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

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2592873 A1 2006/07/20

(21) 2 592 873

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2006/01/13
(87) Date publication PCT/PCT Publication Date: 2006/07/20
(85) Entrée phase nationale/National Entry: 2007/06/28
(86) N° demande PCT/PCT Application No.: KR 2006/000148
(87) N° publication PCT/PCT Publication No.: 2006/075893
(30) Priorités/Priorities: 2005/01/13 (US60/643,150);
2005/05/20 (KR10-2005-0042683)

(51) Cl.Int./Int.Cl. *H04L 9/32* (2006.01)

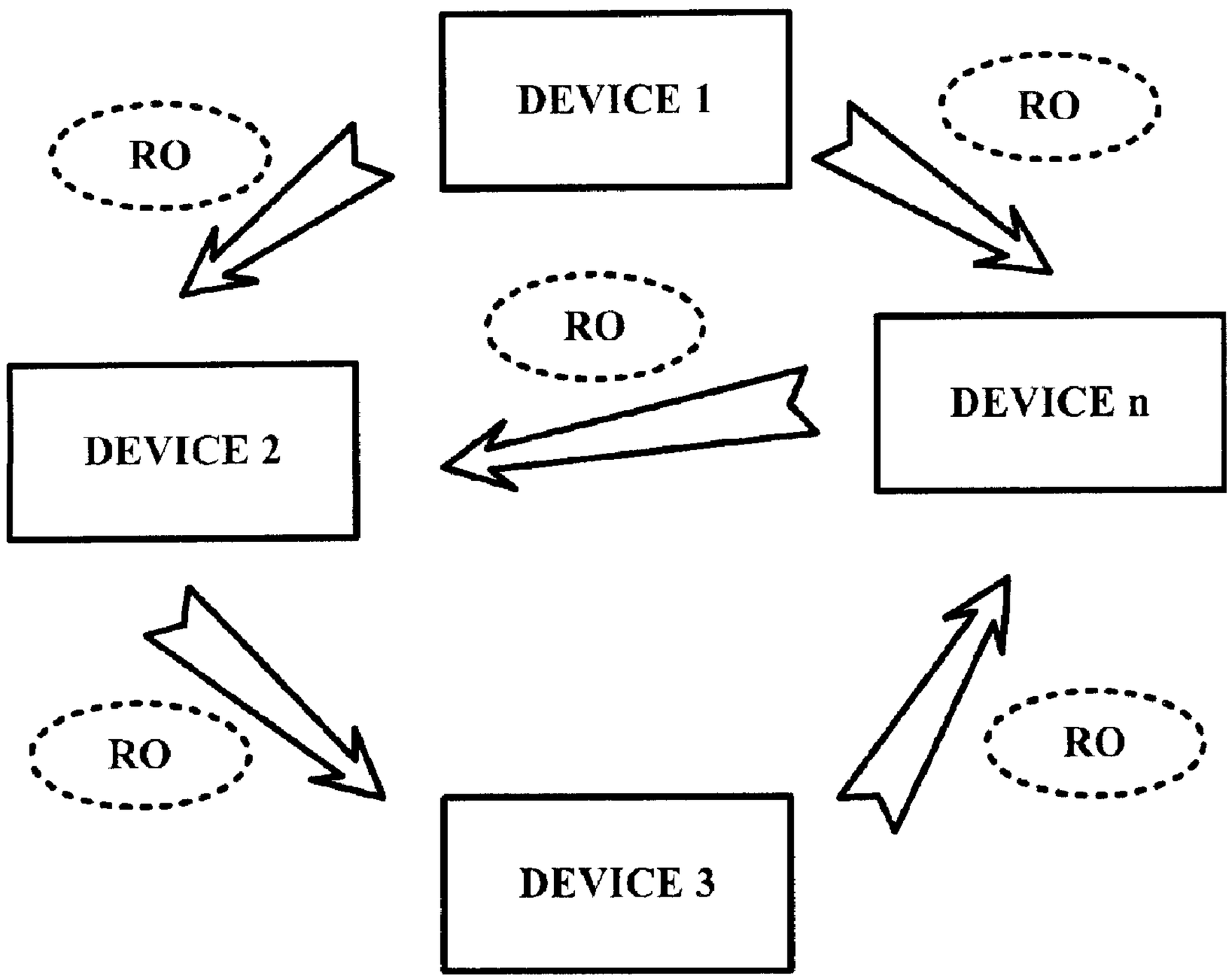
(71) Demandeur/Applicant:
SAMSUNG ELECTRONICS CO., LTD., KR

(72) Inventeurs/Inventors:
OH, YUN-SANG, KR;
JUNG, KYUNG-IM, KR;
CHOI, JAE-JIN, KR

(74) Agent: RIDOUT & MAYBEE LLP

(54) Titre : PROCEDE PERMETTANT DE DEPLACER UN OBJET DE DROITS ENTRE DES DISPOSITIFS, PROCEDE ET DISPOSITIF PERMETTANT D'UTILISER UN OBJET DE CONTENU FONDES SUR LE PROCEDE DE DEPLACEMENT, ET DISPOSITIF

(54) Title: METHOD FOR MOVING A RIGHTS OBJECT BETWEEN DEVICES AND A METHOD AND DEVICE FOR USING A CONTENT OBJECT BASED ON THE MOVING METHOD AND DEVICE



(57) Abrégé/Abstract:
A method for moving a rights object (RO) between devices, a method of using a content object based on the moving method, and devices using the methods are provided. The moving method includes performing authentication between two devices; securing a

(21) 2 592 873

(13) A1

(57) Abrégé(suite)/Abstract(continued):
connection between the devices; and communicating the rights object between the two devices. The using method includes two devices communicating with each other, the first device having use permission of content objects and the second device including the content objects and corresponding rights objects; the first device searching for the content objects; and the first device using the content object that was found. The device includes an authentication module to authenticate another device; a security formation module to secure a connection for the other device; and a transceiving module which communicates a rights object for which the connection has been secured.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 July 2006 (20.07.2006)

PCT

(10) International Publication Number
WO 2006/075893 A1

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/KR2006/000148

(22) International Filing Date: 13 January 2006 (13.01.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/643,150	13 January 2005 (13.01.2005)	US
10-2005-0042683	20 May 2005 (20.05.2005)	KR

(71) Applicant: **SAMSUNG ELECTRONICS CO., LTD.** [KR/KR]; 416, Maetan-dong, Yeongtong-gu, Suwon-si, Gyeonggi-do 442-742 (KR).

(72) Inventors: **OH, Yun-sang**; #8-703 Gaepo Hanshin APT, Dogok 2-dong, Gangnam-gu, Seoul 135-855 (KR). **JUNG, Kyung-im**; #128-903, Park Town Lotte APT, Sunae-dong, Bundang-gu, Seongnam -si, Gyeonggi-do 463-728 (KR). **CHOI, Jae-jin**; #2-405 Woosung APT, Garak-dong, Songpa-gu, Seoul 138-753 (KR).

(74) Agents: **KIM, Dong-jin** et al.; 6th Fl. Youngpoong Bldg., 142, Nonhyun-dong, Gangnam-gu, Seoul 135-749 (KR).

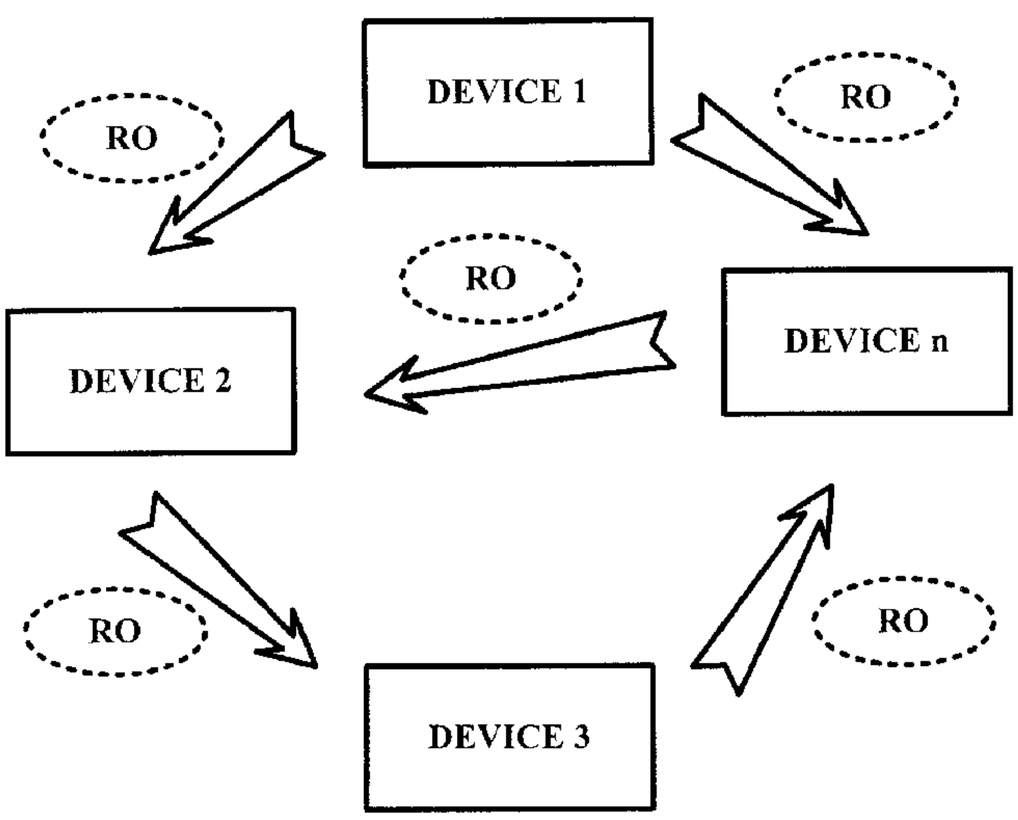
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LC, LK, 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, 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.

(54) Title: METHOD FOR MOVING A RIGHTS OBJECT BETWEEN DEVICES AND A METHOD AND DEVICE FOR USING A CONTENT OBJECT BASED ON THE MOVING METHOD AND DEVICE



(57) Abstract: A method for moving a rights object (RO) between devices, a method of using a content object based on the moving method, and devices using the methods are provided. The moving method includes performing authentication between two devices; securing a connection between the devices; and communicating the rights object between the two devices. The using method includes two devices communicating with each other, the first device having use permission of content objects and the second device including the content objects and corresponding rights objects; the first device searching for the content objects; and the first device using the content object that was found. The device includes an authentication module to authenticate another device; a security formation module to secure a connection for the other device; and a transceiving module which communicates a rights object for which the connection has been secured.

