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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 June 2006 (22.06.2006)

PCT

(10) International Publication Number
WO 2006/065012 A1

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number:
PCT/KR2005/002265

(22) International Filing Date: 14 July 2005 (14.07.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10-2004-0107261
16 December 2004 (16.12.2004) KR

(71) Applicant *(for all designated States except US)*: **ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE** [KR/KR]; 161, Gajeong-dong, Yuseong-gu, Daejon 305-350 (KR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PARK, Jee-Hyun** [KR/KR]; #103-1305 Sang-a Apt., Mannyeon-dong, Seo-gu, Daejeon 302-739 (KR). **JEONG, Yeon-Jeong** [KR/KR]; 124-17, Yongdu-dong, Jung-gu, Daejeon 301-832 (KR). **HWANG, Seong-Oun** [KR/KR]; 2nd floor, 210-74, Sinseong-dong, Yuseong-gu, Daejeon 305-805 (KR). **NAM, Do-Won** [KR/KR]; #1-318 dorm., 161, Gajeong-dong, Yuseong-gu, Daejeon 305-350 (KR). **KIM, Jung-Hyun** [KR/KR]; #2-201 Jinyang Apt., 700-2, Sotae-dong, Dong-gu, Gwangju 501-829 (KR). **YOON, Ki-Song** [KR/KR]; #204-503 Expo Apt., Jeonmin-dong, Yuseong-gu, Daejeon 305-761 (KR). **KIM, Jun-Il** [KR/KR]; #109-1003 Deokjeong Kukdong Apt., Deokjeong-dong, Yangju-si, Gyeonggi-do 482-707 (KR). **JEONG, Sang-Won** [KR/KR]; #301, 20, Mannyeon-dong, Seo-gu, Daejeon 302-834 (KR).

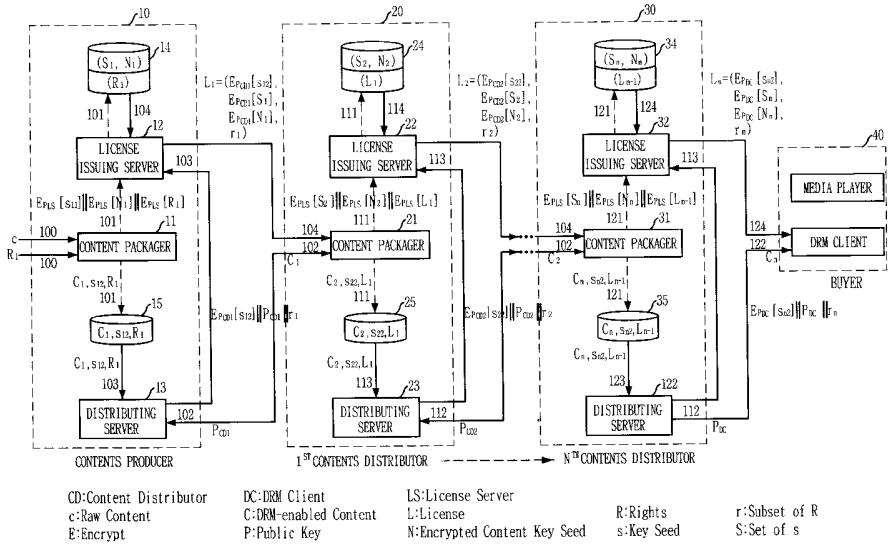
(74) Agent: **SHINSUNG PATENT FIRM**; 2-3F, Line Bldg., 823-30, Yeoksam-dong, Kangnam-ku, Seoul 135-080 (KR).

(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, 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, 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),

[Continued on next page]

(54) Title: SYSTEM FOR ISSUING LICENSES TO PROTECT MULTI-LEVEL DISTRIBUTED DIGITAL CONTENTS AND METHOD THEREOF



(57) Abstract: Provided is a system for issuing licenses to protect multi-level distributed digital contents and a method thereof . The system for issuing licenses includes: a content packaging unit for packaging a target content to distribute and requesting a license issuing server to issue a license for the target content; the licensing issuing unit for issuing a license that contains information about rights for using a target content and information about decrypting a content according to the request of a distributing unit; the distributing unit for requesting the license issuing unit to issue a license according to a content purchasing request of purchaser; and a database for storing information about contents, key seeds and rights.

WO 2006/065012 A1

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.

SYSTEM FOR ISSUING LICENSES TO PROTECT MULTI-LEVEL DISTRIBUTED DIGITAL CONTENTS AND METHOD THEREOF

Description

Technical Field

The present invention relates to a system for issuing licenses to protect multi-level distributed digital contents and a method thereof; and more particularly, to a system for issuing licenses to protect multi-level distributed digital contents, which allows multi-level distribution of the contents while protecting the contents from being forged or modified at each distribution stage by supporting a multi-packaging and a multi-licensing, and a method thereof.

Background Art

Licenses are documents made of an extensible markup language (XML) which contains information for a user to consume secured contents. The license includes decryption keys and encryption options to decrypt the secured contents, and a digital signature using a issuer's certificate in order to protect the contents from being forged during being transmitted.

Various digital methods for producing multimedia contents were introduced and various tools thereof have been generalized. Accordingly, it is very easy to produce multimedia contents, nowadays. Popularization of high speed Internet has brought huge variation in a structure of consuming the multimedia contents. Furthermore, high speed wireless communication network has been expanding due to popularization of a mobile phone and a personal data assistance (PDA). It is expected that such evolution will be accelerated even faster.

In order to support such evolution of digital generation, infrastructure technologies must be developed to transfer, consume and distribute digital contents not only through the Internet but also through a wireless communication network and digital television. The infrastructure technologies must provide providers, distributors and users with means to solve problems such as compatibilities, intellectual property rights protection, and soundness of distribution structure effectively.

Digital rights management (DRM) is a technology to protect intellectual property rights of digital contents. Based on the DRM, the digital contents are protected by encryption and then licenses are issued to authorized users with an encryption key to decrypt the contents.

A content packaging is a process that creates secured contents based on DRM, and such a secured content created through the content packaging is called as a secure container. The secure container includes encrypted contents, metadata related contents and business rules.

Currently, DRM based digital contents are generally distributed with only consideration of one to one relation between a distributor and a consumer for encrypting contents, creating related metadata, packaging contents and issuing licenses. Since there is no contents protection scheme throughout entire distribution channel from the contents producer to the consumer, the protection of the contents at each of the distribution channel relies on conscience and law.

Therefore, a systemic protection of contents is required. The systemic protection of contents allows that the distributors supply various types of contents one another and that the distributors provide identical contents to the consumers with different conditions to satisfy the consumer. Such a systemic protection of contents is expected to vitalize the digital contents

market.

One of main reasons of limitation of the existing DRM to apply into the digital contents for multi-level distribution is that an encryption key included in the DRM based license cannot be applied into the multi-level distribution. If the DRM is applied into the multi-level distribution, encrypted contents must be decrypted in each stage of distribution and a new packaging must be performed to encrypt the decrypted contents with newly created encryption keys. In this case, the original contents may be outflow due to the decryption in each distribution stage, and it is easy to delete information of original distributor or to forge the contents during the re-packaging.

Therefore, the contents encryption key must be securely distributed and managed to protect the contents at each distribution stage, and the forgery of the packaged contents or the license thereof must be verified at each distribution stage.

Disclosure

Technical Problem

It is, therefore, an object of the present invention to provide a system for issuing licenses to protect multi-level distributed digital contents, which allows multi-level distribution of the digital contents while protecting the digital contents from being forged or modified at each distribution stage by supporting a multi- packaging and a multi- licensing, and a method thereof.

Technical Solution

In accordance with one aspect of the present invention, there is provided a system for issuing a license

for a multi-level distribution of content, including: a content packaging unit for packaging a target content to distribute and requesting a license issuing server to issue a license for the target content; the licensing issuing unit for issuing a license that contains information about rights for using a target content and information about decrypting the content according to the request of a distributing unit; the distributing unit for requesting the license issuing unit to issue a license according to a content purchasing request from a purchaser; and a database for storing information about contents, key seeds and rights.

In accordance with another aspect of the present invention, there is provided a method of issuing a license for multi-level distribution of content, the method including the steps of: a) generating a license key for a target content to distribute at a content packager; b) transmitting a base license issued from an external system and the generated license key information to a license issuing server from the content packager; c) receiving a content purchasing request from a purchaser and requesting the license issuing server to issue a license at a distributing server; and d) checking a validity of the license issuing request, generating an new license and transmitting the generated license to the purchaser at the license issuing server.

