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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 April 2006 (27.04.2006)

PCT

(10) International Publication Number
WO 2006/043784 A1

(51) International Patent Classification:
G06F 17/00 (2006.01)

(21) International Application Number:
PCT/KR2005/003494

(22) International Filing Date: 20 October 2005 (20.10.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10-2004-0084181 20 October 2004 (20.10.2004) KR
10-2005-0033480 22 April 2005 (22.04.2005) KR

(71) Applicants *(for all designated States except US)*: **ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE** [KR/KR]; 161 Gajeong-dong, Yuseong-gu, Daejeon 305-350 (KR). **Inka Entworks. Inc.** [KR/KR]; Haesung Building 5, 747-2 Yeoksam-dong, Kangnam-gu, Seoul 135-925 (KR).

(72) Inventors; and

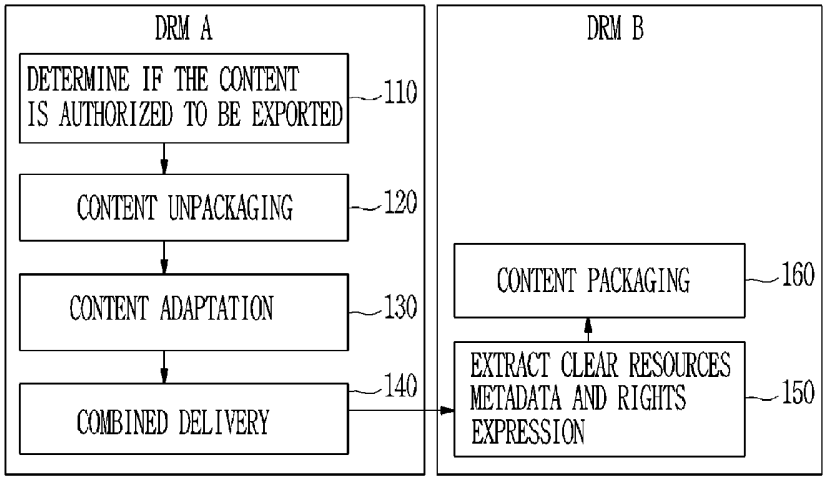
(75) Inventors/Applicants *(for US only)*: **YOON, Ki Song** [KR/KR]; Expo Apt. 204-503, Jeonmin-dong, Yuseong-gu, Daejeon 305-761 (KR). **JEONG, Yeon Jeong** [KR/KR]; 124-17 Yongdoo-dong, Chung-gu, Daejeon 301-832 (KR). **HWANG, Seong Oun** [KR/KR]; 2F., 210-74 Shinsung-dong, Yuseong-gu, Daejeon 305-805 (KR). **NAM, Do Won** [KR/KR]; Yoodeung Maeul Apt. 106-1502, Taepyung-dong, Chung-gu, Daejeon 301-150 (KR). **KIM, Jeong Hyun** [KR/KR]; 103, 162-5 Shinsung-dong, Yuseong-gu, Daejeon 305-805 (KR). **PARK, Ji Hyun** [KR/KR]; Chowon Apt. 103-1110, Manyeun-dong, Seo-gu, Daejeon 302-740 (KR). **JEONG, Sang Won** [KR/KR]; 301, 20 Manyeun-dong, Seo-gu, Daejeon 302-834 (KR). **KIM, Jun Il** [KR/KR]; Keokdong Apt. 108-1003, Hoicheon-eup, Yangju, Kyunggi-do 482-050 (KR). **AHN, Seong Min** [KR/KR]; 7/4, 1113-19 Hwagok-dong, Kangseo-gu, Seoul 157-010 (KR). **KIM, Seong Han** [KR/KR]; Toigye Apt. 363-1903, 18/3, 875 Keumjeong-dong, Gunpo, Kyunggi-do 435-050 (KR). **JANG, Wan Ho** [KR/KR]; Saetbyul Hanyang Apt. 305-209, 1101-8 Bisan-dong, Dongan-gu, Anyang, Kyunggi-do 431-050 (KR).

(74) Agent: **SHIN, Young Moo**; Ace Tower 4th Floor 1-170, Soonhwa-dong, Chung-gu, Seoul 100-130 (KR).

(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,

[Continued on next page]

(54) Title: APPARATUS AND METHOD FOR SUPPORTING CONTENT EXCHANGE BETWEEN DIFFERENT DRM DOMAINS



(57) Abstract: Provided is a system for exchanging contents between a first DRM apparatus and a second DRM apparatus, wherein each of which belongs to different DRM domain. The first DRM apparatus includes unpackaging means for unpackaging first DRM formatted contents into clear resources, metadata, and rights expression; converting means for converting each of the clear resources, metadata, and rights expression into its own predefined neutral format, respectively; generating means for generating neutral formatted contents by combining the converted resources, metadata, and rights expression; adding predetermined header information thereto; and transmitting means for transmitting the neutral-formatted contents to said second DRM apparatus. The second DRM apparatus includes extracting means for extracting clear resources, metadata, and rights expression from the neutral-formatted contents transmitted from said first DRM apparatus; and packaging means for packaging the extracted clear resources, metadata, and rights expression into second DRM formatted contents.

WO 2006/043784 A1

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, KP, 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*

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.

Description

APPARATUS AND METHOD FOR SUPPORTING CONTENT EXCHANGE BETWEEN DIFFERENT DRM DOMAINS

Background Art

[1] 1. Field of the Invention

[2] The present invention relates to digital rights management (DRM) mechanism and, more particularly, to method and apparatus for exchanging contents between different DRM domains.

[3]

[4] 2. Description of Related Art

[5] In general, audio, video and other contents in different DRM domains, which are provided through various wired, wireless, and broadcasting networks such as the Internet and other wireless communications networks, can only be executed by the corresponding DRM devices. Recently, various DRM devices have come into widespread use. However, since they do not provide interoperability and cannot execute the contents governed by different DRM domains, access to various contents is limited. Even though various devices, such as MP3 players, cellular phones, portable audio/video (PAV) devices, etc, are used by the same user, it is impossible to exchange contents between the devices each of which uses different DRM devices. Accordingly, the usefulness of the contents would be restricted. Even if a universal DRM device supporting all DRM formats were developed, since conventional DRM devices are not still compatible with various different DRM formats, users demands for access to various contents will not be satisfied.

[6] Thus, there is an urgent need for mechanism for supporting content exchange between different DRM format devices.

[7] SUMMARY OF THE INVENTION

[8] The present invention is directed to a data structure of neutral- formatted contents that enables contents to be exchanged between different DRM domains.

