Europäisches Patentamt
European Patent Office
Office européen des brevets

Bescheinigung

Die Übereinstimmung der angehefteten Druckschrift mit der gemäß Artikel 98 EPÜ veröffentlichten europäischen Patentschrift wird hiermit beglaubigt.

Certificate

The conformity of the attached publication with the specification of the European patent published under Article 98 EPC is hereby certified.

Attestation

La publication accompagnant cette attestation est certifiée conforme au fascicule du brevet européen publié conformément à l'article 98 CBE.

Europäisches Patent Nr.

European Patent No.

Brevet européen n°

1177687

München, den
Munich,
Munich, le
14.10.09

Die Präsidentin des Europäischen Patentamts:
im Auftrag

For the President of the European Patent Office

La Présidente de l'Office européen des Brevets
p.o.

Eva Pachta
Eva Pachta

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 1 177 687 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
12.08.2009 Bulletin 2009/33

(21) Application number: **00912860.4**

(22) Date of filing: **31.03.2000**

(51) Int Cl.:
H04N 5/913 $^{(2006.01)}$ *H04L 29/06* $^{(2006.01)}$
H04L 9/08 $^{(2006.01)}$ *H04N 7/16* $^{(2006.01)}$

(86) International application number:
PCT/IB2000/000432

(87) International publication number:
WO 2000/062540 (19.10.2000 Gazette 2000/42)

(54) **METHOD OF FOR PROVIDING SECURE COMMUNICATION OF DIGITAL DATA BETWEEN DEVICES**

VERFAHREN ZUR SICHEREN ÜBERTRAGUNG DIGITALER DATEN ZWISCHEN VORRICHTUNGEN

MÉTHODE DE SECURISATION DES ECHANGES DE DONNEES NUMERIQUES ENTRE DISPOSITIFS

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **13.04.1999 EP 99400901**

(43) Date of publication of application:
06.02.2002 Bulletin 2002/06

(73) Proprietor: **Nagra Thomson Licensing**
92100 Boulogne-Billancourt (FR)

(72) Inventors:
- **MAILLARD, Michel**
  F-78120 Rambouillet (FR)
- **DAUVOIS, Jean-Luc**
  F-75116 Paris (FR)
- **DUBLANCHET, Frédéric**
  75906 Paris Cedex 15 (FR)
- **LEPORINI, David**
  75906 Paris Cedex 15 (FR)

(74) Representative: **Wenger, Joel-Théophile et al**
Leman Consulting S.A.
Chemin de Précossy 31
1260 Nyon (CH)

(56) References cited:

EP-A- 0 714 204	**EP-A- 0 814 474**
EP-A- 0 858 184	**WO-A1-97/24832**
WO-A1-98/56179	**WO-A1-99/07150**

- **MOLVA R.; ETIQUE P.-A.; HUBAUX J.-P.: 'Strong authentication in intelligent networks' UNIVERSAL PERSONAL COMMUNICATIONS, 1994. RECORD., 1994 THIRD ANNUAL INTERNATIONAL CONFERENCE, SAN DIEGO, CA, USA 27 September 1994, NEW YORK, NY, USA,IEEE, pages 629 - 634, XP010131591**

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The present invention relates to a method of and apparatus for providing secure communication of digital data between devices. More specifically, the present invention relates to preventing illegal copying and redistribution of digitally recorded data.

[0002] The introduction of digital technology in the audiovisual field has brought considerable advantages to the consumer in comparison with analog technologies, notably in relation to the quality of reproduction of sound and image and the durability of the supporting medium. The compact disk has all but replaced traditional vinyl records and a similar trend is expected with the introduction of new digital products aimed at the multimedia and home entertainment markets generally, notably the DVD (digital video disk or digital versatile disk) players.

[0003] A particular problem associated with digitally recorded data lies in its ease of reproduction and the possibilities for piracy that arise therefrom. A single digital recording may be used to make any number of perfect copies without any degradation in quality of the sound or image. This problem is a serious one, particularly with the advent of recordable digital products such as the minidisk or DAT, and the reluctance of entertainment companies to license copyright works whilst this problem remains has acted as a break on the introduction into the market of new media products.

[0004] At present, the most practically available solution against unauthorised reproduction of copyright works has been a legal one, and a number of countries in Europe and elsewhere have introduced anti-piracy legislation to combat the increasing number of pirate films, CDs etc being brought onto the market. For obvious reasons, a legal solution is less than optimal from the point of view of preventative action.

[0005] Technological solutions proposed to date to prevent the unauthorised copying and distribution of digitally recorded data have been extremely basic, relying for example on the idea of using some form of digital " handshake " between devices in the digital audiovisual system, for example, between the digital data, or DVD, player and the digital recorder, and between the DVD player and the digital television, so as to verify the origin of the device receiving the data from the DVD player. Such protection is, however, effective against only the most low level of copying activity, since the handshake signal is typically not protected in any way and may be easily read and reproduced so as to convert, for example, an unauthorised recorder device into an apparently authorised recorder device.

[0006] The document WO98/56179 describes a method for managing access to a device by sending a first message to a second device; receiving a digital certificate encrypted using a first private key; receiving the first message encrypted using a second private key; authenticating the second device; and establishing a communication channel between the devices. According to a particular embodiment, this document describes a system for managing access between a service provider and a set-top box having a smart card coupled thereto, the set-top box sends a first message to the smart card; receives a smart card (first) digital certificate encrypted using a private key; authenticates the smart card; contacts the service provider and sends a second message to the service provider; receives a service provider (second) digital certificate encrypted using another private key; receives the second message encrypted using yet another private key; authenticates the service provider; provides confirmation to the service provider; and establishes a communication channel with the service provider. Particularly, the two messages contain at least set-top box identification data.

[0007] In the publication "Strong authentication in intelligent networks", Universal personal Communications, 1994 Third Annual International Conference, San Diego, CA, USA (September 27, 1994), the authors describe a way to provide a secure communication between two devices over an unsecured channel such as Internet. In this document, the solution proposed rely on an authority, also connected to the Internet carrying out the authentication of each device and as the result of a positive authentication, provide to each device a key allowing them to encrypt/decrypt the data exchanged between these devices.

[0008] The aim of the present invention is to overcome the disadvantages associated with the prior art techniques and to provide a technological solution against the unauthorised copying and reproduction of digitally recorded copyright works.

[0009] In a first aspect, the present invention provides a method of providing secure communication of digital data between devices, said method comprising the steps of communicating from one device an identifier of a device to an independent security module and performing device validation depending on the identity of the communicated identifier.

[0010] In such a method, a independent security module is used to validate a device in, for example, a digital audiovisual system. For example, in a system in which data is communicated from a DVD player to a digital recorder, the user of the system might possess an appropriate smartcard for validating the recorder and/or the player before any data is transferred. Thus, by using a security module to validate devices, an extra level of security can be added to the system.

[0011] Indeed, the use of an independent security module can lead to a highly personalized digital audiovisual system. For instance, the security module may enable data to be transferred from a DVD player to a digital television only if both the player and television are validated by the security module, thus enabling the digital data to be viewed only on the user's personal television.

[0012] The use of a security module to validate linked devices also provides an advantage in that device validation can become independent of the link between the devices. Thus, if the communication link is intercepted by a third party, the identifiers of the devices cannot be obtained as they are not passed between the devices but from the individual devices to a security module.

[0013] Such security modules can take any convenient form depending on the physical size and characteristics of the modules. For example, the security module may be detachable, for example removably insertable into a socket provided in the device or a separate module connected to the device. In some cases a smart card equivalent to a bank card may be used (as or as part of the security module), but other formats, such as PCMCIA type cards, are equally possible. Thus, the security module may be easily replaced in order to update the rights provided by the security module, for example to invalidate certain devices in the event of the system provider becoming aware of cloning of those devices.

[0014] The device identifier may take any convenient form. For example, the identifier may be a public key associated with the device.

[0015] The security module may perform device validation by comparing the communicated identifier with at least one stored identifier. The stored identifiers may be stored in a memory of the security module. The identifiers may be stored in the form of a list, the received identifier being compared with the identifiers in the list in order to validate the device. This can provide for fast and efficient validation of the device.

[0016] Each stored identifier may be associated with a respective one of a valid device or an invalid device. Upon receipt of the identifier, the security module may compare the received identifier with stored identifiers associated with invalid devices, and/or with stored identifiers associated with valid devices.

[0017] Thus, the security module may contain at least one of a "revocation list" for blacklisting non-compliant devices and an "authorization list" for restricting transfer of data to between pre-registered devices only. Device identifiers intentionally published by third parties, for example, on the Internet, can be added to the revocation list when periodically updating the security module in order to prevent data from being transferred to or from these devices. However, the use of an authorization list can also prevent device identifiers intentionally published on the Internet from working since these identifiers will not be valid anywhere except in, for example, a home network.

[0018] The authorization list is therefore likely to be much shorter than the revocation list, thus saving memory capacity, and is likely to require less-frequent updating. Thus, in a second aspect the present invention provides a method of providing secure communication of digital data between devices, said method comprising the steps of comparing an identifier communicated from one device with at least one stored identifier, each stored identifier being associated with a respective valid device, and validating the device if the communicated identifier is identical to the or one of the stored identifiers.

[0019] It is preferable that said at least one stored identifier is stored in an independent security module.

[0020] In a preferred embodiment of the invention, certificates are passed between the device and the security module to validate the device.

[0021] In a second aspect the present invention provides a method of providing secure communication of digital data between a device and a security module, said method comprising the steps of transferring to the security module a random number and an identifier of the device encrypted by a public key of the security module, the security module decrypting the random number and device identifier using a private key of the security module, validating the device using the device identifier and, upon validation of the device, using the random number to encrypt and decrypt data communicated between the security module and the device.