WO 2006/075893 A1

Description

METHOD FOR MOVING A RIGHTS OBJECT BETWEEN DEVICES AND A METHOD AND DEVICE FOR USING A CONTENT OBJECT BASED ON THE MOVING METHOD AND DEVICE

Technical Field

[1] The present invention relates to a digital rights management method and apparatus, and more particularly, to a method and device for moving a rights object (RO) between devices and a method and device for using a content object based on the moving method and device.

Background Art

[2] Recently, digital rights management (DRM) has been actively researched and developed. Commercial services using DRM have already been used or will be used. DRM needs to be used because of the following various characteristics of digital content.

[3] Unlike analog data, digital content can be copied without loss and can be easily reused, processed, and distributed, and only a small amount of cost is needed to copy and distribute the digital content. However, a large amount of cost, labor, and time are needed to produce the digital content. Thus, when the digital content is copied and distributed without permission, a producer of the digital content may lose profit, and enthusiasm for creation may be discouraged. As a result, development of digital content business may be hampered.

[4] There were several efforts to protect digital content. Conventionally, digital content protection has been concentrated on preventing non-permitted access to digital content, permitting only people who have paid charges to access the digital content. Thus, people who have paid charges for the digital content are allowed to access and decrypt digital content while people who have not paid charges are not allowed to access and decrypt digital content. However, when a person who has paid charges intentionally distributes the digital content to other people, the other people can use the digital content without paying charges.

[5] To solve this program, DRM was introduced. In DRM, anyone is allowed to freely access encoded digital content, but a license, referred to as a rights object, is needed to decode and execute the digital content. Accordingly, the digital content can be more effectively protected by using DRM.

[6] FIG. 1 is a diagram illustrating typical digital rights management (DRM). DRM generally involves handling content that is protected by being encrypted or scrambled

and handling licenses allowing access to such encrypted content.

[7] FIG. 1 illustrates a plurality of devices, e.g. device A (110) and device B (150), which desire to access encrypted content, a content provider 120 which provides content, a rights object (RO) issuer 130 which issues an RO containing a license for executing content, and a certificate authority 140.

[8] The device A (110) obtains desired content from the content provider 120, wherein the desired content is encrypted content. The device A (110) purchases an RO containing a license for using the encrypted content from the RO issuer 130. Thereafter, the device A (110) can use the encrypted content using the purchased RO.

[9] Encrypted content can be freely circulated or distributed. Therefore, the device A (110) can freely transmit encrypted content to device B (150). In order for the device B (150) to play back the encrypted content transmitted by the device A (110), the device B (150) needs an RO which can be purchased from the RO issuer 130.

[10] The certificate authority 140 issues a certificate signed with a message specifying an identifier of a device whose public key has been identified, a certificate number, the name of the certificate authority 140, and the expiration dates of the public key of the device and the certificate. The devices, e.g. device A (110) and device B (150), can determine whether devices currently communicating with them are legitimate devices by referencing certificates of the devices issued by the certificate authority 140. The devices may be equipped with certificates issued by the certificate authority 140 when manufacturing the devices A (110) and B (150). The devices A (110) and B (150) may have their certificates reissued by the certificate authority 140 when their certificates expire.

[11] Certificates issued to devices by the certificate authority 140 are signed with a private key of the certificate authority 140. Thus, devices can examine certificates issued to other devices which are currently communicating with them using their public keys. Certificates issued by the certificate authority 140 may be stored in places that are easily accessible by devices or may be stored in the devices.

[12] FIG. 1 illustrates that an RO and encrypted content are directly transmitted between the device A (110) and the device B (150). However, recently, methods of transmitting an RO and encrypted content between devices via a portable storage device have been developed.

[13] In such portable storage device-based methods, a device can store an RO in a portable storage device and can use encrypted content using the RO stored in the porta ble storage device. Therefore, DRM may also be applied to communication between a device and a portable storage device, which is illustrated in FIG. 2.

[14] FIG. 2 is a diagram illustrating DRM for communication between a portable storage device and a device. Referring to FIG. 2, a device A (210) can obtain encrypted

content from a content provider 220. The encrypted content is content protected through DRM. To use, e.g. to play, the encrypted content, a Rights Object (RO) for the encrypted content is needed. An RO contains a definition of a right, a right to content, and constraints to the right and may further include a right to the RO itself. An example of the right to the content may be a playback, or other rights known in the art. Examples of the constraints may be the number of playbacks, a playback time, and a playback duration, or other constraint known in the art. An example of the right to the RO may be a move or a copy, or other right to the RO known in the art. In other words, an RO containing a right to move may be moved to another device or a secure multi media card (MMC). An RO containing a right to copy may be copied to another device or a secure MMC. When the RO is moved, the original RO before the move is de-activated (i.e., the RO itself is deleted or a right contained in the RO is deleted). However, when the RO is copied, the original RO may be used in an activated state even after the copy.

[15] Referring to FIG. 2, the device A (210) receives encrypted content from the content provider 220 and issues a request for an RO to an RO issuer 230 to obtain a right to play back the encrypted content. When receiving the RO from the RO issuer 230, the device A (210) can play back the encrypted content using the RO. The device A (210) may transmit the RO to the device B (250), which possesses the encrypted content, using a portable storage device. The portable storage device may be a secure multimedia card 260 having a DRM function. In this case, the device A (210) and the secure multimedia card 260 authenticate each other, and the device A (210) transmits the RO to the secure multimedia card 260. Then, in order to play back the encrypted content, the device A (210) may issue a request for the RO to the secure multimedia card 260 and receive a right to play back the encrypted content, i.e., a content encryption key, from the secure multimedia card 260 in return. The secure multimedia card 260 and the device B (250) authenticate each other. Then, the secure multimedia card 260 may transmit the RO to the device B (250) or may allow the device B (250) to play back the encrypted content.

Disclosure of Invention

Technical Problem

[16] As described above, in conventional DRM methods, an RO and a content object are transmitted from a service provider to arbitrary devices. Therefore, in order for a device to use a content object, the device must have both the content object and an RO corresponding to the content object. In addition, a consumed RO cannot be exposed outside the device where the consumed RO is currently located, with current state information of the consumed RO kept intact. Therefore, a user may not be able to

properly maintain the RO for which the user has already made payment when purchasing a new device or replacing the device with another device.

Technical Solution

[17] The present invention provides a method and apparatus for transmitting a rights object (RO) between devices, and a method and apparatus for using a content object in which an RO can be transmitted from one device to another together with current state information of the RO and a device can use a content object not only by consuming an RO stored in the device but also by consuming an RO stored in another device.

[18] These and other aspects of the present invention will be described in or be apparent from the following description of exemplary embodiments of the invention.

[19] According an exemplary embodiment of the present invention, there is provided a method of moving a rights object (RO) including two arbitrary devices authenticating each other, securing a connection between the two arbitrary devices, and communicating an RO between the two arbitrary authenticated devices.

[20] According to another exemplary embodiment of the present invention, there is provided a method of using content objects including a first device and a second device communicating with each other, the first device having use permission of content objects and the second device including the content objects and rights objects corresponding to the content objects; the first device searching for the content objects of the second device; and the first device using the content object from the second device found as a result of the search .

[21] According to still another exemplary embodiment of the present invention, there is provided a device including an authentication module which is configured to authenticate another device; a security formation module which is configured to secure a connection for the another device that has been authenticated by the authentication module; and a transceiving module which transmits or receives a rights object for which the connection has been secured by the security formation module.

[22] According to yet another exemplary embodiment of the present invention, there is provided a device of using a content object including a rights object management module which is configured to manage rights objects by searching for devices storing a desired content object and a rights object corresponding thereto; a transceiving module which is configured to send request information for use permission of the desired content object to a device on which the rights object is stored and to receive the use permission of the desired content object from the device on which the rights object is stored; and a content object use module which is configured to use the desired content object .

Description of Drawings

[23] The above and other aspects of the present invention will become more apparent by describing in detail certain exemplary embodiments thereof with reference to the attached drawings in which:

[24] FIG. 1 is a diagram illustrating typical digital rights management (DRM);

[25] FIG. 2 is a diagram illustrating DRM for communication between a portable storage device and a device;

[26] FIG. 3 is a diagram illustrating the format of a rights object (RO) according to an exemplary embodiment of the present invention;

[27] FIG. 4 is a block diagram of a device of moving ROs between devices according to an exemplary embodiment of the present invention;

[28] FIG. 5 is a diagram illustrating a procedure in which ROs are moved among devices according to an exemplary embodiment of the present invention;

[29] FIG. 6 is a diagram illustrating a method of using content objects and consuming ROs according to an exemplary embodiment of the present invention;

[30] FIG. 7 is a diagram illustrating the use of content objects stored in one device by means of another device according to an exemplary embodiment of the present invention;

[31] FIG. 8 is a flowchart illustrating a method of moving ROs between devices according to an exemplary embodiment of the present invention;

[32] FIG. 9 is a flowchart illustrating a method of using content objects and consuming ROs according to an exemplary embodiment of the present invention;

[33] FIG. 10 is a flowchart illustrating a method of using content objects stored in one device by means of another device according to an exemplary embodiment of the present invention; and

[34] FIG. 11 is a diagram illustrating an authentication procedure performed between a device and a multimedia card according to an exemplary embodiment of the present invention.

Mode for Invention

[35] Advantages and aspects of the present invention and methods of accomplishing the same may be understood more readily by reference to the following detailed description of exemplary embodiments and the accompanying drawings. The present invention may be embodied in many different forms and should not be construed as being limited to the exemplary embodiments set forth herein. Rather, these exemplary embodiments are provided so that this disclosure will be thorough and complete and will fully convey the concept of the invention to those skilled in the art, and the present invention will only be defined by the appended claims. Like reference numerals refer to like elements throughout the specification.

[36] The present invention will now be described more fully with reference to the ac-

companying drawings, in which exemplary embodiments of the invention are shown.

[37] Before the detailed description is set forth, terms used in this specification will be described briefly. The description of terms is provided to convey a better understanding of the specification to those having ordinary skill in the art, and terms that are not explicitly defined herein are not intended to limit the broad aspect of the invention.

[38] - Public-Key Cryptography

[39] Public-key cryptography is referred to as an asymmetric cipher in which a key used for encryption is different from a key used for decryption. A public-key algorithm is open to the public, but it is impossible or difficult to decrypt original content with only a cryptographic algorithm, an encryption key, and ciphered text. Examples of a public-key cryptographic system include Diffie-Hellman cryptosystems, Rivest-Shamir-Adleman (RSA) cryptosystems, ElGamal cryptosystems, elliptic curve cryptosystems, or other cryptosystems known in the art. The public-key cryptography is about 100-1000 times slower than symmetric-key cryptography and is thus usually used for key exchange and digital signature not for encryption of content.

[40] - Symmetric-Key Cryptography

[41] Symmetric-key cryptography is a symmetric cipher referred to as secret-key cryptography using the same key encryption and decryption. A data encryption standard (DES) is a most usual symmetric cipher. Recently, applications using an advanced encryption standard (AES) have increased.

