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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 March 2007 (08.03.2007)

PCT

(10) International Publication Number
WO 2007/026276 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/IB2006/052890

(22) International Filing Date: 22 August 2006 (22.08.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
200510099453.5 29 August 2005 (29.08.2005) CN

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

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CHIU, Tom** [US/CN]; Philips Electronics China, 21/F Kerry Office Building 218 Tian Mu, Xi Road, Shanghai 200070 (CN). **YUAN, Hairong** [CN/CN]; Philips Electronics China, 21/F Kerry Office Building 218 Tian Mu, Xi Road, Shanghai 200070 (CN). **BOLTZE, Thomas** [DE/CN]; Philips Electronics China, 21/F Kerry Office Building 218 Tian Mu, Xi Road, Shanghai 200070 (CN).

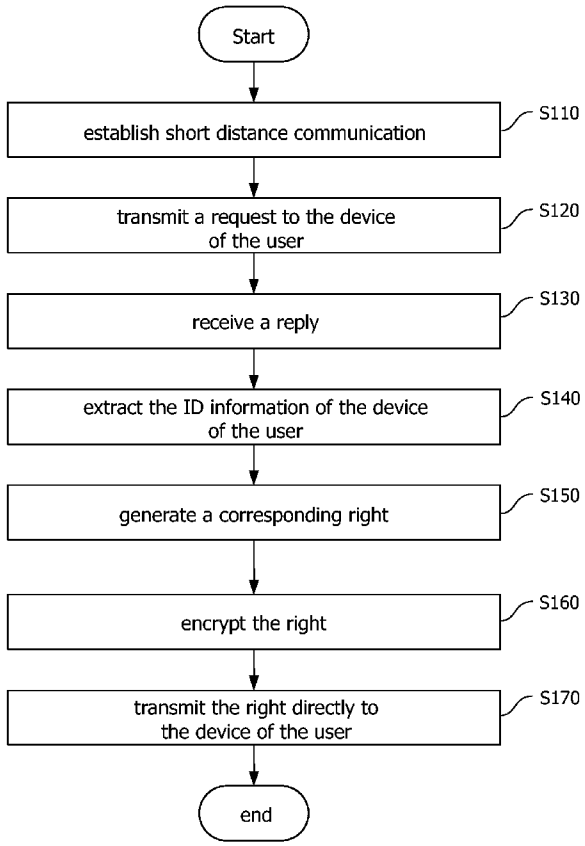
(74) Common Representative: **KONINKLIJKE PHILIPS ELECTRONICS N.V.**; c/o Haque, Azir, Philips Electronics China, 21/F Kerry Office Building, 218 Tian Mu Xi Lu Road, Shanghai 200070 (CN).

(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, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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: METHOD AND APPARATUS FOR AUTHORIZING TO USE A CONTENT



(57) Abstract: The present invention relates to a DRM (Digital Right Management) method and apparatus, and particularly to a method and apparatus for authorizing to use a content. Provided is a method for authorizing to use a content, enabling a device of a content provider to authorize a device of a user to use the content, wherein both the device of the content provider and the device of the user are capable of performing short distance communication, comprising the steps of: establishing a short distance communication with the device of the user when the device of the content provider and the device of the user are located within a predetermined short distance; authorizing the device of the user to use the content within the predetermined short distance. According to the present invention, the authorization process is secure and convenient in operation.

WO 2007/026276 A2

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).

Declaration under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *without international search report and to be republished upon receipt of that 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.

METHOD AND APPARATUS FOR AUTHORIZING TO USE A CONTENT

FIELD OF THE INVENTION

The present invention relates to a DMA (Digital Right Management) method and apparatus, and more particularly, to a method and apparatus for authorizing to use a content.

BACKGROUND OF THE INVENTION

The amount of digital contents becomes larger and larger along with the rapid development of the network and digital technologies. With the widespread distribution of the digital contents via electronic devices or internet, the digital contents owners wish that their intellectual property right for the digital contents should be protected while the contents are being distributed and used by users.

The existing digital content right management adopts two types of basic approaches: for the first type, the digital content right management is performed by transmitting decryption key through secure transmission path; for the second type, the digital content right management is performed in a central controlled manner.

In the first approach of the digital content right management, firstly the digital content is encrypted with predetermined encryption key; then, the encrypted digital content is distributed through common transmission path. And the decryption key corresponding to the predetermined encryption key is distributed to the user of the digital content through secure transmission path. A disadvantage of this approach is that both the provider and user of the digital content have to remember complex passwords, however, this kind of complex passwords are often difficult to be remembered and the operation is troublesome. Another disadvantage of this approach is that complex arrangement and high cost are required to setup a secure transmission path.