[9] The present invention is also directed to an apparatus and method for supporting effective content exchange between different DRM format devices by using neutral-formatted contents.

[10] A first aspect of the present invention provides an apparatus for exporting given DRM formatted contents to a target DRM apparatus with a different DRM format. The apparatus comprises means for unpackaging the given DRM formatted contents into clear resources, metadata, and rights expression; means for converting each of the unpackaged clear resources, metadata, and rights expression into its own predefined

neutral format, respectively; and means for generating neutral-formatted contents by combining the converted resources, metadata, and rights expression and adding predetermined header information thereto; and means for transmitting the neutral-formatted contents to the target DRM apparatus.

[11] A second aspect of the present invention provides an apparatus for importing predefined neutral-formatted contents in a given DRM domain, comprising extracting means for extracting clear resources, metadata, and rights expression from the predefined neutral-formatted contents; and packaging means for packaging the extracted clear resources, metadata, and rights expression into the given DRM formatted contents, wherein the given DRM formatted contents are executed by various DRM apparatuses in the given DRM domain.

[12] A third aspect of the present invention provides an apparatus for exporting and importing contents. The apparatus comprises means for unpackaging contents in its own DRM format into clear resources, metadata, and rights expression; means for converting each of the unpackaged clear resources, metadata, and rights expression into a predefined neutral format, respectively; and means for generating neutral-formatted contents by combining the converted resources, metadata, and rights expression and adding predetermined header information thereto; means for transmitting the neutral-formatted contents to different DRM domain; means for extracting clear resources, metadata, and rights expression from neutral-formatted contents transmitted from a different DRM domain; and means for packaging the extracted clear resources, metadata, and rights expression into given DRM formatted contents.

[13] A fourth aspect of the present invention provides a method for exporting given DRM formatted contents to a target DRM apparatus with a different DRM format. The method comprises the steps of unpackaging the given DRM formatted contents into clear resources, metadata, and rights expression; converting each of the unpackaged clear resources, metadata, and rights expression into its own predefined neutral format, respectively; and generating neutral-formatted contents by combining the converted resources, metadata, and rights expression and adding predetermined header information thereto; and transmitting the neutral-formatted contents to the target DRM apparatus.

[14] A fifth aspect of the present invention provides a method of importing predetermined neutral-formatted contents in a given DRM domain, comprising the steps of extracting clear resources, metadata, and rights expression from the predefined neutral formatted contents; and packaging the extracted clear resources, metadata, and rights expression into the given DRM formatted contents, wherein the given DRM formatted contents are executed by various DRM apparatuses in the given DRM

domain.

[15] A sixth aspect of the present invention provides a method of exporting and importing contents, comprising the steps of unpackaging given DRM formatted contents into clear resources, metadata, and rights expression; converting each of the unpackaged clear resources, metadata, and rights expression into its own predefined neutral format, respectively; and generating neutral-formatted contents by combining the converted resources, metadata, and rights expression and adding predetermined header information thereto; transmitting the neutral-formatted contents to a different DRM domain; extracting clear resources, metadata, and rights expression from the neutral-formatted contents transmitted from a different DRM domain; and packaging the extracted clear resources, metadata, and rights expression into given DRM formatted contents.

[16] A seventh aspect of the present invention provides a data structure of a neutral format of contents that are exchangeable between DRM apparatuses in different DRM domains. The data structure comprises header part and body part. The header part includes version of the neutral format; header length; resource encryption algorithm type and resource encryption key; type of hash algorithm applied to the header and the body part and a hash code value; and type of digital signature algorithm and a digital signature value; and the body part includes resources encrypted using the resource encryption algorithm; rights expression in its own predefined neutral format; and metadata in its own predefined neutral format.

[17] An eighth aspect of the present invention provides system for exchanging contents between a first DRM apparatus and a second DRM apparatus, wherein each of which belongs to a different DRM domain. The first DRM apparatus includes unpackaging means for unpackaging first DRM formatted contents into clear resources, metadata, and rights expression; converting means for converting each of the clear resources, metadata, and rights expression into a corresponding neutral format, respectively; generating means for generating neutral formatted contents by combining the converted resources, metadata, and rights expression and adding predetermined header information thereto; and transmitting means for transmitting the neutral-formatted contents to said second DRM apparatus. The second DRM apparatus includes extracting means for extracting clear resources, metadata, and rights expression from the neutral-formatted contents transmitted from said first DRM apparatus; and packaging means for packaging the extracted clear resources, metadata, and rights expression into second DRM formatted contents.

[18]

Brief Description of the Drawings

[19] The above and other features and advantages of the present invention will become more apparent to those of ordinary skill in the art by describing in detail preferred embodiments thereof with reference to the attached drawings in which:

[20] FIG. 1 is a diagram illustrating a process for exchanging contents between different DRM clients according to the present invention.

[21] FIG. 2 is a diagram illustrating the adaptation process according to an exemplary embodiment of the present invention;

[22] FIG. 3 shows a data structure of the contents in a neutral format according to an exemplary embodiment of the present invention;

[23] FIG. 4 shows main components of a source DRM client (DRM A) and a target DRM client (DRM B) for exporting/importing contents according to an exemplary embodiment of the present invention;

[24] FIG. 5 is a diagram illustrating an export/import software authentication process according to an exemplary embodiment of the present invention;

[25] FIG. 6 is a diagram illustrating a key exchange process between the source export/import module and the target export/import module according to an exemplary embodiment of the present invention;

[26] FIG. 7 is a diagram illustrating a device authentication process according to an exemplary embodiment of the present invention; and

[27] FIG. 8 shows a diagram that more specifically illustrates the export/import process between the different DRM clients according to an exemplary embodiment of the present invention.

[28]

[29] DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[30] Before describing the present invention in detail, some terms used in this specification will be defined.

[31] "DRM" stands for digital rights management.

[32] "Clear resources" represent the information that can be rendered in a form that is meaningful to users, such as mp3 files.

[33] "Packaging" refers to an operation for producing contents in which clear resources, metadata and rights expression are combined. Software for performing packaging is called a "packager."

[34] "Unpackaging" refers to an operating for extracting clear resources, metadata and rights expression from the contents. Software for performing unpackaging is called an "Unpackager."

[35] "PAV" stands for portable audio video device. PAVs are used for reproducing/executing audio and/or video contents.