[0022] In order to enable the devices to function more effectively it is desired to provide a securised or encrypted communication link between the devices. The implementation of a secure link between the devices can be used to enable information needed to prepare or play a recording to be passed freely between the devices. Unfortunately, the independence of activities between a manufacturer of a DVD player and a manufacturer of recording equipment responsible for the recorder may lead to a number of problems regarding the provision of encryption keys for this purpose.

[0023] For example, a player manufacturer may not place sufficient confidence in the integrity of security at the manufacturing site of a recorder to entrust the manufacturer with, for example, a secret symmetric algorithm key needed by the recorder to decrypt communications encrypted using the equivalent key held by the DVD player.

[0024] Furthermore, the separation of activities may make it impractical to envisage a situation in which the recorder is sent to a broadcast system manager for personalisation with the appropriate keys. For this reason, it is necessary to envisage a solution which allows the greatest independence of operation for the player and recorder.

[0025] In order to solve such problems, in a preferred embodiment of the present invention, data is communicated between first and second devices, and upon validation of each device by the security module, the security module communicates to the first device a random key generated in the security module and encrypted using the random number generated by the first device, the first device decrypting the key using the random number generated thereby, and communicates to the second device the key encrypted using the random number generated by the second device, the second device decrypting the key using the random number generated thereby, the key thereafter being used to encrypt data communicated to the security module by the devices and data communicated between the devices.

[0026] Accordingly, in preferred embodiment of the present invention, the method of providing secure communication of digital data between devices comprises the step of providing a security module, generating a random key (SK) in the security module and encrypting data communicated between the devices using the random key.

[0027] By this method, the generation of an encryption key for securing communication between the devices is performed by a security module in communication with the devices, and so key generation is performed independently of the devices.

[0028] Such a method can provide a secure, flexible and upgradeable device interface-independent system for providing secure communication of digital data between devices. The system can be based on a smartcard for generating the session key, and therefore can be cheap and enable fast action against piracy by the ease of providing updated smartcards, particularly as the responsibility of updating security can be the responsibility of a dedicated smartcard provider and not the device manufacturers.

[0029] In a third aspect the present invention provides apparatus for providing secure communication of digital data between devices, said apparatus comprising a security module receiving an identifier of a device and performing device validation depending on the identity of the received identifier.

[0030] In a fourth aspect the present invention provides apparatus for providing secure communication of digital data between devices, said apparatus storing at least one identifier, each stored identifier being associated with a respective valid device, comparing an identifier of a device with said at least one stored identifier, and validating the device if the identifier of the device is identical to the or one of the stored identifiers.

[0031] In a fifth aspect the present invention provides a system for providing secure communication of data between a device and a security module, said device communicating to the security module a random number and an identifier of the device encrypted by a public key of the security module, the security module decrypting the random number and device identifier using a private key of the security module, validating the device using the device identifier, and using the random number to encrypt and decrypt data communicated between the security module and the device. Whilst the invention has been described with reference to a first and second device, it will be appreciated that the same principle may be used to set up a chain of communication between a series of such devices.

[0032] Suitable algorithms for use in this invention for generating private/public keys may include RSA, Fiat-Shamir, or Diffie-Hellman, and suitable symmetric key algorithms may include DES type algorithms, for example. However, unless obligatory in view of the context or unless otherwise specified, no general distinction is made between keys associated with symmetric algorithms and those associated with public/private algorithms.

[0033] The terms "scrambled" and "encrypted", and "control word" and "key" have been used at various parts in the text for the purpose of clarity of language. However, it will be understood that no fundamental distinction is to be made between "scrambled data" and "encrypted data" or between a "control word" and a "key".

[0034] Additionally, the terms "encrypted" and "signed", and "decrypted" and "verified" have been used at various parts in the text for the purpose of clarity of language. However, it will be understood that no fundamental distinction is to be made between "encrypted data" and "signed data", and "decrypted data" and "verified data".

[0035] Similarly, the term "equivalent key" is used to refer to a key adapted to decrypt data encrypted by a first mentioned key, or vice versa.

[0036] Features described above relating to method aspects of the present invention can also be applied to apparatus aspects, and vice versa.

[0037] Preferred features of the present invention will now be described, by way of example only, together with example embodiments which are useful for understanding the invention, with reference to the accompanying drawings, in which:

Figure 1 shows the elements of a digital audiovisual system;

Figure 2 shows the distribution of certificates in a digital audiovisual system;

Figure 3 shows the connection of a security module to a device;

Figure 4 shows the connection of a security module to two devices;

Figure 5 shows the steps associated with the validation of a device by the security module and subsequently providing secure communication between the device and the security module;

Figure 6 shows the steps associated with the generation of a secure channel of communication between a device and a security module;

Figure 7 illustrates the descrambling of data received by a device;

Figure 8 shows the steps associated with the provision of secure communication between two devices;

Figure 9 shows the transfer of data between two devices over a secure communication link;

Figure 10 shows the steps associated with the setting up of a secure communication link between a

DVD player and a digital television and the subsequent operations carried out to descramble data received from the DVD player by the digital television; and

Figure 11 shows the steps associated with the setting up of a secure communication link between a DVD player and a digital recorder and the subsequent operations carried out to descramble data received from the DVD player by the digital recorder.

[0038] Referring to Figure 1, elements of a digital audiovisual system 10 for recordal and replaying of digital data will first be described. Whilst the invention will be discussed in relation to the playing of audiovisual data on a DVD player, it may also conveniently be applied, for example, to the playing of exclusive audio information subsequently recorded on a DAT or minidisc recorder or even to the communication of software recorded on the hard disc of a computer.

[0039] Typically the audiovisual system comprises a DVD player 12 for the playback of digital audiovisual data stored, for example, on disk or tape. The DVD player is linked to a digital display 14 for the display of the data played by the DVD player 12. The display 14 is preferably provided in the form of a digital television. The communication link 16 between the player 12 and display 14 may take many forms, for example, a radio, telephone or infra-red link. However, preferably, the communication link is implemented by connection of the player and television on a bus, for example, a IEEE 1394 bus link.

[0040] The system additionally includes a digital recorder 18, such as a DVHS or DVD recorder, adapted to communicate with the DVD player 12, for example, via an IEEE 1394 bus 20. The recorder 18 receives a digital recording support (not shown) on which information is recorded. The recorder 18 includes a direct link 22 to the display 14. However, digital audiovisual data may be passed from the player 12 to the recorder 18 prior to display.

[0041] Whilst the elements of player 12, display 14 and recorder 18 have been indicated separately, it is conceivable that some or all of these elements may be merged, for example, to provide a combined player/television set.

[0042] In order to provide secure communication of data between devices in the digital audiovisual system, for example, to prevent the unauthorised copying and distribution of digitally recorded data, a validation system is used to validate one or more of the devices in the audiovisual system prior to any communication of data between the devices.

[0043] A preferred device validation system is based on the transfer of certificates between a device and a security module. With reference to Figure 2, each device and security module is assigned a unique certificate for validation purposes.

[0044] In a first stage of a certificate distribution system a certification authority (CA) 50 delivers encrypted certificates to both consumer electronics (CE) manufacturers 52 and security providers (SP) 54.

[0045] The CA 50 communicates to each CE manufacturer 52 a respective encrypted certificate Cert$_{CA}$(CEman_Kpub) shown at 56. This certificate contains, inter alia, a manufacturer public key CEman_Kpub and is encrypted by a system, or CA, private key CA_Kpri. To enable the contents of the certificate to be decrypted by the CE manufacturer 52, the CA 50 communicates to the CE manufacturer 52 the CA public key CA_Kpub. It should be mentioned that the private key CA_Kpri is unique to and held exclusively by the CA 50.

[0046] In a similar manner, the CA 50 communicates to each security provider 54 a respective encrypted certificate Cert$_{CA}$(SP_Kpub) shown at 58. This certificate contains, inter alia, a security provider public key SP_Kpub and is encrypted by the CA private key CA_Kpri. To enable the contents of the certificate to be decrypted by the security provider 54, the CA 50 communicates to the security provider 54 the CA public key CA_Kpub.

[0047] In a second stage of the certificate distribution system, each consumer electronics (CE) manufacturer 52 and security provider (SP) 54 assigns respective certificates to its own products.

[0048] Each CE manufacturer 52 assigns to each of its CE devices 60 a respective encrypted certificate Cert$_{CEman}$(Device_Kpub) shown at 62. This certificate contains, inter alia, a unique device public key Device_Kpub, together with an indication of the device capability (recorder, player, etc.). The certificate is encrypted by an equivalent key to the public key CEman_Kpub. To enable the contents of the certificate to be decrypted, the CE manufacturer 52 stores in the CE device the CA public key CA_Kpub and the encrypted certificate Cert$_{CA}$(CEman_Kpub) of the CE manufacturer 52. Thus, the public key Device_Kpub of the CE device 60 can serve as an identifier of the device.

[0049] Similarly, each security provider 54 assigns to each security module 64 a respective encrypted certificate Cert$_{SP}$(SM_Kpub) shown at 66. Such security modules 66 can take any convenient form depending on the physical size and characteristics of the modules. For example, the security module may be removably insertable into a socket provided in a CE device 60 or may be a separate module connected to the device 60. In some cases a smart card equivalent to a bank card may be used, but other formats such as PCMCIA type cards are equally possible.

[0050] The encrypted certificate assigned to the security module 64 contains, inter alia, a unique security module public key SM_Kpub. The certificate is encrypted by an equivalent key to the public key SP_Kpub. To enable the contents of the certificate to be decrypted, the security provider 54 stores in the security module 64 the CA public key CA_Kpub and the encrypted certificate Cert$_{CA}$(SP_Kpub) of the security provider. Thus, the public key SM_Kpub of the security module 64 can serve as an identifier of the security module.

[0051] A signature may be included in any of the above certificates to enable the contents of the certificate to be verified following decryption of the certificate. The contents of the certificate may be signed using the key used to encrypt the certificate.