Advantageous Effects

The present invention supports the multi-packaging and the multi-licensing for contents. That is, if one of distributors initially packages a content and issues a license thereof, a next distributor is also allowed to repackage the content by resetting rights and conditions for own and distributes the repackaged content. Since

distributors are allowed to sell the repackaged content to other distributors or to consumers directly, the multi-level distribution can be applied into the content distribution market. As a result, it is possible to effectively sell the content. Also, various conditions of different distributors can be applied to a same content, and rights of previous level distributors can be protected according to the present invention.

If the multi-level distribution is applied into the content market according to the present invention, the distributors are allowed to sell the content to a consumer by buying a target content from other distributors. Such a way of selling and buying content is convenient to the consumer and the distributor at the same time. That is, the consumer is not required to find one having a target content among many distributors. Although a distributor wants sell a content that the distributor does not have, the distributor are not required to perform complicated operations such as buying a target packaged content from other distributor, un-packaging content, and then creating metadata and packaging again. Therefore, the content buying and selling are effectively achieved for distributors as well as consumers.

When a multi-level license is issued to distributors participating for distributing an identical content, the distributors are allowed set own rules of using contents into the content according to the present invention. Therefore, a multi-rule business is allowed and the rights of previous level distributor can be also protected.

According to the present invention, the encryption key of content is managed based on distributed management scheme instead of central management scheme. Such a way of managing the encryption key prevents the encryption key from being outflow.

According to the present invention, rights of

distributor can be controlled using a license having information about the content. Therefore, a distributor A is allowed to set selling conditions for a content within rights defined in the own license, and a distributor B who bought the content from A is allowed to sell the content within rights defined by the distributor A.

Description of Drawings

The above and other objects and features of the present invention will become apparent from the following description of the preferred embodiments given in conjunction with the accompanying drawings, in which:

Fig. 1 is a block diagram illustrating a system for issuing a license to protect digital contents distributed in multi-level in accordance with a preferred embodiment of the present invention;

Fig. 2 is a block diagram showing a secure container in accordance with a preferred embodiment of the present invention;

Fig. 3 is a block diagram depicting a contents packager shown in Fig. 1;

Fig. 4 is a block diagram of a license issuing server shown in Fig. 1;

Fig. 5 is a flowchart of a method for issuing a license to protect digital contents distributed in multi-level in accordance with a preferred embodiment of the present invention;

Fig. 6 is a flowchart of a method for creating a license key by a contents packager in accordance with a preferred embodiment of the present invention;

Fig. 7 is a flowchart of a method of transmitting a base license and a license key information from a contents packager to a license issuing server in accordance with a preferred embodiment of the present invention;

Fig. 8 is a flowchart of a method for requesting a buy from a consumer to a distribution server in accordance with a preferred embodiment of the present invention;

Fig. 9 is a flowchart of a method of requesting issuing of license to a license issuing server from a distribution server;

Fig. 10 is a flowchart of a method of checking a validity of a request of issuing a license at a license issuing server in accordance with a preferred embodiment of the present invention; and

Fig. 11 is a flowchart of a method of creating a license at a license issuing server.

Best Mode for the Invention

Other objects and aspects of the invention will become apparent from the following description of the embodiments with reference to the accompanying drawings, which is set forth hereinafter.

Fig. 1 is a block diagram illustrating a system for issuing a license to protect digital contents distributed in multi-level in accordance with a preferred embodiment of the present invention.

The present invention relates to a system for issuing a license based on a digital rights management (DRM) in a multi-level contents distribution environment.

Io order to protect the digital contents in the multi-level contents distribution environment, the license issuing system according to the present embodiment includes: contents packagers 11, 21 and 31 for creating an encryption key, license issuing server 12, 22 and 32 for issuing a license containing rights, conditions and decryption information for contents; distributing servers 13, 23 and 33 for processing a purchase request from consumers; and database 14, 24 and 34.

Terms used for describing the multi-level contents packaging processing system according to the present invention will be described at first.

A distributor is a party that sells a packaged content to a consumer or other distributor with predetermined conditions. A consumer is a party that purchases the packaged content from the distributor to use the contents according to its' original purpose.

A term 'multi-level distribution' denotes distribution of digital contents between content distributors. A term 'resale' denotes a sale of packaged content that purchased from other distributor.

A secure container denotes a secured content that is created by the packaging, and a secure container includes an encrypted content, related metadata and business rules.

A license denotes a rule for using the packaged content and approval information including decryption keys.

A multi-packaged content is a secure container that is repeatedly packaged at multiple distribution levels in order to distribute the packaged content among distributors.

A multi-license denotes a certification to allow distributors to distribute, to sell and to use a related content in multi-level. A base license is a multi-license purchased from a previous distributor in order to create the multi-packaged content.

A content key is a symmetric key used to encrypt an original content, and a license key denotes a symmetric key used to encrypt the content key.

The license issuing system according to the present embodiment supports the multi-packaging and the multi-licensing for multi-level distribution. Therefore, a distributor 20 is allowed to issues a license with own rights and to repackage the content for distribution although a content producer 10 initially issues a license after packaging a content. Such a repackaged content may

be sold to other distributor 30 or a final consumer 40 directly.

Hereinafter, operations of the multi-level content distribution system according to the present embodiment will be described with reference to Fig. 1.

The content producer 10 initially packages an original content C with a user's rights R1 in operation 100.

The content packager 11 generates three key seeds s_k, s_{11} and s_{12} to create an encryption key. Then, the content packager 11 creates a symmetric key K from the key seed s_k, a symmetric key L_{11} from the key seed s_{11} and a symmetric key L_{12} from the key seed s_{12}. The original content C is encrypted using the symmetric key K, the symmetric key K is encrypted using the symmetric key L_{11}, and the encrypted value is encrypted using the symmetric key L_{12} again as shown in Eq. 1. Herein, N_1 denotes the encrypted value.

$$K = f(s_k), L_{11} = f(s_{11}), L_{12} = f(s_{12})$$
certificate
$$N_1 = E_{L_{10}}(E_{L_{11}}(K)) \qquad \text{Eq. 1}$$

In Eq. 1, f denotes a function for generating a symmetric key and E is a function of symmetric key encryption.

The content packager 11 transmits the key seed s_{11}, the encrypted value N_1 and the rights R_1 to the license issuing server 12. In order to securely transmit data, each of data is encrypted using a public key of the license issuing server ($[E_{P_{LS}}(s_{11}) \| E_{P_{LS}}(N_1) \| E_{P_{LS}}(R_1)]$) in operation 101. Then, the secure container C_1, the key seed s_{12} and the rights R_1 are stored in the database 15 of the distributing server in operation 101. The license issuing server 12 stores the received information in the database 14 of the license issuing server in operation 102.

The distributing server retrieves the key seed s_{12} from the database and encrypted the key seed s12 to a public key of a distributor. Also, the distributing server

transmits the certificate public key P_{CD1} of the distributor to the license issuing server with information about the rights R_1 selected by the consumer ($[E_{P_{CD1}}(s_{12}) \| P_{CD1} \| r_1]$) and requests the license issuing server to issue the license in operation 103.

The license issuing server 12 retrieves information such as s_{11}, N_1, R_1 from the database 14 in operation 104 when the license issuing server 12 receives the request of issuing the license. Then, the license issuing server 12 creates a licenser L_1 using the retrieved information and other information received from the distributing server 13. The license includes information about the key seeds s_{11} and s_{12}, the encrypted value N_1 and the rights R_1. Such a license is encrypted as like as following Eq. 2.

$$L_1 = E_{P_{CD_1}}(s_{12}) \| E_{P_{CD_1}}(S_1) \| E_{P_{CD_1}}(N_1) \| r_1 \,,\; S_1 = set\ of\ s_{1i} \qquad \text{Eq. 2}$$

The created license is transmitted to a purchaser CD_1 in operation 104.

In case of repackaging a packaged content, the content packager 21 creates two encryption key seeds s_{21} and s_{22}. Then, license keys L_{21} and L_{22} are created from the created encryption key seeds. The content packager extracts the encryption key seeds s_{11}, s_{12} and encrypted value N_1 from the license, and then N_1 is decrypted by s_{12}. Then, the decrypted value is encrypted in sequence using license keys L_{21} and L_{22} to create N_2. Such a process is shown following Eq. 3.

$$L_{21} = f(s_{21}), L_{22} = f(s_{22})$$
$$N_2 = E_{L_{22}}(E_{L_{21}}(D_{L_{12}}(N_1))) \qquad \text{Eq. 3}$$

In Eq. 3, *f* denotes a function for generating a symmetric key, *E* denotes a function of symmetric key encryption and *D* denotes a function of symmetric key decryption.