[42] - Digital Signature

[43] A digital signature is generated by a signer to indicate that a document has been written. Examples of a digital signature are an RSA digital signature, an ElGamal digital signature, a Digital Signal Algorithm (DSA) digital signature, a Schnorr digital signature, or other digital signature known in the art. When the RSA digital signature is used, a sender encrypts a message with the sender's private key and sends the encrypted message to a recipient. The recipient decrypts the encrypted message. In this case, it is proved that the message has been encrypted by the sender.

[44] - Certificate

[45] A certification authority certifies users of a public key with respect to a public-key cipher. A certificate is a message containing a public key and a person's identity information which are signed by the certification authority using a private key. Accordingly, the integrity of the certificate can be easily considered by applying the public key of the certification authority to the certificate, and therefore, attackers are prevented from modulating a user's public key.

[46] - Random Number

[47] A random number is a sequence of numbers or characters with random properties.

Since it is expensive to generate a complete random number, a pseudo-random number may be used.

[48] - Portable Storage Device

[49] A portable storage device used in the present invention includes a non-volatile memory such as a flash memory which data can be written to, read from, and deleted from and which can be connected to a device. Examples of such portable storage device are smart media, memory sticks, compact flash (CF) cards, xD cards, multimedia cards, or other portable storage devices known in the art.

[50] - Rights Object

[51] A rights object is a kind of license, which includes a right to use an encrypted content or constraints to the right. The term 'the rights object' used in the present invention will be described in more detail with reference to FIG. 3.

[52] FIG. 3 is a diagram illustrating the format of a rights object (RO) according to an exemplary embodiment of the present invention.

[53] Referring to FIG. 3, the RO includes a version field 300, an asset field 320, and a permission field 340.

[54] The version field 300 contains version information of a DRM system. The asset field 320 contains information regarding content data, the consumption of which is managed by the RO. The permission field 340 contains information regarding usage and action that are permitted by a right issuer with respect to the content protected through DRM.

[55] The information stored in the asset field 320 will now be described in detail.

[56] The 'id' information indicates an identifier used to identify the RO. The 'uid' information is used to identify the content the usage of which is dominated by the RO and is a uniform resource identifier (URI) of content data of a DRM content format (DCF).

[57] The 'KeyValue' information contains a binary key value used to encrypt the content, which is referred to as a content encryption key (CEK). The CEK is a key value used to decrypt encrypted content to be used by a device. When the device receives the CEK from a secure MMC, it can use the content.

[58] The permission field 340 is a right to use content permitted by the right issuer. Types of permission include 'Play', 'Display', 'Execute', 'Print', 'Export', or other known permissions in the art.

[59] 'Playback' is a right to display DRM content in an audio/video format. For example, if the encrypted content is a movie or music file, the Play permission may optionally have a constraint. If a specified constraint is present, the DRM agent grants a right to Play according to the specified constraint. If no specified constraints are present, the DRM agent grants unlimited Play rights.

[60] The 'Display' permission indicates a right to display DRM content through a visual device. A DRM agent does not allow access based on Display with respect to content such as gif or jpeg images that cannot be displayed through the visual device. Here, the DRM agent may be a control module, which will be described later in detail with reference to FIG. 7.

[61] The 'Display' permission indicates a right to display DRM content through a visual device.

[62] The 'Execute' permission indicates a right to execute DRM content such as JAVA games and other application programs.

[63] The 'Print' permission indicates a right to generate a hard copy of DRM content such as jpeg images.

[64] The 'Play' permission, the 'Display' permission, the 'Execute' permission, and the 'Print' permission will hereinafter collectively be generally referred to as playback permission.

[65] The 'Export' permission indicates a right to send DRM contents and corresponding ROs to a DRM system other than an open mobile alliance (OMA) DRM system or a content protection architecture.

[66] The 'Export' permission must have a constraint. The constraint specifies a DRM system of a content protection architecture to which DRM content and its RO can be sent. The Export permission is divided into a move mode and a copy mode. When an RO is exported from a current DRM system to another DRM system, the RO is de-activated from the current DRM system in the move mode but is not deactivated from the current DRM system in the copy mode.

[67] FIG. 4 is a block diagram of a device for moving ROs between devices according to an exemplary embodiment of the present invention.

[68] Referring to FIG. 4, the device includes a control module 400, an authentication module 410, a security formation module 420, a transceiving module 430, a content object use module 440, an RO management module 450, a content/RO storage module 460, and an interface module 470.

[69] In the present and following embodiments, a module means, but is not limited to, a software or hardware component, such as a Field Programmable Gate Array (FPGA) or Application Specific Integrated Circuit (ASIC), which performs certain tasks. A module may advantageously be configured to reside on the addressable storage medium and configured to execute on one or more processors. Thus, a module may include, by way of example, components, such as software components, object-oriented software components, class components and task components, processes, functions, attributes, procedures, subroutines, segments of program code, drivers, firmware, microcode, circuitry, data, databases, data structures, tables, arrays,

variables, or other similar components known in the art. The functionality provided for in the components and modules may be combined into fewer components and modules or further separated into additional components and modules.

[70] The authentication module 410 enables authentication between devices that transmit/receive an RO to/from each other. The security formation module 420 forms security between the devices.

[71] The transceiving module 430 allows the devices to transmit/receive an RO to/from each other in a secure state. If a content object and an RO corresponding to the content object are located in different devices and the transceiving module 430 is included in the device that stores the content object, the transceiving module 430 may issue a request for the RO to the device that stores the RO, and receive the RO from the device that stores the RO.

[72] The content object use module 440 uses a content object stored in the device or in another device.

[73] If a content object to be used by the device and an RO corresponding to the content object are located in different devices and the RO management module 450 is included in the device that stores the content object, the RO management module 450 searches for the device that stores the RO.

[74] The content/RO storage module 460 stores content objects and respective cor-responding ROs.

[75] The interface module 470 enables a device which does not possess a content object and a device which possesses both the content object and an RO corresponding to the content object to communicate with each other.

[76] The control module 400 controls the authentication module 410, the security formation module 420, the transceiving module 430, the content object use module 440, the RO management module 450, the content/RO storage module 460, and the interface module 470 and searches for the device or another device for a content object.

[77] A method of transmitting an RO between devices according to an exemplary embodiment of the present invention will now be described in detail with reference to FIG. 5.

[78] FIG. 5 is a diagram illustrating a procedure in which ROs are moved among a plurality of devices according to an exemplary embodiment of the present invention, and FIG. 8 is a flowchart illustrating a method of moving the ROs among the plurality of devices according to an exemplary embodiment of the present invention, illustrating movement of the ROs sequentially over time.

[79] Referring to FIG. 5, devices 1 through n can freely transmit/receive ROs to/from one another. A method of transmitting an RO between two devices without the aid of a

portable storage device will now be described in detail with reference to FIG. 8.

[80] Referring to FIG. 8, two arbitrary devices are respectively labeled as device 1 (810) and device 2 (820). In operation S810, devices 1 and 2 authenticate each other. Here, the authentication between devices 1 and 2 may be carried out using a typical authentication method.

[81] In operation S820, a security formation module 420 forms security between devices 1 and 2. In detail, the formation of security involves generating a security key (operation S822) and allowing devices 1 and 2 to share the security key with each other (operation S824). In operation S830, a transceiving module (not shown) of one of devices 1 and 2, which stores an RO, communicates with a transceiving module (not shown) of the other, which needs to receive the RO. When the RO is transmitted between devices 1 and 2, current state information specifying a consumption state of the RO may be transmitted between devices 1 and 2 together with the RO. An RO provider may decide whether to transmit the current state information together with the RO. In other words, if the RO provider would like to allow only a limited number of rights contained in the RO to be used according to constraints regarding the RO, the RO provider may decide to transmit the current state information together with the RO. On the other hand, if the RO provider would like to allow all of the rights contained in the RO to be used regardless of the constraints regarding the RO, the RO provider may decide not to transmit the current state information together with the RO. This decision may be made arbitrarily by the RO provider.

[82] A method of using a content object stored in a device regardless of whether an RO corresponding to the content object is stored in the device or in another device according to an exemplary embodiment of the present invention will now be described in detail with reference to FIGS. 6 and 9.

[83] FIG. 6 is a diagram illustrating a method of using content objects and consuming ROs according to an exemplary embodiment of the present invention.

[84] Referring to FIG. 6, for convenience, a device which stores a content object will now be referred to as a content object storage device, and a device which only stores an RO will now be referred to as a RO-only storage device. Device 11, which is a content object storage device, can use a content object stored in device 11 by consuming both an RO stored in device 11 and an RO stored in device 21, which is a RO-only storage device, at the same time or by only consuming the RO stored in device 11. On the other hand, device 12, which is also a content object storage device, does not have an RO and can thus use a content object stored in device 12 by consuming a plurality of ROs respectively stored in devices 21, 22, 23, ..., 2n. In other words, a content object can be used by consuming a plurality of ROs respectively stored in a plurality of devices, and an RO can be consumed for a plurality of content

objects respectively stored in a plurality of devices.

[85] This will now be described in further detail with reference to FIG. 9. FIG. 9 is a flowchart illustrating a method of using a content object according to an exemplary embodiment of the present invention. Referring to FIG. 9, for convenience, a device which stores a content object will now be referred to as a first device 910, and a device which only stores an RO will now be referred to as a second device 920.

[86] In operation S910, an RO management module 450 of the first device 910 determines whether an RO corresponding to a content object stored in the first device 910 is stored in the first device 910. In operation S912, if the RO corresponding to the content object stored in the first device 910 is determined, in operation S910, not to be stored in the first device 910, an authentication module 410 of the first device 910 authenticates the second device 920, and an authentication module 410 of the second device 920 authenticates the first device 910. The authentication between the first device 910 and the second device 920 may be carried out using a typical authentication method. In operation S914, a security formation module 420 of the first device 910 forms security between the first device 910 and the second device 920.

[87] The formation of security between the first device 910 and the second device 920 may involve generating a security key and making the first device 910 and the second device 920 share the security key as described above with reference to FIG. 8.

[88] In operation S920, a transceiving module 430 of the first device 910 sends request information for use permission of the content object stored in the first device 910 to the second device 920. In operation S930, the second device 920 receives the request information sent from by the first device 910 and grants the permission to use the content object stored in the first device 910 to the first device 910, and the first device 910 receives the use permission of the content object stored in the first device 910. In operation S940, a content object use module 440 of the first device 910 uses the content object stored in the first device 910. The transmission of the request information sent from the first device 910 and the use permission of the content object stored the first device 910 may be carried out in a secure state.

[89] The first device 910 is illustrated in FIG. 9 as only storing a content object. The first device 910, however, may store both a content object and an RO corresponding to the content object and consume the RO as described above with reference to FIG. 6. Also, the first device 910 may consume two or more ROs at the same time or may use a plurality of content objects by consuming a single RO as described above with reference to FIG. 6.