[0052] Validation of a device in the digital audiovisual system is carried out by the exchange of certificates between the device and a security module. As shown in Figure 3, in a first embodiment the security module 64 is connected to the device 60 via a communication link 70 to enable the security module to validate that device only. However, as shown in Figure 4, the security module may alternatively be connected to two or more connected devices 60a, 60b via respective communication links 70a, 70b.

[0053] Validation of a single device by a security module will now be described with reference to Figure 5.

[0054] The validation procedure can be initiated at any time, for example, upon switching the device on, disc insertion, zapping of the device by the user, establishment of connection with the security module etc.

[0055] The validation procedure is initiated by the security module. As shown at 100, the security module 64 communicates to the device 60 the encrypted certificate Cert$_{\text{CA}}$(SP_Kpub) of the security provider 54. At 102, the device decrypts the contents of the encrypted certificate Cert$_{\text{CA}}$(SP_Kpub) using the public key CA_Kpub of the CA 50 to enable the public key SP_Kpub of the security provider 54 to be extracted from the certificate.

[0056] Following communication of the encrypted certificate Cert$_{\text{CA}}$(SP_Kpub) to the device 60, at 104 the security module 64 communicates its own unique encrypted certificate Cert$_{\text{SP}}$(SM_Kpub) to the device 60. At 106 the device decrypts the contents of the encrypted certificate Cert$_{\text{SP}}$(SM_Kpub) using the public key SP_Kpub of the security provider previously extracted by the device 60 from the encrypted certificate Cert$_{\text{CA}}$(SP_Kpub) in order to enable the public key SM_Kpub of the security module 64 to be extracted from the certificate.

[0057] At 108, the device 60 communicates to the security module 64 the encrypted certificate Cert$_{\text{CA}}$ (CEman_Kpub) of the CE manufacturer 52. At 110, the security module 64 decrypts the encrypted certificate Cert$_{\text{CA}}$(CEman_Kpub) using the public key CA_Kpub of the CA 50 to enable the public key CEman_Kpub of the CE manufacturer 52 to be extracted from the certificate.

[0058] Following communication of the encrypted certificate Cert$_{\text{CA}}$(CEman_Kpub) to the security module 64, at 112 the device 60 generates a random number X. The random number X performs no function in the validation of the device by the security module. Instead, the random number X is used to generate a secure authenticated channel (SAC) between the device 60 and the security module 64. This is described in more detail below.

[0059] At 114 the device 60 performs bit shuffling of random number X and the encrypted certificate Cert$_{\text{CEman}}$(Device_Kpub) stored in the device 60 in order to scramble the random number X and encrypted certificate Cert$_{\text{CEman}}$(Device_Kpub). The bit shuffled random number X and encrypted certificate Cert$_{\text{CEman}}$ (Device_Kpub) are subsequently encrypted at 116 using the public key SM_Kpub of the security module 64 previously communicated to the device 60 by the security module at step 104, and communicates the encrypted bit shuffled random number and encrypted certificate Cert$_{\text{CEman}}$(Device_Kpub) to the security module 64 at step 118.

[0060] At 120, the security module 64 decrypts the encrypted bit shuffled random number and encrypted certificate Cert$_{\text{CEman}}$(Device_Kpub) using an equivalent key SM_Kpriv to the public key SM_Kpub. The bit shuffling of the shuffled random number and encrypted certificate Cert$_{\text{CEman}}$(Device_Kpub) is reversed at step 122.

[0061] An algorithm used to bit shuffle the random number X and encrypted certificate Cert$_{\text{CEman}}$(Device_Kpub) may be stored in the security module 64 to enable the bit shuffling to be reversed. Alternatively, the security module 64 may send to the device 60 a random number, referred to as a random challenge, Z, following receipt of the encrypted certificate Cert$_{\text{CA}}$(CEman_Kpub). The random challenge Z is bit shuffled by the device 60, encrypted using the security module public key SM_Kpub and transmitted to the security module, preferably at the same time as the bit shuffled random number X and encrypted certificate Cert$_{\text{CEman}}$(Device_Kpub). The security module 64 decrypts the encrypted shuffled random challenge Z and compares the bit shuffled random challenge with the unshuffled random challenge stored therein in order to determine how the random challenge Z has been shuffled by the device 60. The security module 64 uses the result of this challenge to reverse the bit shuffling applied to the random number X and encrypted certificate Cert$_{\text{CA}}$(CEman_Kpub) by the device.

[0062] Returning to Figure 5, the random number is extracted and stored by the security module 64 at step 124. At 126, the security module 64 decrypts the encrypted certificate Cert$_{\text{CEman}}$(Device_Kpub) using the public key CEman_Kpub of the CE manufacturer 52 previously transmitted to the security module 64 by the device 60 in order to enable the public key Device_Kpub of the device 60 to be extracted from the certificate.

[0063] Validation of the device 60 is carried out by the security module 64 using the public key Device_Kpub of the device 60 at step 128. The security module compares the received device public key Device_Kpub with a list of device public keys previously stored in the security module. The list of device public keys may be generated by the CA 50 and stored, for example, in memory, such as non-volatile memory, in the security module 64 by the security provider 54.

[0064] The security module 64 supports two types of list. A "revocation list" contains device public keys associated with invalid devices and is used to blacklist non-compliant devices. An "authorization list" contains device public keys associated with valid devices and is used to restrict transfer of data to between pre-registered devices only.

[0065] Device identifiers intentionally published by third parties, for example, on the Internet, can be added to the revocation list by the CA 50 when periodically updating the security module 64 in order to prevent data from being transferred to or from these devices or clones of these devices. However, the use of an authorization list can also prevent device identifiers intentionally published on the Internet from working since these identifiers will not be valid anywhere except in, for example, a home network.

[0066] A flag embedded within the encrypted device certificate or the encrypted security module certificate determines the list with which the received device public key is compared. For example, the security module may compare the received device public key with stored public keys associated with invalid devices when the flag has a setting "0", and compare the received device public key with both stored public keys associated with invalid devices and stored public keys associated with valid devices when the flag has a setting "1".

[0067] If the device 60 is determined to be an invalid device, the security module 64 terminates communication with the device 60. If, as shown in Figure 4, the security module is in communication with other devices, communication with those devices is also terminated.

[0068] If the device is determined to be a valid device, the security module 64 generates a secure authenticated channel (SAC) of communication between the device 60 and the security module 64. Figure 6 shows the steps associated with the generation of a secure authenticated channel of communication between a device and a security module.

[0069] In step 200 the security module 64 generates a random session key SK. The random session key SK is TDES encrypted at step 202 by the security module 64 using the random number X transmitted to the security module 64 by the device 60. The encrypted session key $TDES_X(SK)$ is transmitted to the device 60 at step 204.

[0070] At step 206, the device 60 decrypts the encrypted session key $TDES_X(SK)$ using the random number X and stores the session key SK in memory at step 208. The session key SK is thereafter used to encrypt data transferred between the device 60 and the security module 64.

[0071] Thus, following validation of the device, key distribution is undertaken by the security module in order to create a secure channel of communication between the device and the security module. Updating of the session key (SK) can also be initiated at any time, for example, upon switching the device on, disc insertion, zapping of the device by the user, establishment of connection with the security module etc.

[0072] With reference to Figure 1, the DVD player 12 typically transmits scrambled data to the display 14 and recorder 18. The steps associated with the descrambling of data received by a device will now be described with reference to Figure 7,

[0073] A DVD disk typically stores encrypted Entitlement Control Messages (ECMs) together with the scrambled audio and/or visual data. An ECM is a message related to the scrambled audio and/or visual data. The message contains a control word (which allows for the descrambling of the data) and the access criteria of the data. The access criteria and control word are transmitted by the DVD player 12 to, for example, display 14 via the communication link 16.

[0074] The data stored on the disk typically comprises a number of distinct components; for example a television programme includes a video component, an audio component, a sub-title component and so on. Each of these components is individually scrambled and encrypted. In respect of each scrambled component of the data, a separate ECM is required. Alternatively, a single ECM may be required for all of the scrambled components of a service The control word typically changes every few seconds, and so ECMs are also periodically inserted in the data to enable the changing control word to be descrambled. For redundancy purposes, each ECM typically includes two control words; the present control word and the next control word.

[0075] Upon receipt of scrambled data and an encrypted ECM from the DVD player 12, the display 14 extracts the ECM from the scrambled data and passes the extracted ECM to descrambling circuitry for decrypting the ECM and extracting the control word from the decrypted ECM.

[0076] The descrambling circuitry may be implemented in a detachable conditional access module 40 or CAM, commonly embodied in the form of a PCMCIA, or PC, card insertable in a socket in the recipient device. Alternatively, the CAM 40 may be physically separate from the recipient device, the CAM 40 and display 14 being communicably linked by any suitable communication link 42, for example via a serial or parallel interface.

[0077] The CAM 40 may itself further include a slot to receive a smart card. In such systems, the smartcard controls whether the end user has the right to decrypt the ECM and to access the programme. If the end user does have the rights, the ECM is decrypted by a processor 41 within the smart card and the control word extracted. The processor 41 of the CAM 40 may then descramble the scrambled data to supply the recipient device with a clear data stream for, for example, decompression and subsequent display. Alternatively, the descrambling of the data may be carried out within the display 14 using the control word information communicated to the display 14 from the CAM 40.

[0078] In the case where scrambled data is communicated from the DVD player 12 to the digital recorder 18 for subsequent viewing, the manufacturer of the DVD disk may wish to restrict access to the recorded data. For example, the disk manufacturer may wish to prohibit any further copying of the recorded data. In such situations, the access rights, or eXtended Control Management Information (XCMI), are contained is an eXtended Entitlement Control Message (XECM) which includes any access rights as determined by the disk manufacturer. Upon receipt of the XECM, the processor 41 of the CAM 40 decrypts the XECM, modifies the XECM, for example to prohibit any copying of the recorded data, re-encrypts the ECM and passes the modified, re-encrypted ECM back to the recorder device.

