user into an appropriate slot on a terminal and is thereby connected through a power-transfer interface E to the power supply of the terminal and through a data interface D to a computer system in the terminal. Power and data transfer may be accomplished in known manner by electrical contacts, inductively or optically. The data carrier 4 itself, usually an IC card or chipcard, is equipped with a complete microprocessor system containing a processor CPU and various storage devices ROM, RAM, EEPROM.

The data carriers may perform various functions, including a plurality of different functions. This may be, for example, an ID function in which the data stored on the data carrier allows the user access to a secure area or grants the user permission to carry out a specific action. In the case of a cheque card, the stored data, possibly in combination with a secret number to be entered by the user, authorizes the user to make a withdrawal from an account. - In the aforementioned cases, for data evaluation use will probably be made exclusively of terminals having a permanent data link to the computer centre, this making it possible for the keys required for the safeguarding of the data against tampering or unauthorized reading to be kept in a central, protected location -.

Data carriers of chipcard size, however, are also suitable for acting as electronic purses which, when loaded with an amount of money, can be used to pay for goods or services. While, in this case, loading or reloading is carried out at special terminals connected to the computer centre, e.g. a bank, the withdrawal of amounts can also take place at vending machines, card telephones, public-transport ticket machines or carpark ticket machines which, however, in the form of terminals belonging to the system, are not connected to the computer centre.

At such terminals, the transfer of a key or of encrypted data to or from the computer centre is not possible and the terminal must, without the support of the computer centre, detect whether a data carrier belongs to the system, whether an amount of money stored on the data carrier is sufficient for a desired withdrawal and whether the withdrawal, once effected, has been correctly implemented on the data carrier.

Fig. 2 shows an example of a withdrawal operation on a chipcard, in the form of an electronic purse, at a terminal which is not connected to the computer centre.

In this case, the uppermost section of the chart contains the transaction-securing data as stored on the chipcard and in the terminal prior to the transaction. The below-following sections show in chronological sequence the operations which take place on the chipcard (in the left-hand column), the transfers taking place between chipcard and terminal (in the centre column) and the operations in the terminal (in the right-hand column).

Before being issued to a user, the chipcard was provided by the computer centre with a certificate, a cryptogram generated using an asymmetrical key process, e.g. the known RSA algorithm, and representing an electronic signature. The cryptogram was generated using the signature function S_{glob}, available only in the computer centre, of a global key pair S_{glob}, V_{glob} - said global key pair S_{glob}, V_{glob} satisfying the aforementioned asymmetrical key

algorithm - and contains - in addition to an identification number (ID number) uniquely identifying the chipcard and an indication of the period of validity $T_{gült}$ - the verification function V_{card} of a card-specific key pair, said card-specific key pair enabling the chipcard to generate electronic signatures using a further asymmetrical key process. The associated signature function S_{card} is likewise stored on the card and remains thereon. In addition, a storage device on the chipcard contains further card-specific keys K_{auth}, K_{red}, used to perform symmetrical key processes, such as DES (Data Encryption Standard), Triple DES or IDEA, as well as further information, such as the name of the user, the amount of money stored and a sequence number indicating the number of withdrawals made.

The key V_{glob}, required in order to verify the certificates of the system chipcards, and two master keys KM_{auth} and KM_{red} are stored in all terminals belonging to the system. From the master keys, the terminals are able, by combining said keys with the identification numbers of the cards being processed, to reproduce the keys K_{auth} and K_{red} stored on the cards, said keys K_{auth} and K_{red} being used to execute symmetrical key processes.

When the chipcard is brought into contact with a terminal, as soon as this is detected by the card, e.g. by the presence of a supply voltage, the certificate is transferred to the terminal. If the terminal is in possession of the global key V_{glob}, then its computer is able to verify the certificate and in the process learns the identification number of the card, the validity of the card and the verification function V_{card}. The identification number and V_{card} are temporarily stored by the terminal and are thus available for subsequent checking and computing operations.