[90] A method of enabling a device which does not have a content object and an RO to use a content object stored in another device according to an exemplary embodiment of the present invention will now be described in detail with reference to FIGS. 7 and 10.

[91] FIG. 7 is a diagram illustrating the use of content objects stored in one device by means of another device according to an exemplary embodiment of the present invention.

[92] Referring to FIG. 7, devices A1, …, and An do not have content objects and simply consume content objects stored in other devices. On the other hand, device B stores both an RO and a content object. The content object stored in device B may be used by device A1, in which case, the RO stored in device B is consumed by device A1. Once the use of the content object stored in device B by device A1 is terminated, the content object may also be used by device An, in which case, the RO stored in device B is also consumed by device An.

[93] This exemplary embodiment of the present invention will now be described in further detail with reference to FIG. 10. FIG. 10 is a flowchart illustrating a method of using content objects stored in one device by means of another device according to an exemplary embodiment of the present invention.

[94] Referring to FIG. 10, in operation S1010, device A (1010) which has a function of using content objects communicates with device B (1020) which includes both content objects and respective corresponding ROs. The communication between device A (1010) and device B (1020) may be carried out via interface modules 470 of device A (1010) and device B (1020), respectively. The communication between device A (1010) and device B (1020) may be via wire medium or wireless medium. In addition, the communication between device A (1010) and device B (1020) may be carried out using an internet (IP) protocol, a universal serial bus (USB), or a memory card interface. In operation S1020, a control module 400 of device A (1010) searches device B (1020) for a content object desired by device A (1010). When device A (1010) discovers the desired content object from device B (1020) and chooses the searched content object, device A (1010) and device B (1020) may authenticate each other in operation S1022, and security formation modules 420 of device A (1010) and device B (1020) may form security between device A (1010) and device B (1020), as shown in operation S1024. As described above, the formation of security between device A (1010) and device B (1020) may involve generating a security key and making device A (1010) and device B (1020) share the security key.

[95] In operation S1030, a content object use module 440 of device A (1010) uses the searched content object. In operation S1040, device A (1010) consumes an RO corresponding to the searched content object.

[96] In operation S1030, device A (1010) may issue a request for transmission of the searched content object to device B (1020) (operation S1032). Operation S1032 is optional, and thus, device B (1020) may transmit the searched content object entirely or partially to device A (1010) regardless of whether device A (1010) issues a request

for transmission of the searched content object to device B (1020). In operation S1036, a transceiving module 430 of device A (1010) receives the searched content object from device B (1020) and uses the received content object.

[97] The descriptions of the methods of transmitting an RO between devices and using a content object according to the present invention may directly apply to a computer-readable recording medium storing a computer program for executing each of the methods of transmitting an RO between devices and using a content object according to the present invention.

[98] In order that devices can communicate with each other to transmit/receive an RO to/from each other, it is advantageous for the devices to authenticate each other first. Since authentication between devices is very similar to authentication between a device and a multimedia card, only the authentication between a device and a multimedia card will now be described in detail.

[99] FIG. 11 is a diagram illustrating an authentication procedure performed between a device 10 and a multimedia card 20 according to an exemplary embodiment of the present invention. Here, a subscript 'H' of an object indicates that the object is possessed or generated by a host (device) and a subscript 'S' of an object indicates that the object is possessed or generated by a multimedia card.

[100] Referring to FIG. 11, an identifier ID_H, a certificate $CERTIFICATE_H$, and an encrypted random number $ENCRYPTED\ RANDOM\ NUMBER_H$ are generated or possessed by a host, i.e., the device 10, and an identifier ID_S, a certificate $CERTIFICATE_S$, and an encrypted random number $RANDOM\ NUMBER_S$ are generated or possessed by the multimedia card 20.

[101] FIG. 11 illustrates how the device 10 and the multimedia card 20 authenticate each other and exchange random numbers with each other. The random numbers may be used for generating a session key. In FIG. 11, a plurality of horizontal arrows respectively represent a plurality of processes of the authentication between the device 10 and the multimedia card 20 and accompany short descriptions of the processes and parameters and data transmitted in the processes. In addition, the direction of each of the horizontal arrows represents the direction in which parameters and data are transmitted between the device 10 and the multimedia card 20.

[102] The device 10 may issue commands, and the multimedia card 20 may perform its operations in response to the commands issued by the device 10.

[103] For example, in operation S10, the device 10 transmits an authentication request command to the multimedia card 20, and the multimedia card 20 transmits the identifier $IDENTIFIER_S$, the certificate $CERTIFICATE_S$, and the encrypted random number $RANDOM\ NUMBER_S$ of the multimedia card 20 to the device 10 in response to the authentication request command.

[104] Alternatively, both the device 10 and the multimedia card 20 may issue commands. In this case, in operation S20, the multimedia card 20 may transmit the identifier $IDENTIFIER_S$, the certificate $CERTIFICATE_S$, and the encrypted random number $RANDOM\ NUMBER_S$ of the multimedia card 20 to the device 10 together with a authentication response command.

Industrial Applicability

[105] As described above, according to the present invention, it is possible to provide users with methods of transmitting ROs between devices, using content objects, and consuming ROs that can be applied to an environment where various types of devices such as mobile phones, home electronic appliances, small memory storage devices, and portable imaging devices are connected to one another based on the digital convergence concept by using DRM technology.

[106] While the present invention has been particularly shown and described with reference to exemplary embodiments thereof, it will be understood by those of ordinary skill in the art that various changes in form and details may be made therein without departing from the spirit and scope of the present invention as defined by the following claims. Therefore, it is to be understood that the above-described exemplary embodiments have been provided only in a descriptive sense and will not be construed as placing any limitation on the scope of the invention.

Claims

[1] A method of moving a rights object comprising:
performing authentication between two arbitrary devices;
securing a connection between the two arbitrary devices; and
communicating the rights object between the two authenticated arbitrary devices.

[2] The method of claim 1, wherein the securing a connection comprises:
generating a security key as a result of the authentication; and
the two arbitrary devices sharing the security key.

[3] The method of claim 1, wherein the communicating comprises communicating current state information which includes a consumption state of the rights object and the rights object.

[4] The method of claim 3, wherein the communicating is performed at an option of a provider of the rights object.

[5] A method of using a content object comprising:
determining whether the content object and a rights object corresponding to the content object are stored in a same device;
if the content object and the rights object are not stored in the same device, a first device which stores the content object sending request information for use permission of the content object to a second device which stores the rights object;
the first device receiving use permission information from the second device; and
the first device using the stored content object.

[6] The method of claim 5, wherein, if the content object and the rights object are not stored in the same device, the determining comprises:
the first device and the second device authenticating each other; and
securing a connection between the first device and the second device.

[7] The method of claim 6, wherein the securing the connection comprises:
generating a security key as a result of the authentication; and
the first device and the second device sharing the security key.

[8] The method of claim 5, wherein the request information for use permission of the content object is transmitted in a secure state.

[9] The method of claim 5, wherein the request information for use permission of the content object is received in a secure state.

[10] The method of claim 5, wherein the rights object is a rights object stored in the first device.

[11] The method of claim 5, wherein the rights object comprises at least one rights object.

[12] A method of using content objects comprising:
a first device and a second device communicating with each other, the first device having use permission of content objects and the second device including the content objects and rights objects corresponding to the content objects;
the first device searching for the content objects of the second device; and
the first device using the content object from the second device found as a result of the search.

[13] The method of claim 12 further comprising the first device consuming a rights object corresponding to content object which is found as a result of the search and stored in the second device.

[14] The method of claim 12, wherein the searching comprises:
when the first device searches for content objects of the second device, the first and second devices authenticating each other; and
securing a connection between the two authenticated devices.

[15] The method of claim 14, wherein the securing the connection comprises:
generating a security key; and
the first and second devices sharing the security key.

[16] The method of claim 12, wherein the communicating comprises communicating using an IP protocol, a USB, or a memory card interface.

[17] The method of claim 12, wherein the communicating comprises:
the second device transmitting the searched content objects entirely or partially to the first device; and
the first device using the content objects which are found as a result of the search and received from the second device entirely or partially.

[18] The method of claim 17, further comprising the first device requesting transmission of a desired content object to the second device, before the content objects, which are found as a result of the search, are transmitted.

[19] A computer-readable medium storing a computer program for executing a method of moving a rights object, the method comprising:
performing authentication between two arbitrary devices;
securing a connection between the two arbitrary devices; and
communicating the rights object between the two authenticated arbitrary devices.

[20] A device comprising:
an authentication module which is configured to authenticate another device;
a security formation module which is configured to secure a connection for the another device that has been authenticated by the authentication module; and
a transceiving module which transmits or receives a rights object for which the connection has been secured by the security formation module.

[21] The device of claim 20, wherein the security formation module generates a security key as a result of the authentication performed by the authentication module and makes the device that comprises the security formation module and the another device that has been authenticated share the security key.

[22] The device of claim 20, wherein the transceiving module transmits current state information which specifies a consumption state of the rights object together with the rights object.

[23] The device of claim 22, wherein a provider of the rights object chooses whether to transmit the current state information together with the RO.

[24] A device for using a content object comprising:
a rights object management module which is configured to manage rights objects by searching for devices storing a desired content object and a rights object cor-responding thereto;
a transceiving module which is configured to send request information for use permission of the desired content object to a device on which the rights object is stored and to receive the use permission of the desired content object from the device on which the rights object is stored; and
a content object use module which is configured to use the desired content object.

[25] The apparatus of claim 24 further comprising:
an authentication module which is configured to enable a second device on which the desired content object is stored and the device on which the rights object is stored to authenticate each other; and
a security formation module which is configured to secure a connection between the device on which the desired content object is stored and the device on which the rights object is stored.

[26] The apparatus of claim 25, wherein the security formation module generates a security key as a result of the authentication performed by the authentication module and makes the device on which the desired content is stored and the device on which the rights object is stored share the security key.

[27] The apparatus of claim 24, wherein the transceiving module transmits the request information for the use permission of the desired content object in a secure state.

[28] The apparatus of claim 24, wherein the transceiving module transmits the use permission of the desired content object in a secure state.

[29] An apparatus for using a content object comprising:
an interface module which communicates with a device which includes both content objects and respective corresponding rights objects;
a control module which searches the device for a desired content object; and

a content object use module which uses the desired content object which is found as a result of the search.

[30] The apparatus of claim 29, wherein the content object use module consumes a rights object corresponding to the desired content object which is found as a result of the search and is stored in the device.

[31] The apparatus of claim 29 further comprising:
an authentication module which authenticates the device when the control module searches the device for the desired content object; and
a security formation module which secures a connection for the device if the device is successfully authenticated by the authentication module.