The content packager 21 transmits the key seed s_{21}, the encrypted value N_2 and the license L_1 to the license issuing server. In order to securely transmit data, each data is encrypted using the public key of the license issuing server 22 as like as following Eq. 4 in operation 111.

$$E_{P_{LS}}(S_2) \| E_{P_{LS}}(N_2) \| E_{P_{LS}}(L_1) \ , \ S_2 = set of s_{21} \qquad \text{Eq. 4}$$

Then, the repackaged secure container C_2, the encryption key seed s_{22} and a base license L_1 are stored in the database of the distributing server 25. The license issuing server 22 stores the received information in the database 24 of the license issuing server in operation 111.

The operation for purchasing is identical to the previous purchasing operation.

If other distributor CD_2 accesses the distributing server of the distributor CD_1 to purchase contents, the distributing server receives a certificate public key P_{CD2} of distributor from a packager of the distributor CD_2. The purchaser receives a secure container C_2 from the distributing server.

The distributing server retrieves a key seed s_{22} from the database and encrypts it with the public key of distributor. The distributing server transmits the encrypted public key to the license issuing server with the distributor's certificate public key P_{CD2} and the rights selected by the purchaser ($[E_{P_{CD_2}}(s_{22}) \| P_{CD_{2\|}} | r_2]$). Then, the distributing server requests the license issuing server to issue the license.

When the license issuing server receives the request, the license issuing server retrieves the information about S_2, N_2 and L_1 from the database. Then, the license issuing server creates the license L_2 using the retrieved information and the information from the distributing

server. The license includes information about the encryption key seed S_2, s_{22}, encrypted content encryption key N_2 and rights r_2. Such a license is encrypted with a public key P_{CD2} of purchaser as shown in following Eq. 5. Then, the created license is transmitted to the purchaser CD_2.

$$L_2 = E_{P_{CD_2}}(s_{22}) \| E_{P_{CD_2}}(S_2) \| E_{P_{CD_2}}(N_2) \| r_2 \,,\; S_2 = set\,of\,s_{2i}$$

Eq. 5

Meanwhile, the operations can be generalized and may be expressed as following equations for an N-level distributor.

Generation of symmetric keys L_{i1}, L_{i2} and N_i using key seed s_{i1} and s_{i2} in a packager of the N-level distributor can be expressed as following Eq. 6.

$$\begin{aligned} L_{n1} &= f(s_{n1}), L_{n2} = f(s_{n2}) \\ N_n &= E_{L_{n2}}(E_{L_{n1}}(D_{L_{n-1,2}}(N_{n-1}))) \end{aligned} \qquad \text{Eq. 6}$$

In Eq. 6, *f* denotes a function for generating a symmetric key, *E* denotes a function of symmetric key encryption and *D* denotes a function of symmetric key decryption.

Data transmitted from the content packager to the license issuing server in operation 121 can be expressed as following Eq. 7.

$$\begin{aligned} &E_{P_{LS}}(S_n) \| E_{P_{LS}}(N_n) \| E_{P_{LS}}(L_{n-1}) \\ &S_n = set\,of\,s_{ni},\ 1 \le i \le n \end{aligned} \qquad \text{Eq. 7}$$

The content packager stores data in the distributing server's database in operation 121 and the data include the repackaged content C_n, the key seed s_{n2} and the base license L_{n-1}.

When the N+1 distributor requests to purchase contents, the distributing server retrieves the public key

P_{CDn+1} of the purchaser in operation 122. The purchaser receives a secure container C_n from the distributing server in operation 122.

The distributing server retrieves the key seed s_{n2} from the database, encrypts the key seed s_{n2} with the public key CD_{n+1} of the distributor, transmits the public key to the license issuing server with the distributor certificate public key P_{CDn+1} and the rights r_n selected by the purchaser ($[E_{P_{CD_{n+1}}}(S_{n2}) \| P_{CD_{n+1}} \| r_n]$) and requests to issue the license in operation 123.

If the license issuing server receives the request, the license issuing server retrieves the information S_n, N_n and L_{n-1} from the database in operation 124. Then, the license issuing server creates the license L_n using the retrieved information and other information received from the distributing server. The license includes the encryption key seed information S_n, s_{n2}, the encrypted content encryption key information N_n and the rights r_n. Such a license is encrypted with the public key of the purchaser as like as following Eq. 8.

$$L_n = E_{P_{CD_{n+1}}}(s_{n2}) \| E_{P_{CD_{n+1}}}(S_n) \| E_{P_{CD_{n+1}}}(N_n) \| r_n$$
$$S_n = set\,of\,s_{i1},\ 1 \le i \le n \qquad \text{Eq. 8}$$

Then, the created licenser is transmitted to the purchaser CD_2 in operation 124.

Fig. 2 is a block diagram showing a secure container in accordance with a preferred embodiment of the present invention.

As shown in Fig. 2, the secure container includes contents 201 which are encrypted with a symmetric key K, metadata 202 and a digital signature 203.

Fig. 3 is a block diagram depicting a contents packager shown in Fig. 1.

Hereinafter, a content packager 310 of a 2nd distributor for creating a secured content will be

described with reference to Fig. 3.

The content packager 310 includes: a multi-packaging analyzing unit 311 for extracting information about the packager content 301 such as the metadata, the encrypted content and the digital signature; a metadata analyzing unit 312 for analyzing metadata included in the packaged content; and a multi-packaging unit 313 for repackaging content using the analysis result of the multi-packaging analyzing unit 311 and the metadata analyzing unit 312.

The content packager 310 includes a license engine unit 314 for analyzing the license 302 and inspecting the right information; an encryption key generating unit 315 for creating an encryption key; an encrypting unit 316 for encrypting contents or major information; and a communicating unit 317 for communicating to the license issuing server and the distributing server.

A content packager 320 of an n^{th} distributor such as 3^{rd} or a 4^{th} distributor has same configuration and performs identical operations.

As described above, a distributor who purchases the pre-packaged content and a license thereof is allowed to set a sale condition of the content within the rights defined in the license. Also, other distributor B who purchases this content from the distributor A is allowed to sell or to use only within the rights defined by the distributor A.

Fig. 4 is a block diagram of a license issuing server shown in Fig. 1.

In order to issue the multi-level license, the license issuing server 12, 22 or 32 includes: a key managing unit for securely storing license key information; a base license managing unit 402 for securely storing a base license; a license engine unit 403 for analyzing the base license and checking a validity of the issuing request; a license generating unit 405 for generating a license; and a

communication unit 401 for communicating to an external system.

Fig. 5 is a flowchart of a method for issuing a license to protect digital contents distributed in multi-level in accordance with a preferred embodiment of the present invention. That is, the license issuing server 12, 22 or 32 performs the method shown in Fig. 5 in the present invention.

As shown in Fig. 5, the content packager generates a license key at step S500 and transmits the base license and the license key information to the license issuing server at step S502.

Then, a purchaser requests the distributing server to buy contents at step S504. Accordingly, the distributing server requests the license issuing server to issue a license.

The license issuing server checks the validity of the license issuing request at step S506. If it is valid, the license issuing server generates the license at step S508, and transmits the generated license to the purchaser at step S510. If it is not valid, the license issuing server transmits an error message at step S512.

Fig. 6 is a flowchart of a method for creating a license key by a contents packager in accordance with a preferred embodiment of the present invention. That is, Fig. 6 shows details of the step 500 shown in Fig. 5.

The content packager generates an encryption key seed at step S600 and generates an encryption key from the seed at step S602. Then, the content packager extracts the license key and the encrypted content key from the license at step S604. The encrypted content key is decrypted using the extracted license key at step S606. Then, the content key is encrypted using the generated encryption key.

The step 500 may be divided into the packaging of original content and the repackaging of packaged content.

These packaging and repackaging steps were described with reference to Fig. 1.

Fig. 7 is a flowchart of a method of transmitting a base license and license key information from a contents packager to a license issuing server in accordance with a preferred embodiment of the present invention. That is, Fig. 7 shows details of step 502 shown in Fig. 5.

