(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 July 2006 (27.07.2006)

PCT

(10) International Publication Number
WO 2006/077544 A1

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/IB2006/050198

(22) International Filing Date: 19 January 2006 (19.01.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
05100405.9 24 January 2005 (24.01.2005) EP

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **VAN DER VELDE, Wytse, H.** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **PETKOVIC, Milan** [YU/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **CONRADO, Claudine, V.** [BR/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **VAN DER VEEN, Minne** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agents: **GROENENDAAL, Antonius, W., M.** et al.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

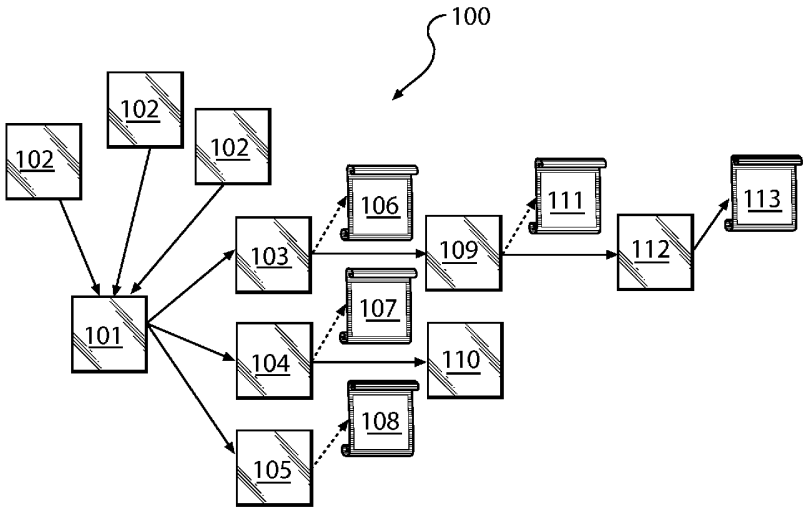
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) **Title:** A METHOD FOR DISCOURAGING ILLEGAL DISTRIBUTION OF CONTENT WITHIN A DRM SYSTEM FOR COMMERCIAL AND PERSONAL CONTENT



(57) **Abstract:** The present invention relates to methods, devices and a system for preventing unauthorized distribution of content items in a network containing compliant devices (102). A basic idea of the present invention is to link the authorization to create content rights (111) for a particular content item to a specific user (109), or a specific group of users. By employing a content ID certificate (106) in the network of compliant devices, which certificate is signed by an authorized certificate authority (103) and comprises a content ID, a fingerprint of the content item and the public key of the user who introduced the content item in the network, Content providers may, after various verifications of the certificate, be deemed authorized to create content rights for the particular content item. Consequently, unauthorized introduction and distribution of content in the network is prevented.

WO 2006/077544 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A method for discouraging illegal distribution of content within a DRM system for commercial and personal content

The present invention relates to methods, devices and a system for preventing unauthorized distribution of content items in a network containing compliant devices.

In prior art DRM systems, content rights are associated with content items, such as audio files, movies, electronic books etc. Content rights typically contains rules (e.g. play, copy, distribute etc.) and necessary cryptographic keys for encrypting/decrypting the content item(s) with which they are associated. Content rights should only be transferred to devices that are compliant and operated by users that have appropriate user rights, i.e. rights specifying who can use the content rights. Note that a content right and a user right may be merged in one single license, as is known from Open Mobile Alliance (OMA) DRM. Compliant devices comply with a given standard and adhere to certain operation rules. They also communicate by means of a certain protocol such that they answer questions and requests, which are posed to them, in the expected way. Compliant devices are considered to be trusted, which e.g. means that they will not illegally output content on a digital interface and that ownership of a device is not important. Device compliancy management, i.e. compliant device identification, renewability of devices, and revocation of devices, can be effected by using known techniques.

In general, content providers do not want to authorize users to create their own content rights, due to the risk of uncontrollable distribution of commercial content items. Consequently, the content provider digitally signs the content rights before they are distributed. Further, it must be enforced that the compliant devices check the signatures of the content rights and refuse content rights which are not properly signed by the content provider. Typically, the devices are comprised in a network or domain.