[36] FIG. 1 is a diagram illustrating a process for exchanging contents between different

DRM clients according to the present invention. It is assumed that the DRM A client desires to export (transmit) contents and the DRM B client desires to import (receive) it. As shown in FIG. 1, in step 110, it is checked if the contents have authorization to be exported, by referring to the rights expression contained in the contents.

[37] If the contents have been determined to have authorization to be exported, it is then unpackaged into the clear resources, the metadata, and the rights expression in step 120. The unpackaged clear resources, metadata, and rights expression are respectively converted into each predefined neutral format in step 130. This work is called "content adaptation" in this specification. The content adaptation will be explained in detail later with reference to FIG. 2.

[38] In step 140, the resources, the metadata, and the rights expression in their own neutral format are then combined and the header part for additional information is added thereto, so that the neutral formatted-contents are produced and then encrypted. The neutral formatted-contents are transmitted to the DRM B client. This work is called "combined delivery" in this specification. In combined delivery, there are one header and one body including the neutral-formatted resources, metadata and rights expression. The header includes the locations of the body items so that they can be extracted separately. Hash code value is evaluated based on the header and body, except for a hash code value itself, and the digital signature.

[39] In order to accomplish secure contents transfer between the different DRM domains, the neutral-formatted contents are encrypted using, for example, a public key infrastructure (PKI) mechanism or a key sharing mechanism. A basic algorithm necessary to encrypt the contents may include an asymmetric encryption algorithm for secure key transfer and integrity check (e.g., RSA), a resource encryption algorithm (e.g., AES-128), and a hash algorithm (e.g., SHA-1). It is noted that such encryption algorithms are exemplary, and the different algorithms can be selected with the negotiation between source and target DRM clients. In one embodiment, the selected algorithms may be specified in the header part or is reported to the target client through message exchange between the source and target clients.

[40] The DRM B client, which desires to import the neutral-formatted contents, receives and unpackages it into the clear resources, the metadata, and the rights expression (step 150). The extracted clear resources, metadata and rights expression are then re-packaged for adaptation to the DRM B client (step 160). Accordingly, the re-packaged contents can be executed or reproduced by DRM B format devices.

[41] FIG. 2 is a diagram illustrating the adaptation process according to an exemplary embodiment of the present invention. As shown in FIG. 2, the adaptation process 200 for producing the neutral-formatted contents may include a resource adaptation process 210, a rights expression adaptation process 220, and a metadata adaptation process 23

0. For each adaptation according to the present invention, the corresponding neutral format is defined. It should be guaranteed that the adaptation process 200 takes place in a trusted environment.

[42] The resource adaptation process 210 is the process in which the clear resources received from the source DRM client is converted into predefined neutral-formatted resources, which are not dependent on the specific DRM format devices. The resource adaptation process 210 randomly generates a content encryption key (CEK) to encrypt the clear resources using an encryption algorithm such as AES-128. The key used for encryption may be inserted into the rights expression in the neutral-formatted contents. Hash is evaluated based on both a header and a body, excluding the hash code and the digital signature, and written in the hash code field of the header part. The hash code information is digitally signed using a private key and saved in the digital signature field.

[43] The rights expression adaptation process 220 converts the given rights expression into the corresponding predefined neutral format. In this embodiment, MPEG-21 rights expression language (REL) is used as the neutral format of rights expression. The neutral rights expression can be added or missed depending on the policy or right existence of a source DRM domain and a target DRM domain.

[44] The metadata adaptation process 230 converts the given metadata into the corresponding predefined neutral format. In this embodiment, Dublin Core may be used as the neutral format of metadata. Alternatively, metadata not included in Dublin Core can also be specified in extended XML format with Dublin Core expression. The metadata in extended XML can be recognized by the specific DRM client. The neutral metadata can be added or missed depending on the policy or metadata existence of source DRM domain and target DRM domain.

[45] FIG. 3 shows a data structure of the contents in a neutral format according to an exemplary embodiment of the present invention. As shown in FIG. 3, the data structure of the contents in the neutral format can be adapted to be exchanged between different DRM domains. The data structure of the contents may be composed of a header part 310 and a body part 320. In the header part 310, neutral format version, header length, hash code value calculated based on the header 310 and body 320, resource (or contents) encryption key, a type of encryption algorithm used for encryption of the resources, a digital signature, locations of body items (i.e., resources, rights expression, and metadata), etc. For example, AES-128 may be used as a resource encryption algorithm, and SHA-1 may be used as a hash algorithm for producing the hash code value. However, the fields in the header 310 are not limited to such fields, and some of them may be changed or new fields may be added thereto according to agreement between the DRM format devices.

[46] The body 320 contains the encrypted resources in its own neutral format, the rights expression in its own neutral format, and the metadata in its own neutral format, which have been produced via the content adaptation process 200. In one embodiment, the predefined neutral format of the rights expression may be the MPEG-21 REL, and the predefined neutral format of the metadata may be the Dublin Core metatag.

[47] FIG. 4 shows main components of a source DRM client (DRM A) and a target DRM client (DRM B) for exporting/importing contents according to an exemplary embodiment of the present invention. As shown in FIG. 4, the DRM A and DRM B clients 400a and 400b may be data processing system which can produce, manage, export, import and/or execute contents in corresponding formats. For example, the DRM A and DRM B clients may include a PC, a PDA, a cellular phone, etc.

[48] The DRM A client 400a includes an unpackaging module 410a for unpackaging DRM A formatted contents into the clear resources, the rights expression and the metadata; an export/import module 420a for exporting/importing the contents from/to a different DRM client (for example, DRM B client 400b); and a packaging module 430a for packaging the clear resources, the metadata, and the rights expression into the DRM A-formatted contents. In one embodiment, the unpackaging module 410a checks whether or not the DRM A formatted contents have authorization to be exported to the different DRM client, such as DRM B client, and then unpackages only the contents authorized to be exported.

[49] Specifically, the export/import module 420a may include an export submodule 421a and an import submodule 422a. The export submodule 421a packages the clear resources, the metadata, and the rights expression, which have been extracted from the DRM A-formatted contents by the unpackaging module 410a, into the neutral-formatted contents and transmit (or export) it to the target DRM client, i.e., the DRM B client 400b. The import submodule 422a receives (imports) the neutral-formatted contents from the DRM B client and then extracts from it the clear resources, the metadata, and the rights expression. In addition, the export submodule 421a may perfo rm authentication for the target DRM client. Also, in order to safely export the contents, it may authenticate the export/import module at the target DRM client.

[50] The packaging module 430a serves to package the clear resources, the metadata, and the rights expression extracted by the import module 422a into the DRM A-formatted contents.