The content packager retrieves the certificate of the license issuing server from the license issuing server at step S700. The license key is encrypted with the public key of the license issuing server at step S702 and a message to be transmitted to the license issuing server to use a content ID, a content title and the encrypted license key information at step S704. Then, the digital signature is attached on the generated message at step S706 and the digital signed message is transmitted to the license issuing server at step S706.

Fig. 8 is a flowchart of a method for requesting a distribution server to purchase contents by a purchaser in accordance with a preferred embodiment of the present invention. That is, Fig. 8 shows details of the step 504 shown in Fig. 5.

The purchaser logs into the distributing server at step S800, selects rights and conditions of target content from the distributing server at step S802 and transmits the certificate of the purchaser to the distributing server at step S804.

Fig. 9 is a flowchart of a method of requesting a license issuing server to issue a license from a distribution server.

If the distributing server requests the license issuing server to issue a license, the license key is retrieved from the database that manages the license key at step S901, and the retrieved license key is encrypted with the certificate public key of the purchaser at step S902.

Then, the distributing server creates a message including the selected rights and conditions, the license key generated at step S902 and the certificate of the purchaser at step S904. Then, the digital signature is attached on the generated message as the certificate private key of the distributing server at step S906. Then, the generated message with the digital signature is transmitted to the license issuing server at step S908.

Fig. 10 is a flowchart of a method of checking a validity of a request of issuing a license at a license issuing server in accordance with a preferred embodiment of the present invention. That is, Fig. 10 shows details of the step S506 shown in Fig. 5.

Referring to Fig. 10, when the license issuing server receives the request of issuing the license from the distributing server at step S1002, the license issuing server retrieves a corresponding base license from the base license managing unit at step S1004 and checks whether the rights and conditions received from the distributing server are matched with the rights and the conditions in the base license using the license engine unit at step S1006.

Fig. 11 is a flowchart of a method of creating a license at a license issuing server. That is, Fig. 5 shows details of step S508.

Referring to Fig. 11, the license issuing server retrieves the license key information from the key managing unit at step S1100, and extracts the license key information included in the base license at step S1102. The information related to key obtained at steps S1100 and S1102 are encrypted using the certificate public key of the purchaser at step S1104.

Then, the rights and the condition information for the license are generated using the rights and condition information received from the distributing server at step S1106 and the license XML is generated using the

information obtained in the step S1104 and S1106 at step S1108. Then, the digital signature of the license issuing server is attached to the generated license XML at step S1110.

The above described method according to the present invention can be embodied as a program and stored on a computer readable recording medium. The computer readable recording medium is any data storage device that can store data which can be thereafter read by the computer system. The computer readable recording medium includes a read-only memory (ROM), a random-access memory (RAM), a CD-ROM, a floppy disk, a hard disk and an optical magnetic disk.

While the present invention has been described with respect to certain preferred embodiments, it will be apparent to those skilled in the art that various changes and modifications may be made without departing from the scope of the invention as defined in the following claims.

What is claimed is:

1. A system for issuing a license for a multi-level distribution of content, comprising:

a content packaging means for packaging a target content to distribute and requesting a license issuing server to issue a license for the target content;

the licensing issuing means for issuing a license that contains information about rights for using a target content and information about decrypting a content according to the request of a distributing means;

the distributing means for requesting the license issuing means to issue a license according to a content purchasing request of purchaser; and

a database for storing information about contents, key seeds and rights.

2. The system as recited in claim 1, wherein if a content is already distributed by a content producer, the content packaging means analyzes an externally distributed and packaged content, repackages the content according to a distributing request of other distributor, decrypts an externally issued license, encrypts the license key according to the content purchasing request of other distributor and transmits the encrypted license key to the license issuing means.

3. The system as recited in claim 2, wherein the content packaging means includes:

a multi-packaging analyzing means for analyzing a packaged content received from an external system and extracting metadata, a encrypted content and an digital signature from the packaged content;

a metadata analyzing means for analyzing the extracted metadata;

a multi-packaging means for generating a new content by including the encrypted content, modified metadata and a new digital signature;

a license engine means for analyzing an externally issued license and checking information about rights for using a content;

an encryption key generating means for generating an encryption key;

an encryption means for decrypting a license key analyzed at the license engine means or encrypting the license key using the encryption key in response to a license issuing request, and transmitting the encrypted license key to the license issuing means; and

a communication means for communicating to a license issuing means and a distributing means of an external license issuing system.

4. The system as recited in claim 1, wherein the content packaging means encrypts a content that is initially distributed by a content producer, and packages the content with metadata having information about the content and a digital signature for preventing the content from being forged or modified.

5. The system as recited in claim 1, wherein the license issuing means includes:

a communicating means for communicating to an external system to issue a license from an external system through the content packaging means and transmitting the issued license to an external system;

a key managing means for managing license key information included in the license;

a base license managing means for storing and managing a base license issued from the external system;

a license engine means for analyzing a base license

issued from the external system, checking a validity of a license issuing request, transmitting the base license to the license generating means if it is valid, and requesting a new license to be issued; and

the license generating means for generating a new license based on the transmitted base license.

6. The system as recited in claim 5, wherein the content packaging means packages metadata having the content information, an encoded content and a digital signature.

7. The system as recited in claim 5, wherein the license includes a license key for decrypting a content, information about rights to use the content and a digital signature.

8. A method of issuing a license for multi-level distribution of content, the method comprising the steps of:

a) generating a license key for a target content to distribute at a content packager;

b) transmitting a base license issued from an external system and the generated license key information to a license issuing server from the content packager;

c) receiving a content purchasing request from a purchaser and requesting the license issuing server to issue a license at a distributing server; and

d) checking a validity of the license issuing request, generating a new license and transmitting the generated license to the purchaser at the license issuing server.

9. The method as recited in claim 8, wherein the step a) includes the steps of:

a-1) generating a key seed to generate an encryption

key;

a-2) generating the encryption key from the key seed;

a-3) extracting a license key and an encrypted content key from the base license;

a-4) decrypting the encrypted content key using the extracted license key; and

a-5) re-encrypting the content key using the encryption key.

10. The method as recited in claim 8, wherein the step b) includes the steps of:

b-1) retrieving a certificate from the license issuing server;

b-2) encrypting the license key with a public key as a certification of a license issuing server;

b-3) generating a message to be transmitted to the license issuing server using a content ID, a content title and an encrypted license key information;

b-4) digital signing the message; and

b-5) transmitting the digital signed message and the base license to the license issuing server.

11. The method as recited in claim 8, wherein the content purchasing request in the step c) includes the steps of:

logging in the distributing server by the purchaser;

selecting rights and conditions for a target content to purchase at the distributing server by the purchaser;

transmitting the certificate of the purchaser to the distributing server.

12. The method as recited in claim 8, wherein the license issuing request in the step d) includes the steps of:

obtaining a license key from a database that manages

a license key;

encrypting the license key with a public key of a purchaser's certificate;

generating a license issuing request message including rights and conditions selected by a purchaser, an encrypted license key and a certificate of a purchaser;

digitally signing the license issuing request message using a certificate private key of the distributing server; and

transmitting the digital signed message to the license issuing server.

13. The method as recited in claim 8, wherein the step for checking the validity of the license issuing request includes the steps of:

receiving a license issuing request from the distributing server;

retrieving a corresponding base license from the base license managing unit; and

determining rights and conditions received from the distributing server are matched with rights and conditions in the base license using a license engine.

14. The method as recited in claim 13, wherein the step for generating the license includes the steps of:

retrieving key information for retrieving license key information from a key managing unit;

extracting information about a license key from the base license;

encrypting the information related the keys in the step for retrieving the key information and the step for extracting the license key using a public key of a purchaser's certificate;

generating rights and conditions for a license using the rights and the condition received from the distributing

server;

generating an extensible markup language (XML) based license using the information obtained from the step of encryption and the step of generating the rights; and

digitally signing the XML based license.

