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

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2425176 A1 2003/04/07

(21) 2 425 176

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2000/10/05
(87) Date publication PCT/PCT Publication Date: 2003/04/07
(85) Entrée phase nationale/National Entry: 2003/04/07
(86) N° demande PCT/PCT Application No.: DE 2000/003506
(87) N° publication PCT/PCT Publication No.: 2001/025879
(30) Priorités/Priorities: 1999/10/07 (199 48 319.1) DE;
2000/04/27 (100 20 561.5) DE

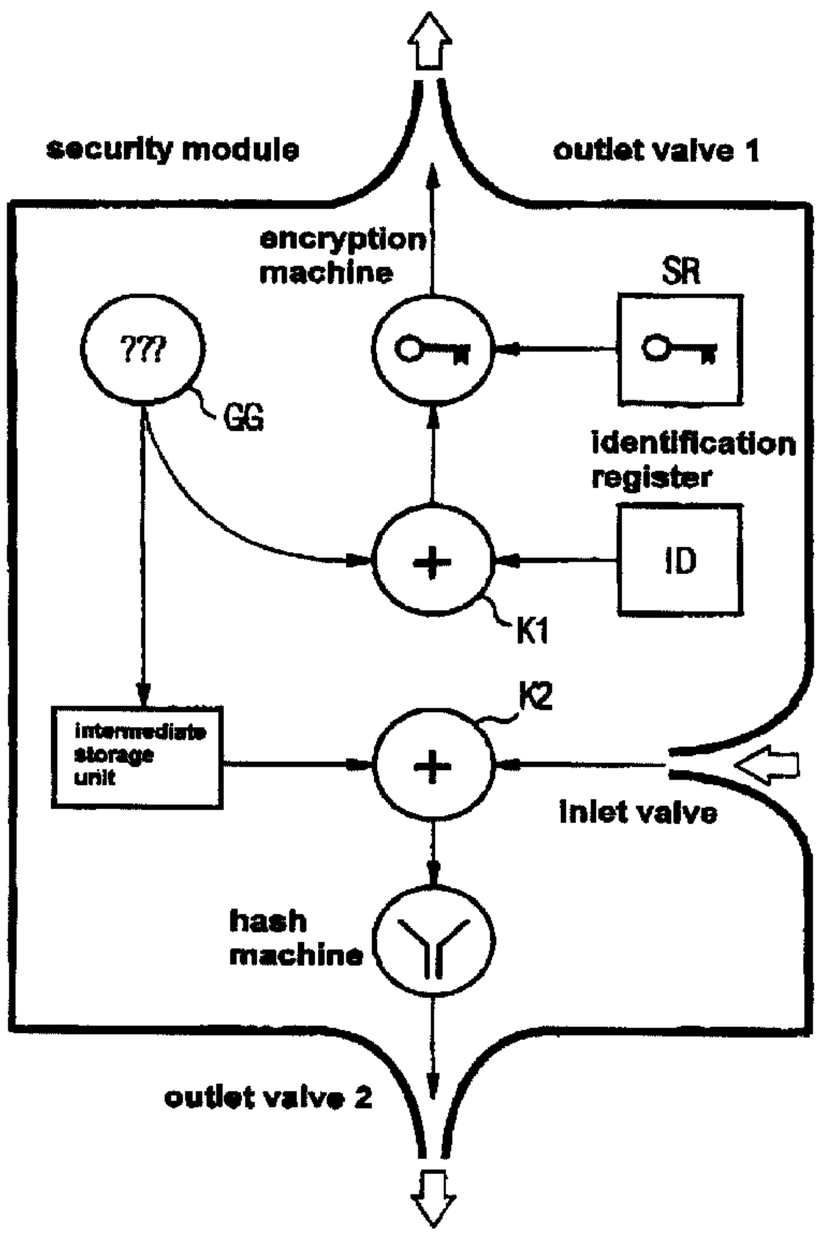
(51) Cl.Int.^{7}/Int.Cl.^{7} G07B 17/00

(71) Demandeur/Applicant:
DEUTSCHE POST AG, DE

(72) Inventeurs/Inventors:
LANG, JURGEN, DE;
MEYER, BERND, DE

(74) Agent: OGILVY RENAULT

(54) Titre : MODULE DE SECURISATION ET PROCEDE DE CREATION DE DOCUMENTS INFALSIFIABLES
(54) Title: SECURITY MODULE AND METHOD FOR PRODUCTION OF FORGE-PROOF DOCUMENTS