In the next step, the terminal initiates a so-called challenge and response process in that it generates in known manner a random number R_1 and communicates it to the card. Thereupon, the processor on the chipcard produces a cryptogram e_1 in which further data to be transferred to the terminal is encrypted together with the random number R_1 using the key K_{auth}, said key K_{auth} employing a symmetrical key algorithm. In particular, said cryptogram contains the amount of money stored on the chipcard, so that the terminal learns the extent to which money can be withdrawn from the card. The cryptogram e_1 is now transferred together with a second random number R_2 generated on the card, said second random number R_2 initiating a challenge and response process in the opposite direction.

While the cryptogram e_1 was being produced on the chipcard, the terminal has calculated - from the two master keys KM_{auth} and KM_{red} with the aid of the identification number of the card - the card-specific keys K_{auth} and K_{red} and is now in a position to decrypt the cryptogram e_1. Once it knows the amount to be withdrawn (which is dependent on the amount entered by the user on the terminal), the terminal compares said amount with the amount

stored on the card and, unless the latter is lower, produces a withdrawal cryptogram e_2, which, in addition to the amount to be withdrawn, contains the second random number R_2. Said cryptogram is calculated using the further key K_{red}, which employs a symmetrical key algorithm, and is transferred to the chipcard together with a third random number R_3. Here, it is basically possible, without any major loss of security, to use the key K_{auth} once again instead of the further key K_{red} and to make do without the key K_{red}.

In the next step, following the decryption of the cryptogram e_2, the money is actually withdrawn from the chipcard. For this purpose, the chipcard produces a withdrawal data record D_B with the originally stored amount of money, the amount of money withdrawn and the current amount of money as well as with further information provided for in the system, such as withdrawal/sequence number, withdrawal date, currency. The chipcard confirms said data record with an electronic signature in that, using the signature function S_{card} of the initially mentioned further key pair employing an asymmetrical key process, it produces an acknowledgement cryptogram e_3 in which is encrypted, in addition to the withdrawal data record and the identification number, also the random number R_3.
Once the terminal has temporarily stored the verification function V_{card} belonging to S_{card}, it can decrypt the cryptogram e_3 and thus verify the data record and the authenticity of the data.
If no error is found, the temporarily stored identification number and the verification function V_{card} are deleted and the delivery of the product or ticket or the establishment of a telephone connection dialled by the user is initiated.

In a similar manner, it is possible to secure the readout of information from a portable data carrier, e.g. a chipcard serving as an ID card. In this case, the chipcard first of all authenticates itself vis-à-vis the checking apparatus (terminal). This is accomplished using a symmetrical key process. Subsequently, the terminal transmits a read command, cryptogram-secured using a symmetrical algorithm, and, with said read command, its authentication to the chipcard. The chipcard communicates the information with a digital signature generated using an asymmetrical key process.

If there is an especially great need for security and if the terminal is remote from the computer centre and not connected thereto, it is possible, also in such a case, to employ an asymmetrical key process permitting the transmission of a certificate. Usually, however, it will be sufficient to use a symmetrical key process, because, in this case, there is virtually no risk of duplicates of chipcards being made by an authorized person and a third person obtaining access to a key stored in the terminal would also have to gain possession of a valid chipcard in order to be able to provide the electronic signature which, ultimately, gives the authorization associated with the ID card.

In accordance with one aspect of this invention, there is provided a system for the secure reading and editing of data on intelligent data carriers (4), especially IC cards, with terminals (2a, 2b) associated with a master computer centre (1) and equipped with interfaces (E, D) suitable for temporary communication with the data carriers, wherein stored on each data carrier, in addition to the information to be read or edited and in addition to an item of identification information, is a key (K_{auth}) which is available also to the terminals for the authentication of the data carrier in question using a symmetrical key process, characterized by the following features: a certificate stored on the data carrier for communication to the terminal is formed from data carrier specific data (ID) including a verification-specific function (V_{card}) with aid of a global signature function (S_{glob}) serving for the certification of the data carriers to be used in the system, means for verification of the certificate in the terminal with aid of a global verification function (V_{glob}) stored in the terminal and for the temporary storage of data carrier-specific data (ID) and the verification-specific function (V_{card}), means for deriving at least one key from the data carrier-specific data and of at least one master key stored in the terminal, means for data exchange between the data carrier and the terminal including communication of a data modification command of the terminal to the data carrier with a symmetrical key process, in particular a so-called challenge and response process, means for generating and communicating a data record documenting the data to be read from the chip card in form of a cryptogram formed with a signature-specific function (S_{card}) to the terminal and means for verifying the cryptogram with aid of the verification-specific function (V_{card}) in the terminal and for subsequently