FIG. 1

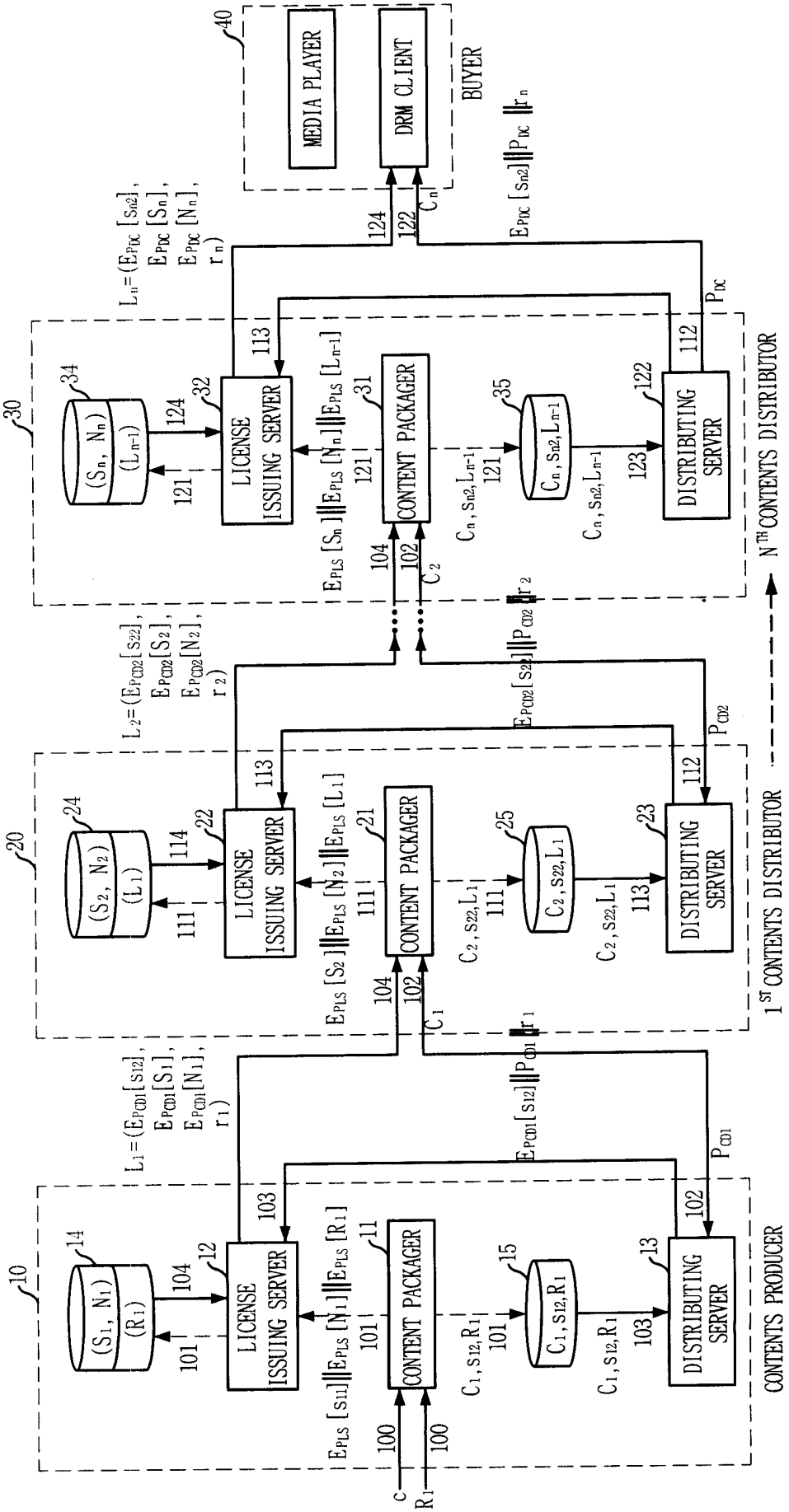

CONTENTS PRODUCER
1ST CONTENTS DISTRIBUTOR
2ND CONTENTS DISTRIBUTOR
NTH CONTENTS DISTRIBUTOR
BUYER
MEDIA PLAYER
DRM CLIENT
LICENSE ISSUING SERVER
CONTENT PACKAGER
DISTRIBUTING SERVER
CD:Content Distributor
c:Raw Content
E:Encrypt
DC:DRM Client
C:DRM-enabled Content
P:Public Key
LS:License Server
L:License
N:Encrypted Content Key Seed
R:Rights
s:Key Seed
r:Subset of R
S:Set of s