(57) Abrégé/Abstract:
The invention relates to a security module characterized in that said module contains a data input port via which information can be inputted into the security modul. The security module has at least two data output ports whereby data can be outputted via a first data output port and transferred to an authentication unit and whereby data can be outputted via a second data output port. Said data can be transferred to a document to be exported. Said security module has at least two combination machines. A first combination machine generates a first result value for a first data output and a second combination machine generates a result value for the second data output. The invention relates to the use of a security module for generating forge-proof documents.

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
12. April 2001 (12.04.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/25879 A3

(51) Internationale Patentklassifikation[7]: **G07B 17/00**

(21) Internationales Aktenzeichen: PCT/DE00/03506

(22) Internationales Anmeldedatum:
5. Oktober 2000 (05.10.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:

199 48 319.1	7. Oktober 1999 (07.10.1999)	DE
100 20 561.5	27. April 2000 (27.04.2000)	DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **DEUTSCHE POST AG** [DE/DE]; Heinrich-von-Stephan-Strasse 1, 53175 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **LANG, Jürgen** [DE/DE]; Schau ins Land 15, 51429 Bergisch Gladbach (DE). **MEYER, Bernd** [DE/DE]; Zum Stöckerhof 2 c, 53639 Königswinter (DE).

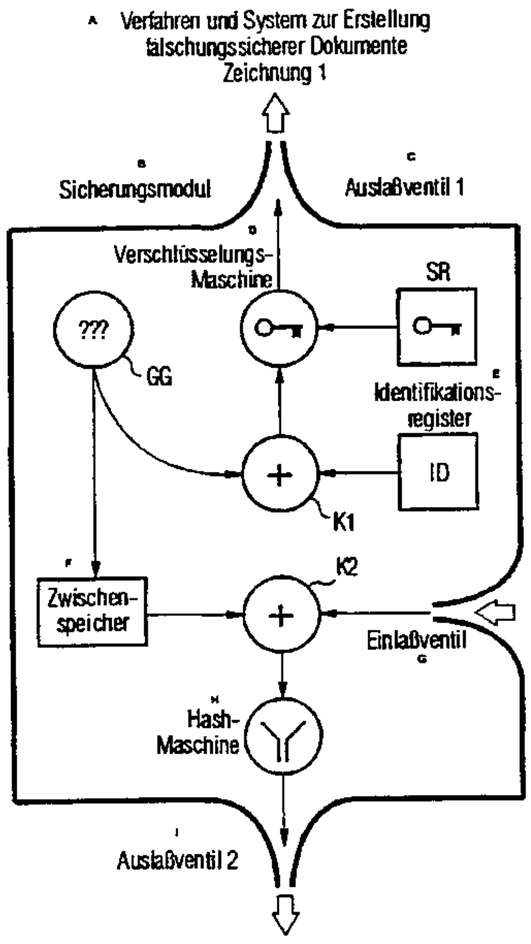
(74) Anwalt: JOSTARNDT, Hans-Dieter; Eupener Strasse 266, 52076 Aachen (DE).

(81) Bestimmungsstaaten *(national)*: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE,

[Fortsetzung auf der nächsten Seite]

(54) Title: SECURITY MODULE AND METHOD FOR PRODUCTION OF FORGE-PROOF DOCUMENTS

(54) Bezeichnung: SICHERUNGSMODUL UND VERFAHREN ZUR ERSTELLUNG FÄLSCHUNGSSICHERER DOKUMENTE



A. METHOD AND SYSTEM FOR THE GENERATION OF FORGE-SAFE DOCUMENTS
DRAWING 1
B. SAFETY MODULE
C. OUTLET VALVE 1
D. ENCRYPTING MACHINE
E. IDENTIFICATION REGISTER
F. INTERMEDIATE MEMORY
G. INLET VALVE
H. HASH MACHINE
I. OUTLET VALVE 2

(57) Abstract: The invention relates to a security module characterized in that said module contains a data input port via which information can be inputted into the security modul. The security module has at least two data output ports whereby data can be outputted via a first data output port and transferred to an authentication unit and whereby data can be outputted via a second data output port. Said data can be transferred to a document to be exported. Said security module has at least two combination machines. A first combination machine generates a first result value for a first data output and a second combination machine generates a result value for the second data output. The invention relates to the use of a security module for generating forge-proof documents.

