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

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2432593 C 2011/08/02

(11)(21) 2 432 593

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 2001/12/21
(87) Date publication PCT/PCT Publication Date: 2002/07/04
(45) Date de délivrance/Issue Date: 2011/08/02
(85) Entrée phase nationale/National Entry: 2003/06/20
(86) N° demande PCT/PCT Application No.: IB 2001/002712
(87) N° publication PCT/PCT Publication No.: 2002/052389
(30) Priorités/Priorities: 2000/12/22 (CH2000 2519/00); 2001/01/26 (CH2001 0137/01)

(51) Cl.Int./Int.Cl. *H04L 9/28* (2006.01), *G07F 7/10* (2006.01), *H04L 9/30* (2006.01), *H04L 9/32* (2006.01)

(72) Inventeur/Inventor:
JAQUIER, JEAN-LUC, CH

(73) Propriétaire/Owner:
NAGRAVISION S.A., CH

(74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : METHODE ANTI-CLONAGE
(54) Title: ANTI-CLONING METHOD

C-5	A
C-4	B
C-3	C
C-2	D
C-1	E
Cn	F

(57) Abrégé/Abstract:
The invention aims at providing a method for preventing the use of more than one identical security module for identifying and using resources managed by a management centre. Therefor, the invention provides an anti-cloning method based on storage of identification numbers of user units connected to said security module. When a connection is set up with a management centre, said numbers are transmitted and compared with the numbers of a previous transmission. Differences are allowed insofar as new numbers are added to the previously transmitted list. The security module is declared to be invalid if the previously stored numbers are not present in the transmitted numbers.

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
4 juillet 2002 (04.07.2002)

PCT

(10) Numéro de publication internationale
WO 02/052389 A2

(51) Classification internationale des brevets[7] : G06F 1/00

(21) Numéro de la demande internationale :
PCT/IB01/02712

(22) Date de dépôt international :
21 décembre 2001 (21.12.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :

2000 2519/00	22 décembre 2000 (22.12.2000)	CH
2001 0137/01	26 janvier 2001 (26.01.2001)	CH

(71) Déposant *(pour tous les États désignés sauf US)* : **NAGRAVISION SA** [CH/CH]; Route de Genève 22, CH-1033 Cheseaux-sur-Lausanne (CH).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **JAQUIER, Jean-Luc** [CH/CH]; Route de Corsy 35, CH-1093 La Conversion (CH).

(74) Mandataire : **LEMAN CONSULTING SA**; Route de Clémenty 62, CH-1260 Nyon (CH).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) **Title:** ANTI-CLONING METHOD

(54) **Titre :** METHODE ANTI-CLONAGE

C-5	A
C-4	B
C-3	C
C-2	D
C-1	E
Cn	F

(57) **Abstract:** The invention aims at providing a method for preventing the use of more than one identical security module for identifying and using resources managed by a management centre. Therefor, the invention provides an anti-cloning method based on storage of identification numbers of user units connected to said security module. When a connection is set up with a management centre, said numbers are transmitted and compared with the numbers of a previous transmission. Differences are allowed insofar as new numbers are added to the previously transmitted list. The security module is declared to be invalid if the previously stored numbers are not present in the transmitted numbers.

(57) **Abrégé :** Le but de la présente invention est de proposer une méthode qui permette d'empêcher l'utilisation de plus d'un module de sécurité identique pour l'identification et l'utilisation des ressources gérées par un centre de gestion. Ce but est atteint par une méthode anti-clonage basée sur la mémorisation des numéros d'identification des unités utilisateurs connectées avec ledit module de sécurité.Lors d'une connexion avec un centre de gestion, ces numéros sont transmis et comparés avec les numéros d'une précédente transmission. Des différences sont acceptées pour autant que de nouveaux numéros s'ajoute à la liste précédemment transmise. Le module de sécurité est déclaré invalide si les numéros précédemment mémorisés ne se retrouvent pas dans les numéros transmis.

WO 02/052389 A2

ANTI-CLONING METHOD

FIELD OF THE INVENTION

The present invention concerns a method for detecting a duplication of a security module, particularly during the interaction of this security module with several user units.

BACKGROUND

User units are connected to one or several networks offering products or services for sale. These products or services are subject to a conditional use, or control. For this reason, these units have a security module in charge of the identification and management of the access authorization to said networks.

These user units may take several forms, for example a pay-television decoder, a computer, a mobile phone, a palmtop, a PDA, a radio, a television, a multimedia station, or an automatic teller machine.

This security module is generally in the form of a smart card, a credit card or a SIM card, usually including a cryptographic processor. This card supplies the necessary information for identifying itself on a network by means of decryption operations using keys stored in the memory of the cryptographic processor, which is reputed be inviolable.