In the second approach of the digital content right management, the central controlled mechanism is such a digital content right management scheme that is provided to large enterprises (e.g. content provider). In such a scenario, digital contents are provided in a central server, users or terminal equipments requesting to use the digital contents have to register via the digital content right management system, and all the requests for using the

digital contents will be handled by a central server. All the usage rules of the digital content right are constituted and maintained by the administrator of the digital content right management system according to the demand of the digital content owner. At present, there are a number of technologies to implement an authorization domain system, for example, the international patent application WO2004/038568, filed on Oct 15th, 2003, by the same applicant of the present application, has disclosed a method and apparatus for authorizing to use contents. The entire contents of this patent application document are hereby incorporated as reference. In the digital content right management approaches, the authorization of digital contents can only be performed through authorization domain digital right manage system. The constitution and maintenance of authorization domain digital right manage system are complex, and therefore, a high cost is needed. A further disadvantage of this approach is that a complex system is needed to determine the credible level of the authorized object (the authorized user or user's device of contents).

The OMA (Open Mobile Alliance) also proposed a solution to enable the digital content protection. The OMA digital content right management system firstly must register users or terminal equipments requesting to use the digital contents through digital content right management agent (DRM agent), and the users can receive and use the right for using the content defined by the digital content owner through the authorized terminal equipments. In this solution, the registered digital content right management agent (DRAM agent), users, or terminal equipments must be included when the issuer of the digital content right defines the Right Object.

Along with the popularity of digital electronic devices and multimedia editing tools, more and more individuals and mid-and-small scale enterprises possess considerable amount of digital contents, and they would like to share the digital contents with their families, friends and commercial partners. Needless to say, they wish that the procedure to authorize their families, friends or commercial partner to use contents be safe. Furthermore, the procedure of share is simple and convenient, without the necessity of remembering complex keys, performing complex operation, and authorizing the others, through a central controlled authorization system, to use digital contents.

OBJECT AND SUMMARY OF THE INVENTION

The present invention is an improvement with respect to the existing technical

solutions. In the present invention, a content provider authorize, within a short distance of which the provider feels secure, the content to the device of the user, so as to implement a secure and convenient authorization process.

One object of the present invention is to provide a method for authorizing to use a content, enabling a device of a content provider to authorize a device of a user to use the content, wherein both the device of the content provider and the device of the user are capable of performing short distance communication, comprising the steps of: establishing a short distance communication with the device of the user when the device of the content provider and the device of the user are located within a predetermined short distance; authorizing the device of the user to use the content within the predetermined short distance.

According to an embodiment of the invention, the short distance communication is NFC (Near Field Communication), and the predetermined short distance is a distance within which the NFC is able to perform communication.

According to another embodiment of the invention, the short distance authorization step comprises: acquiring means for acquiring an ID information of the device of the user; generating means for generating a corresponding right for using the content according to the ID information; and

transmitting means for transmitting the right for using the content directly to the device of the user within the predetermined short distance.

The present invention further provides an authorization apparatus for authorizing to use a content, enabling a device of a content provider to authorize a device of a user to use the content, wherein both the device of the content provider and the device of the user are capable of performing short distance communication, comprising: establishing means for establishing a short distance communication with the device of the user when the device of the content provider and the device of the user are located within a predetermined short distance; authorizing means for authorizing the device of the user to use the content within the predetermined short distance.

According to the present invention, it is within a predetermined short distance that a provider's device of a content fulfils the authorization for the device of the user, for example, within a scope that the content provider's eyesight can reach, such that the security of the authorization process is enhanced greatly. Meanwhile, since the device of

the user is located within a predetermined short distance scope, the content provider may in some extent have more knowledge about the reliability of the user and user's device of the content.

Furthermore, according to the present invention, since the authorization for the device of the user is performed directly by the device of the content provider without any intermediate, this reduces the complexity of the authorization process, and also enhances the security of the authorization process.

Other objects and advantages of the present invention will be apparent and the present invention will be more fully understood from the following description taken in conjunction with the accompanying drawings and the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention and related advantages thereof will be further elaborated by means of the following exemplary embodiments and the appended drawings, wherein:

Fig.1 shows a schematic flow chart for authorizing to use an encrypted content according to an embodiment of the present invention;

Fig.2 shows a schematic block diagram of an apparatus for authorizing to use an encrypted content according to an embodiment of the present invention.

Throughout the drawings, the same or similar elements are denoted by the same reference numerals.