(57) Zusammenfassung: Erfindungsgemäß zeichnet sich das Sicherungsmodul dadurch aus, dass es einen Dateneingang enthält, durch den Informationen in das Sicherungsmodul eingegeben werden können, dass das Sicherungsmodul wenigstens zwei Datenausgänge enthält, wobei durch einen ersten Datenausgang

[Fortsetzung auf der nächsten Seite]

WO 01/25879 A3

Description

Security module and method for producing forgery-proof documents

The invention relates to a security module.

The invention also relates to a method for producing forgery-proof documents, whereby input data is input into a data input port of a security module.

The invention has the objective of creating a security module by means of which forgery-proof documents can be generated.

This objective is achieved according to the invention in that a security module is configured in such a way that it has a data input port via which information can be input into the security module, in that the security module has at least two data output ports, whereby data can be output via a first data output port and then transferred to an authentication unit and whereby data can be output via a second data output port and then be transferred to a document to be issued, in that the security module has at least two combination machines, whereby a first combination machine generates a result value for the first data output port and whereby a second combination machine generates a result value for the second data output port.

In order to enhance the security of the data, it is advantageous for the security module to be configured in such a way that it has a secret generator that generates an unpredictable secret.

In this context, it is particularly advantageous for the secret generator to be connected to the first combination machine and/or to the second combination machine in such a way that a secret generated by the secret generator is introduced into the first combination machine and/or into the second combination machine.

When the security module is used in systems that effectuate payments, especially payments for services, it is particularly practical for the security module to be configured in such a way that it has an identification register, whereby an output value of the identification register is connected to the first combination machine in such a manner that a value of the identification register is introduced into a data combination issued by the first combination machine.

The security of the data can be advantageously further enhanced in that the security module has at least one encryption machine that encrypts an output value of one of the combination machines.

Here, it is practical for the encryption machine to be connected to a key register, whereby at least one value contained in the key register can be used in the encryption machine for encryption purposes.

An advantageous implementation of the security module is characterized in that it has a hash machine.

Further advantages, special features and practical refinements of the invention can be gleaned from the subordinate claims and from the following presentation of preferred embodiments with reference to the drawing.

The drawing, Figure 1, shows a schematic diagram of a security module suitable for producing forgery-proof documents.

The security module shown in Figure 1 has a data input port via which information can be input into the security module.

The security module also has two data output ports DA1 and DA2.

The first data output port DA1 can output data that is transferred to an external unit, for instance, an authentication unit.

The second data output port DA2 can transmit data to a document that is going to be issued.

The security module also has at least two combination machines K1, K2. The first combination machine K1 generates a result valuc for the first data output port DA1. The second combination machine K2 generates a result value for the second data output port DA2.

Furthermore, the security module has at least one secret generator GG that generates an unpredictable secret. The secret generator is connected to the first combination machine K1 as well as to the second combination machine K2. The secret generator GG and the combination machine K2 are preferably connected by means of an intermediate memory unit.

The intermediate memory unit preferably serves the function of temporarily storing the secret generated by the secret generator.

The security module also has an idcntification register that is connected to the first combination machine K1 in such a way that a value of the identification register is introduced into a data combination that is output by the first combination machine.

An encryption machine contained in the security module is programmed in such a way that it encrypts an output value of one of the combination machines, namely, combination machine K1 in the case described here.

In order to save memory space, it is practical to use an asymmetrical key pair based on a suitable security standard such as, for example, RSA, for purposes of the encryption and the signature. Since no random texts predefined by the user can be introduced into the cncryption, signature and hash value formation, this step is warranted.

The key length is preferably at least 128 bits, advantageously much more, for instance, at least 1024 bits, RSA.