FIG. 2

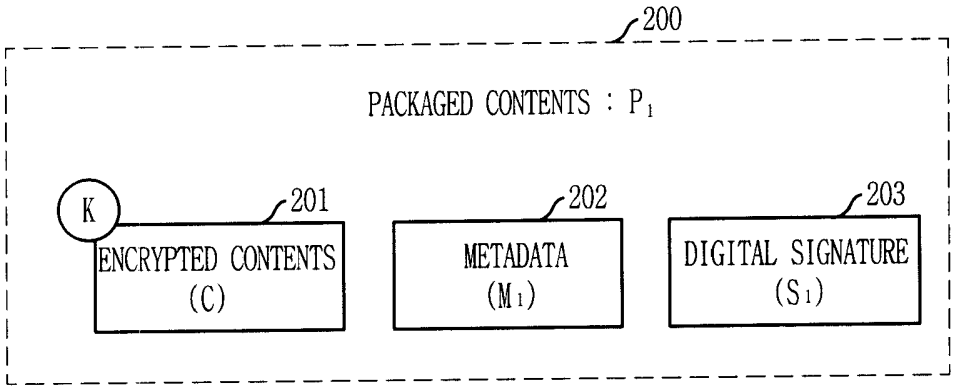

200
PACKAGED CONTENTS : P1
K
201
ENCRYPTED CONTENTS
(C)
202
METADATA
(M1)
203
DIGITAL SIGNATURE
(S1)

FIG. 3

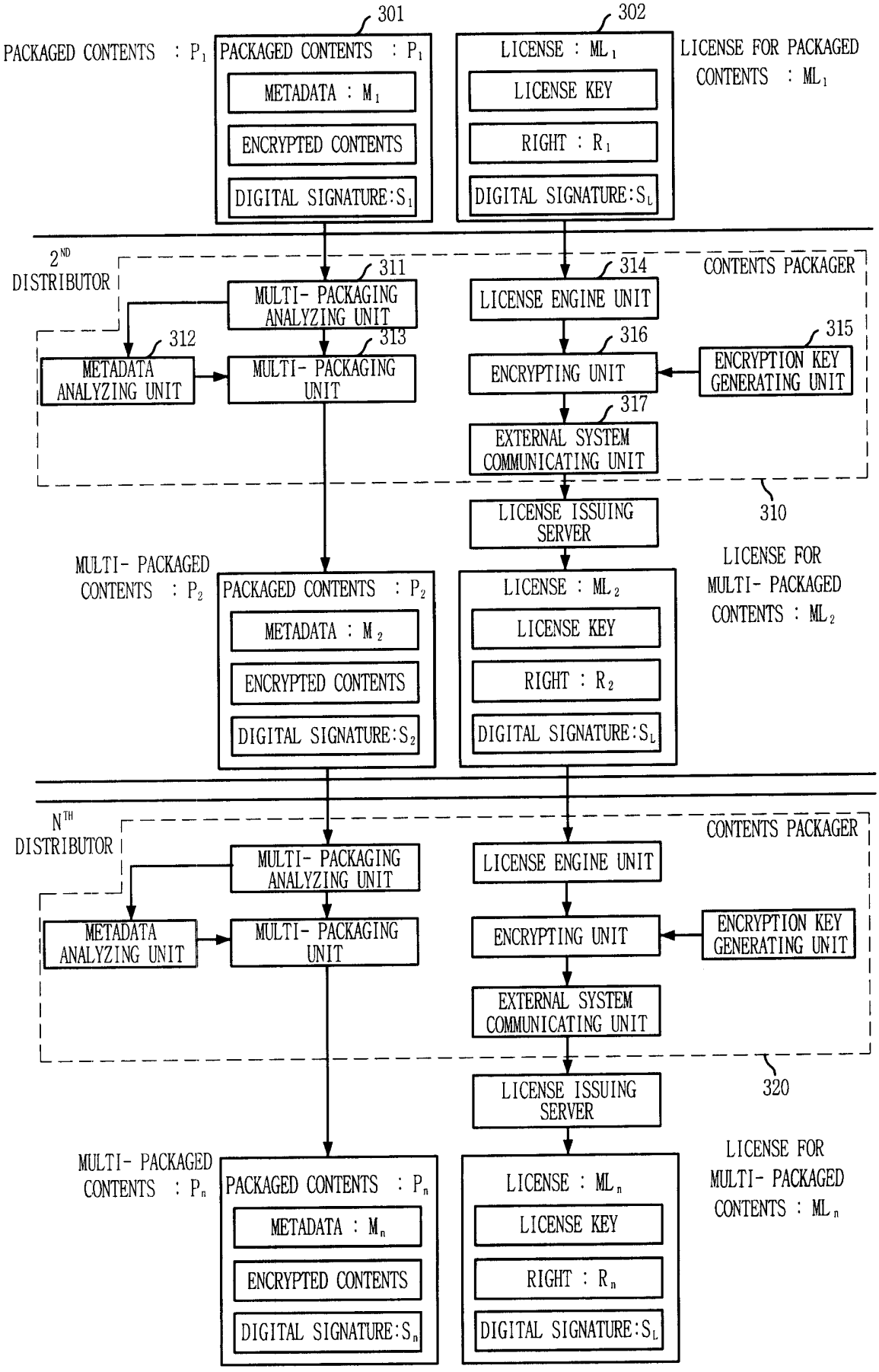

301
302
PACKAGED CONTENTS : P1
PACKAGED CONTENTS : P1
METADATA : M1
ENCRYPTED CONTENTS
DIGITAL SIGNATURE:S1
LICENSE : ML1
LICENSE KEY
RIGHT : R1
DIGITAL SIGNATURE:SL
LICENSE FOR PACKAGED CONTENTS : ML1
2ND DISTRIBUTOR
CONTENTS PACKAGER
311
314
315
312
313
316
317
MULTI- PACKAGING ANALYZING UNIT
LICENSE ENGINE UNIT
ENCRYPTION KEY GENERATING UNIT
METADATA ANALYZING UNIT
MULTI- PACKAGING UNIT
ENCRYPTING UNIT
EXTERNAL SYSTEM COMMUNICATING UNIT
310
LICENSE ISSUING SERVER
MULTI- PACKAGED CONTENTS : P2
PACKAGED CONTENTS : P2
METADATA : M2
ENCRYPTED CONTENTS
DIGITAL SIGNATURE:S2
LICENSE : ML2
LICENSE KEY
RIGHT : R2
DIGITAL SIGNATURE:SL
LICENSE FOR MULTI- PACKAGED CONTENTS : ML2
NTH DISTRIBUTOR
CONTENTS PACKAGER
MULTI- PACKAGING ANALYZING UNIT
LICENSE ENGINE UNIT
METADATA ANALYZING UNIT
MULTI- PACKAGING UNIT
ENCRYPTING UNIT
ENCRYPTION KEY GENERATING UNIT
EXTERNAL SYSTEM COMMUNICATING UNIT
320
LICENSE ISSUING SERVER
MULTI- PACKAGED CONTENTS : Pn
PACKAGED CONTENTS : Pn
METADATA : Mn
ENCRYPTED CONTENTS
DIGITAL SIGNATURE:Sn
LICENSE : MLn
LICENSE KEY
RIGHT : Rn
DIGITAL SIGNATURE:SL
LICENSE FOR MULTI- PACKAGED CONTENTS : MLn

FIG. 4

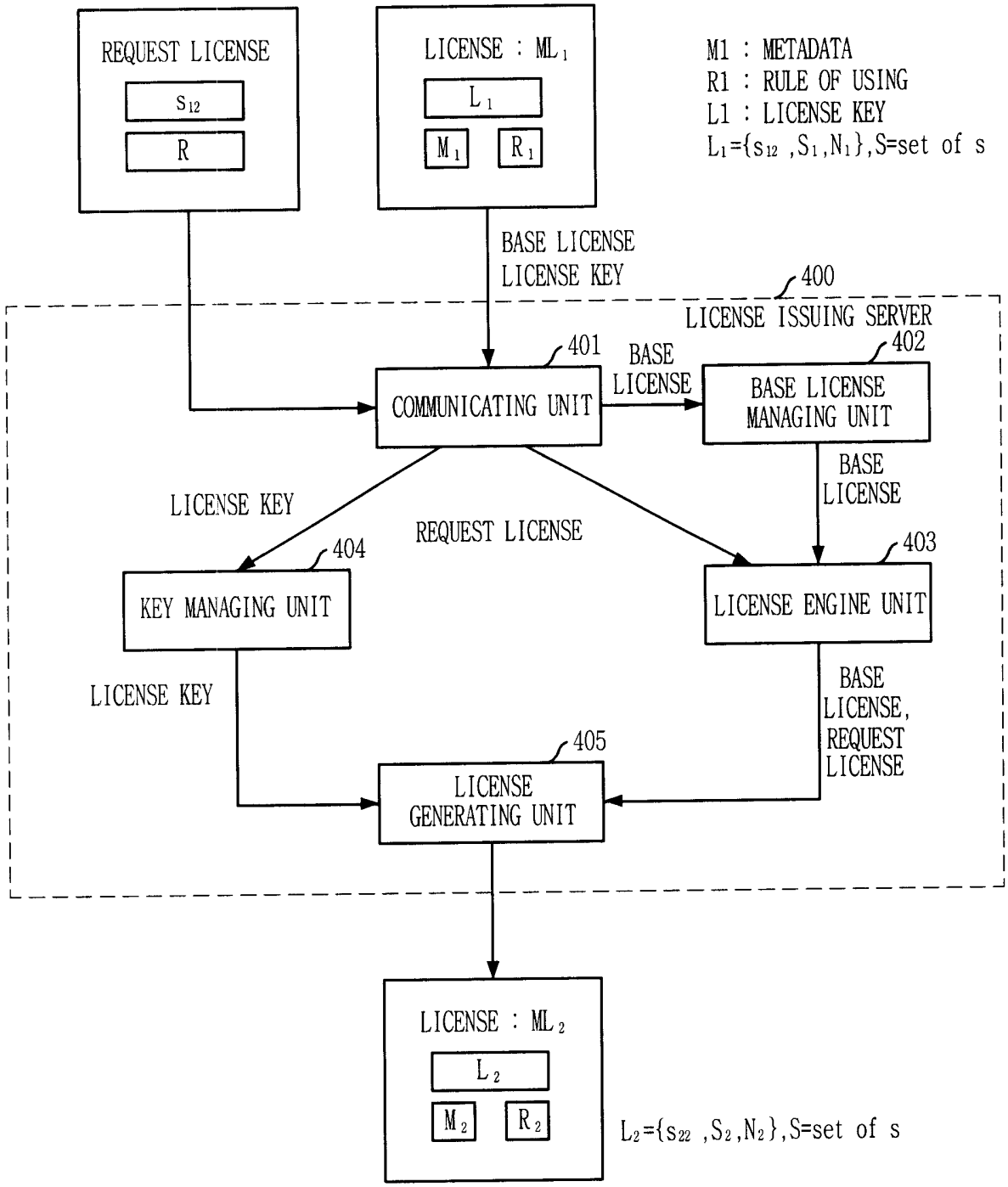

REQUEST LICENSE
S_{12}
R
LICENSE : ML_1
L_1
M_1
R_1
M1 : METADATA
R1 : RULE OF USING
L1 : LICENSE KEY
$L_1=\{s_{12}, S_1, N_1\}$, S=set of s
BASE LICENSE
LICENSE KEY
400
LICENSE ISSUING SERVER
401
COMMUNICATING UNIT
BASE LICENSE
402
BASE LICENSE MANAGING UNIT
BASE LICENSE
LICENSE KEY
REQUEST LICENSE
404
KEY MANAGING UNIT
403
LICENSE ENGINE UNIT
LICENSE KEY
BASE LICENSE, REQUEST LICENSE
405
LICENSE GENERATING UNIT
LICENSE : ML_2
L_2
M_2
R_2
$L_2=\{s_{22}, S_2, N_2\}$, S=set of s