The above described approach is suitable for DRM systems in which only content provider(s) distribute content rights. However, if users wish to introduce personal content items, such as e.g. photos or home videos, they have to involve the content provider to create content rights for the personal content items. This is undesired, since the content provider should not be able to control personal content. In DRM systems in which

commercial content items as well as personal content items are distributed, a compliant device may be authorized to create a content right for a specific personal content item. This content right may be signed by the compliant device, and if it is not signed, any compliant device shall reject the content right. This has the effect that personal content only can enter the network of devices via a compliant device. In environments with stricter security requirements, the content rights may be signed by an independent and trusted third party authority, i.e. a party which is trusted by concerned communicating parties.

A problem to be solved in prior art DRM systems, in which commercial content items as well as personal content items are introduced, is that they are susceptible to attacks involving substitution of content item identifiers. A content item identifier uniquely identifies a corresponding content item in the system.

In DRM systems in which commercial content items as well as personal content items are distributed, any user is authorized to create a content right for a specific personal content item, which content right may be signed by a compliant device as mentioned above or by the user himself, and hence the user effectively becomes a content provider in his own right. Any user may also acquire commercial content items from a content provider and introduce them in the system. A malicious user may substitute a specific personal content item for a commercial content item following the creation of the content right associated with the specific personal content item. This will involve hacking of the compliant device to obtain a key to decrypt the commercial content item, such that the commercial content item comes in the clear. The malicious user then has to re-encrypt the unauthorized obtained commercial content with a content key that is present in the content right that is associated with the specific personal content. Thereafter, the re-encrypted commercial content item is associated with the content identifier of the specific personal content item. The malicious user may then use this commercial content item with the same rights as his own personal content item. As a highly undesired consequence, a great number of commercial content items may be introduced in the network, if it is encrypted with the leaked content key.

Hence, to avoid this attack, a secure link between a content item and a corresponding content item identifier is required. This has been solved by employing fingerprints of content. These fingerprints are used to uniquely identify the content to which they refer. A known method of generating fingerprints is described in detail in WO 02/065782, which belongs to the applicant of the present patent application. The compliant device adds fingerprint information to the content right before signing it. When a content right is used, the compliant device must check whether the fingerprint information that is

included in the content right also can be found in the actual content item. If the fingerprint information cannot be found in the actual content item, the content right must be rejected.

However, a problem that remains in the approach of employing fingerprints is that it does not prevent a user from unauthorized introduction and distribution of commercial content in the network. As can be seen from the above, in DRM systems in which commercial content items as well as personal content items are introduced and distributed, any user can create content rights for any content item.

An object of the present invention is to solve the above given problems and to provide methods, devices and a system for preventing unauthorized distribution of commercial content.

This object is attained by a method in accordance with claim 1, a device in accordance with claim 9, a method in accordance with claim 11, a device in accordance with claim 13 and a system in accordance with claim 14.

According to a first aspect of the present invention, there is provided a method comprising the step of creating a content identifier certificate comprising at least unique content identification data for a content item introduced in the network, as well as an identifier of a content introducer having introduced the content item in the network. Further, the method comprises the step of signing the content identifier certificate, such that it is ensured that the content introducer, which is identified by said identifier, introduced the content item in the network.

According to a second aspect of the present invention, there is provided a device comprising means arranged to create a content identifier certificate comprising at least unique content identification data for a content item introduced in the network, as well as an identifier of a content introducer having introduced the content item in the network. Further, the device comprises means arranged to sign the content identifier certificate.

According to a third aspect of the present invention, there is provided a method comprising the step of receiving a content identifier certificate comprising at least unique content identification data for a content item introduced in the network, as well as an identifier of a content introducer having introduced the content item in the network, which content identifier certificate has been signed by an authorized certificate authority. Further, the method comprises the step of verifying the signed content identifier certificate when a content provider requests to create a content right for the introduced content item.