[51] The DRM B client 400b has substantially the same configuration as the DRM A client 400a, and thus the description thereof is omitted. The drawings are intended to help the understanding of the export/import concept according to the present invention and should not be construed as limiting the physical configuration of the present invention. For example, FIG. 4 shows that the export/import modules 420a and 420b

are installed on the DRM A client 400a and the DRM B client 400b, respectively, but the export/import modules could be implemented as an independent device (e.g., export/import server), separate from the DRM clients. In addition, although FIG. 4 shows that contents are exchanged between two different DRM clients, it could be easily understood that the contents may be exchanged among a plurality of different DRM clients, by using the data structure of the neutral format.

[52] FIG. 5 is a diagram illustrating an export/import software authentication process according to an exemplary embodiment of the present invention. The source export/ import software and the target export/import software, which are separately installed in the different DRM clients, authenticate each other for the security purpose, before exchanging the key or communicating each other. Also, it should be confirmed whether both of them are tampered or not. As shown in FIG. 5, the authentication between the export/import software may be performed using a certificate authority (CA) server.

[53] FIG. 6 is a diagram illustrating a key exchange process between the source export/ import module and the target export/import module according to an exemplary embodiment of the present invention. When they send and receive messages, the messages should be encrypted for secure transfer against eavesdrops or attacks. Please note that the authentication of the source/target software and devices should be done in advance.

[54] Since the exchange of a content encryption key (CEK) in clear text format between the two modules is not safe, the following two ways may be considered: certificate-based CEK 610 exchange and shared key mechanism for producing the same key at both sides, without exchanging a key, such as Diffie-Hellman algorithm.

[55] FIG. 7 is a diagram illustrating a device authentication process according to an exemplary embodiment of the present invention. Device authentication is to check the target PAV device has been authorized to execute the imported contents. In this embodiment, device authentication is performed based on the export/import access control list. Since the export/import process is to exchange contents over different DRM domains, the process should be under the control depending on business policies and/or technical requirements. In one embodiment, the (source) export/import module 710 of DRM A client first requests from the (target) export/import module 720 for a device certificate of the DRM B format device 740 connected to a device I/O module 730. Assume that the device certificate has been inserted into the device. The (target) export/import module 720 then transmits the device certificate (or identifier) of the DRM B format device 740 to the (source) export/import module 710. The (source) export/import module 710 authenticates the device by checking the device certificate with the export/import access control list. In other embodiment, instead of a device

certificate, a device identifier, which has been assigned by a device-identifying server (not shown), may be used to perform device authentication.

[56] In the export/import access control list, for each of access control items, it is listed if it is permitted to be exported/imported. The access control items may include devices with different vendors, models, or versions and/or DRM software with different vendors, models, or versions. The export/import access control list may be downloaded from a related server and updated periodically or non-periodically. Alternatively, the export/import module may access the related server to access the list during the device authentication process.

[57] FIG. 8 shows a diagram that more specifically illustrates the export/import process between the different DRM clients according to an exemplary embodiment of the present invention. For convenience, it is assumed the contents are exported from the (source) DRM A client 400a to the (target) DRM B client 400b.

[58] Content purchase: (1)

[59] (1) The DRM A client 400a purchases and downloads DRM A-formatted contents from a DRM content provider (server). In this embodiment, before exporting the downloaded DRM A-formatted contents, the (source) DRM A client checks whether it is authorized to be exported, based on the rights expression in the contents.

[60] Software authentication: (2)

[61] (2) For the sake of safe content exchange, authentication is performed between the source export/import module 420a of the DRM A client and the target export/import module 420b of the DRM B client.

[62] Device authentication: (3) ~ (6)

[63] (3) The source export/import module requires the device ID of the DRM B format device connected to the DRM B client, via the target export/import module 420b.

[64] (4) The target export/import module 420b then sends the device ID to the source export/import module 420a.

[65] (5)-(6) The source export/import module 420a authenticates the DRM B format device based on the export/import access control list.

[66] Key exchange between export/import modules: (7)

[67] (7) For security, the key may be exchanged between the source and target export/import modules 420a and 420b.

[68] Export/Import: (8) ~ (12)

[69] (8) The unpackaging module 410a of the DRM A client unpackages the DRM A-formatted contents into the clear resources, metadata, and rights expression and then sends them to the source export/import module 420a.

[70] (9) The source export/import module 420a packages the clear resources, metadata and right expression into the neutral format, via the adaptation process, and sends it to

the target export/import module 420b.

[71] (10) The target export/import module 420b receives the neutral-formatted contents and extracts the resources, the metadata, and the rights expression from it. It then sends the results to the packaging module 430b.

[72] (11) The packaging module 430b packages then into the DRM B formatted contents, which is executable by the DRM B format device, and sends it to the device I/O module.

[73] (12) The device I/O module transmits it to the DRM B format device.

[74] The present invention can be provided in the form of computer code stored on computer-readable recording media such as floppy disks, hard disks, CD ROMs, flash memory cards, PROM RAM, ROM, and magnetic tape, which can be implemented on one or more different types of products. The computer code may be written in a programming language such as C, C++, or JAVA.

[75] As described above, the present invention provides the content structure having the neutral format for content exchange between the different DRM format devices and the export/import method and device using the same. According to the present invention, by exchanging the contents of the different DRM formats, use of various contents can be supported to thereby satisfy demands of users, convenience of users is increased, and practical use of the contents is also increased.

[76] Although exemplary embodiments of the present invention have been described with reference to the attached drawings, the present invention is not limited to these embodiments, and it should be appreciated to those skilled in the art that a variety of modifications and changes can be made without departing from the spirit and scope of the present invention.

[77]

Claims

[1] An apparatus for exporting given DRM formatted contents to a target DRM apparatus with a different DRM format, the apparatus comprising:
means for unpackaging the given DRM formatted contents into clear resources, metadata, and rights expression; and
means for converting each of the unpackaged clear resources, metadata, and rights expression into its predefined neutral format, respectively; and
means for generating neutral-formatted contents by combining the converted resources, metadata, and rights expression and adding predetermined header information thereto; and
means for transmitting the neutral-formatted contents to the target DRM apparatus.

[2] The apparatus of claim 1, further comprising means for determining whether the given DRM formatted contents are authorized to be exported or not.

[3] The apparatus of claim 1, wherein said converting means includes means for encrypting the resources using a predetermined encryption algorithm and inserting a resource encryption key into the predefined neutral-formatted rights expression.