This security module can be in charge of exchanging confidential information with the user unit, for example when producing the key that starts the cryptographic operations associated to the identification or the payment of a product.

These security modules can be connected to several user units according to the user's needs. Such a use is allowed by the administrator of the network, and this is why the security module is generally moveable. This situation is found in the field of pay television or that of mobile phones.

Due to the value that this security module represents, particularly in electronic purse applications, the temptation is great for pirates to clone these modules.

Although the operating center is able to detect the simultaneous use of two modules having the same serial number, if this use is done at different moments it is not possible for the operating center to determine if the use is by the same module or by a clone.

A first solution is described in U.S. Pat. No. 4,672,533 and proposes to create session number that must change with each connection with the operating center. It is a previous identification to all transactions and although it answers the need to detect copies of the cards it can only function in an environment in which the on-line connection with the operating center is obligatory.

SUMMARY OF THE INVENTION

The objective of the present invention is to propose a method that allows preventing the use of more than one identical security module for the identification and use of resources administered by at least one operating center.

This objective is achieved by an anti-cloning control method for a security module comprising at least one unique identification number destined to be connected to a user unit comprising at least one unique identification number, the user unit being connectable to an operating center, the method comprising the steps of:

collecting by the security module the unique identification number of each user unit to which said module is connected,

transmitting, upon request by the operating center, the unique identification number of the security module and the unique identification numbers specific to the user units previously connected to this security module,

comparing by the operating center these user unit identification numbers with a list previously memorized during the last connection with said center,

authorizing said security module if the list transmitted by the user unit in the transmitting step corresponds with the list previously memorized, if not authorizing this security module provided that the unknown user unit identification numbers follow the list previously memorized.

In this way the control of validity of the security module is not only based on the static data but also integrates a variable data that retraces the different user units that are used.

Thanks to this method a security module copied integrally differs from the original from its first use with a user unit.

BRIEF DESCRIPTION OF THE DRAWINGS

A more thorough understanding of the many features and advantages of the present invention will be obtained with reference to the following detailed description and accompanying drawings in which:

FIG. 1 is a schematic diagram of a memory zone of a valid security module at a first point in time according to an embodiment of the invention.

FIG. 2 is a schematic diagram of the memory zone of FIG. 1 in a valid security module at a second point in time.

FIG. 3 is a schematic diagram of the memory zone of FIG. 1 in a pirated security module at a third point in time.

DETAILED DESCRIPTION

Let us take for example a security module A that contains unique numbers i, j, k. During this first use, the memory zone of the security module will store the unique number 1 of the user unit Ul. The original security unit will then contain the image i, j, k, l. A clone of this security module A (made before the first use described above) connected to a unit Up will contain the image i, j, k, p.

The first security module that will be connected to the operating center by the user unit will transmit its information, for example i, j, k, l. If the clone module is equally connected, the image of the units connected to this module will necessarily contain i, j, k, l. In our case the member I is absent and indicates that this module is not the one previously connected. The clone is thus detected.

According to the chosen control protocol, the operating center, in case it detects such a module, can declare this security module invalid, blocking the use of the true module for the same occasion.

According to an embodiment of the invention, it is sufficient to memorize two unique numbers to obtain the desired objective, that is, the number of the current user unit and the number of the previous user unit. When the security module is moved to another user unit the current number becomes the previous number, the user unit number becoming the new current number.

Thanks to this method a security module can immediately become operational with a user unit without demanding an authorization by an operating center. A link with the operating center can be carried out every n transactions, according to the duration of use, randomly, or on request of the operating center. If the memory of the security module is full, a demand can be made that a connection be carried out with the operating center before liberating space in the memory.

This invention can thus cover the case where a user unit would function without a link with an operating center. This can be the case of pay terminals limited to small amounts or of access to services such as pay television or the reception of digital radio (DAB) for example. In this case the speed of availability is an asset to convince the user of using this type of services and it is acceptable to carry out only sporadic controls. When the user connects a ticket distributor which has a on-line communication with the center, the verification is done at that moment.

This configuration will be advantageously described by FIGS. 1 to 3 that represent the memory zone of a security module.

Let us take for example FIG. 1, of a module N comprising two zones, one for the number of the current user unit Cn, the other for the previous terminal number C- 1 .

In the module N is the user unit number C in the previous zone C- 1 and the user unit number D in the current zone Cn.

Let us take for example a connection of this security module to a first user unit E and then a second unit F. The memory of the module will contain the identification numbers such as illustrated by FIG. 2. The current zone Cn contains the user identification F.

During a connection with an operating center these numbers A to F are transmitted and memorized in the center for control. The previous memorized image contained the identification numbers A to D and there is then the identity between the memorized image and a part of the transmitted numbers.