According to a fourth aspect of the present invention, there is provided a device comprising means arranged to receive a content identifier certificate comprising at least unique content identification data for a content item introduced in the network, as well as an identifier of a content introducer having introduced the content item in the network, which content identifier certificate has been signed by an authorized certificate authority. Further, the device comprises means arranged to verify the signed content identifier certificate when a content provider requests to create a content right for the introduced content item.

According to a fifth aspect of the present invention, there is provided a system comprising at least one compliant device arranged to create a content identifier certificate comprising at least unique content identification data for a content item introduced in the network, as well as an identifier of a content introducer having introduced the content item in the network. Further, the system comprises an authorized certificate authority arranged to sign the content identifier certificate.

A basic idea of the present invention is to link the authorization to create content rights for a particular content item to a specific user, or a specific group of users. In DRM systems, in which commercial content items as well as personal content items are introduced and distributed, any user is authorized to create a content right for a specific personal content item and hence effectively becomes a content provider in his own right. Since compliant devices do not have access to information regarding ownership of a content item, any user can create content rights for any content item. According to the present invention, a content identifier (ID) certificate is introduced in the network of compliant devices. The content ID certificate comprises unique content identification data for the particular content item with which it is associated. The unique content identification data comprises e.g. a content ID and a fingerprint of the particular content item with which the content ID is associated. The certificate is signed by a unit that is authorized by the content provider, which unit in the following will be referred to as a Certificate Authority (CA). Note that the CA may be a trusted third party, but it may alternatively be a trusted compliant device to which the authority to sign certificates has been distributed. This signing is effected in order to prevent malicious users from tampering with the content ID certificate. Whenever a user wants to use a content right to access a corresponding content item, the compliant device on which the content item is to be rendered verifies correctness of the signature of the content ID certificate and compares the actual fingerprint of the content item with the

fingerprint comprised in the content ID certificate. In the prior art, the content right can be used to access the content item if there is a match.

As previously mentioned, since the content item fingerprint is included in the content ID certificate, content ID substitution attacks are prevented. However, unauthorized introduction and distribution of content items in the network by means of creating content rights is not hindered by including the content item fingerprint. If a malicious user has obtained cryptographically protected, i.e. encrypted, commercial content via the DRM system, he may hack the compliant device which handles the content, in order to procure a secret decryption key to create a clear text copy of the commercial content. Hence, the malicious user can create a new content right for the commercial content. To overcome this problem, the present invention links a user (i.e. a content provider) and a content item.

This is accomplished by including, in the content ID certificate, an identifier, e.g. a public key, of the user/content provider who introduced the content item in the network. The user/content provider who introduced the content item in the network is occasionally referred to herein as a "content introducer". When a user is to create a content right for a particular content item, the compliant device which is employed will check that the user's public key is present in the content ID certificate signed be the CA. If the user's public key is present in the content ID certificate, the user is deemed authorized to create content rights for the particular content item. On the contrary, if the content ID certificate does not comprise the user's public key, the user is not authorized to create content rights for the particular content item. Hence, unauthorized introduction and distribution of content in the network is prevented.

According to an embodiment of the present invention, a compliant device checks that the content ID certificate has been signed by an authorized certificate authority by means of decrypting the certificate with a public key of the authorized certificate authority. The public key corresponds to the authorized certificate authority's private key that was used to sign the certificate.

In another embodiment of the present invention, the user that wishes to create a content right for a particular content item provides the compliant device with his public key. This is effected by inserting a smart card containing the requesting user's public key into the compliant device.

In accordance with another embodiment of the present invention, a compliant device is assigned as an authorized certificate authority in the network. This brings a great deal of flexibility to the network.

In accordance with yet another embodiment of the present invention, the authorized certificate authority is a trusted third party. This enhances security in the network. According to a further embodiment of the invention, the content identifier comprises a unique numeral to identify the content item with which it is associated. For example, content ID = 4556 denotes content item A, content ID = 67 denotes content item B, etc.

Further features of, and advantages with, the present invention will become apparent when studying the appended claims and the following description. Those skilled in the art realize that different features of the present invention can be combined to create embodiments other than those described in the following.