DETAILED DESCRIPTION OF THE INVENTION

Fig.1 shows a schematic flow chart for authorizing to use an encrypted content according to an embodiment of the present invention. The authorization process is used for a provider's device of a content authorizing, within a short distance in Peer-to-Peer way, the device of the user to use the content, wherein the device of the content provider and the device of the user are capable of performing short distance communication.

A content may be a document, a digital photograph, or a section of digital video recording. A content may be encrypted by means of various encryption methods. More suitably, a user's device ID of a content is used to encrypt the content.

Of course, the content may also be unencrypted. For example, the authorized device is a reliable device, which cannot play a content without acquiring a right for using the content.

A content may be transmitted to the device of the user from a provider's device of the content, and a content may also be stored in a certain server, of course, a content may also have been stored in the device of the user. As for how to acquire a content itself, it may be performed in many existing ways.

Firstly, establish a short distance communication (step S110).

A short distance communication with the device of the user is established when the device of the content provider and the device of the user are located within a predetermined distance. The predetermined value is a short distance within which the content provider could trust the user of the content or the device of the user. For example, the predetermined value is within the scope that the content provider's eyesight could reach, thus, the content provider could get to know and trust the user of the content and the device of the user.

Another example of the predetermined value is a distance within which Near Field Communication (NFC) is able to perform communication. Here, both the device of the content provider and the device of the user are capable of performing NFC communication. The NFC is a short distance communication technology, which is developed on the basis of Contactless IC Card technology. It has inherent security and lower power consumption just due to the short distance communication. Operating when approached, without the necessity to establish a communication connection manually, makes it very suitable to use in consumption electronic product field.

In the ECMA340 (NFCIP Near Field Communication – Interface and Protocol -1), there defined two communication modes of NFC: Active Communication Mode and Passive Communication Mode. NFCIP-1 device supports the transmission rate of 106kbps, 212kbps, and 424kbps.

In the active communication mode, both an initiator device and a target device use the RF field generated by themselves to perform the communication. The active communication mode is a standard mode of peer-to-peer communication.

In the passive communication mode, the initiator device is responsible to generate

the RF field, and the target device responds to the request from the initiator device in the RF field. The passive communication mode is an extended mode of peer-to-peer communication. In this mode, the target device does not generate a RF field so as to save power. The passive communication mode is compatible with ISO 14443A communication mode.

In order to establish an NFC connection between a provider's device of a content and the device of the user, the secure communication connection could be established as long as they are close to each other within a predetermined value, without other arrangements.

Other short distance communication technologies, such as IrDA (Infrared Data Association), Bluetooth, WIFI (Wireless Fidelity, also referred to as 802.11b standard), Zigbee, and so on, may also be used to establish a short distance communication, when the distance between a provider's device of a content and the device of the user is within a predetermined value of which the content provider feels secure.

Secondly, send a request to the device of the user (step S120).

A request, which demands to authorize a right for using the content, is sent to the device of the user.

Thirdly, receive a reply (step S130).

A reply, in which an ID information (identification information) of the device of the user is contained, is received from the device of the user. An example of the ID information of the device of the user is the ID number of the device of the user. The ID information may also be the ID number of the user of the content.

Then, extracted the ID information of the device of the user (step S140).

The ID number of the device of the user is extracted from the reply of the device of the user.

Step S120, S130, and S140 are used to acquire an ID information of a user's device of a content. Similarly, acquiring an ID information of a user's device of a content could also be implemented by the following steps of: firstly, receiving a request, which demands to use the content and in which the ID information of the device of the user is contained, from the device of the user; then, extracting the ID information of the device of the user

from the request.

Next, generate a corresponding right for using the content (step S150).

The generated right for using the content contains the ID number of the device of the user. The right for using the content may take the form of a right for using the content certificate of a content. Table 1 shows an example of the right for using the content certificate of a content.

Content right for using the content certificate

ID number of a content
Key
ID number of a user's device of a content
Right for using the content
Digital signature

Table1

The key is a decryption key for the encrypted content. For example, when the content is encrypted with the user's device ID of the content, the decryption key for the content is the user's device ID of the content.

A right for using the content of a content could be set in a flexible manner. The right for using the content may be one or more of the following: a content could be used when a user's application device of the content coincides with a specific CPU type; the content could be used when a operation system of a user's application content of the content is in accordance with a specific type; the content could be used when a user of the content is at a specific IP address; a user of the content may use the content at a specific time, for example, a certain timing in a certain day, or a certain day in a certain week; a user of the content could use the content when the user belongs to a certain type, for example, sex, age, career, nationality, and so on of the user.