The hash value is prefcrably generated according to standard SHA-1. The hash machine irreversibly links introduced data to a secret. As a result, when the same data is linked again in the same manner, an identical result is obtained without allowing any conclusions about the secret. Preferably, the secret is temporary since this improves the level of security. This, however, is not nccessary. For instance, the secret can be permanently stored into a data memory unit.

The operating principle of the security module will be explained below with reference to the especially preferred example of the franking of mailed letters.

However, the security module is likewise suitable for other encryption purposes. The use of the security module for producing forgery-proof documents is particularly advantageous. The expression "forgery-proof document" should be understood in its broadest sense. In addition to the franking described as examples, the forgery-proof documents can also be transportation tickets or entrance tickets. The capability to generate every single documcnt on the basis of individual data also allows the creation of unique documents such as personal identity cards, seat tickets or lists containing personalized values.

The security module preferably processes information that can bc individualized such as, for example, certificates and digitally signed licenses.

In a preferred example of an application for the franking of letters at Deutsche Post AG, this is done as follows:

A digital signature is a digital data seal that is generated with a private signature key and that uses an associated public key, which is provided with a signature key certificate, to recognize the owner of the signature key and thc integrity of the data (see Article 2, Clause 1 of SigG - German Signature Law). Using the terminology employed there, a checking unit is able to examine the digital signature of a document producer and thus also its identity, as well as the integrity of the data contained in the document if the checking unit knows the public signature key of the document producer that is provided with a signature key certificate.

Every security module produced is "digitally licensed" by the client system producer. In order to communicate with the security modules, the authentication unit creates its own signed communication license in the same format.

The certification and the signed licensing preferably take place as follows:

The security module internally generates a key pair whose public key P_{SB} is digitally licensed using the private signature key of the client system issuer S_I (issuer). Like the public key of the authentication unit, the public key of the client system issuer P_I is generated and certified by the certification unit (CA), where it is available for checking.

Altogether, the following keys, certificates and signed licenses are used in the system.

The security module contains a private key of the security module, a public key of the security module and a license of the public key of the security module signed by the client system issuer.

Preferably, at least one private key of the authentication unit and one public key of the authentication unit are available to the authentication unit.

The security module checks the validity of the signed license, for example, by contacting a certification unit.

The authentication unit checks the validity of the signed license of a security module – and thus the identity of the client system issuer via the identity of the natural person who is responsible for the client system issuer according to the attribute entry in the certificate – by contacting the certification unit.

The issuer of the signature cards ensures that the appertaining attributes (for instance, legal authorization to issue licenses for security modules) are exclusively issued in coordination with the unit to which the forgery-proof documents are submitted.

A regular replacement of the key pair of the security module is not necessary although it is possible. The envisaged duration of validity of the key should be as long as possible in order to increase the user-friendliness. Preferably, the key of the security module is valid for several months or years, whereby values between 3 months and 15 years are options. Preferably, the duration of validity lies between 3 and 10 years, 6 years being particularly suitable.

At any time, the client system producer is authorized to change the keys with which it digitally licenses the licenses of the issued security modules. At the latest after one year, the client system producer is obliged to change the signature key with which it digitally signs the licenses of the issued security modules and concurrently to block the old signature key. The client system producer identifies the signature key in coordination with the authentication unit.

A unit authorized to check the forgery-proof documents rejects transactions when a corruption of a key is noted. When the security module is employed to produce forgery-proof postage stamps, the unit authorized to check the documents is the postal service operator, for example, Deutsche Post AG. In this case, a corruption of a key of a client system issuer results in an immediate rejection on the part of the postal system of any transactions with security modules of the client system producer whose signed licenses have been produced with this key.

The administration of the keys of the certification unit is done in accordance with the applicable statutory and legal administrative stipulations. In Germany, these are the German Signature Law (SigG) and the German Signature Regulations (SigV). The security can be further improved by incorporating internal processing stipulations.

The keys of the authentication unit can be changed at any time without the need for changes to be made in the client systems.

An authentication process will be described below with reference to the use of symmetrical keys of the authentication unit.