[0079] In this type of system, sensitive data (control words, modified XECMs or descrambled data) may be passed between the CAM and the display 14 or recorder 18 and problems of security may arise at this interface. To overcome such problems, prior to communication of any data, for example, an ECM from the display 14 to the smartcard, a secure authenticated channel (SAC) 42 is created, as described above with reference to Figures 5 and 6, between the display 14 and the CAM 40. In order to create the SAC 42 between the display 14 and the CAM 40, the CAM 40 must store, for example in the smartcard, the list of device public keys in order to validate the display 14.

[0080] As shown in Figure 4, the security module may be connected to two or more connected devices 60a, 60b via respective communication links 70a, 70b. As well as validating both of these devices, each device being validated as described in Figure 5, the security module can create a secure communication channel between the devices. Figure 8 shows the steps associated with the provision of secure communication between two devices.

[0081] The provision of secure communication between device A 60a and device B 60b is carried out after both of the devices 60a, 60b have been validated by the security module. With reference to Figure 8, at step 300 the security module 64 generates a random session key SK. The random session key SK is encrypted at step 302 by the security module 64 using the random number X transmitted to the security module 64 by the device A 60a during validation of the device. The encryption is preferably conducted using a symmetric algorithm, such as Triple DES (TDES).

[0082] The encrypted session key $TDES_x(SK)$ is transmitted to the device A 60a at step 304.

[0083] At step 306, the device A 60a decrypts the encrypted session key $TDES_X(SK)$ using the random number X and stores the session key SK in memory.

[0084] At step 308, the random session key SK is additionally TDES encrypted by the security module 64 using random number Y transmitted to the security module 64 by the device B 60b during validation of the device. The encrypted session key $TDES_Y(SK)$ is transmitted to the device B 60b at step 310. At step 312, the device B 60b decrypts the encrypted session key $TDES_X(SK)$ using the random number Y and stores the session key SK in memory.

[0085] Thus, the session key SK is transmitted to each device over a respective SAC. The session key SK can then be used by, for example, device A 60a to encrypt data transmitted to device B 60b via communication link 75.

[0086] With reference to Figure 9, at step 400, device 60a encrypts data D using the session key SK. The encryption algorithm used in a symmetric algorithm, such as Triple DES (TDES) algorithm or such like.

[0087] The encrypted data $TDES_{SK}(D)$ is transmitted to device 60b via communication link 75 at step 402. At step 404, device B 60b decrypts the encrypted data $TDES_{SK}(D)$ using the session key SK to obtain the data D.

[0088] As discussed above, there is no generation of session keys by any of the devices; session keys are generated only by the security module. Therefore, the above method provides a very simple but yet secure method of providing secure communication between devices, as the data transmitted by one device can only be decrypted by a device which has established a secure authenticated channel with the same security module as that one device.

[0089] As discussed with reference to Figure 7, in addition to carrying out validation of devices and the creation of SACS, the security module may transmit control words, access rights and/or scrambled data to a device. Figures 10 and 11 illustrate examples in which a security module sets up a secure communication link between two devices and subsequently transmits data associated with scrambled data to a device.

[0090] Figure 10 shows, in a first example, the steps associated with the setting up of a secure communication link between a DVD player and a digital television and the subsequent operations carried out to descramble data received from the DVD player by the digital television.

[0091] In step 500, the security module 64 determines the validity of each of the DVD player 12 and the digital TV 14, using steps as described above with reference to Figure 5. If the two devices are determined to be valid, the security module 64 establishes secure authenticated channels (SACs) with the DVD player 12 and the digital TV, using the steps as described above with reference to Figure 6. As a result of establishing the SACs, a session key SK is stored in each of the devices and in the security module.

[0092] In step 502, data comprising Control System Scrambled (CSS) data and proprietary encrypted ECMs containing control words for descrambling the data are encrypted by the DVD player 12 using the session key SK and transmitted to the digital TV via the communication link 16.

[0093] The encrypted data is received by the digital TV 14 in step 504 and decrypted using the session key SK. The scrambled data is passed to a demultiplexer 90 which, in step 506, separates the CSS data from the encrypted ECMs. The encrypted ECMs are passed over the SAC by the digital TV 14 to the security module 64 in step 508. For transfer to the security module 64 over the SAC, the encrypted ECMs are further encrypted by the digital TV 14 using the session key SK generated by the security module 64.

[0094] As shown in Figure 10, the security module is notionally divided into a standardized security part 66 and a proprietary security part 68. The twice-encrypted ECMs are received at the standardized security part 66 in step 510 and decrypted once using the session key SK. In step 512, the proprietary encrypted ECMs are passed to the proprietary security part 68 which, in step 514, decrypts and validates the encrypted ECMs using an equivalent key to the proprietor's key used to encrypt the ECMs, and processes the ECM, if authorised, to extract the control words, or CSS keys, from the ECM.

[0095] In step 516, the CSS keys are passed to the standardized security part 66 which encrypts the CSS keys using the session key SK and passes the encrypted CSS keys to the digital TV 14 over the SAC. The received encrypted CSS keys are decrypted by the digital TV 14 using the session key at step 518 and subsequently passed to a descrambler 92 for use in descrambling the CSS data. At 520, the descrambled data is transmitted to display 94 for display.

[0096] As will be readily understood from the above, control words are always encrypted using the session key SK before being transmitted between any of the devices and the security module.

[0097] In the above example, the control words are contained in ECMs. However, the ECMs may be contained in XECMs together with XCMI, or access rights, which are processed by the proprietary security part 68, for example, to determine whether the user's rights to view the data have expired.

[0098] Figure 11 shows, in the second example, the steps associated with the setting up of a secure communication link between a DVD player and a digital recorder and the subsequent operations carried out to descramble data received from the DVD player by the digital recorder.

[0099] In step 600, the security module 64 determines the validity of each of the DVD player 12 and the digital recorder 18, using steps as described above with reference to Figure 5. If the two devices are determined to be valid, the security module 64 establishes secure authenticated channels (SACs) with the DVD player 12 and the digital recorder 18, using the steps as described above with reference to Figure 6. As a result of establishing the SACs, a session key SK is stored in each of the devices and in the security module.

[0100] In step 602, data comprising Control System Scrambled (CSS) data and proprietary encrypted XECMs containing control words for descrambling the data and XCMI are encrypted by the DVD player 12 using the session key SK and transmitted to the recorder via the communication link 20.

[0101] The encrypted data is received by the recorder 18 in step 604 and decrypted using the session key SK. The scrambled data is passed to a demultiplexer 90 which, in step 606, separates the CSS data from the encrypted XECMs. The encrypted XECMs are passed over the SAC by the recorder 18 to the security module 64 in step 608. For transfer to the security module 64 over the SAC , the encrypted XECMs are further encrypted by the recorder 18 using the session key SK generated by the security module 64.

[0102] As shown in Figure 11, the security module is notionally divided into a standardized security part 66 and a proprietary security part 68. The twice-encrypted XECMs are received at the standardized security part 66 in step 610 and decrypted once using the session key SK. In step 512, the proprietary encrypted XECMs are passed to the proprietary security part 68 which, in step 614, decrypts and validates the encrypted XECMs using an equivalent key to the proprietor's key used to encrypt the XECMs, and processes the XECMs, if authorised, to update the XCMI, for example, to limit the number of times which the user may replay the data, to prohibit any further re-recording of the data etc.

[0103] In step 616, the modified XECMs are encrypted using a proprietary algorithm PA and a user key 96 stored in the security module 68. This adds security to the data recorded by the recorder 18; the control words for descrambling the CSS data can only be extracted from the modified XECM if the user has access to the user key. Thus, playback and viewing of the recorded data is restricted to the holder of the security module.

[0104] In step 618, the encrypted XECMs are passed to the standardized security part 66 which further encrypts the encrypted XECMs using the session key SK and passes the encrypted XECMs to the recorder over the SAC. The received encrypted XECMs are decrypted once by the recorder using the session key at step 620 and subsequently passed to a recording medium 98, such as DAT tape, for storing the CSS data and the encrypted XECMs.

[0105] It will be understood that the present invention has been described above purely by way of example, and modifications of detail can be made within the scope of the invention as set out in the claims.

[0106] For example, whilst the above examples have described the provision of a communication link between devices using an IEEE 1394 digital interface, unidirectional links such as 8-VSB and 16-VSB may also be used.

[0107] It is not essential for a device to pass certificates directly to a security module. For example, where a first device is unable to receive data from a security module, the first device may pass its certificates to a second device in two-way communication with the security module for validation of the first device.

[0108] In the described examples, only one security module is provided. However, different security modules may coexist within a network comprised of a number of devices connected via various interfaces.

Claims

1. A method of providing secure communication of digital data between at plurality of devices, one of them being connected with a detachable and removable security module, said method comprising the steps

of:

- encrypting by each device (60, 60b) a random number (x) and a certificate including a device identifier by a public key of the security module,
- transmitting by each device (60a, 60b) said encrypted certificate and a random number (X) to the security module (64),
- validating, by the security module (64), each device (60a, 60b), by comparing the received identifier with at least one stored identifier,
- generating a random key (SK) in the security module; and
- transmitting the random key (SK) to each device (60a, 60b) encrypted by the respective random number (X) of said device,

and using the random key (SK) for securing the communication between the devices.

2. A method according to Claim 1, wherein each stored identifier is associated with a respective one of a valid device or an invalid device.

3. A method according to Claim 2, wherein the communicated identifier is compared with stored identifiers associated with invalid devices.

4. A method according to Claim 2 or 3, wherein the communicated identifier is compared with stored identifiers associated with valid devices.