FIG. 1

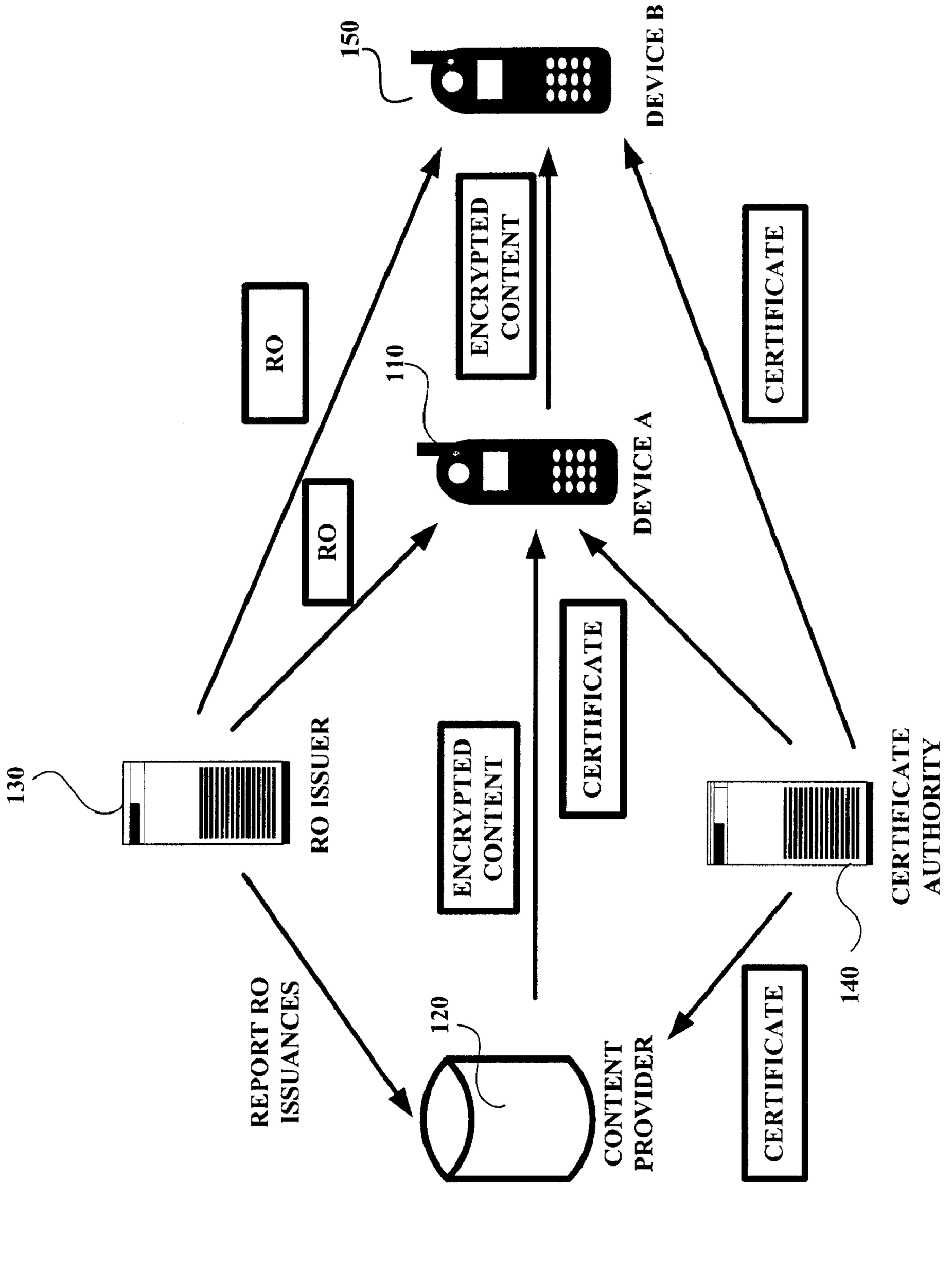

150
DEVICE B
RO
ENCRYPTED CONTENT
CERTIFICATE
110
RO
DEVICE A
130
RO ISSUER
ENCRYPTED CONTENT
CERTIFICATE
CERTIFICATE AUTHORITY
REPORT RO ISSUANCES
120
CONTENT PROVIDER
140
CERTIFICATE

FIG. 2

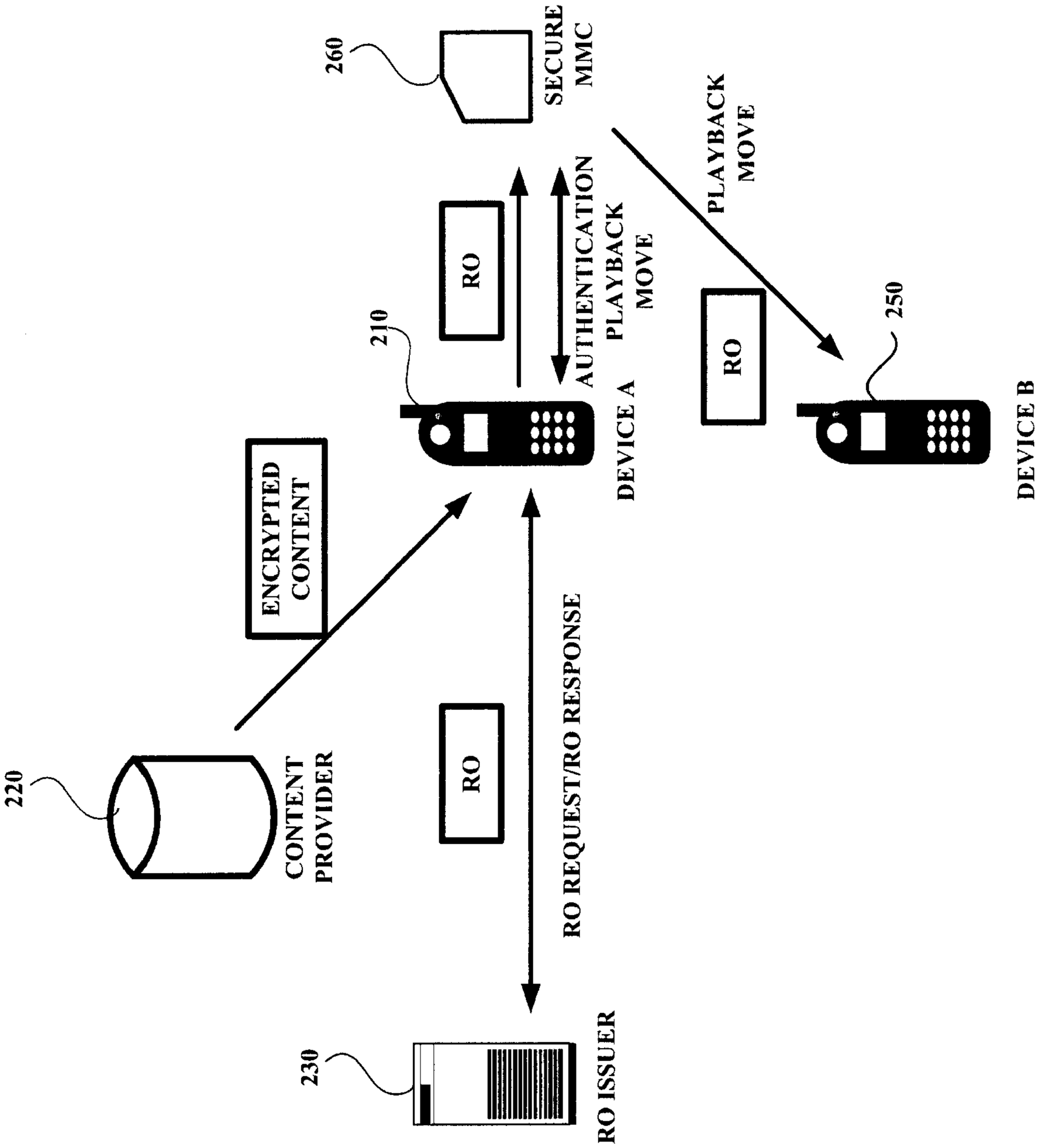

260
SECURE MMC
RO
AUTHENTICATION
PLAYBACK MOVE
PLAYBACK MOVE
210
250
DEVICE A
DEVICE B
ENCRYPTED CONTENT
220
CONTENT PROVIDER
RO
RO REQUEST/RO RESPONSE
230
RO ISSUER

FIG. 3

	DESCRIPTION	Type
VERSION(300)	DRM System Version	1 byte
ASSET (320)	Asset Name	Not Fixed
	Content URI	URI (256 byte)
	Subscription id	Not Fixed
	Content Encryption Key	128 bits
	...	...
PERMISSION (340)	RO ID	Not Fixed
	Constraint	Constraint
	Constraint	Constraint
	Constraint	Constraint
	Constraint	Constraint
	Move or Copy	4 bytes
	Constraint	Constraint
	...	...

ASSET (320)	Id	
	uid	
	Inherit	
	Key Value	
	...	
PERMISSION (340)	Idref	
	Playback	
	Display	
	Excute	
	Print	
	Export	Mode
		Constraint
	...	