Symmetrical keys allow very fast encrypting and decrypting. The use of symmetrical keys presupposes that the key of the sender matches the key of the recipient. In the case of communication between the authentication unit and numerous client systems, symmetrical keys can be employed if the authentication unit has sufficient memory capacity for the individual keys that match the appertaining client systems.

The use of asymmetrical keys, in contrast, means that the sender encrypts the communication with the public key of the recipient and that the recipient decrypts the communication with its private key.

Depending on the area of application, either symmetrical or asymmetrical keys should be employed. The methods described, however, can fundamentally function with symmetrical keys as well as with asymmetrical keys.

Security tasks of the security module

For purposes of initialization, communication with the authentication unit and deactivation, the security module essentially has to perform the following tasks:

Key generation

Generation and storage of an asymmetrical key pair within the security module.

Issuing the public key

Issuing the generated public key within the scope of the digital signature of the license by the client system issuer. The private key must never leave the security module.

Certificate storage

Permanent storage of one's own public key or of one's own signed license within the scope of the initialization.

Signature generation

Generation of a digital signature employing one's own private signature key.

Signature check

Checking the digital signature of an authentication module of the authentication unit using the signed license of the authentication unit and its certificate according to a suitable security standard such as, for instance, SigG.

Certificate check

Checking a certificate through an inquiry to the certification unit.

Temporary certificate storage

Temporary storage of a certificate or of a signed license within the scope of a communication session.

Asymmetrical encryption

Encryption of data with a verified public key of a communication partner.

Asymmetrical decryption

Decryption of data with one's own private key, the data having been encrypted with one's own public key.

Random number generation

Generation and permanent storage of a demonstrably high-quality random number within a numerical space of at least 16 bytes.

Storage of a session key

Temporary storage of a session key having a length of 16 bytes.

Storage of two identification numbers of the loading operation

Storage of each of the two most recent identification numbers having a length of 16 bytes each.

Storage of the current register value of the currency depot

Storage of the currency and of the sum that can currently be used to produce postage stamps; "descending register".

Storage of the ascending register value

Storage of all of the sums that have been spent for franking with the security module, preferably in a single currency, for example, the euro; "ascending register".

User identification

Personal identification of the security module user who is authorized for certain utilization options by using a PIN to be encrypted with the user's own public key.

Status output of the identification number of the loading operation

Output of the validity of the current loading system to the client system without the possibility of changes by the client system.

Status output of the register value of the currency depot

Output of the currently available depot value to the client system without the possibility of changes by the basic system.

Hash formation of the transmission-specific data

Formation of a hash value, for example, according to SHA-1 of the transmission-specific data transmitted by the client system and of the stored random number.

Reduction of register values of a currency depot

Preferably, the security module works together with a digital currency depot. This currency depot can be integrated into the security module or else be accommodated separatcly. A separate accommodation is cffcctuated, for example, in a digital wallet. The storage operation ensures that only actually available sums will be used. During the utilization, where, for instance, a hash value is formed, the sum and thus also the register value associated with it are reduced.

Digital signature of the transmission-specific data

Formation and issuing of the digital signature of the transmission-specific data for each hash formation of the transmission-specific data.

Error log

Logging the activity of valid as well as invalid communication attempts with the security module.

Self-test

Carrying out a self-test during each activation.

Deactivation

Deactivation of the security module after identification and request by an operator.

Security level according to FIPS PUB 140

The objective of the security module is to ensure the confidentiality and integrity of information that is stored and processed in the security module within a client system. In order to attain a uniform security level with different client systems and different security modules, the correspondence with and certification according to a pre-specified security level, for example, according to a security level defined by FIPS PUB 140 (FIPS PUB 140: "Security Level") is advantageous.

The use of FIPS PUB 140, Security Level 4, is particularly advantageous.

The security level recommended for the execution is FIPS PUB 140, Security Level 3 because it combines a high degree of data security with simple handling.

It is particularly advantageous for the system to fulfill requirements that exceed FIPS PUB 140-1.

In order to further enhance the security of the data, it is advantageous to carry out the safety-relevant processes of the client system as follows:

The security module is produced and initialized in a secure environment in accordance with the security standard coordinated with Deutsche Post AG. The risk of corruption of the signature key employed to create the signed licenses of the produced security module is minimized by inspections. In the production process, a key pair is generated, a

public key for generating the signed license by the client system issuer is created, a signed license of the security module (including the security module ID) is stored in the security module and the attribute entry is stored in an employed certificate.