5. A method according to Claim 1, wherein the certificate is signed to enable the authenticity of the communicated certificate to be verified.

6. A method according to Claim 1, wherein the extracted random number (X) is stored in the security module such that data communicated between the security module to the device may thereafter be encrypted and decrypted by the random number in the security module and the device.

Patentansprüche

1. Verfahren zum sicheren Übertragen von digitalen Daten zwischen einer Anzahl von Geräten, wobei eines der Geräte an ein abnehmbares und austauschbares Sicherheitsmodul angeschlossen ist, wobei das Verfahren die folgenden Schritte umfasst:

- Verschlüsselung einer Zufallszahl und eines eine Gerätekennung umfassenden Zertifikates durch jedes Gerät (60a, 60b) durch einen öffentlichen Schlüssel des Sicherheitsmoduls,
- Übertragung des verschlüsselten Zertifikates und einer Zufallszahl (X) durch jedes Gerät zum Sicherheitsmodul (64),
- Validierung jedes Gerätes (60a, 60b) durch das Sicherheitsmodul (64), indem die erhaltene Kennung mit mindestens einer gespeicherten Kennung verglichen wird,
- Erzeugung eines Zufallsschlüssels (SK) im Sicherheitsmodul und
- Übertragung des Zufallsschlüssels (SK) an jedes durch die betreffende Zufallszahl (X) verschlüsselte Gerät (60a, 60b),

und Verwendung des Zufallsschlüssels (SK) zur Absicherung der Übertragung zwischen den Geräten.

2. Verfahren gemäß Anspruch 1, bei dem jede gespeicherte Kennung mit der jeweiligen Kennung eines gültigen oder ungültigen Gerätes verknüpft ist.

3. Verfahren gemäß Anspruch 2, bei dem die übertragene Kennung mit gespeicherten Kennungen von ungültigen Geräten verglichen wird.

4. Verfahren gemäß Anspruch 2 oder 3, bei dem die übertragene Kennung mit gespeicherten Kennungen von gültigen Kennungen verglichen wird.

5. Verfahren gemäß Anspruch 1, bei dem das Zertifikat unterzeichnet wird, um die Authentizität des übertragenen Zertifikates verifizieren zu können.

6. Verfahren gemäß Anspruch 1, bei dem die extrahierte Zufallszahl (X) im Sicherheitsmodul gespeichert wird, so dass danach zwischen dem Sicherheitsmodul und dem Gerät übertragene Daten durch die Zufallszahl im Sicherheitsmodul und im Gerät ver- und entschlüsselt werden können.

Revendications

1. Méthode de communication sécurisée de données numériques entre une pluralité de dispositifs, l'un d'entre eux étant lié à un module de sécurité détachable et amovible, ladite méthode comprenant les étapes suivantes:

- encryption par chaque dispositif (60a, 60b) d'un nombre aléatoire (X) et d'un certificat, incluant un identificateur de dispositif par une clé publique du module de sécurité,
- transmission par chaque dispositif (60a, 60b) dudit certificat encrypté et du nombre aléatoire (X) vers le module de sécurité (64),
- validation, par le module de sécurité (64), chaque dispositif (60a, 60b), en comparant l'identifiant reçu avec au moins un identifiant stocké,
- génération d'une clé aléatoire (SK) dans le module de sécurité, et

- transmission de la clé aléatoire (SK) à chaque dispositif (60a, 60b) cryptée par le nombre aléatoire (X) dudit dispositif,

et en utilisation de la clé aléatoire (SK) pour assurer la communication entre les dispositifs.

2. Méthode selon la revendication 1, dans laquelle chaque identifiant stocké est associé respectivement à un dispositif valide ou invalide.

3. Méthode selon la revendication 2, dans laquelle l'identifiant communiqué est comparé à des identifiants stockés associés aux dispositifs invalides.

4. Méthode selon la revendication 2 ou 3, dans laquelle l'identifiant communiqué est comparé à des identifiants stockés associés aux dispositifs valides.

5. Méthode selon la revendication 1, dans laquelle le certificat est signé pour permettre de vérifier l'authenticité du certificat transmis.

6. Méthode selon la revendication 1, dans laquelle le nombre aléatoire extrait (X) est stocké dans le module de sécurité de tel sorte que les données transmises entre le module de sécurité de le dispositif soit par la suite être encrypté et décrypté par le nombre aléatoire dans le module de sécurité et de le dispositif.