[4] The apparatus of claim 3, wherein the predetermined resources encryption algorithm includes AES-128.

[5] The apparatus of claim 1, wherein the predefined neutral format of the rights expression is MPEG-21 REL.

[6] The apparatus of claim 1, wherein the predefined neutral format of the metadata is Dublin Core format.

[7] The apparatus of claim 1, wherein the metadata not included in the predefined neutral format is specified in extended XML format with Dublin Core format.

[8] The apparatus of claim 1, further comprising encryption means for encrypting the neutral-formatted contents.

[9] The apparatus of claim 8, wherein said encryption means encrypts the neutral-formatted contents using a public key infrastructure (PKI) encryption algorithm.

[10] The apparatus of claim 9, wherein said encryption means evaluates a hash code value on the neutral-formatted contents, records the hash code value in a hash code field of the header, digitally signs the hash code value using a private key, and records the digitally signed hash code value in a digital signature field of the header.

[11] The apparatus of claim 9, further comprising means for transmitting a resource encryption key encrypted by using the public key of the target apparatus to the

target DRM apparatus.

[12] The apparatus of claim 7, wherein said encryption means encrypts the neutral-formatted contents based on a shared key encryption algorithm.

[13] The apparatus of claim 1, further comprising a device authentication means for authenticating a device that is connected to the target DRM apparatus to execute the contents.

[14] The apparatus of claim 13, wherein said device authentication means authenticates the device by checking a device certificate, which has been inserted into the device, with an export/import control list provided by a related server.

[15] The apparatus of claim 12, wherein said device authentication means authenticates the device by checking a device identifier, which has been assigned to the device by a device identifying server, with an export/import control list provided by a related server.

[16] An apparatus for importing predefined neutral-formatted contents in a given DRM domain, comprising:
extracting means for extracting clear resources, metadata, and rights expression from the predefined neutral-formatted contents; and
packaging means for packaging the extracted clear resources, metadata, and rights expression into the given DRM formatted contents;
wherein the given DRM formatted contents are executed by various DRM apparatuses in the given DRM domain.

[17] The apparatus of claim 16, wherein said extracting means includes means for decrypting the neutral-formatted contents.

[18] An apparatus for exporting and importing contents, comprising:
means for unpackaging contents in its own DRM format into clear resources, metadata, and rights expression;
means for converting each of the unpackaged clear resources, metadata, and rights expression into its own predefined neutral format, respectively; and
means for generating neutral-formatted contents by combining the converted resources, metadata, and rights expression and adding predetermined header information thereto;
means for transmitting the neutral-formatted contents to a different DRM domain;
means for extracting clear resources, metadata, and rights expression from neutral-formatted contents transmitted from a different DRM domain; and
means for packaging the extracted resources, metadata, and rights expression into contents in its own DRM format.

[19] A method for exporting given DRM formatted contents to a target DRM

apparatus with a different DRM format, the method comprising the steps of:
unpackaging the given DRM formatted contents into clear resources, metadata, and rights expression;
converting each of the unpackaged clear resources, metadata, and rights expression into its own predefined neutral format, respectively; and
generating neutral-formatted contents by combining the converted resources, metadata, and rights expression and adding predetermined header information thereto; and
transmitting the neutral-formatted contents to the target DRM apparatus.

[20] The method of claim 19, further comprising the step of determining whether the given DRM formatted contents are authorized to be exported or not.

[21] The method of claim 19, wherein said converting step includes the step of encrypting the resources using a predetermined encryption algorithm and inserting an encryption key into the predefined neutral-formatted rights expression.

[22] A method of importing predefined neutral-formatted contents in a given DRM domain, comprising the steps of:
extracting clear resources, metadata, and rights expression from the predefined neutral formatted contents; and
packaging the extracted clear resources, metadata, and rights expression into the given DRM formatted contents;
wherein the given DRM formatted contents are executed by various DRM apparatuses in the given DRM domain.

[23] A method of exporting and importing contents, comprising the steps of:
unpackaging given DRM formatted contents into clear resources, metadata, and rights expression;
converting each of the unpackaged clear resources, metadata, and rights expression into its own predefined neutral-format, respectively;
generating neutral-formatted contents by combining the converted resources, metadata, and rights expression and adding predetermined header information thereto;
transmitting the neutral-formatted contents to a different DRM domain;
extracting clear resources, metadata, and rights expression from the neutral-formatted contents transmitted from a different DRM domain; and
packaging the extracted clear resources, metadata, and rights expression into given DRM formatted contents.

[24] A data structure of a neutral format of contents that are exchangeable between DRM apparatuses in different DRM domains, wherein the data structure

comprising header part and body part, the header part including:
version of the neutral format;
header length;
resource encryption algorithm type and a resource encryption key;
type of hash algorithm applied to the header part and the body part and a hash code value; and
a type of digital signature algorithm and a digital signature value; and
the body part including:
resources encrypted using the resource encryption algorithm;
rights expression in its own predefined neutral format; and
metadata in its own predefined neutral format.

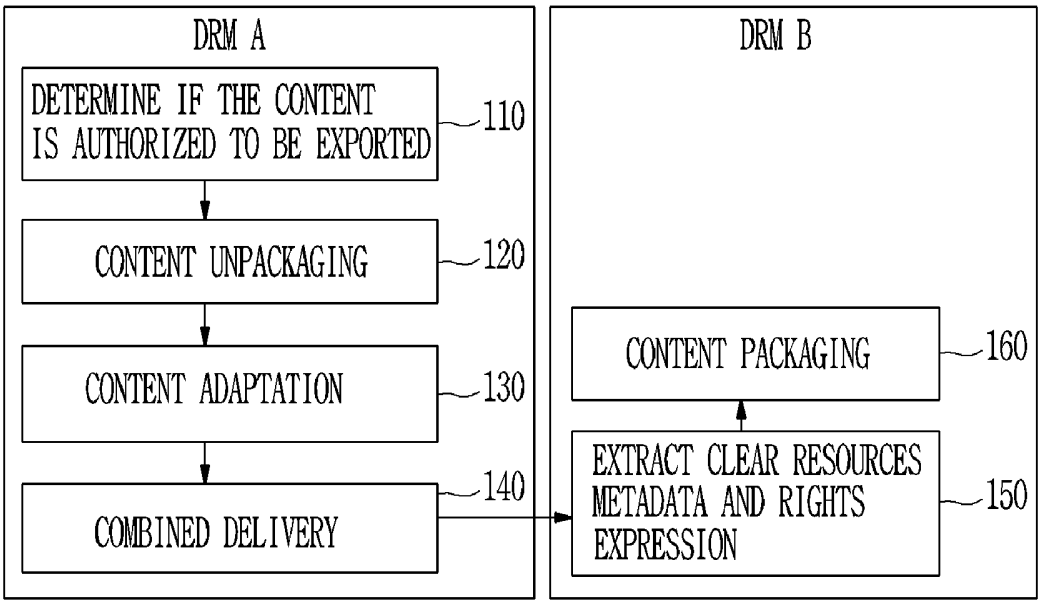
[25] A system for exchanging contents between a first DRM apparatus and a second DRM apparatus, wherein each of which belongs to a different DRM domain, said first DRM apparatus including:
unpackaging means for unpackaging first DRM formatted contents into clear resources, metadata, and rights expression;
converting means for converting each of the clear resources, metadata, and rights expression into its own predefined neutral format, respectively;
generating means for generating neutral formatted contents by combining the converted resources, metadata, and rights expression; adding predetermined header information thereto; and
transmitting means for transmitting the neutral-formatted contents to said second DRM apparatus; and
said second DRM apparatus including:
extracting means for extracting clear resources, metadata, and rights expression from the neutral-formatted contents transmitted from said first DRM apparatus; and
packaging means for packaging the extracted clear resources, metadata, and rights expression into second DRM formatted contents.