deleting the temporarily stored data carrier-specific data (ID, V_{card}) in the terminal.

In accordance with a further aspect of this invention, there is provided a process for the secure reading and editing of data on intelligent data carriers, especially chip cards, with terminals (2a, 2b) associated with a master computer centre (1) and equipped with interfaces (E, D) suitable for temporary communication with the data carriers, wherein stored on each data carrier, in addition to the information to be read or edited and in addition to an item of identification information, is a key (K_{auth}) which is available also to the terminals for the authentication of the data carrier in question using a symmetrical key process, characterized by the following steps: communicating a certificate stored on the data carrier to the terminal, whereby the certificate is formed from data carrier-specific data (ID) including a verification-specific function (V_{card}) with aid of a global signature function (S_{glob}) serving for the certification of the data carriers to be used in the system, verification of the certificate in the terminal with aid of a global verification function (V_{glob}) stored in the terminal and for the temporary storage of data carrier-specific data (ID) and the verification-specific function (V_{card}), deriving at least one key from the data carrier-specific data and of at least one master key stored in the terminal, a data exchange taking place between the data carrier and the terminal including communication of a data modification command of the terminal to the data carrier with a symmetrical key process, in particular a so-called challenge and response process, generating and communicating a data record documenting the data to be read from the chip card in form of a cryptogram formed with a signature-specific function

(S_{card}) to the terminal, verifying the cryptogram with aid of the verification-specific function (V_{card}) in the terminal and for subsequently deleting the temporarily stored data carrier-specific data (ID, V_{card}) in the terminal.

In accordance with yet a further aspect of this invention, there is provided a process for the secure reading and editing of data on intelligent data carriers, especially chip cards, with terminals (2a, 2b) associated with a master computer centre (1) and equipped with interfaces (E, D) suitable for temporary communication with the data carriers, wherein stored on each data carrier, in addition to the information to be read or edited and in addition to an item of identification information, is a key (K_{auth}) which is available also to the terminals for the authentication of the data carrier in question using a symmetrical key process, characterized by the following steps: communicating a certificate stored on the data carrier to the terminal, whereby the certificate is formed from data carrier-specific data (ID) including a verification-specific function (V_{card}) with aid of a global signature function (S_{glob}) serving for the certification of the data carriers to be used in the system, verification of the certificate in the terminal with aid of a global verification function (V_{glob}) stored in the terminal and for the temporary storage of data carrier-specific data (ID) and the verification-specific function (V_{card}), deriving at least one key from the data carrier-specific data and of at least one master key stored in the terminal, a data exchange taking place between the data carrier and the terminal including communication of a data modification command of the terminal to the data carrier with a symmetrical key process, in particular a so-called challenge and response process, generating and communicating a data record (DB)

documenting the data modification in form of a cryptogram formed with a signature-specific function (S_{card}) to the terminal, verifying the cryptogram with aid of the verification-specific function (V_{card}) in the terminal and for subsequently deleting the temporarily stored data carrier-specific data (ID, V_{card}) in the terminal.