FIG. 1

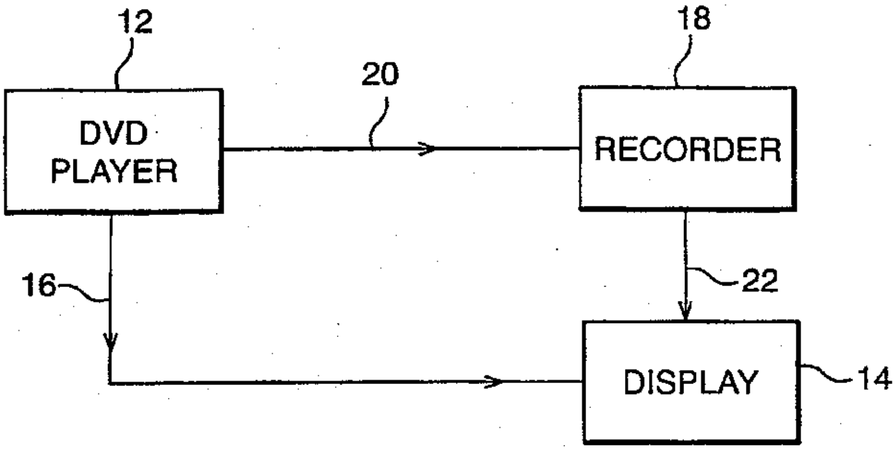


FIG. 3

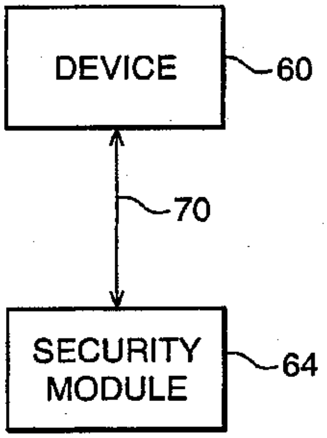


FIG. 4

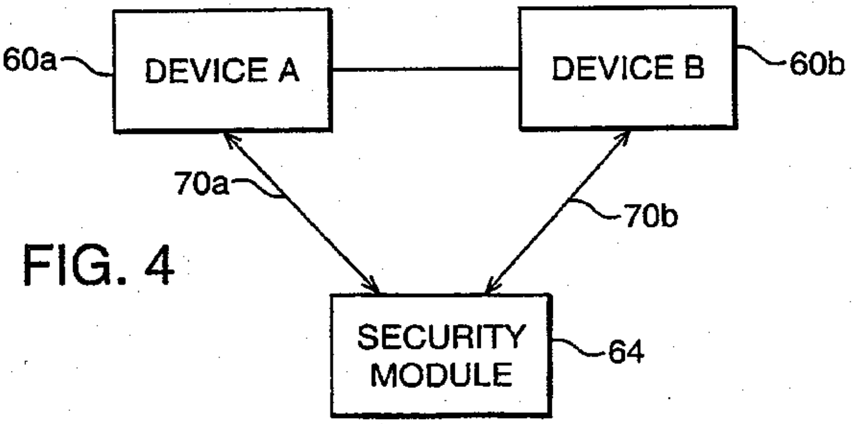


FIG. 2

FIG. 2

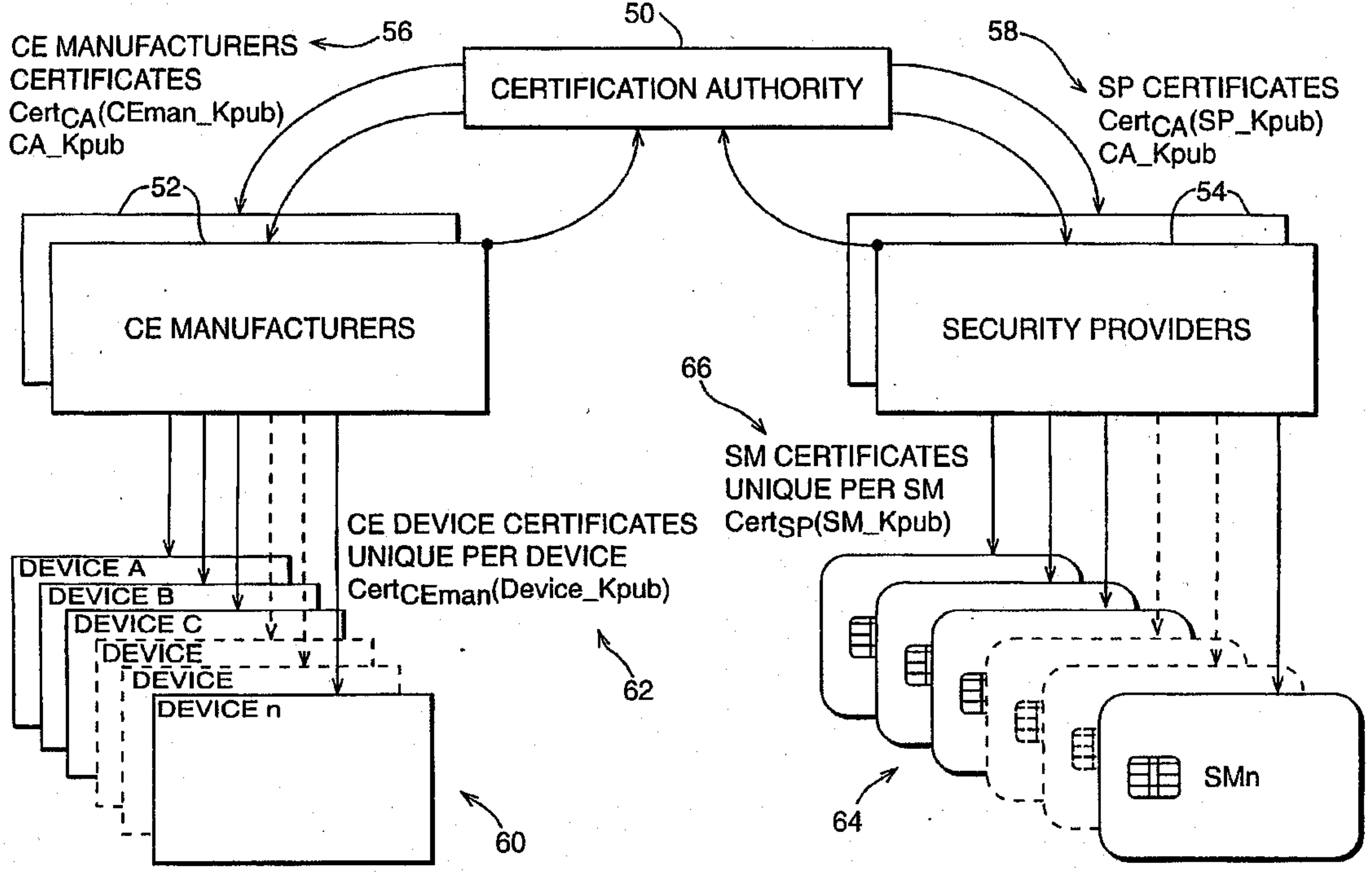

50
CERTIFICATION AUTHORITY
56
CE MANUFACTURERS
CERTIFICATES
Cert$_{CA}$(CEman_Kpub)
CA_Kpub
58
SP CERTIFICATES
Cert$_{CA}$(SP_Kpub)
CA_Kpub
52
CE MANUFACTURERS
54
SECURITY PROVIDERS
66
SM CERTIFICATES
UNIQUE PER SM
Cert$_{SP}$(SM_Kpub)
CE DEVICE CERTIFICATES
UNIQUE PER DEVICE
Cert$_{CEman}$(Device_Kpub)
DEVICE A
DEVICE B
DEVICE C
DEVICE
DEVICE
DEVICE n
62
60
SMn
64

FIG. 5

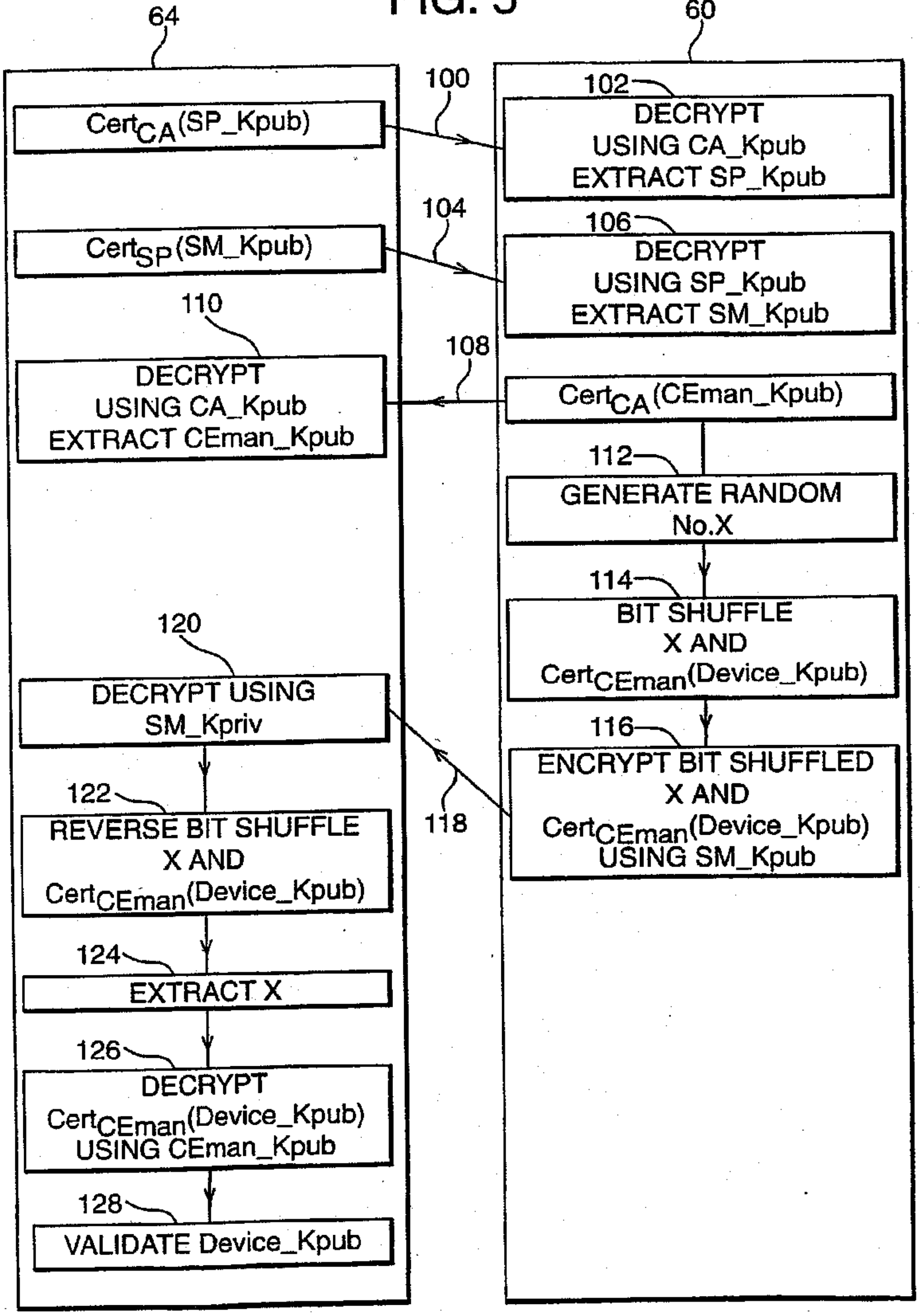

64
60
100
102
104
106
108
110
112
114
116
118
120
122
124
126
128
Cert$_{CA}$(SP_Kpub)
DECRYPT USING CA_Kpub EXTRACT SP_Kpub
Cert$_{SP}$(SM_Kpub)
DECRYPT USING SP_Kpub EXTRACT SM_Kpub
DECRYPT USING CA_Kpub EXTRACT CEman_Kpub
Cert$_{CA}$(CEman_Kpub)
GENERATE RANDOM No.X
BIT SHUFFLE X AND Cert$_{CEman}$(Device_Kpub)
ENCRYPT BIT SHUFFLED X AND Cert$_{CEman}$(Device_Kpub) USING SM_Kpub
DECRYPT USING SM_Kpriv
REVERSE BIT SHUFFLE X AND Cert$_{CEman}$(Device_Kpub)
EXTRACT X
DECRYPT Cert$_{CEman}$(Device_Kpub) USING CEman_Kpub
VALIDATE Device_Kpub