[26] The system of claim 25, wherein said exporting means of said first DRM apparatus performs authentication of said importing means of said second DRM apparatus, before transmitting the neutral-formatted contents to said second DRM apparatus.

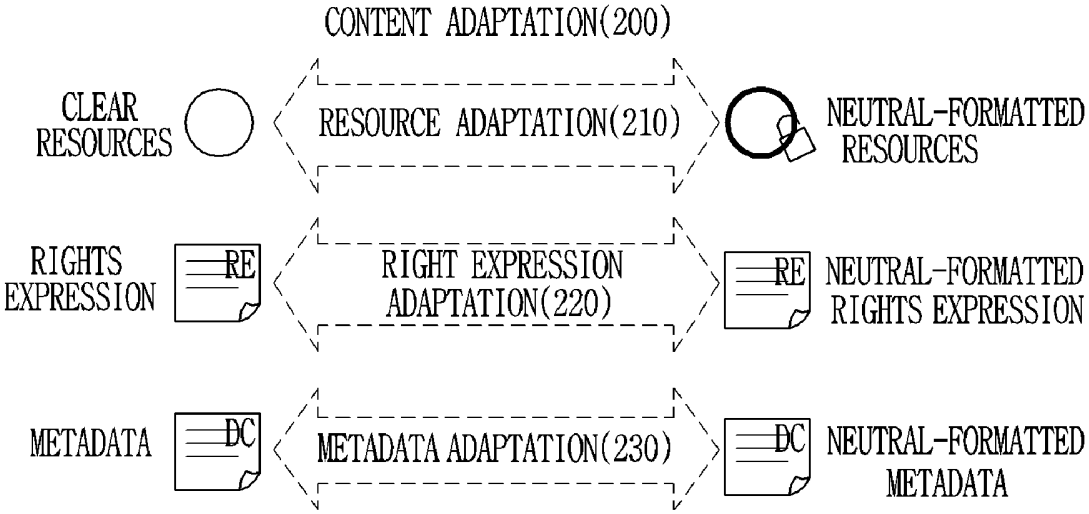
[27] The system of claim 26, wherein the authentication is performed by a certificate authority server.

WO 2006/043784 PCT/KR2005/003494

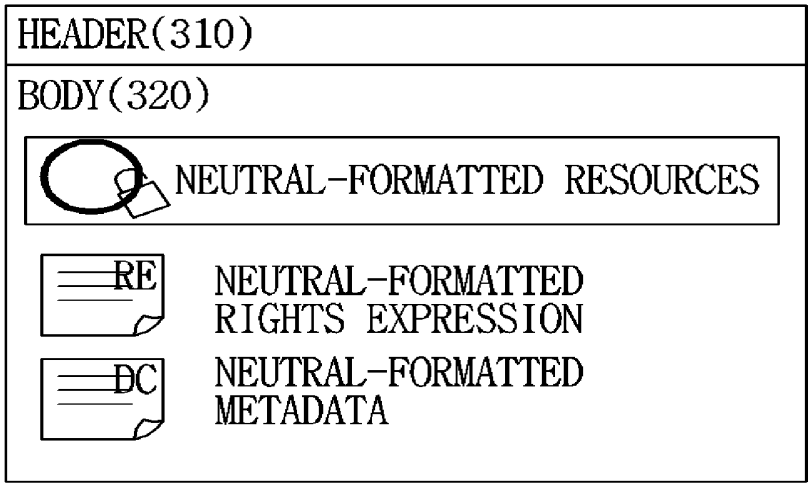
[Fig. 1]



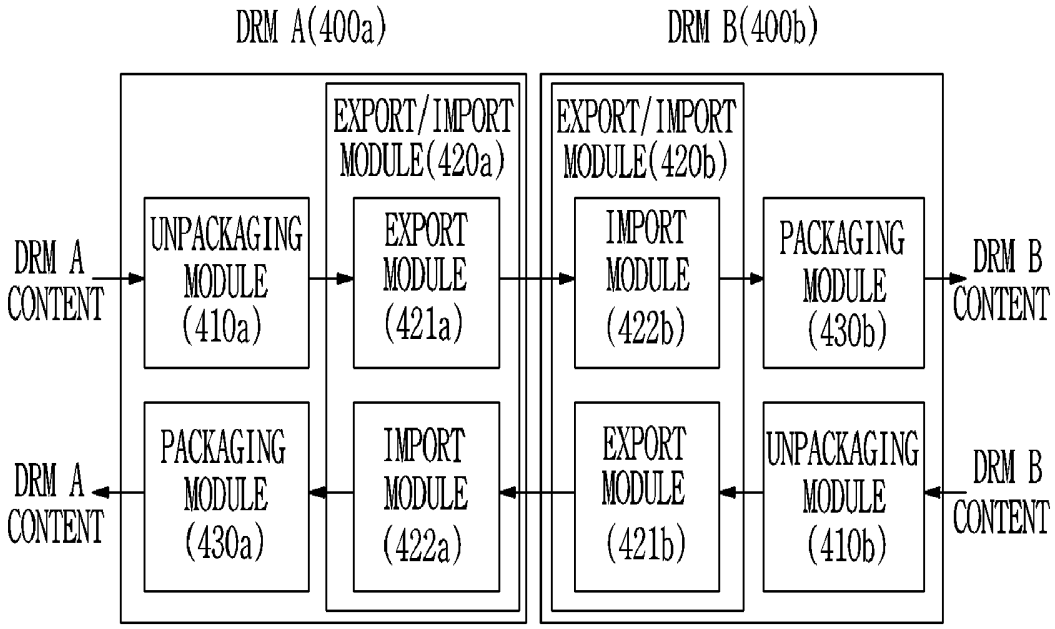
[Fig. 2]