FIG. 5

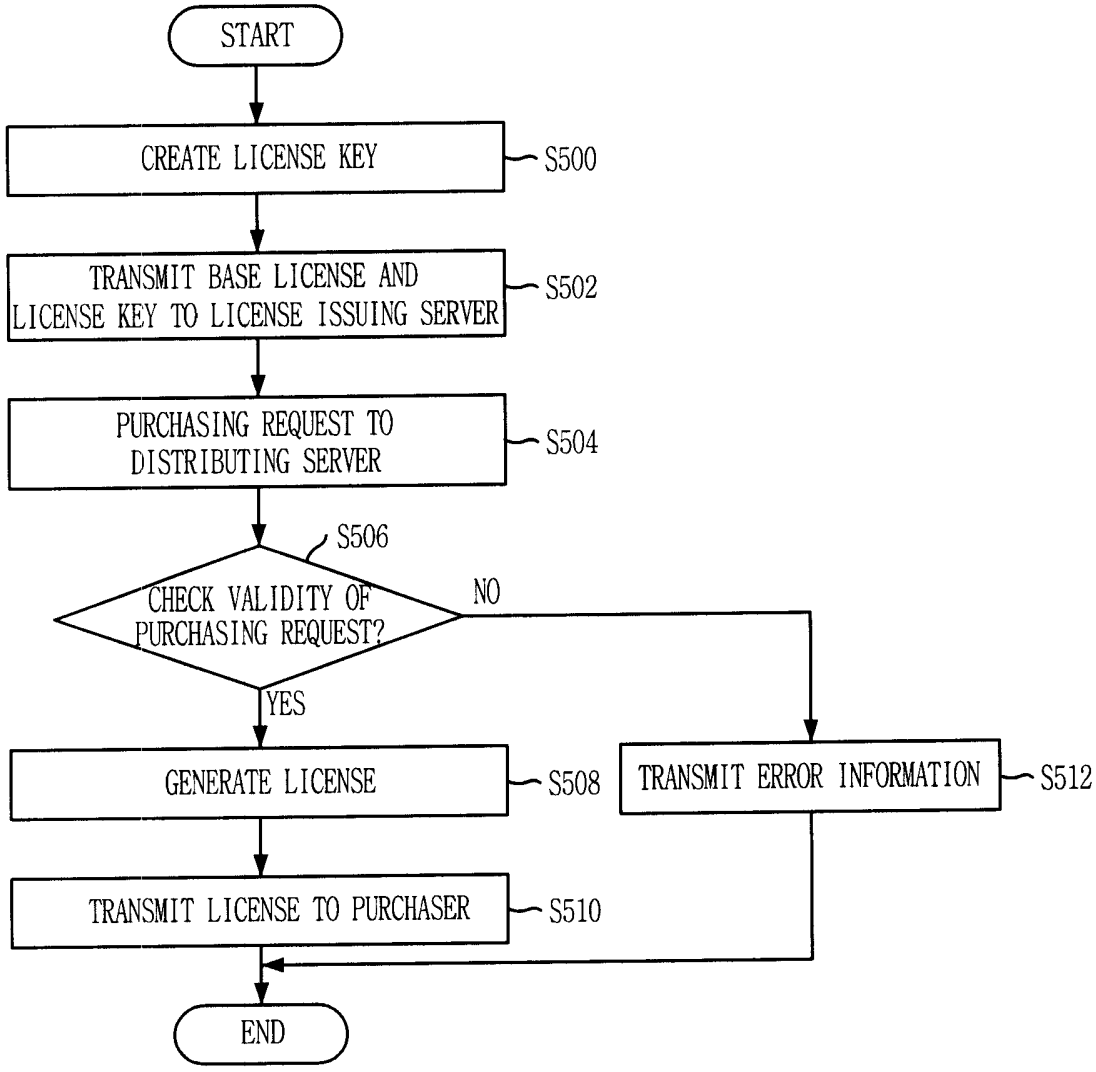

START
CREATE LICENSE KEY
S500
TRANSMIT BASE LICENSE AND LICENSE KEY TO LICENSE ISSUING SERVER
S502
PURCHASING REQUEST TO DISTRIBUTING SERVER
S504
S506
CHECK VALIDITY OF PURCHASING REQUEST?
NO
YES
GENERATE LICENSE
S508
TRANSMIT ERROR INFORMATION
S512
TRANSMIT LICENSE TO PURCHASER
S510
END

FIG. 6

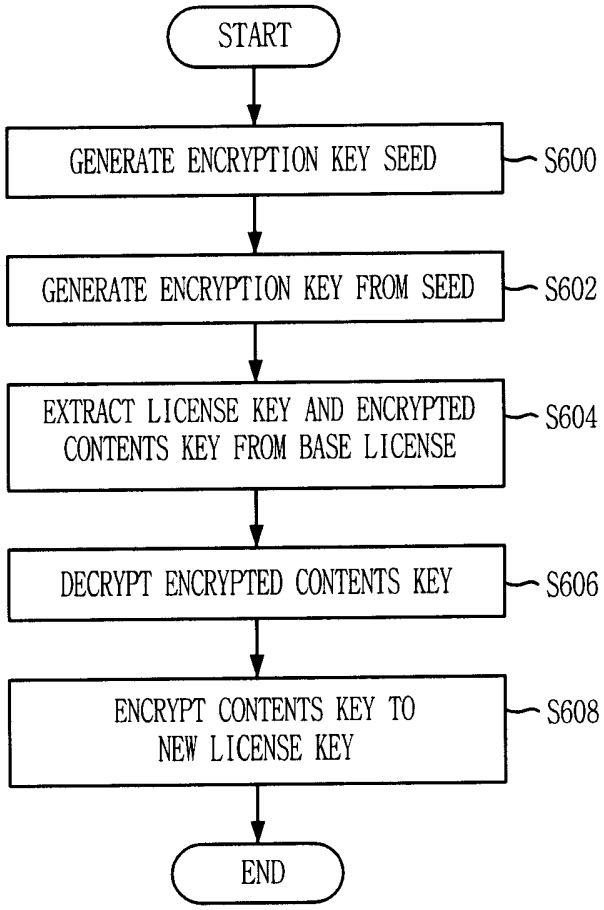

START
GENERATE ENCRYPTION KEY SEED
S600
GENERATE ENCRYPTION KEY FROM SEED
S602
EXTRACT LICENSE KEY AND ENCRYPTED CONTENTS KEY FROM BASE LICENSE
S604
DECRYPT ENCRYPTED CONTENTS KEY
S606
ENCRYPT CONTENTS KEY TO NEW LICENSE KEY
S608
END

FIG. 7

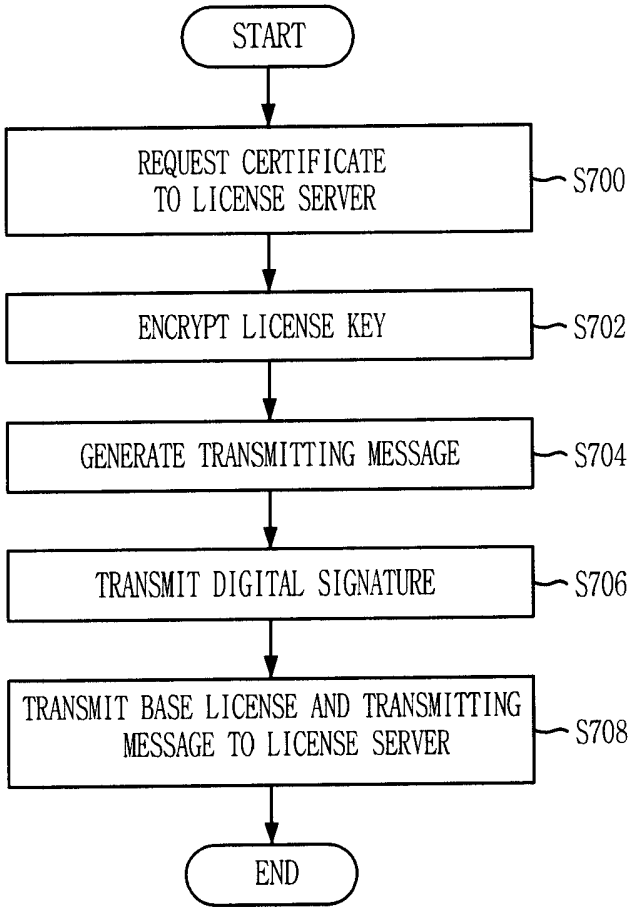

START
REQUEST CERTIFICATE TO LICENSE SERVER
S700
ENCRYPT LICENSE KEY
S702
GENERATE TRANSMITTING MESSAGE
S704
TRANSMIT DIGITAL SIGNATURE
S706
TRANSMIT BASE LICENSE AND TRANSMITTING MESSAGE TO LICENSE SERVER
S708
END