FIG. 6

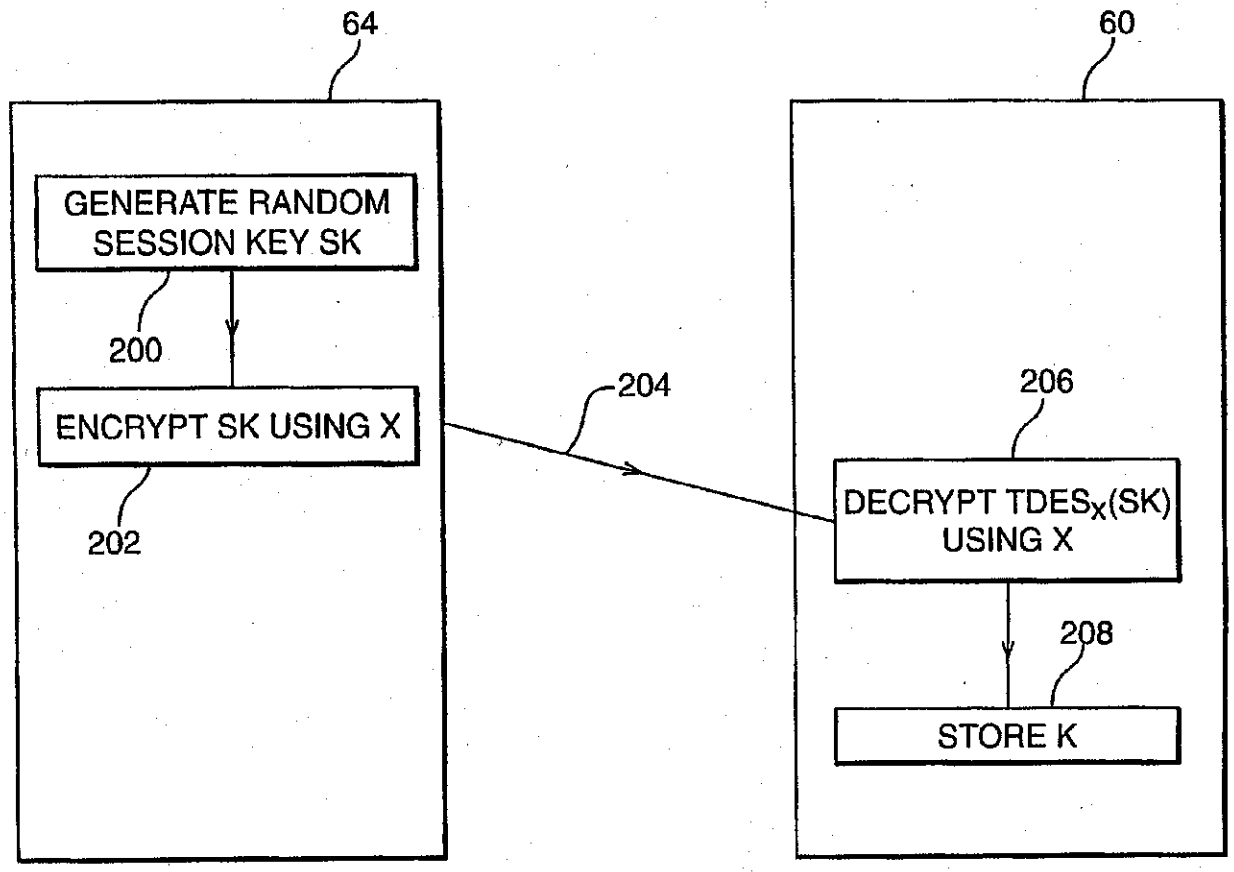

64
GENERATE RANDOM SESSION KEY SK
200
ENCRYPT SK USING X
202
204
60
206
DECRYPT TDES$_X$(SK) USING X
208
STORE K

FIG. 7

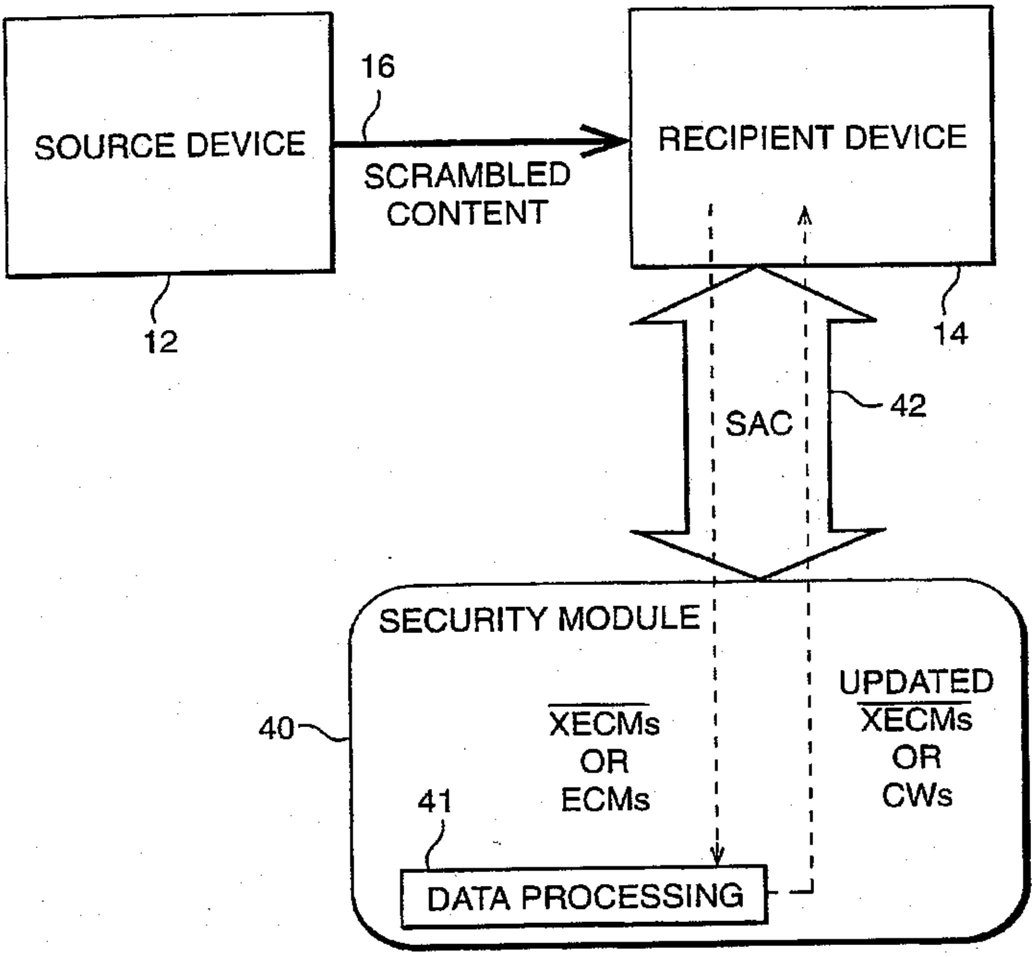


FIG. 8

FIG. 9

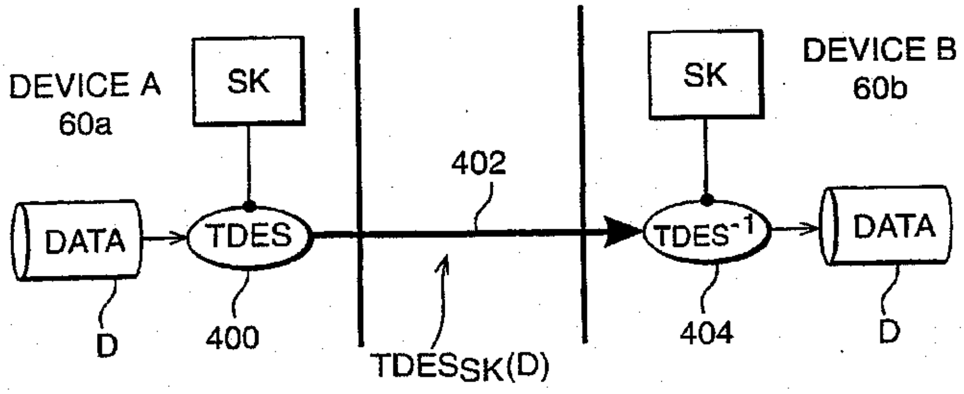
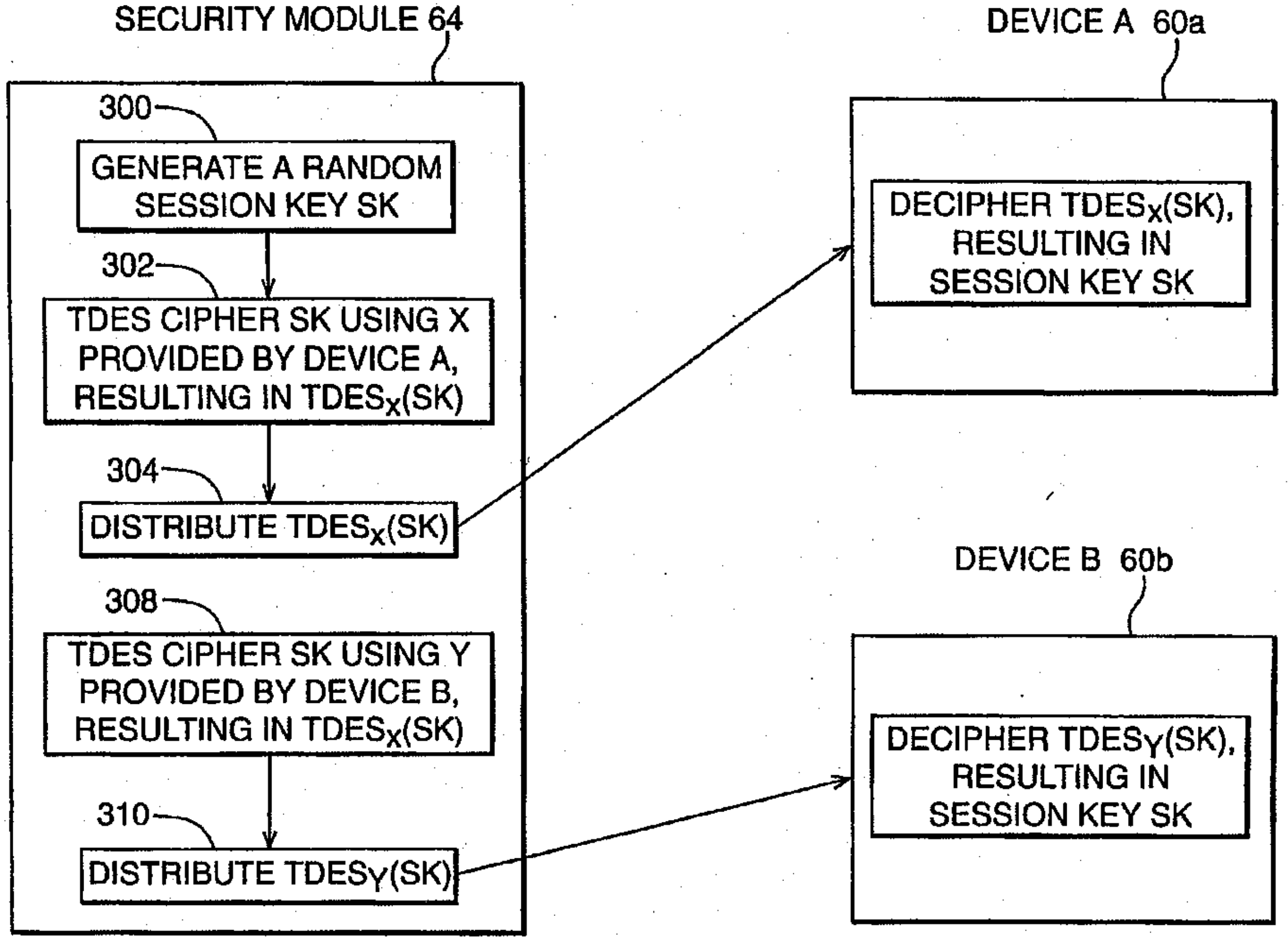