New Patent Claims

1. System for the secure reading and editing of data on intelligent data carriers (4), especially IC cards, with terminals (2a, 2b) associated with a master computer centre (1) and equipped with interfaces (E, D) suitable for temporary communication with the data carriers, wherein stored on each data carrier, in addition to the information to be read or edited and in addition to an item of identification information, is a key (K_{auth}) which is available also to the terminals for the authentication of the data carrier in question using a symmetrical key process,
characterized by the following features:

- a certificate stored on the data carrier for communication to the terminal is formed from data carrier specific data (ID) including a verification-specific function (V_{card}) with aid of a global signature function (S_{glob}) serving for the certification of the data carriers to be used in the system,
- means for verification of the certificate in the terminal with aid of a global verification function (V_{glob}) stored in the terminal and for the temporary storage of data carrier-specific data (ID) and the verification-specific function (V_{card}),
- means for deriving at least one key from the data carrier-specific data and of at least one master key stored in the terminal,
- means for data exchange between the data carrier and the terminal including communication of a data modification command of the terminal to the data carrier with a symmetrical key process, in particular a so-called challenge and response process,

- means for generating and communicating a data record documenting the data to be read from the chip card in form of a cryptogram formed with a signature-specific function (S_{card}) to the terminal and
- means for verifying the cryptogram with aid of the verification-specific function (V_{card}) in the terminal and for subsequently deleting the temporarily stored data carrier-specific data (ID, V_{card}) in the terminal.

2. System according to claim 1, characterized therein that the key to be used in the symmetrical key process for the authentication of a data carrier is derived from a master key (KM_{auth}) using data carrier-specific data, especially an identification number, that said master key is stored in all terminals belonging to the system and that the key (K_{auth}) required for the authentication of a data carrier vis-à-vis a terminal is in each case calculated from the stored master key and from the data carrier-specific data communicated from the data carrier.

3. System according to any one of the claims 1 or 2, characterized therein that a further key (K_{red}) usable in a symmetrical key process is available on each data carrier and in each terminal, said further key (K_{red}) being used to authenticate the terminal vis-à-vis a therewith communicating data carrier.

4. System according to claim 3, characterized therein that the further key (K_{red}) is stored in each case on the data carrier and in the terminal or is derived from a stored master key (KM_{red}) using data carrier-specific data.

5. Process for the secure reading and editing of data on intelligent data carriers, especially chip cards, with terminals (2a, 2b) associated with a master computer centre (1) and equipped with interfaces (E, D) suitable for temporary communication with the data carriers, wherein stored on each data carrier, in addition to the information to be read or edited and in addition to an item of identification information, is a key (K_{auth}) which is available also to the terminals for the authentication of the data carrier in question using a symmetrical key process,
characterized by the following steps:

- communicating a certificate stored on the data carrier to the terminal, whereby the certificate is formed from data carrier-specific data (ID) including a verification-specific function (V_{card}) with aid of a global signature function (S_{glob}) serving for the certification of the data carriers to be used in the system,
- verification of the certificate in the terminal with aid of a global verification function (V_{glob}) stored in the terminal and for the temporary storage of data carrier-specific data (ID) and the verification-specific function (V_{card}),
- deriving at least one key from the data carrier-specific data and of at least one master key stored in the terminal,
- a data exchange taking place between the data carrier and the terminal including communication of a data modification command of the terminal to the data carrier with a symmetrical key process, in particular a so-called challenge and response process,
- generating and communicating a data record documenting the data to be read from the chip card in form of a

cryptogram formed with a signature-specific function (S_{card}) to the terminal,

- verifying the cryptogram with aid of the verification-specific function (V_{card}) in the terminal and for subsequently deleting the temporarily stored data carrier-specific data (ID, V_{card}) in the terminal.