Activation of the security module by the client system

In order to activate the security module from the client system, the security module is requested to submit its signed license (including its public key P_{SB}) as well as a random number X_{auth} having a length of 16 bytes to the client system. (The random number especially serves to safeguard against replay attacks whenever there is an unsecured transmission value between the keyboard of the client system and the security module, for instance, in the case of Internet solutions involving a central security module server on the Internet and decentralized PCs as input terminals for login information such as, for example, the PIN.)

Handling of errors

If the signed license and random number are requested several times, for instance, three times in a row, without login data being subsequently transmitted from the client system to the security module, this has to be logged in the security module. In this mode, all that is permissible is a subsequent connection with the authentication unit for error correction with a transmission of the log status, but not the production of forgery-proof documents such as entrance tickets or postage stamps.

After the authentication of the client system or client, the security module reads the current identification number of the loading operation, the preceding identification number, the current value sum and the validity of the value and transmits these to the basic system. There can be no change to these values by this user (FIPS PUB 140: role) in this user utilization possibility (FIPS PUB 140: service).

Patent Claims

1. A security module, **characterized in that** it has a data input port via which information can be input into the security module, in that the security module has at least two data output ports, whereby data can be output via a first data output port and then transferred to an authentication unit and whereby data can be output via a second data output port and then be transferred to a document to be issued, with at least two combination machines (K1, K2), whereby a first combination machine (K1) generates a result value for the first data output port and whereby a second combination machine (K2) generates a result value for the second data output port.

2. The security module according to Claim 1, **characterized in that** it has a secret generator that generates an unpredictable secret.

3. The security module according to Claim 2, **characterized in that** the secret generator is connected to the first combination machine and/or to the second combination machine in such a way that a secret generated by the secret generator is introduced into the first combination machine (K1) and/or into the second combination machine (K2).

4. The security module according to one or more of the preceding claims, **characterized in that** it has an identification register, whereby an output value of the identification register is connected to the first combination machine (K1) in such a manner that a value of the identification register is introduced into a data combination issued by the first combination machine.

5. The security module according to one or more of the preceding claims, **characterized in that** it has at least one encryption machine that encrypts an output value of one of the combination machines (K1).

6. The security module according to Claim 5, **characterized in that** the encryption machine is connected to a key register, whereby at least one value contained in the key register can be used in the encryption machine for encryption purposes.

7. The security module according to one or more of the preceding claims, **characterized in that** it has a hash machine.

8. A method for producing forgery-proof documents, whereby input data is input into a data input port of a security module and whereby the security module generates information that serves to identify individual documents, **characterized in that** the input data is input into a data input port of a security module, where it is combined with data representing a secret and in that the secret is further processed in a processing step separate from the combining operation, and in that data is acquired from the combination of the data representing the secret and the input data.

9. The method according to Claim 8, **characterized in that** the secret is output by a first data output port and in that the data acquired from the combination of the data representing the secret and the input data is output at a second data output port.

10. The method according to one or more of the preceding claims, **characterized in that** the data representing the secret and the input data are combined in a second combination machine (K2).

11. The method according to Claim 10, **characterized in that** the data representing the secret and the input data are irreversibly linked to each other, whereby this irreversible linking is done in such a way that, exclusively when the same data is linked again in the same manner, an identical result is obtained, without allowing any conclusions about the temporary secret.

12. The method according to one or more of Claims 8 through 11, **characterized in that** the data representing the secret is further linked while introducing data of an identification register.

13. The method according to Claim 12, **characterized in that** the result of the combination of the data representing the secret and the data of the identification register (ID) is encrypted in an encryption machine.

14. The method according to Claim 13, **characterized in that** the encryption takes place while introducing a key whose value is stored in a key register (SR).

15. The method according to one of more of Claims 8 through 14, **characterized in that** this data that is output from the first data output port is transferred to an authentication unit.