A detailed description of preferred embodiments of the present invention will be given in the following with reference made to the accompanying drawings, in which:

Fig. 1 shows an authorization hierarchy in which the present invention may be applied; and

Fig. 2 shows an authentication procedure which is performed when a user wishes to access a content item, in accordance with an embodiment of the present invention.

Fig. 1 shows an authorization hierarchy 100 in which the present invention may be applied. Continuous lines indicate authorization steps, which involve the use of public key certificates. These certificates are well known in the art and are hence not shown in Fig. 1. Dotted lines indicate issuing of certificates and/or rights.

A System Authority (SA) 101 is at the top of the hierarchy. All compliant devices has access to the public key of the SA. Typically, the SA public key is built-in into the hardware of each compliant device 102. With this public key, a compliant device can verify any certificate that has been issued by the SA 101. At the next level in the hierarchy, a Certificate Authority (CA) 103, a Device Authority (DA) 104 and a User ID Authority (UIDA) 105 are arranged. The CA 103 authorizes content providers 109 within the system. For example, EMI and Disney may constitute content providers within the network, but as previously mentioned, a compliant device or a user may also represent a content provider. In fact, in DRM systems in which commercial content items as well as personal content items are distributed, any user is authorized to create (via a compliant device) a content right for a specific personal content item and hence effectively becomes a content provider in his own

right. Consequently, in a DRM system in which the present invention is applied, a large number of content providers exist, since the term "content provider" in this context includes both individual users and traditional content providers such as record and motion-picture companies and content distributors.

The CA 103 issues content ID certificates 106 and provides these to the content providers 109. The CA 103 may be a trusted third party or may alternatively be a compliant device. This is primarily a question of flexibility; if a compliant device is authorized to act as CA, it brings flexibility to the system. On the contrary, a third party provider may not want to "distribute" the right to issue content ID certificates to a compliant device for security reasons. The content ID certificate 106 has been described in detail hereinabove and comprises:

(a) the unique content ID and

(b) the content fingerprint for a content item introduced in the network, as well as

(c) the public key of a user having introduced the content item in the network and

(d) a signature of the CA.

Note that it is possible that, in case the CA is a trusted third party, the content ID certificate is created at a content provider in the form of a compliant device, but signed at the CA.

A content provider 109 within the network is authorized to issue content rights 111 for a content item, if the content provider has been provided with a valid content ID certificate 106. Each content right contains the content ID and content key(s) that enable access to cryptographically protected content items with which the content right is associated (which association is made effective by means of the content ID in the content right, since it is compared to the content ID attached to the encrypted content item). The content right 111 also specifies a valid User Right Authority (URA) 112 for a particular content item, in that the content right 111 contains the public key of the URA 112. Hence, the content provider 109 may delegate issuance of user rights 113 to another party, namely the URA 112. This makes the system flexible, because it can support different usage models, including content distributed by a content provider, personal content (when a user/compliant device acts as content provider) and content imported from another DRM system. The content provider 109 who issues the content right 111 also signs it. In practice, the content provider itself is authorized to be URA, and hence issues the content rights 111 and the user rights 113. In fact, the content right and the user right for a particular content item may be combined into one single right.

The URA 112 issues a user right 113 for a certain content item. A user right indicates whether a user is allowed to use a content right to access a content item. The user right comprises a content ID, which is the link between the user right, the content right and the content item. As described hereinabove, these three components all comprise a content ID. The user right further comprises a rights expression that indicates how a user, which user is designated by means of a user ID in the form of a public key included in the user right, may use the content item. Finally, the user right is signed by the URA.

In terms of security aspects involved in handling different types of rights, there is a distinction between user rights 113 and content rights 111. User rights may be freely distributed, because they do not contain any secrets, and the signature prevents modifications. Content rights, on the other hand, contains cryptographic keys for accessing content items. Hence, content rights may only be transferred to compliant devices. Further, the transfer of content rights between devices requires secure communication means, which may be based on secure authenticated channels. Consequently, the content right 111 requires both confidentiality and integrity, whereas the user right 113 requires only integrity.