6. Process for the secure reading and editing of data on intelligent data carriers, especially chip cards, with terminals (2a, 2b) associated with a master computer centre (1) and equipped with interfaces (E, D) suitable for temporary communication with the data carriers, wherein stored on each data carrier, in addition to the information to be read or edited and in addition to an item of identification information, is a key (K_{auth}) which is available also to the terminals for the authentication of the data carrier in question using a symmetrical key process,
characterized by the following steps:

- communicating a certificate stored on the data carrier to the terminal, whereby the certificate is formed from data carrier-specific data (ID) including a verification-specific function (V_{card}) with aid of a global signature function (S_{glob}) serving for the certification of the data carriers to be used in the system,
- verification of the certificate in the terminal with aid of a global verification function (V_{glob}) stored in the terminal and for the temporary storage of data carrier-specific data (ID) and the verification-specific function (V_{card}),
- deriving at least one key from the data carrier-specific data and of at least one master key stored in the

terminal,

- a data exchange taking place between the data carrier and the terminal including communication of a data modification command of the terminal to the data carrier with a symmetrical key process, in particular a so-called challenge and response process,
- generating and communicating a data record (DB) documenting the data modification in form of a cryptogram formed with a signature-specific function (S_{card}) to the terminal,
- verifying the cryptogram with aid of the verification-specific function (V_{card}) in the terminal and for subsequently deleting the temporarily stored data carrier-specific data (ID, V_{card}) in the terminal.

7. Process according to claim 6, characterized therein that the data carrier is used as an electronic purse and in that the data record (DB) documenting the modification of data contains the amount of money valid prior to the editing of the data (withdrawal), the amount of money withdrawn and the amount of money valid after the editing of the data.

8. Process according to any one of claims 6 or 7, characterized therein that the number of data edits is serially counted on the data carrier and a sequence number representing the counting results is communicated to the terminal together with the data record documenting the data modification.

9) Process for the secure editing of data on intelligent data carriers, especially the withdrawal of amounts of money from chipcards used as electronic purses, in a system according to any one of the preceding claims, **characterized by** the following steps:

- authentication of the data carrier vis-à-vis the terminal using a symmetrical key process, especially a so-called challenge and response process, and communication to the terminal of specified data carrier-specific data stored on the data carrier as well as of the second key (V_{card}) of the additional key pair (S_{card}, V_{card}) specifically associated with the data carrier, said second key (V_{card}) serving the purpose of verification;

- communication of a data modification command, secured by a symmetrical key process, from the terminal to the data carrier, the symmetrical key process simultaneously authenticating the terminal vis-à-vis the data carrier;

- execution of the data modification depending on the correct authentication of the terminal;

- generation and communication of a data record (D_B) documenting the data modification, with an electronic signature calculated using an asymmetrical key process by means of the first key (S_{card}) of the additional key pair;

- verification of the electronic signature and of the data record by the terminal by means of the second key (V_{card}) of the additional key pair.

10) Process for the secure reading of data on intelligent data carriers in a system according to any one of claims 2 to 7, **characterized by** the following steps:

- communication to the terminal of specified data carrier-specific data - said data carrier-specific data being stored on the data carrier together with the second key (V_{card}) of the additional key pair (S_{card}, V_{card}) specifically associated with the data carrier, said second key (V_{card}) serving the purpose of verification, and said data carrier-specific data being secured by electronic signature of the computer centre by means of the first key (S_{glob}), kept in a central location, of the further key pair (S_{glob}, V_{glob}), said further key pair (S_{glob}, V_{glob}) satisfying an asymmetrical key algorithm - and verification of the electronic signature by means of the second key (V_{glob}) of said key pair, said second key (V_{glob}) being stored in all terminals;

- communication of a read command, secured by a symmetrical key process, from the terminal to the data carrier, the symmetrical key process, especially a so-called challenge and response process, simultaneously authenticating the terminal vis-à-vis the data carrier;

- communication of the data to be read, together with an electronic signature generated on the data carrier using an asymmetrical key process by means of the first key (S_{card}) of the additional key pair specifically associated with the data carrier;

- verification by the terminal of the electronic signature generated on the data carrier by means of the second key (V_{card}) of the additional key pair specifically associated with the data carrier.