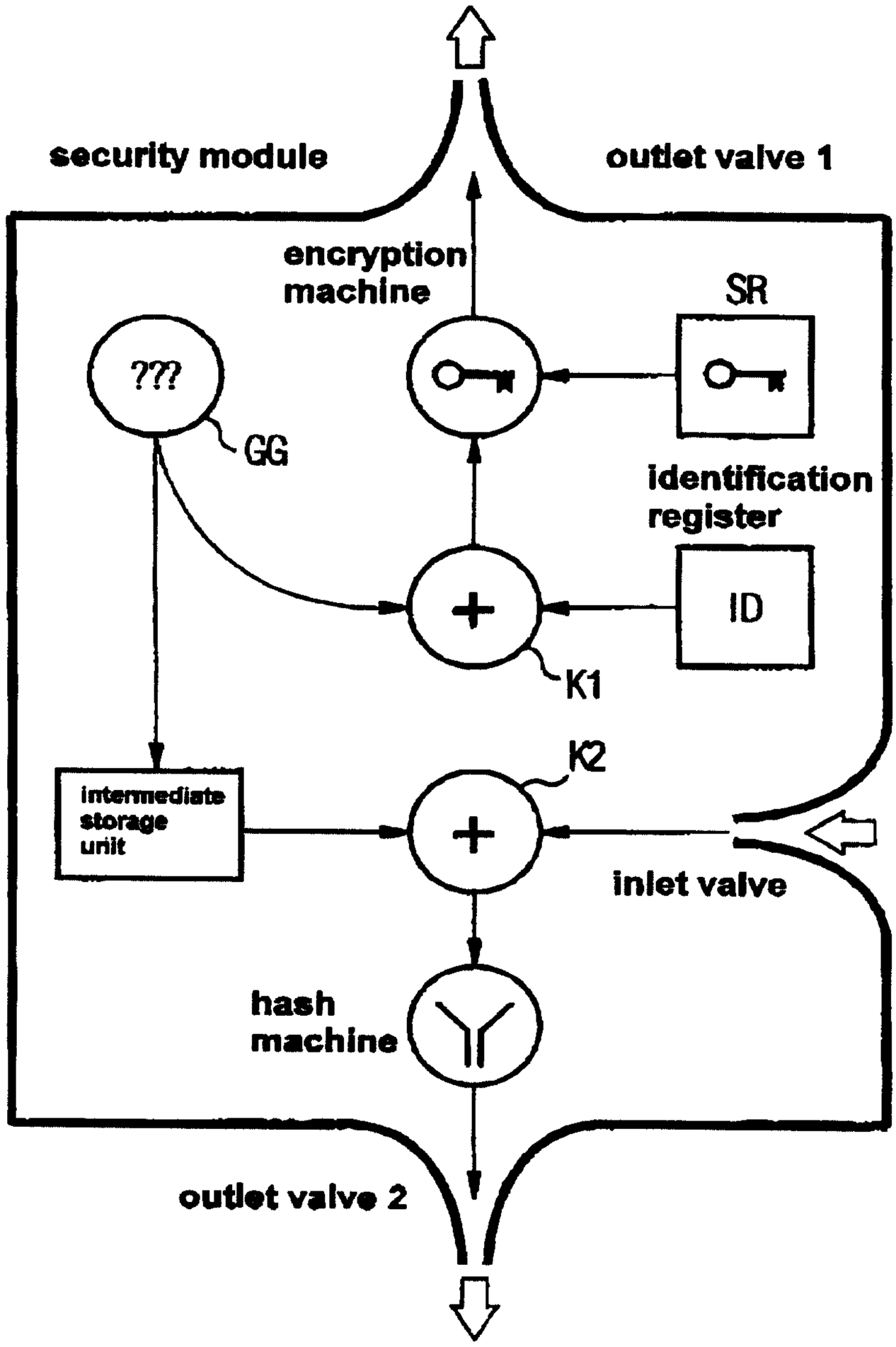
16. The method according to Claim 15, **characterized in that** the authentication unit links the data with another key.