User and device management involves personalization and certification of users and devices, which are then introduced into the system and declared compliant (to certain required properties, as has previously been described). The Device Authority (DA) 104 is a trusted party that authorizes the Device ID Authorities (DIDA) 110 for several device manufacturers. Each device manufacturer (e.g. Philips, Sony) has its own DIDA 110 that gives devices a unique identity and an associated public key by means of a signed device ID certificate 107, hence indicating compliance.

The User ID Authority (UIDA) 105 is responsible for issuing user ID devices (not shown in Fig. 1). This is typically performed during a manufacturing phase. The UIDA 105 associates a user ID device, which device typically comprises e.g. a tamper resistant smartcard or a SIM card, with a certain person by issuing a signed user ID certificate 108 containing the name, or any other identifier, of the user together with the public key of the user ID device. The private key that corresponds to this public key is considered to be the user's private key. However, the user is not given personal access to this private key. This prevents a user from distributing the private key to someone who thus could impersonate him. Therefore, the user's private key is securely stored on the user ID device, which is tamper resistant. The user ID device serves as a token, proving the user's presence. The user ID device should be easy to handle, robust, provide secure computing and hard to clone.

Each authority illustrated in Fig. 1 typically comprise one or more microprocessors or some other device with computing capabilities, e.g. an application specific integrated circuit (ASIC), a field programmable gate array (FPGA), a complex programmable logic device (CPLD), etc., in order the create the various certificates and rights. In the creation of the certificates and rights, as well as in intercommunication between the different authorities, the microprocessors execute appropriate software that is downloaded to the respective authorities and stored in a suitable storage area, such as a RAM, a Flash memory or a hard disk. For intercommunication to be possible, the authorities are arranged with interfaces that enables the communication.

Before a certificate can be used, it has to be validated. Certificate validation implies that at least the integrity (using the signature) and the authenticity (using the chain of certificates that links a certificate to the certificate of the authority, all the way up to the SA) of a certificate is checked.

Referring to Fig. 2, when a user 201, in the following referred to as Alice, wishes to access a content item, she will need the following:

(a) a content ID certificate,

(b) a content right,

(c) a user right, and

(d) a user ID certificate.

It is assumed that device compliancy has already been checked, which is why the above list does not comprise a device ID certificate. The content item has been loaded into a compliant device 202 in encrypted form. The compliant device may e.g. be a CD player, and the content item to be rendered on the device may be an audio CD. The compliant device 202 comprises a microprocessor 213 in order the create the various certificates and rights and to perform cryptographical operations and other computing operations described in the following. The microprocessor 213 executes appropriate software that is downloaded to the compliant device and stored in a RAM 214.

The compliant device 202 verifies (step 203) that the user ID certificate 204 is valid by checking the signature using the built-in public key in the compliant device. Alice 201 will also have to authenticate herself by proving she knows the secret key corresponding to the public key comprised in the user ID certificate. As previously mentioned, the user is not given personal access to this private key in order to prevent the user from distributing the private key, and thus prevent impersonation. Therefore, the user's private key is securely stored on a user ID device 205, e.g. a tamper resistant smartcard, which is inserted (step 206)

into, and read by, the compliant device 202. Further, the compliant device verifies (step 207) the signature of the user right 208, to ensure that the user right is valid. To do this, the compliant device checks the User Right Authority (URA) field in the content right 209 and verifies that the specified URA signed the user right. The compliant device 202 verifies that Alice 201 can use the user right 208. This is done by comparing the user ID, i.e. a user public key, in the user right with the user ID on Alice's user ID certificate 204.

The compliant device verifies (step 210) that the content provider was allowed to sign the content right. Thus, the device checks the signature of the content right 209 using the public key comprised in the content ID certificate 211. To do this, the compliant device must, by using its built-in public key, first verify (step 212) the content ID certificate by checking the signature of the content ID certificate provided by the CA (see Fig. 1). As described in the above, the content right 209 is created and signed by the actor who introduced the corresponding content item in the network. Hence, the public key comprised in the content ID certificate 211 is the public key of the user (i.e. content provider) having introduced the content item in the network, and this public key corresponds to the private key that was employed to sign the content right 209.