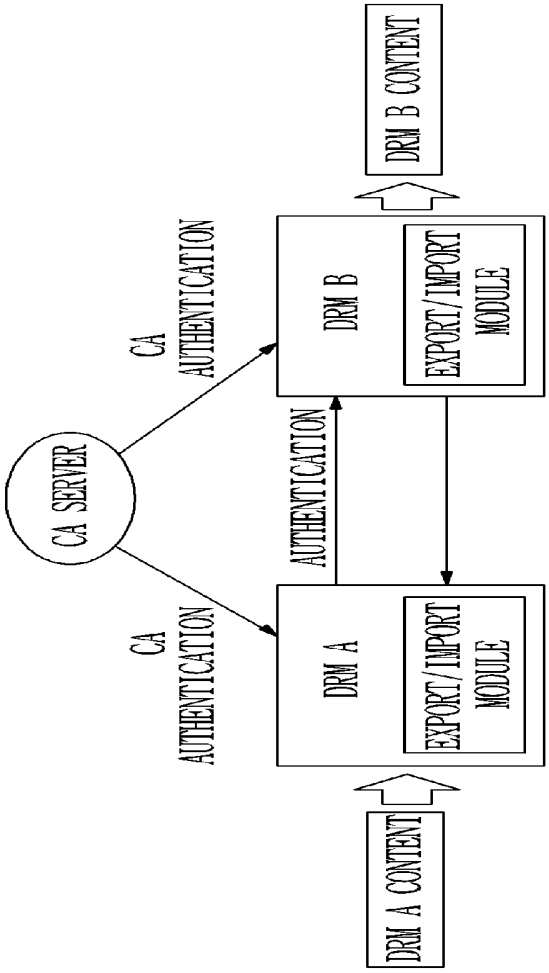
[Fig. 3]



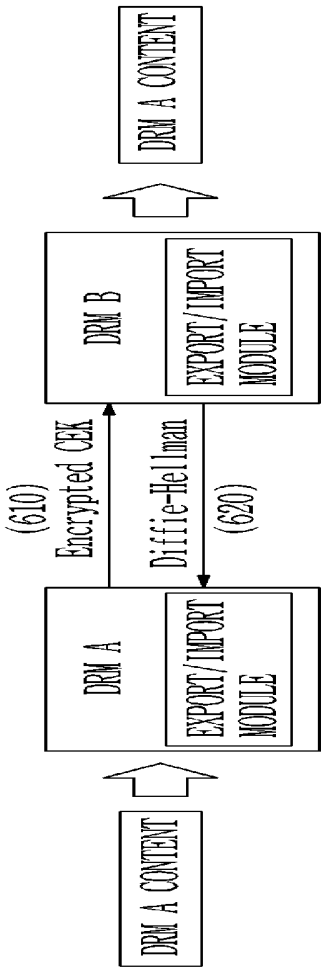
[Fig. 4]


DRM A(400a)
DRM B(400b)
EXPORT/IMPORT MODULE(420a)
EXPORT/IMPORT MODULE(420b)
DRM A CONTENT
UNPACKAGING MODULE (410a)
EXPORT MODULE (421a)
IMPORT MODULE (422b)
PACKAGING MODULE (430b)
DRM B CONTENT
DRM A CONTENT
PACKAGING MODULE (430a)
IMPORT MODULE (422a)
EXPORT MODULE (421b)
UNPACKAGING MODULE (410b)
DRM B CONTENT

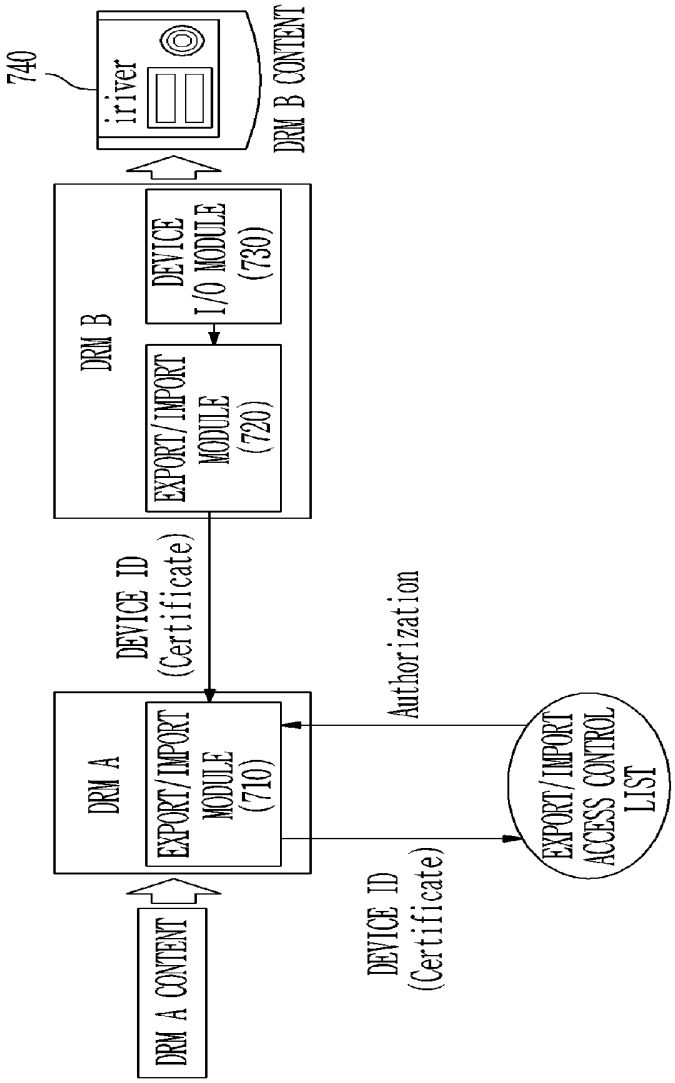
[Fig. 5]