FIG. 4

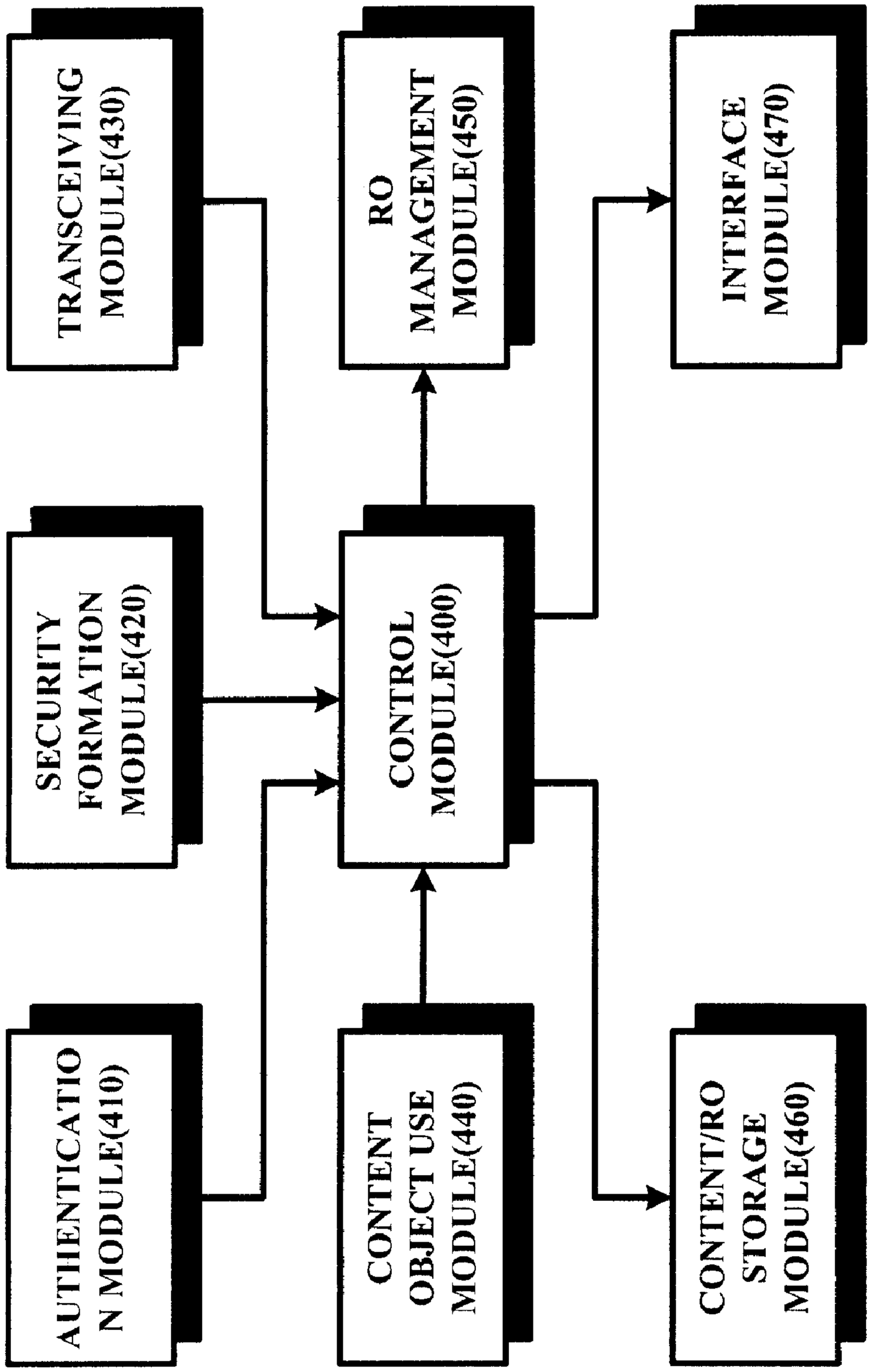

TRANSCEIVING MODULE(430)
RO MANAGEMENT MODULE(450)
INTERFACE MODULE(470)
SECURITY FORMATION MODULE(420)
CONTROL MODULE(400)
AUTHENTICATIO N MODULE(410)
CONTENT OBJECT USE MODULE(440)
CONTENT/RO STORAGE MODULE(460)