Finally, the compliant device 202 will have to verify if the content right can be used to access the encrypted content. To this end, the device computes a fingerprint of the content item and compares it with the fingerprint in the content ID certificate 211. If there is a match, Alice 201 is allowed to access the content item on the compliant device 202. If any of the above steps fail, Alice will not be given access to the content.

According to the present invention, a content ID certificate is introduced in the network of compliant devices. The signing of the certificate by the authorized certificate authority (CA) prevents malicious users from tampering with the content ID certificate. The fingerprint of the content item is included in the content ID certificate to hamper content ID substitution attacks. The problem related to unauthorized introduction and distribution of content items in the network by means of (unauthorized) creation of content rights is overcome by including, in the content ID certificate, the public key of the content introducer. When a user (or a third party content provider) is about to create a content right for a particular content item, the compliant device which is employed will check that the user's public key is present in the content ID certificate signed be the CA, as described hereinabove. If the user's public key is present in the content ID certificate, the user is deemed authorized to create content rights for the particular content item. Hence, unauthorized introduction and distribution of content in the network is prevented.

Even though the invention has been described with reference to specific exemplifying embodiments thereof, many different alterations, modifications and the like will become apparent for those skilled in the art. For example, the content ID certificate could also comprise the public key of a compliant device via which a content item is introduced. This public key may be used to create content rights in accordance with format of licenses used in OMA DRM. The content ID certificate could additionally or alternatively comprise information concerning type of certificate. This may be specified in a rights field, e.g. right = ownership. The described embodiments are therefore not intended to limit the scope of the invention, as defined by the appended claims.

CLAIMS:

1. A method of preventing unauthorized distribution of content items in a network containing compliant devices (102), which method uses unique content identification data for each content item introduced in the network, said method being characterized in that it comprises the steps of:

creating a content identifier certificate (106) comprising at least the unique content identification data for a content item introduced in the network, as well as an identifier of a content introducer (109) having introduced the content item in the network;

signing the content identifier certificate, such that it is ensured that the content introducer, which is identified by said identifier, introduced the content item in the network.

2. The method according to claim 1, further comprising the step of verifying that the content identifier certificate (106) has been signed by an authorized certificate authority (103) by means of decrypting said certificate with a public key of the authorized certificate authority, which corresponds to a private key that was used to sign the certificate, when a request is made to create a content right for the introduced content item.

3. The method according to claim 2, further comprising the steps of:

receiving a request from a content provider (109) to create a content right (111) for the introduced content item; and

verifying that the identifier of the requesting content provider matches the identifier comprised in the content identifier certificate (106).

4. The method according to claim 4, further comprising the step of creating a content right (111) for the content item introduced in the network upon successful verification of the identifier.

5. The method according to claim 1, wherein the unique content identification data comprises a content identifier and a content fingerprint associated with the content item.

6. The method according to claim 5, further comprising the step of verifying, whenever a user wants to use a content right (111) to access a content item, that the content fingerprint of the content identifier certificate (106) matches the actual fingerprint of the content item to which access is requested.

7. The method according to claim 1, wherein the content identifier is set to be a numeral that identifies the content item to which it is associated.

8. The method according to claim 1, wherein the identifier of the content introducer (109) comprises the public key of said content introducer.

9. A device (202) for preventing unauthorized distribution of content items in a network containing compliant devices, said device being characterized in that it comprises:

means (213) arranged to create a content identifier certificate (211) comprising at least unique content identification data for a content item introduced in the network, as well as an identifier of a content introducer having introduced the content item in the network; and

means (213) arranged to sign the content identifier certificate.

10. The device (202) according to claim 9, further comprising means (213) arranged to verify that the content identifier certificate (211) has been signed by an authorized certificate authority (202) by means of decrypting said certificate with a public key of the authorized certificate authority, which corresponds to a private key that was used to sign the certificate, when a content provider (201) requests to create a content right (209) for the introduced content item at the device, means (213) arranged to receive a request from a content provider (201) to create a content right (209) for the introduced content item, and to verify that the identifier of the requesting content provider matches the identifier comprised in the content identifier certificate (211), and means (213) arranged to receive the identifier of the requesting content provider (201) by means of reading a smart card (205) inserted into the device, which smartcard contains the requesting content provider's identifier.