11) Process for the secure editing of data on intelligent data carriers, especially the withdrawal of amounts of money from chipcards used as electronic purses, in a system according to any one of claims 2 to 7, **characterized by** the following steps:

- communication to the terminal of specified data carrier-specific data - said data carrier-specific data being stored on the data carrier together with the second key (V_{card}) of the additional key pair (S_{card}, V_{card}) specifically associated with the data carrier, said second key (V_{card}) serving the purpose of verification, and said data carrier-specific data being secured by electronic signature of the computer centre by means of the first key (S_{glob}), kept in a central location, of the further key pair (S_{glob}, V_{glob}), said further key pair (S_{glob}, V_{glob}) satisfying an asymmetrical key algorithm - and verification of the electronic signature by means of the second key (V_{glob}) of said key pair, said second key (V_{glob}) being stored in all terminals;

- communication of further data stored on the data carrier using a communication process which secures the data by means of a symmetrical key process, said communication process being, in particular, a so-called challenge and response process initiated by the terminal;

- communication of a data modification command, secured by a symmetrical key process, from the terminal to the data carrier, the symmetrical key process, in particular, a so-called challenge and response process, simultaneously authenticating the terminal vis-à-vis the data carrier;

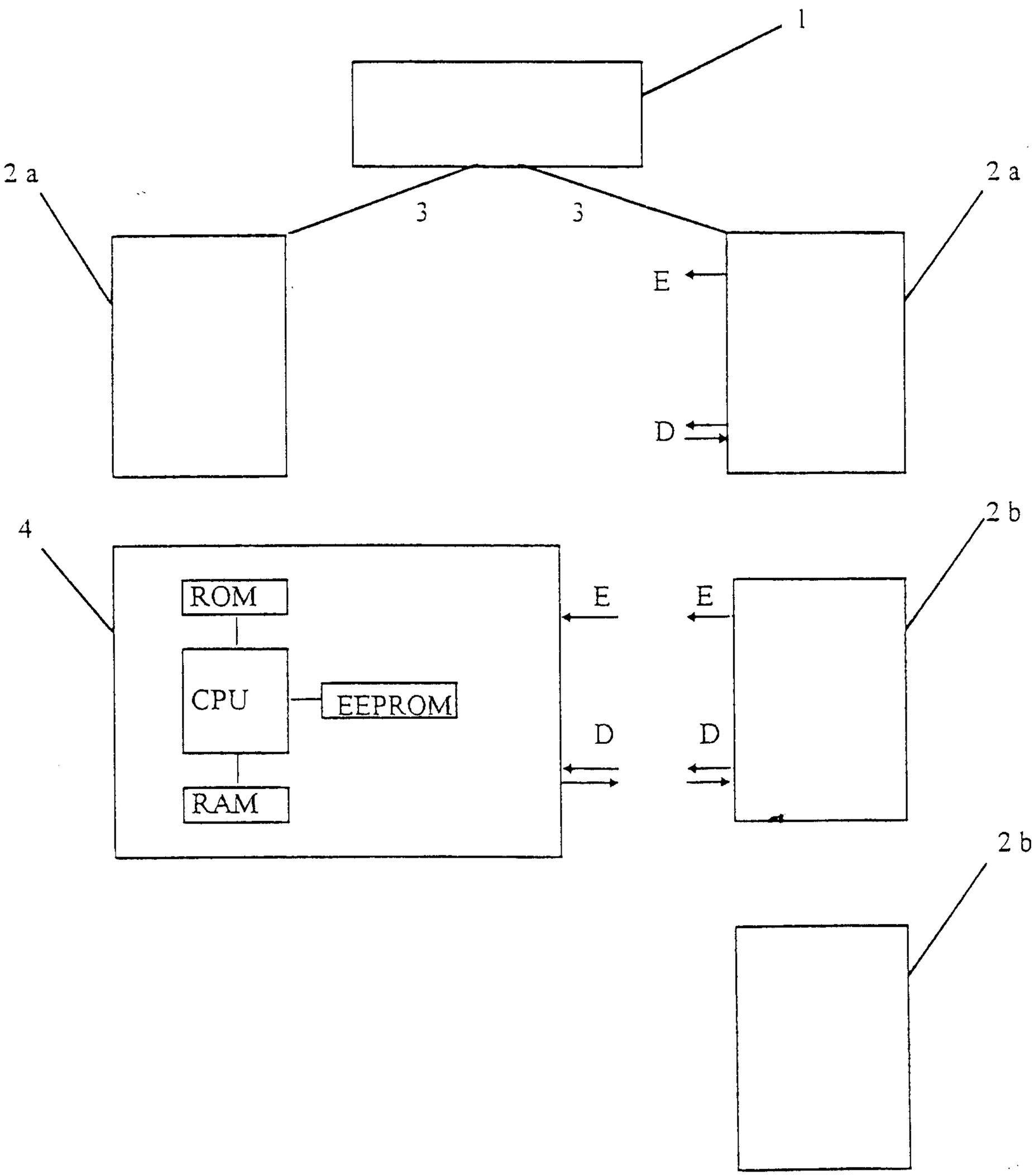
- execution of the data modification in the data carrier depending on the correct authentication of the terminal;