FIG. 5

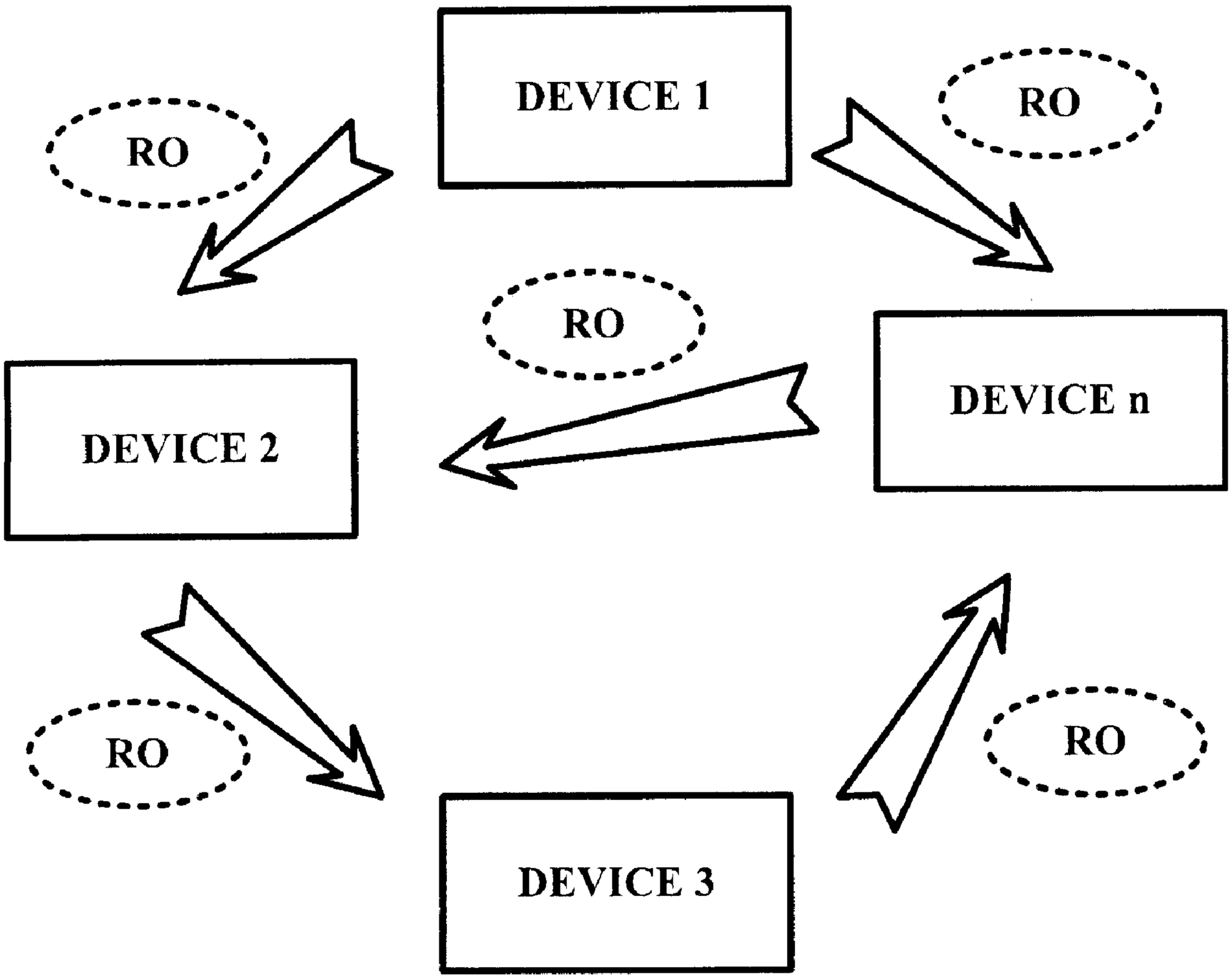


FIG. 6

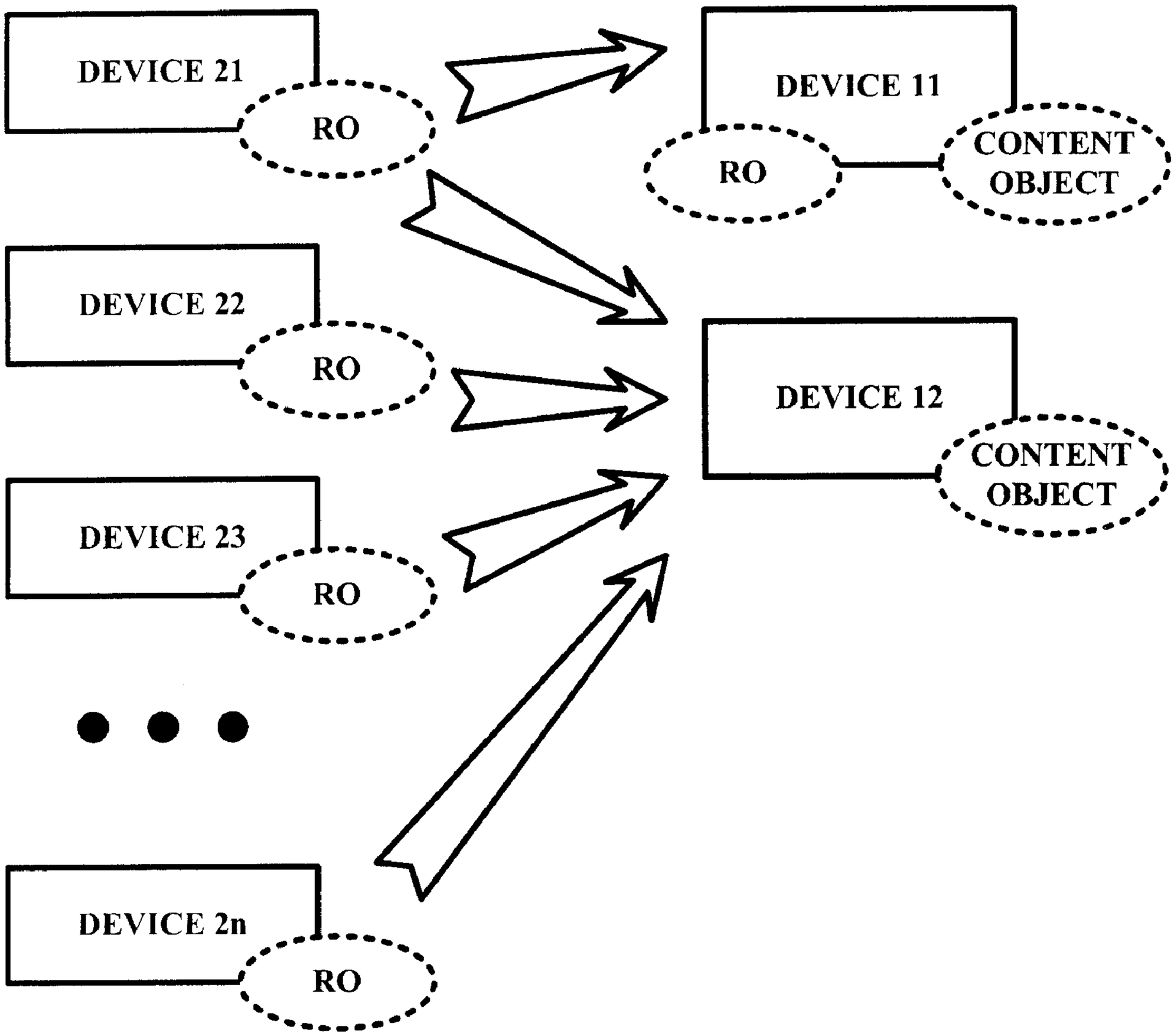

DEVICE 21
RO
DEVICE 11
RO
CONTENT OBJECT
DEVICE 22
RO
DEVICE 12
CONTENT OBJECT
DEVICE 23
RO
DEVICE 2n
RO

FIG. 7

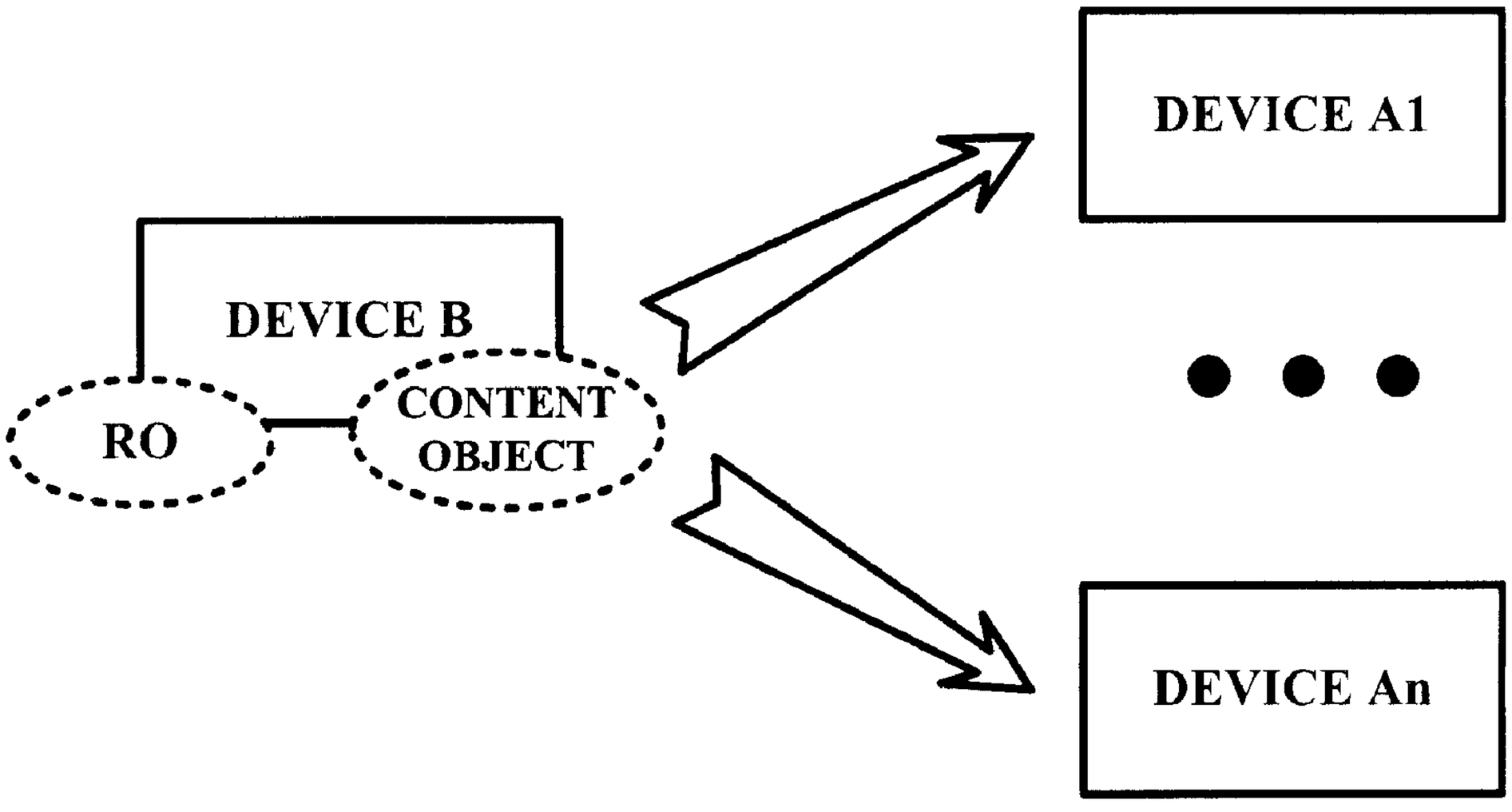

DEVICE A1
DEVICE B
RO
CONTENT OBJECT
DEVICE An

FIG. 8

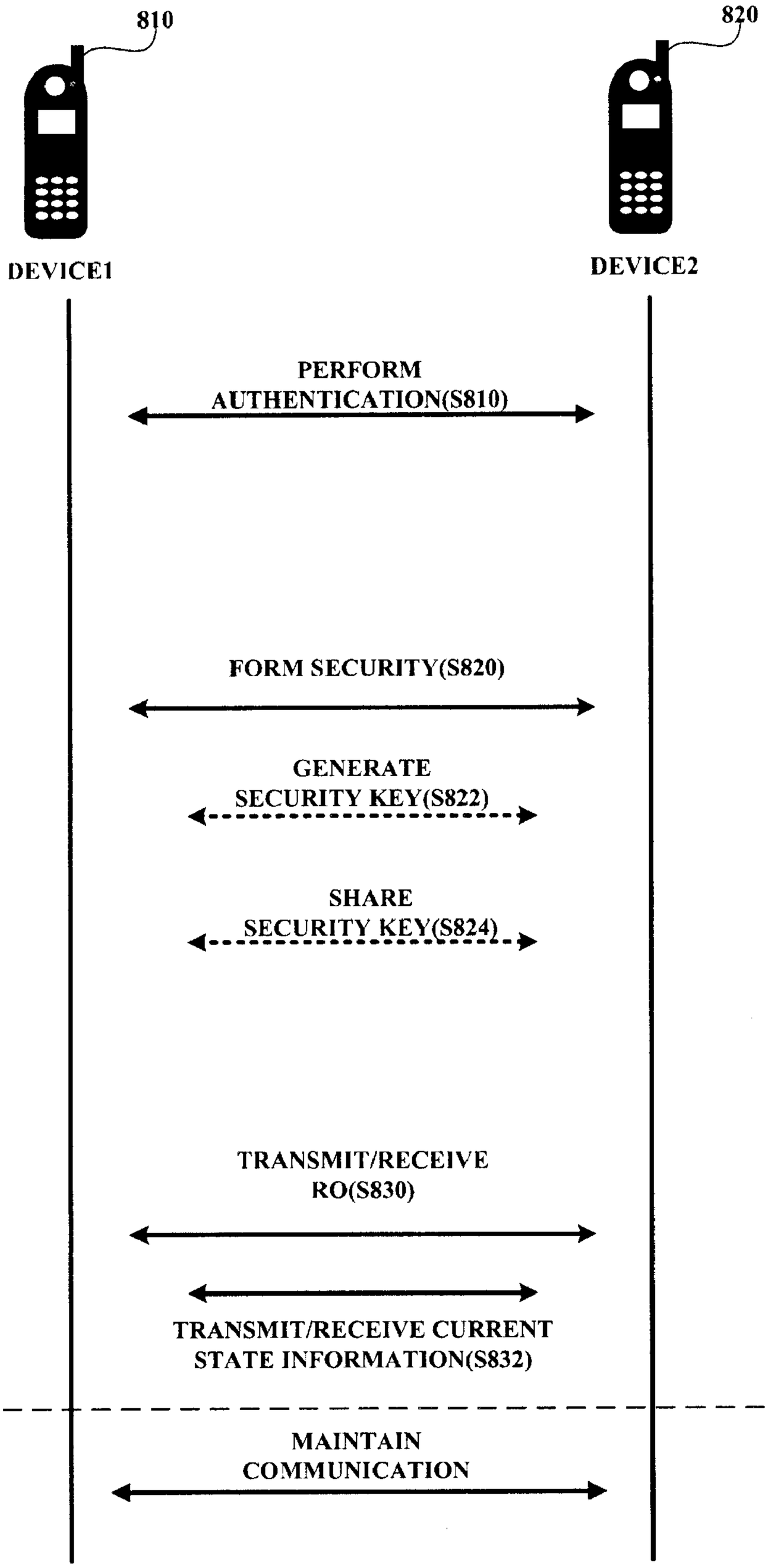

810
820
DEVICE1
DEVICE2
PERFORM AUTHENTICATION(S810)
FORM SECURITY(S820)
GENERATE SECURITY KEY(S822)
SHARE SECURITY KEY(S824)
TRANSMIT/RECEIVE RO(S830)
TRANSMIT/RECEIVE CURRENT STATE INFORMATION(S832)
MAINTAIN COMMUNICATION

FIG. 9

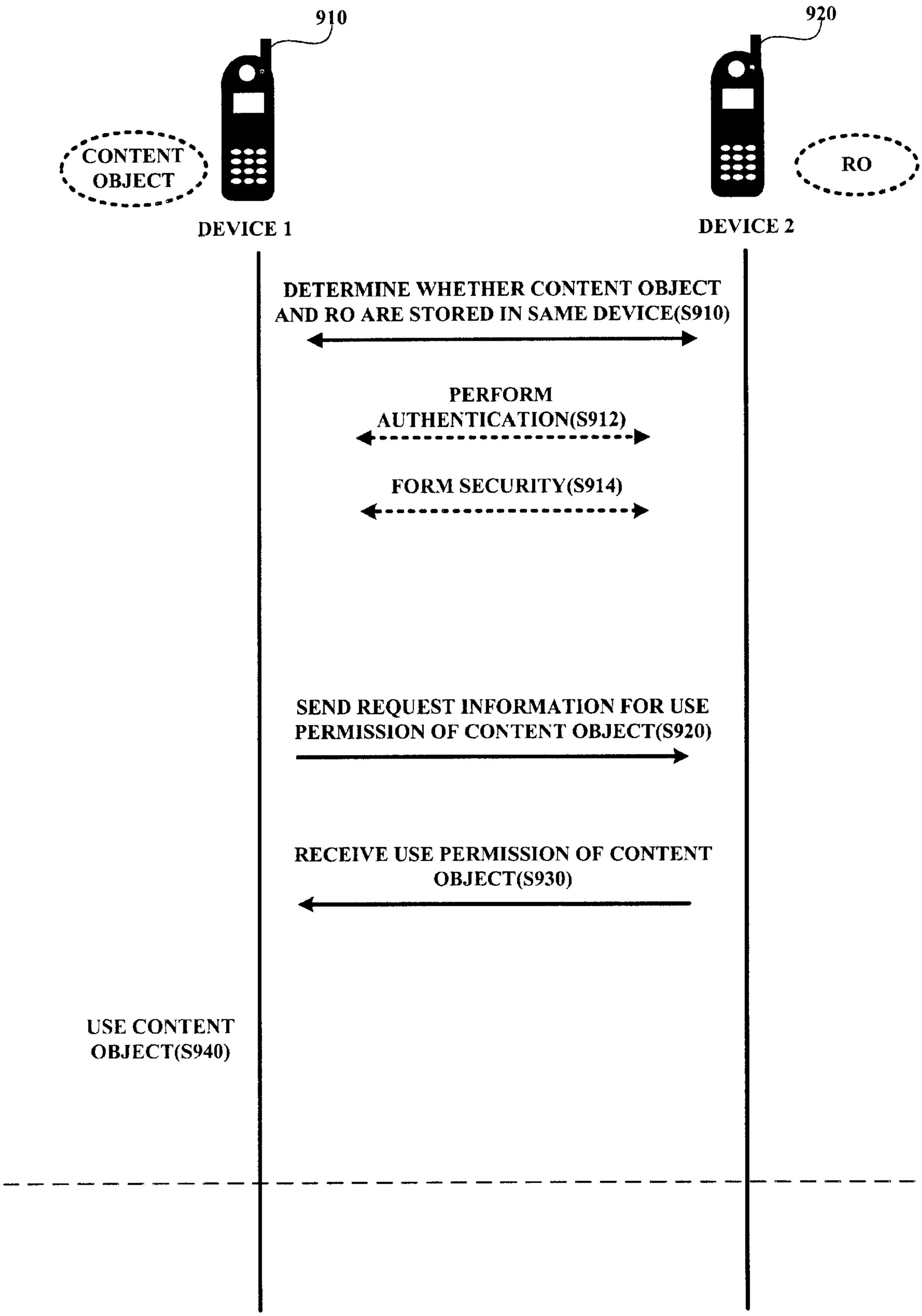

910
920
CONTENT OBJECT
RO
DEVICE 1
DEVICE 2
DETERMINE WHETHER CONTENT OBJECT AND RO ARE STORED IN SAME DEVICE(S910)
PERFORM AUTHENTICATION(S912)
FORM SECURITY(S914)
SEND REQUEST INFORMATION FOR USE PERMISSION OF CONTENT OBJECT(S920)
RECEIVE USE PERMISSION OF CONTENT OBJECT(S930)
USE CONTENT OBJECT(S940)