FIG. 8

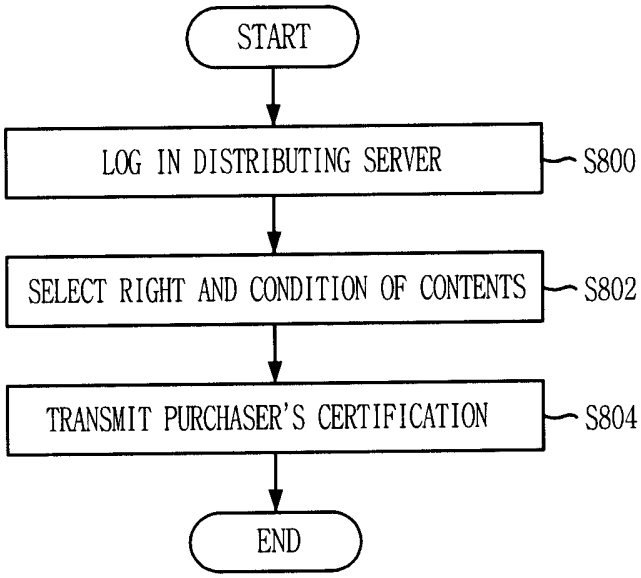

START
LOG IN DISTRIBUTING SERVER
S800
SELECT RIGHT AND CONDITION OF CONTENTS
S802
TRANSMIT PURCHASER'S CERTIFICATION
S804
END

FIG. 9

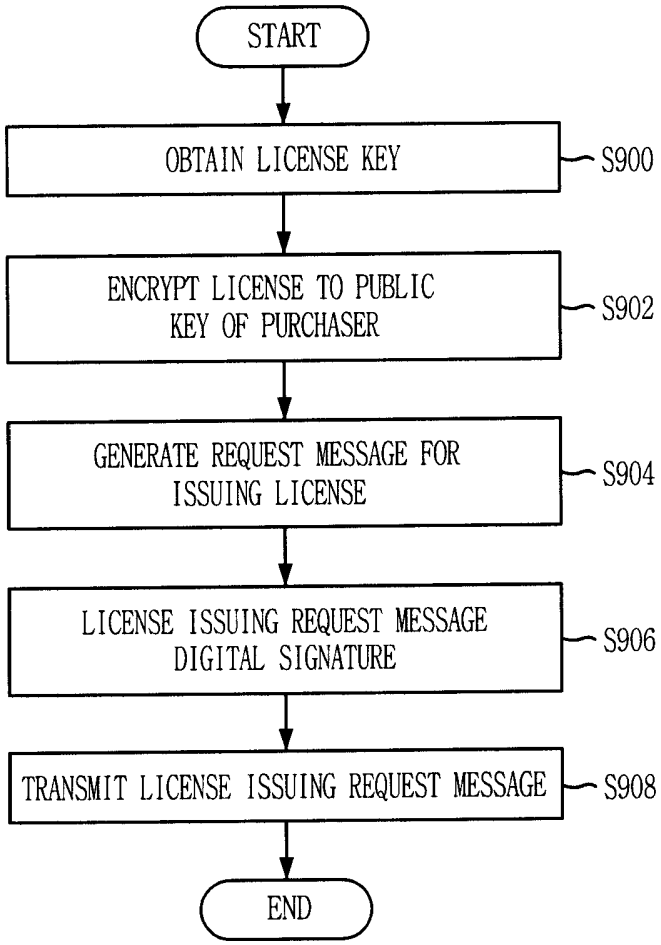

START
OBTAIN LICENSE KEY
S900
ENCRYPT LICENSE TO PUBLIC KEY OF PURCHASER
S902
GENERATE REQUEST MESSAGE FOR ISSUING LICENSE
S904
LICENSE ISSUING REQUEST MESSAGE DIGITAL SIGNATURE
S906
TRANSMIT LICENSE ISSUING REQUEST MESSAGE
S908
END

FIG. 10

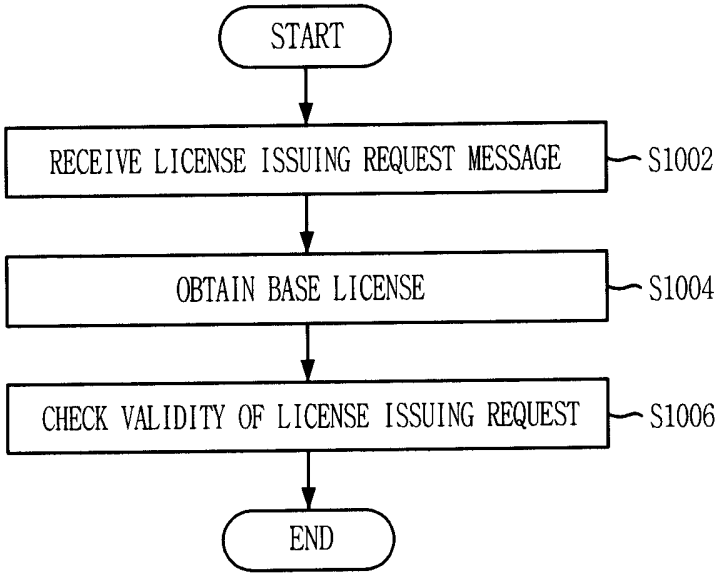
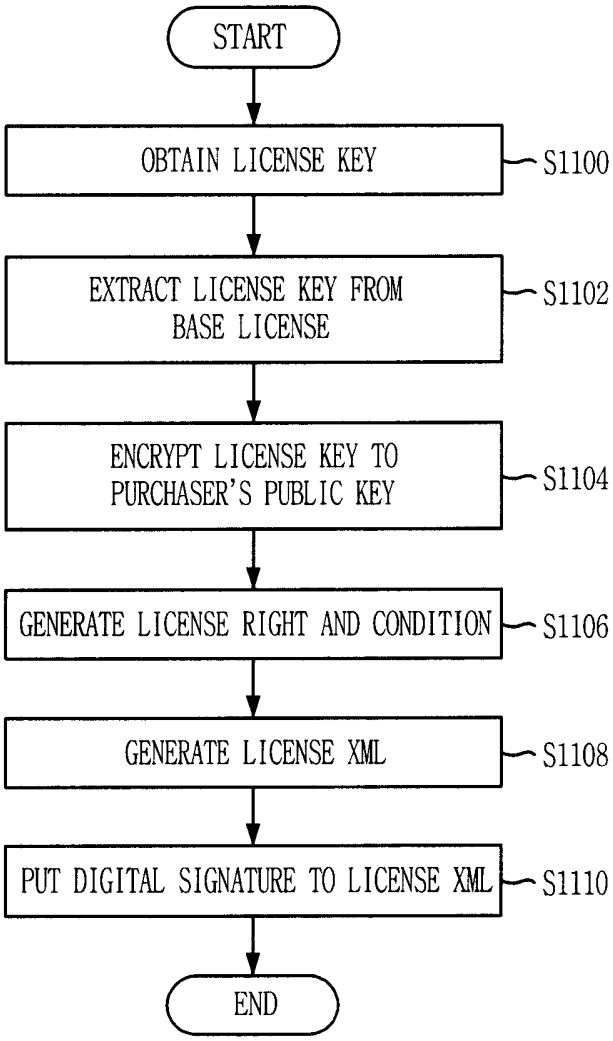

START
RECEIVE LICENSE ISSUING REQUEST MESSAGE
S1002
OBTAIN BASE LICENSE
S1004
CHECK VALIDITY OF LICENSE ISSUING REQUEST
S1006
END

FIG. 11


START
OBTAIN LICENSE KEY
S1100
EXTRACT LICENSE KEY FROM BASE LICENSE
S1102
ENCRYPT LICENSE KEY TO PURCHASER'S PUBLIC KEY
S1104
GENERATE LICENSE RIGHT AND CONDITION
S1106
GENERATE LICENSE XML
S1108
PUT DIGITAL SIGNATURE TO LICENSE XML
S1110
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2005/002265

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 G06F 17/60

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)
IPC7 G06F17/00, G06F17/60, G06F17/90

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
KR, JP as above

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 2003-80327 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 17 OCTOBER 2003 see the whole document	1-14
Y	KR 2004-34165 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 28 APRIL 2004 see the whole document	1-14
A	WO 2002-56580 A (FOURSYS BUSINESS PROMOTION KABUSHIKI KAISHA) 18 JULY 2002 see the whole document	1-14

☐ 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
25 OCTOBER 2005 (25.10.2005)	**27 OCTOBER 2005 (27.10.2005)**
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 PARK, Sung Woo Telephone No. 82-42-481-5790

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/KR2005/002265

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 2003-80327 A	17 OCTOBER 2003	None	
KR 2004-34165 A	28 APRIL 2004	None	
WO 2002-56580 A	18 JULY 2002	CN 1483278 A	17 MAY 2004
		EP 1357734 A	29 COTOBER 2003
		JP 2004146860 A2	20 MAY 2004
		KR 200393191 A	06 DECEMBER 2003
		US 2004107109 A1	03 JUNE 2004