- generation and communication of a data record (D_B) documenting the data modification, together with an electronic signature generated on the data carrier using an asymmetrical key process by means of the first key (S_{card}) of the additional key pair specifically associated with the data carrier;

- verification by the terminal of the electronic signature generated on the data carrier and of the data record using the second key (V_{card}) of the additional key pair specifically associated with the data carrier.

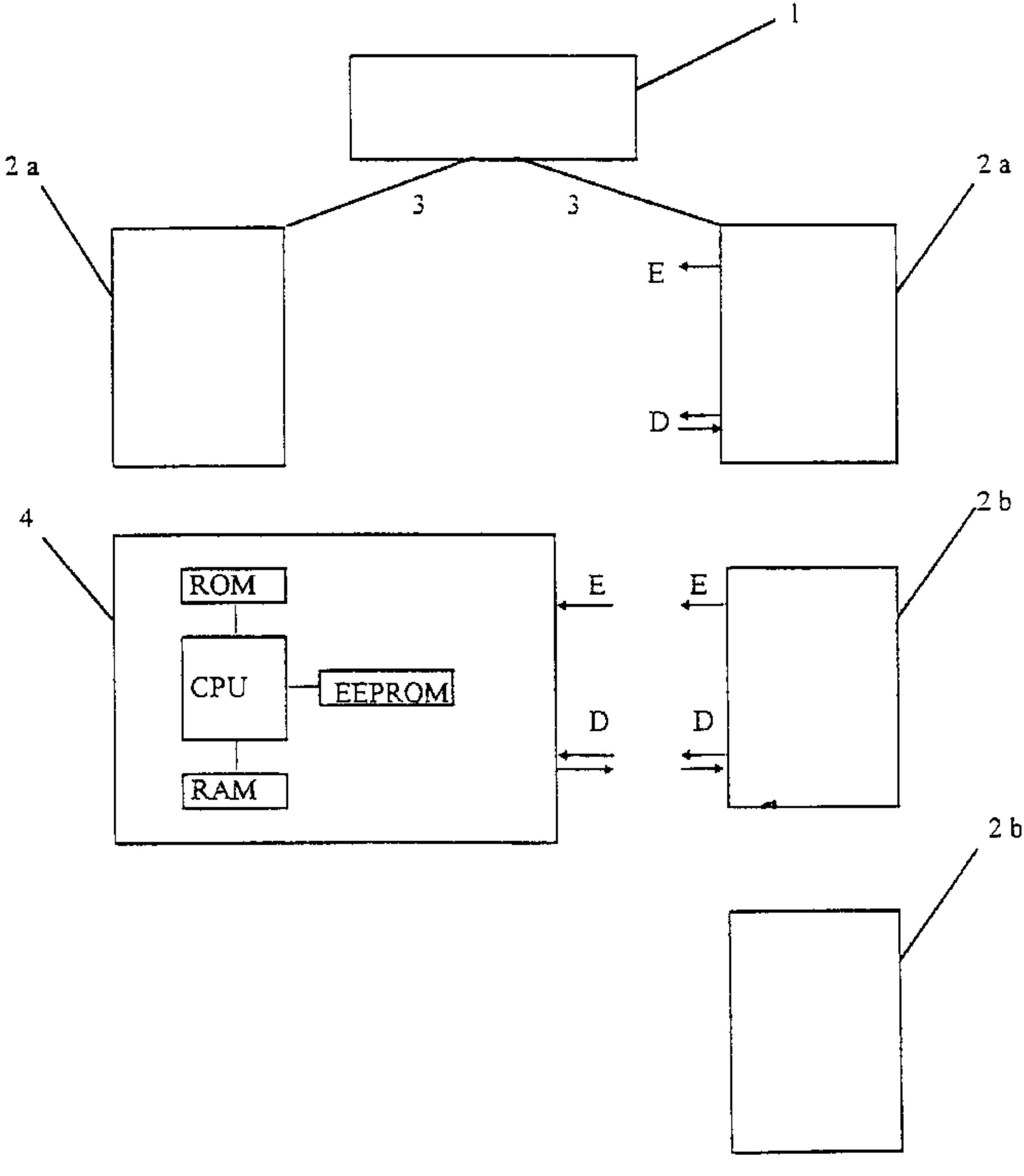
12) Process according to claim 9 or claim 11, characterized in that the data carrier is used as an electronic purse and in that the data record (D_B) documenting the modification of data contains the amount of money valid prior to the editing of the data (withdrawal), the amount of money withdrawn and the amount of money valid after the editing of the data.