FIG. 10

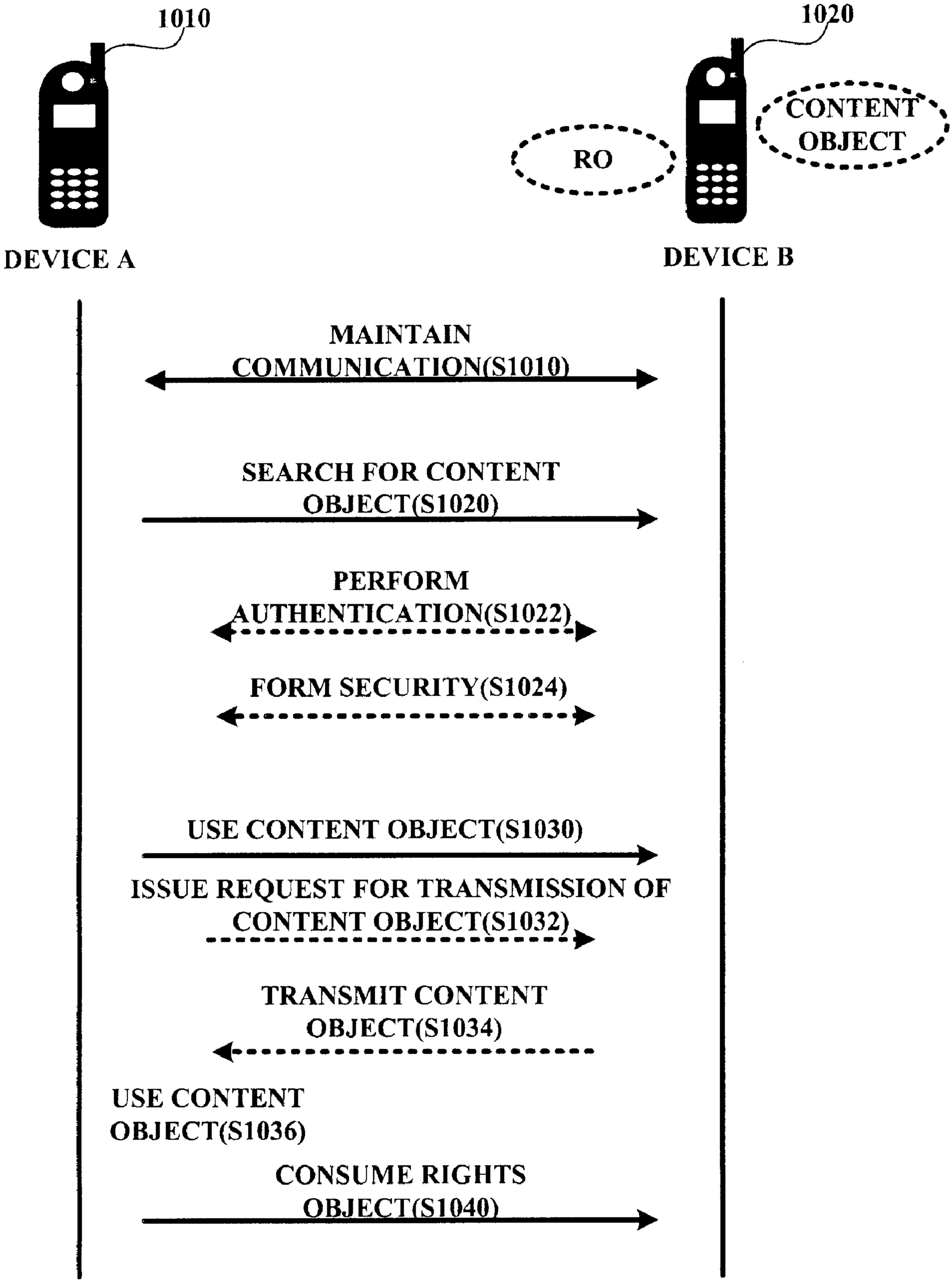

1010
1020
RO
CONTENT OBJECT
DEVICE A
DEVICE B
MAINTAIN COMMUNICATION(S1010)
SEARCH FOR CONTENT OBJECT(S1020)
PERFORM AUTHENTICATION(S1022)
FORM SECURITY(S1024)
USE CONTENT OBJECT(S1030)
ISSUE REQUEST FOR TRANSMISSION OF CONTENT OBJECT(S1032)
TRANSMIT CONTENT OBJECT(S1034)
USE CONTENT OBJECT(S1036)
CONSUME RIGHTS OBJECT(S1040)

FIG. 11

AUTHENTICATION DEVICE

MULTIMEDIA CARD

REQUEST FOR AUTHENTICATION(S10)

ID_H/CERTIFICATE$_H$

EXAMINE CERTIFICATE$_H$(S12)

GENERATE RANDOM NUMBER$_S$(S14)

ENCRYPT RANDOM NUMBER$_S$(S16)

RESPOND TO REQUEST FOR AUTHENTICATION(S20)

ID_S/CERTIFICATE$_S$/ENCRYPTED RANDOM NUMBER$_S$

EXAMINE CERTIFICATE$_S$ AND DECRYPT RANDOM NUMBER$_S$(S22)

GENERATE RANDOM NUMBER$_H$(S24)

ENCRYPT RANDOM NUMBER$_H$(S26)

GENERATE SESSION KEY(S42)

EXAMINE SESSION KEY(S52)

ISSUE REQUEST FOR FINAL AUTHENTICATION(S30)

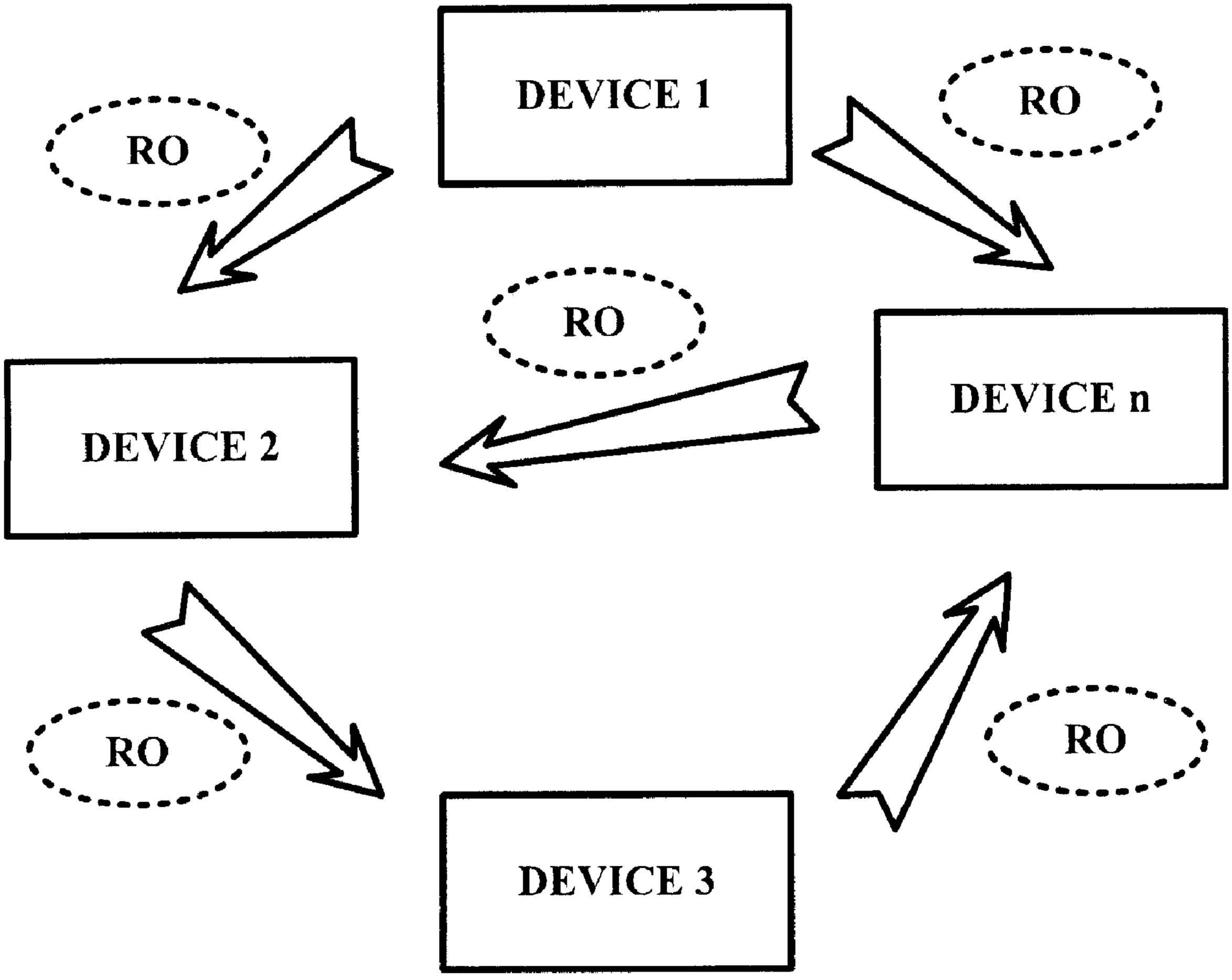
ENCRYPTED RANDOM NUMBER$_H$

DECRYPT RANDOM NUMBER$_H$(S32)

GENERATE SESSION KEY(S40)

RESPOND TO REQUEST FOR FINAL AUTHENTICATION(S50)

ENCRYPTED RANDOM NUMBER$_H$ USING SESSION KEY


DEVICE 1
RO
RO
RO
DEVICE 2
DEVICE n
RO
RO
DEVICE 3