DRM B CONTENT
DRM B
EXPORT/IMPORT MODULE
CA AUTHENTICATION
CA SERVER
AUTHENTICATION
CA AUTHENTICATION
DRM A
EXPORT/IMPORT MODULE
DRM A CONTENT

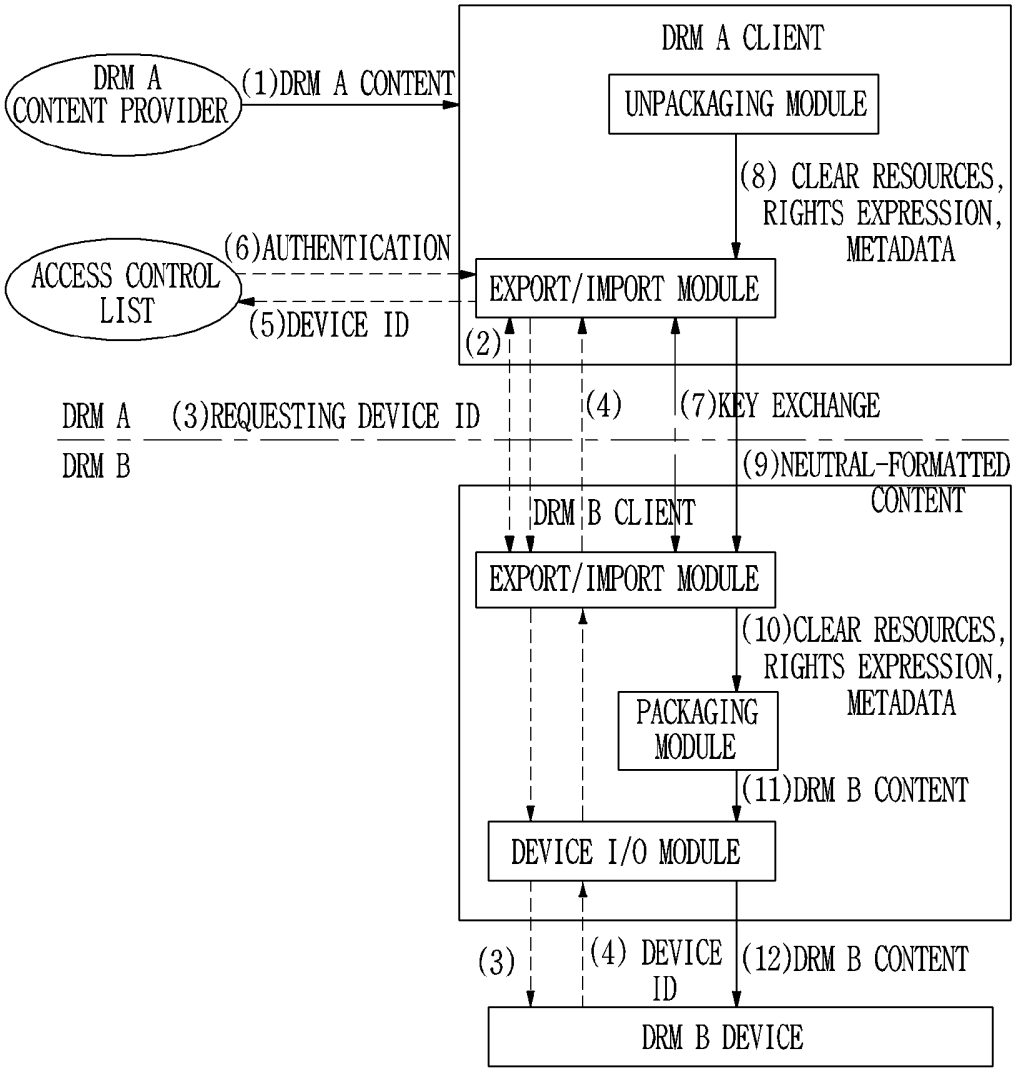
[Fig. 6]


DRM A CONTENT
DRM B
EXPORT/IMPORT MODULE
(610) Encrypted CEK
Diffie-Hellman (620)
DRM A
EXPORT/IMPORT MODULE
DRM A CONTENT

[Fig. 7]


740
iriver
DRM B CONTENT
DRM B
DEVICE I/O MODULE (730)
EXPORT/IMPORT MODULE (720)
DEVICE ID (Certificate)
Authorization
DRM A
EXPORT/IMPORT MODULE (710)
EXPORT/IMPORT ACCESS CONTROL LIST
DRM A CONTENT
DEVICE ID (Certificate)

[Fig. 8]


DRM A CONTENT PROVIDER
(1)DRM A CONTENT
DRM A CLIENT
UNPACKAGING MODULE
(8) CLEAR RESOURCES, RIGHTS EXPRESSION, METADATA
(6)AUTHENTICATION
ACCESS CONTROL LIST
(5)DEVICE ID
EXPORT/IMPORT MODULE
(2)
DRM A
DRM B
(3)REQUESTING DEVICE ID
(4)
(7)KEY EXCHANGE
(9)NEUTRAL-FORMATTED CONTENT
DRM B CLIENT
EXPORT/IMPORT MODULE
(10)CLEAR RESOURCES, RIGHTS EXPRESSION, METADATA
PACKAGING MODULE
(11)DRM B CONTENT
DEVICE I/O MODULE
(3)
(4) DEVICE ID
(12)DRM B CONTENT
DRM B DEVICE

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2005/003494

A. CLASSIFICATION OF SUBJECT MATTER

G06F 17/00(2006.01)i

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)

IPC8 G06F17/00

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

Korean patents and applications for inventios since 1975

Electronic data base consulted during the intertnational search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 2002-19806 A (SAMSUNG ELECTRONICS INC.) 13 MAR. 2002 SEE THE WHOLE DOCUMENTS	1-27
A	KR 2002-73035 A (SAMSUNG ELECTRONICS INC.) 9 SEP. 2002 SEE THE WHOLE DOCUMENTS	1-27
A	KR 2002-83851 A (MARKANY INC.) 4 NOV. 2002 SEE THE WHOLE DOCUMENTS	1-27
A	KR 2004-34165 A (KOREA TELECOMMUNCATION RESEARCH INS.) 28 APR. 2004 SEE THE WHOLE DOCUMENTS	1-27

☐ 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 application or patent 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 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
27 JANUARY 2006 (27.01.2006)	**27 JANUARY 2006 (27.01.2006)**

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
920 Dunsan-dong, Seo-gu, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

JEONG, Jae Hoon

Telephone No. 82-42-481-5787