Figur 1



Figur 2 Figure 2

Chip Card Chipkarte	transfer Übertragung	Terminal Terminal
Certificate No. Zertifikat: S_{glob} (ID-Nr., V_{card}, T_{gilt}) K_{auth}, K_{red}, S_{card}, Name, Betrag, Sequenznr., ggf. weitere Info - additional information, if applicable	Name Amount	V_{glob}, KM_{auth}, KM_{red}
Sequence No.	Certificate Zertifikat ⇒	verification of certificate with V_{glob},
	temporary storage	Überprüfen d. Zertifikats mit V_{glob}, temporär. Speichern von V_{card} und an d ID - Number, Generieren einer generating Zufallszahl R_1 a random number R
Producing a cryptogram	⇐ R_1	calculating from
Erstellen eines Kryptogrammes: $e_1 = K_{auth}$ (ID - Nr., R_1, Betrag, Amount weitere Info), Generieren von R_2 additional information →	generating R_2	(Berechnen von) K_{auth} (aus) KM_{auth} and number and und ID - Nummer und K_{red} aus from KM_{red} and number und ID - Nummer
	e_1, R_2 ⇒	
	determining whether withdrawal is possible producing a cryptogram generating R_3	decrypting e_1 by Entschlüsseln von e_1 mittels K_{auth} → Feststellen ob Abbuchung möglich → Erstellen eines Kryptogramms $e_2 = K_{red}$ (Abb.-Betrag, R_2) Generieren von R_3
	⇐ e_2, R_3	
decrypting e_2 by Entschlüsseln von e_2 mittels K_{red} make withdrawal Abbuchung ausführen, Buchungs - datensatz D_B erstellen, Elektron. Unterschrift mit S_{card} berechnen: $e_3 = S_{card}$ (ID-Nr., D_B, R_3)	producing data record document (electronic signature with S_{card}) Calculating?	
	e_3 ⇒	
verifying electronic signature by decrypting with temporarily stored V_{card}. If signature and documentation data o.k. – delete V_{card} + ID-No, issue wares, ticket or the like.		Prüfen der Elektronischen Unter - schrift durch Entschlüsseln mit temporär.gespeichertem V_{card}, Wenn Unterschrift und Buchungs- daten o.k., V_{card} u. ID-Nr. löschen, Ware, Fahrkarte o.ä. ausgeben.


1
2 a
2 a
3
3
E
D
4
ROM
CPU
EEPROM
RAM
E
D
E
D
2 b
2 b