FIG. 8


SECURITY MODULE 64
300
GENERATE A RANDOM SESSION KEY SK
302
TDES CIPHER SK USING X PROVIDED BY DEVICE A, RESULTING IN TDES$_X$(SK)
304
DISTRIBUTE TDES$_X$(SK)
308
TDES CIPHER SK USING Y PROVIDED BY DEVICE B, RESULTING IN TDES$_X$(SK)
310
DISTRIBUTE TDES$_Y$(SK)
DEVICE A 60a
DECIPHER TDES$_X$(SK), RESULTING IN SESSION KEY SK
DEVICE B 60b
DECIPHER TDES$_Y$(SK), RESULTING IN SESSION KEY SK

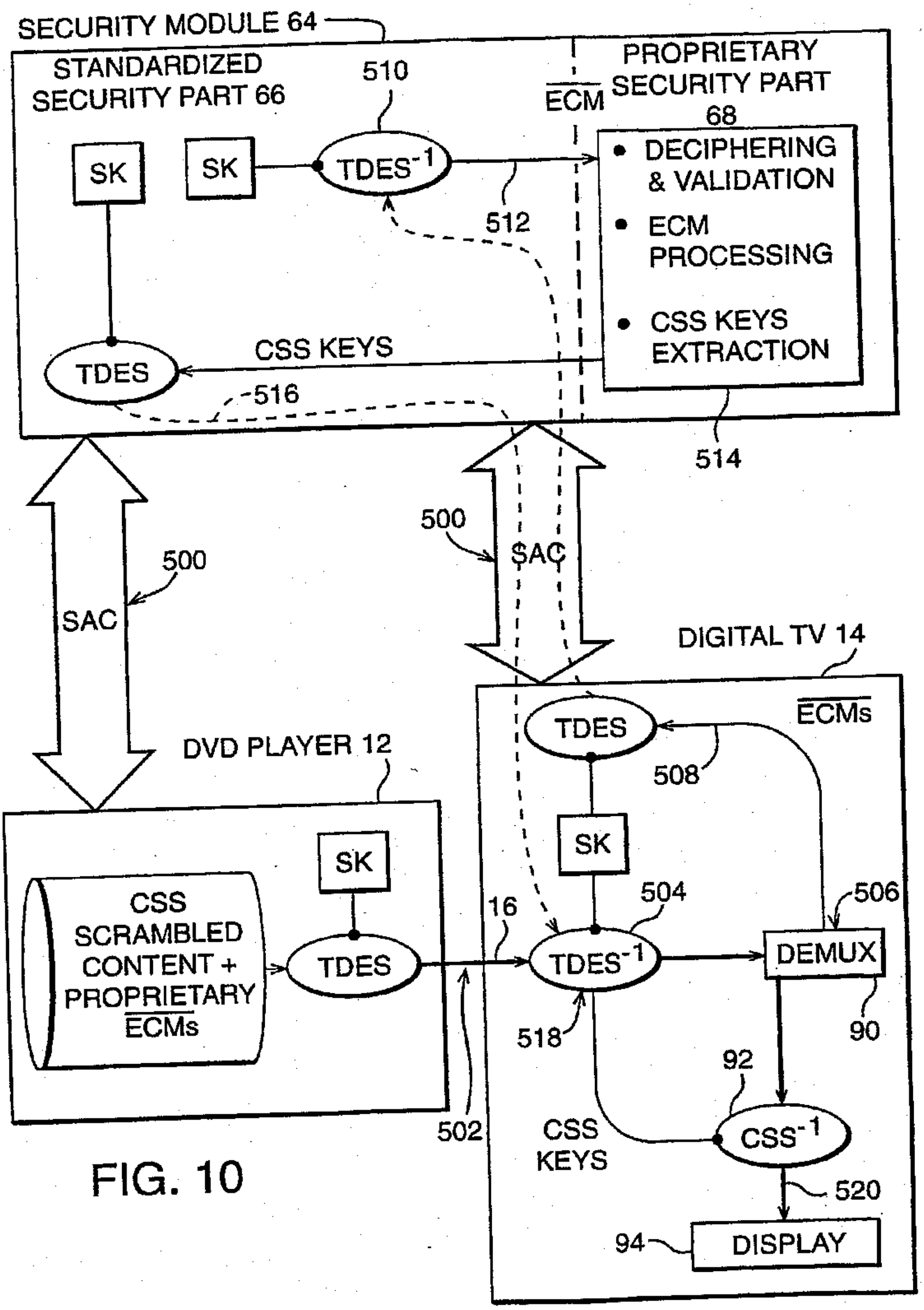

SECURITY MODULE 64
STANDARDIZED SECURITY PART 66
510
$\overline{\text{ECM}}$
PROPRIETARY SECURITY PART 68
SK
SK
TDES^{-1}
512
• DECIPHERING & VALIDATION
• ECM PROCESSING
• CSS KEYS EXTRACTION
CSS KEYS
TDES
516
514
500
SAC
500
SAC
DIGITAL TV 14
$\overline{\text{ECMs}}$
TDES
508
DVD PLAYER 12
SK
SK
CSS SCRAMBLED CONTENT + PROPRIETARY $\overline{\text{ECMs}}$
TDES
16
504
506
TDES^{-1}
DEMUX
518
90
92
502
CSS KEYS
CSS^{-1}
520
94
DISPLAY

FIG. 10

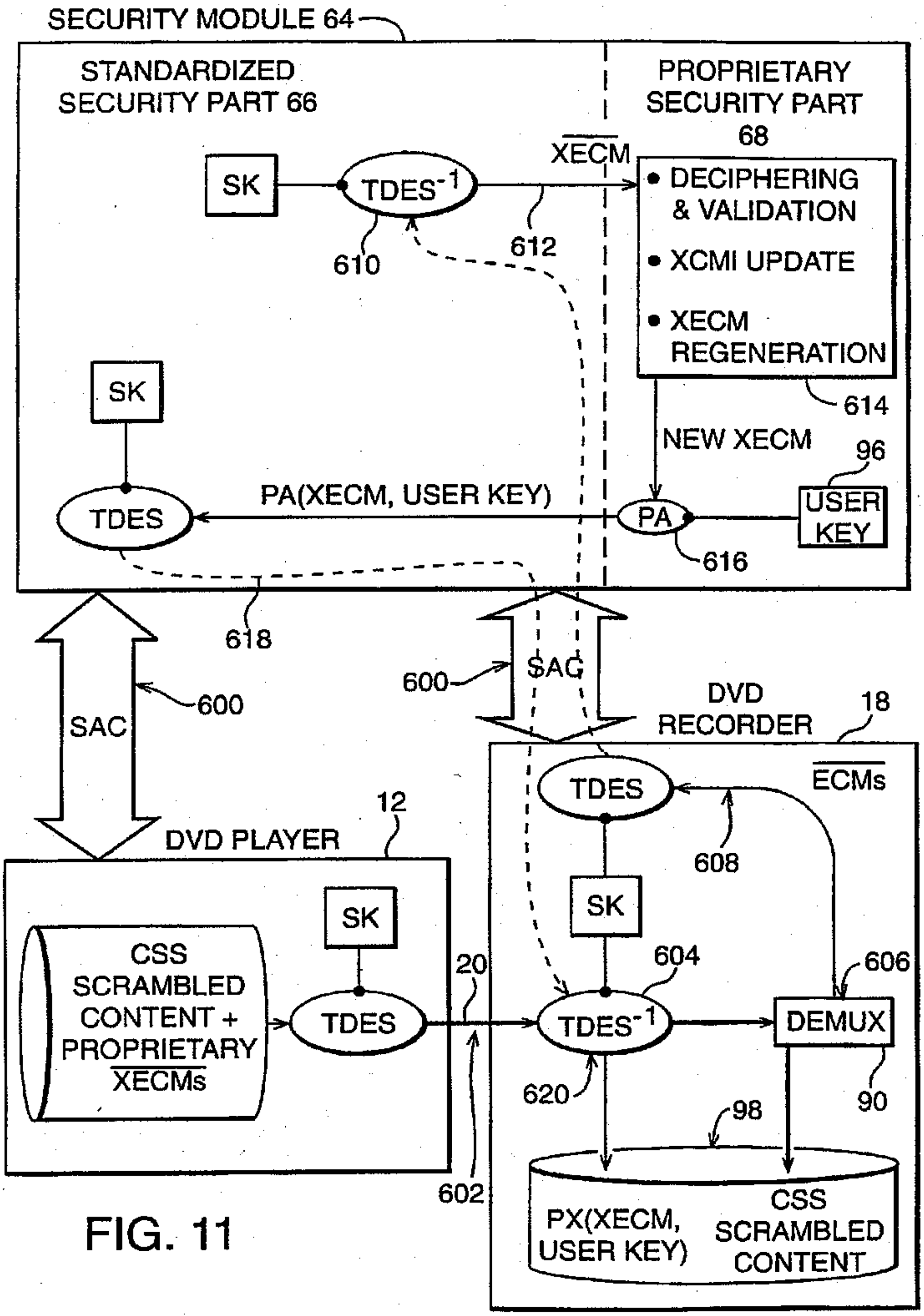

SECURITY MODULE 64
STANDARDIZED SECURITY PART 66
PROPRIETARY SECURITY PART 68
SK
TDES^{-1}
$\overline{XECM}$
610
612
• DECIPHERING & VALIDATION
• XCMI UPDATE
• XECM REGENERATION
614
SK
NEW XECM
96
TDES
PA(XECM, USER KEY)
PA
USER KEY
616
618
SAC
600
SAC
600
DVD RECORDER
18
TDES
$\overline{ECMs}$
608
12
DVD PLAYER
SK
SK
CSS SCRAMBLED CONTENT + PROPRIETARY $\overline{XECMs}$
TDES
20
604
606
TDES^{-1}
DEMUX
620
98
90
602
PX(XECM, USER KEY)
CSS SCRAMBLED CONTENT

FIG. 11

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- WO 9856179 A **[0006]**

Non-patent literature cited in the description

- Strong authentication in intelligent networks. *Universal personal Communications, 1994 Third Annual International Conference,* 27 September 1994 **[0007]**