It should be noted that according to the invention it is not necessary to connect with the operating center with each new connection with the user unit. The control can be carried out sporadically, randomly, or upon demand of the operating center.

A module that has been cloned in the state of FIG. 1 or with the numbers A to D and that has been connected to a user unit K presents a memory zone such as illustrated in FIG. 3.

When this information A to D, K is transmitted to the operating center the member K is unknown and does not follow the previous image which is the user identification F. The operating center can then deduct that there are two security modules with the same single number.

According to a simplified embodiment of the invention, it is not necessary to keep the user identification numbers after a positive control. Only the last numbers are kept as a trace of the previous connections with the user units. By "last" we mean, for example, the last two or three.

From this fact it will be enough that in the subsequently transmitted numbers we find these last numbers to follow the trace of this module.

According to our previous example, once the module of FIG. 1 is accepted by the operating center, the numbers A, B are erased from the memory zone of the module, leaving only C, D.

This module is then connected to a unit E and then a unit F. These data C, D, E, F are transmitted to the operating center for verification. The values C, D being present in the data previously memorized, the module is considered as valid and the user identifications E, F are erased.

In the case of FIG. 3 the cloned module is connected to the unit K that will transmit these data A, B, C, D, K to the operating center. The latter looks for the presence of E, F according to the last connection, and from the fact that these user identifications are not present in the transmitted data, the center can detect the presence of a falsified security module.

According to one embodiment, the data exchanged between the security module and the user unit are encrypted by a pairing key, that is, a key specific to the couple security module/user unit. This key can be of several types, a secret symmetrical key or an asymmetrical key (public key, private key). Following the nature of the key it is possible to use this key as a single user identification such as described above to identify the user unit. In this case it is not the user unit in time as such that is identified but the pair formed by the security module and the user unit.

It is then possible to transmit all or part of this pairing key as a user identification. In fact for the identification operations it is possible to use a part of this key, particularly if we wish that this key is not divulged. According to a particular embodiment it is a key pair public key/private key that is used as a pairing key (asymmetrical keys) and it is the public key that is used as a user identification.

What is claimed is:

1. A method for preventing authorization of a cloned security module comprising the steps of: receiving at an operating center a request for authorization from a security module, the request including an identification number of the security module; receiving at the operating center a first list from the security module, the first list including at least one unique identification number corresponding to at least one user unit to which the security module has been previously connected; comparing at the operating center the first list to a second list including at least one unique identification number corresponding to at least one user unit, the second list having been reported by a security module with an identical identification number; and denying the request if any unique identification number on the second list is not on the first list.

2. The method of claim 1, further comprising the step of: preventing further use of any security module having an identification number the same as the identification number included in the request for authorization.

3. The method of claim 1, wherein the first list contains only the user unit to which the security module has most recently been connected.

4. The method of claim 1, wherein the identification number of the security module is formed by all or part of a pairing key used to encrypt data exchanged between the security module and the user unit.

5. The method of claim 4, wherein the pairing key is asymmetric and the identification number of the security module is formed by the public key.

6. A security module adapted to facilitate the detection of a clone, the security module comprising: a memory, the memory having stored therein at least one identification number of the security module; a processor, the processor being configured to perform the steps of: sending a request for authorization to an operating center, the request including the identification number of the security module; sending a list to the operating center, the list including at least one identification number of a user unit to which the security module has previously been connected; and storing an identification number of a user unit to which the security module is currently

connected in the memory, whereby the list sent by the security module is suitable for comparison against a previously reported list of identification numbers of user units to detest the existence of a closed security module.

7. The security module of claim 6, wherein the processor is further configured to perform the step of deleting any stored identification numbers of user units other than a user unit to which the security module is currently connected if the authorization is received.

8. A system comprising: a user unit; a security module connected to the user unit; and an operating center; wherein the security module is configured to perform the steps of: sending a request for authorization to an operating center, the request including the identification number of the security module, sending a list to the operating center, the list including at least one identification number of a user unit to which the security module has previously been connected; receiving the request and the list from the security module; and comparing the list received from the security module to a second list, the second list having been previously received by the operating center from a security module with an identification number identified to the identification number in the request, and denying the request if any unique identification number on the second list is not on the first list.

9. The system of claim 8, wherein the security module is a smart card.

10. The system of claim 8, wherein the security module is a SIM card.

C-3	A
C-2	B
C-1	C
Cn	D

Fig. 1

C-5	A
C-4	B
C-3	C
C-2	D
C-1	E
Cn	F

Fig. 2

C-4	A
C-3	B
C-2	C
C-1	D
Cn	K

Fig. 3

C-5	A
C-4	B
C-3	C
C-2	D
C-1	E
Cn	F