11. A method of preventing unauthorized distribution of content items in a network containing compliant devices (102), which method uses unique content

identification data for each content item introduced in the network, said method being characterized in that it comprises the steps of:

receiving a content identifier certificate (106) comprising at least the unique content identification data for a content item introduced in the network, as well as an identifier of a content introducer (109) having introduced the content item in the network, which content identifier certificate has been signed by an authorized certificate authority (103);

verifying the signed content identifier certificate when a content provider requests to create a content right for the introduced content item.

12. The method according to claim 11, wherein the unique content identification data comprises a content identifier and a content fingerprint associated with the content item.

13. A device (202) for preventing unauthorized distribution of content items in a network containing compliant devices, said device being characterized in that it comprises:

means (213) arranged to receive a content identifier certificate (211) comprising at least unique identification data for a content item introduced in the network, as well as an identifier of a content introducer having introduced the content item in the network, which content identifier certificate has been signed by an authorized certificate authority;

means (213) arranged to verify the signed content identifier certificate when a content provider (201) requests to create a content right (209) for the introduced content item.

14. A system for preventing unauthorized distribution of content items in a network containing compliant devices (102), said system being characterized in that it comprises:

at least one compliant device (109) arranged to create a content identifier certificate (106) comprising at least unique content identification data for a content item introduced in the network, as well as an identifier of a content introducer having introduced the content item in the network; and

an authorized certificate authority (103) arranged to sign the content identifier certificate.

15. The system according to claim 14, wherein the authorized certificate authority (103) is comprised in said at least one compliant device (109) arranged to create a content identifier certificate (106).

16. The system according to claim 14, wherein the authorized certificate authority (103) is a trusted third party comprised in said at least one compliant device (109) arranged to create a content identifier certificate (106).

17. A computer program product comprising computer-executable components for causing a device (202) to perform the steps recited in claim 1 when the computer-executable components are run on a processing unit (213) included in the device.