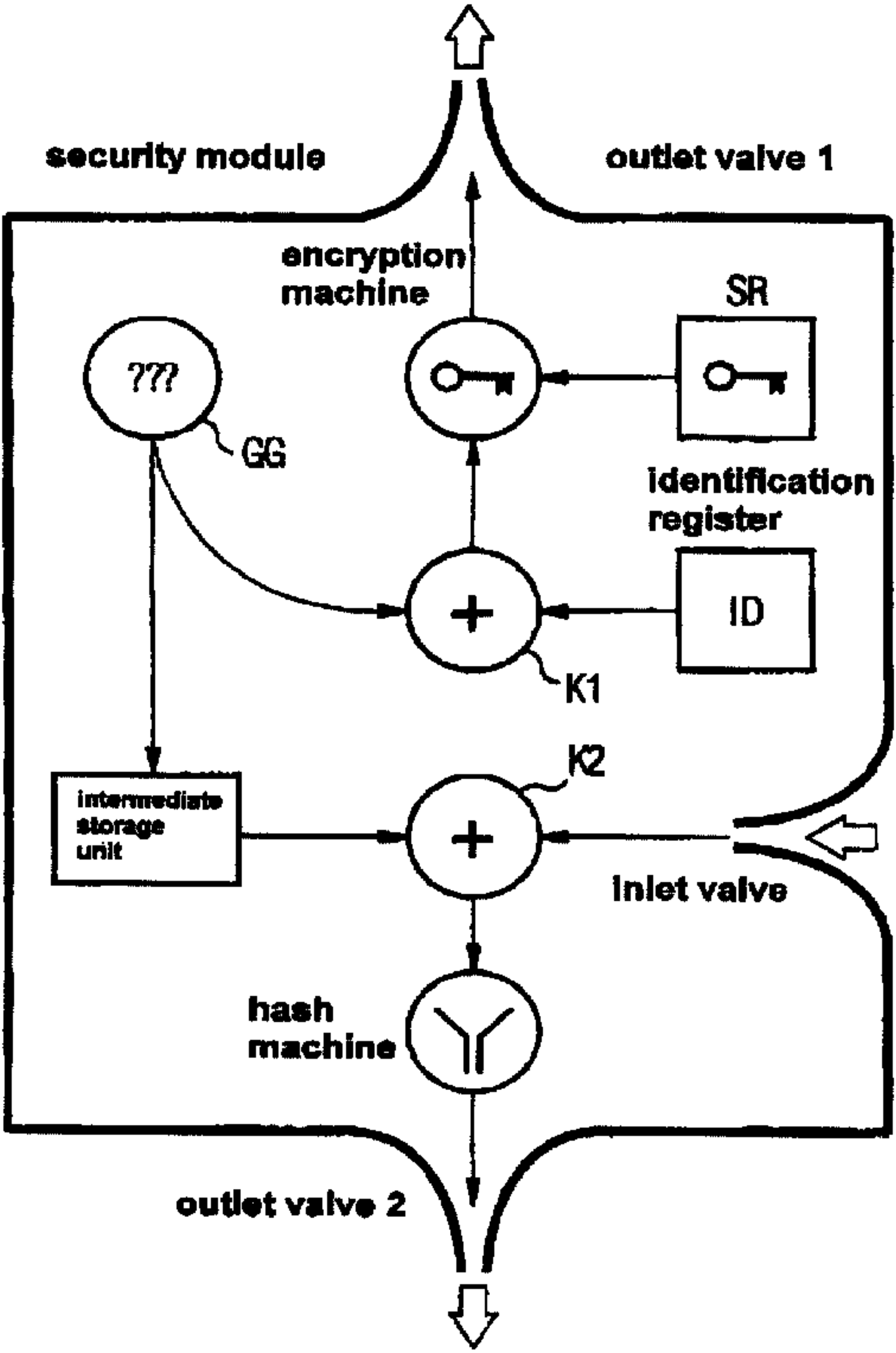
17. The method according to one of more of Claims 8 through 16, **characterized in that** the data that is output from the second data output port is output as forgery-proof information to the forgery-proof documents to be issued.

1/1

Security module and method for producing forgery-proof documents

Drawing 1




security module
outlet valve 1
encryption machine
SR
???
GG
identification register
ID
+
K1
K2
intermediate storage unit
+
inlet valve
hash machine
outlet valve 2