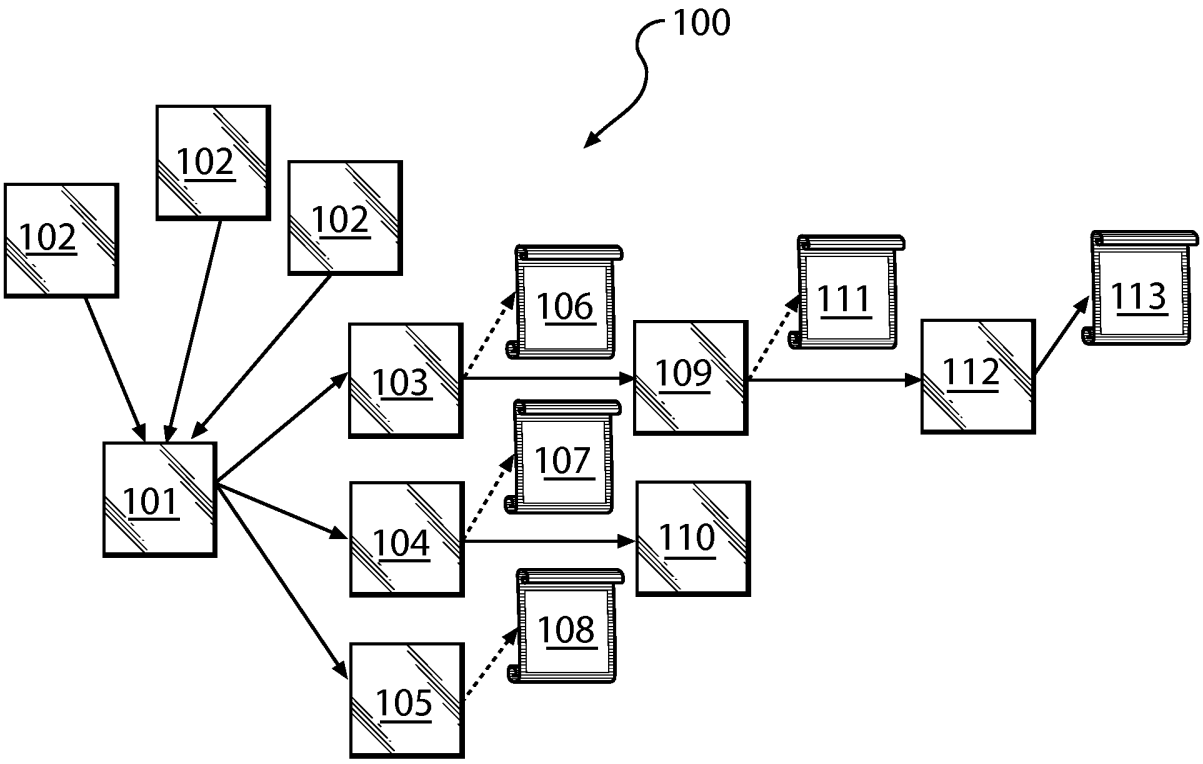


Fig. 1

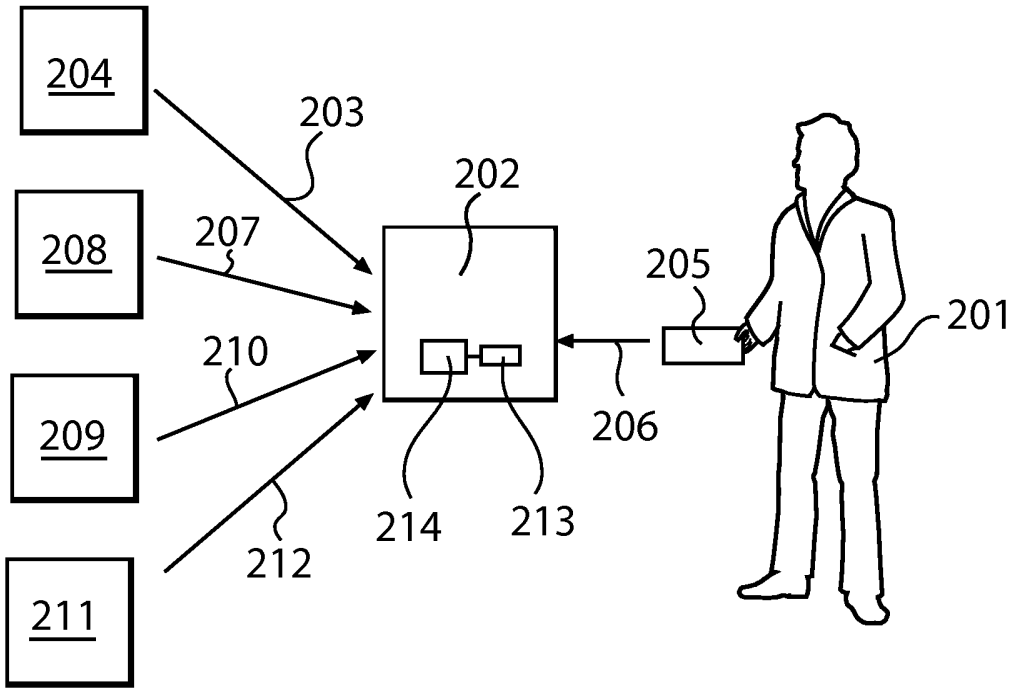


Fig. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2006/050198

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2004/084050 A (KONINKLIJKE PHILIPS ELECTRONICS N.V; CONRADO, CLAUDINE, V; KAMPERMAN,) 30 September 2004 (2004-09-30) abstract page 8, line 13 - line 19 page 9, line 32 - line 30 figure 10	1-17
X	US 6 816 596 B1 (PEINADO MARCUS ET AL) 9 November 2004 (2004-11-09) column 21, line 18 - line 52 column 24, line 52 - column 27, line 43 figure 8	1-17

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 June 2006	29/06/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Horn, M.P.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2006/050198

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2004084050 A	30-09-2004	NONE	
US 6816596 B1	09-11-2004	AU 6927800 A	24-07-2001
		WO 0152019 A1	19-07-2001