The right for using the content of a content may also be one or more of the following: the time for viewing the content is limited; the given times for which the content could be viewed is limited; it is prescribed that the content cannot be copied; it is prescribed that the content cannot be saved; it is prescribed that the content cannot be edited; it is prescribed

that only the video section or the audio section of the content can be used; and so on.

The right for using the content comprises authorizing a set of subscriber equipments to use the content, wherein the set of subscriber equipments include the device of the user. According to the right for using the content, after a user's device of a content among the set of subscriber equipments is authorized, all the other equipments of the set of subscriber equipments can acquire an authorization to use the content from the device of the user.

Next, the right for using the content is encrypted (step S160).

The right for using the content is encrypted, such that only the authorized user of the content can use the content according to the right for using the content, while other users cannot be authorized to use the content. Of course, it may be not necessary to encrypt the right for using the content.

One right for using the content is encrypted with the ID number of the device of the user. The encryption process may be implemented by using One-Way Hash Algorithm such as MD (Message Digest), SHA (Secure Hash Algorithm), CRC (Cyclic Redundancy Check), and so on.

Encrypting a right for using the content may also be performed by using a public key algorithm. The encryption algorithm may be implemented by large integer factorization system (RSA) algorithm, discrete logarithm system (DSA, ElGamal) algorithm, and elliptic curve discrete logarithm system (ECC) algorithm.

Lastly, the right for using the content is transmitted directly to the device of the user (step S170).

The encrypted right for using the content is transmitted directly to the device of the user by a short distance communication device. Since the authorization process is performed within a predetermined short distance scope within which the provider of the content can feel reliable, the security of the authorization process can be enhanced greatly. Meanwhile, since the device of the user is located within the predetermined short distance scope, for example, a scope within which NFC is capable of performing communication, generally several centimeters, the content provider may in some extent have more knowledge about the reliability of the user and user's device of the content.

Furthermore, since the authorization for the device of the user is performed directly by the device of the content provider without any intermediate, this reduces the complexity

of the authorization process, and decreases the cost of devices and systems related during the authorization process.

Fig.2 shows a schematic block diagram of an apparatus for authorizing to use an encrypted content according to an embodiment of the present invention. Authorization apparatus 200 is a part of a provider's device of the content. The device of the content provider may be a mobile electronic apparatus, such as cellular phone, PDA (Personal Digital Assistant), MP3 player, lap top, and so on.

The authorization apparatus 200 according to the present invention is used for a provider's device of a content authorizing a device of the user content (not shown in the fig.) to use one content, wherein both the device of the content provider and the device of the user are capable of performing short distance communication, the apparatus 200 comprising: a short distance communication unit 210 and a short distance authorization unit 220.

The short distance communication unit 210 is used to establish a short distance communication with the device of the user when the device of the content provider and the device of the user are located within a predetermined short distance. An example of the short distance communication unit 210 is NFC communication unit. Secure communication connection will be established as long as two devices provided with NFC communication unit approach to each other within a predetermined value, without any other arrangements.

Other short distance communication unit, such as IrDA (Infrared Data Association) unit, Bluetooth unit, WIFI (Wireless Fidelity, also referred to as 802.11b standard) unit, Zigbee unit, and so on, may also be used to establish a short distance communication when the distance between a provider's device of a content and the device of the user is within a predetermined value of which the content provider feel secure.

The short distance authorization unit 220 is used to perform, within the predetermined short distance, the authorization of using the content for the device of the user. The short distance authorization unit 220 may comprise an acquisition unit 222, a generation unit 224, and a transmission unit 228. The short distance authorization unit 220 may also optionally comprise an encryption unit 226.

The acquisition unit 222 is used to acquire an ID information of the device of the user. The acquisition unit may comprise a request transmitting unit 2221, for transmitting a

request, which demands to authorize a right for using the content, to the device of the user; a request receiving unit 2222, for receiving a reply, in which the ID information of the device of the user is contained, from the device of the user; and an extracting unit 2223, for extracting the ID information of the device of the user from the reply.

The acquisition unit 222 may also only comprises a request receiving unit 2222 and an extracting unit 2223. Wherein, the request receiving unit 2222 may also be used to receive a request, which demands to use the content and in which the ID information of the device of the user is contained, from the device of the user.

The generation unit 224 is used to generate a corresponding right for using the content from the ID information. The generation unit 224 receives the ID information of a content user transmitted from the acquisition unit 222, and generates a corresponding right for using the content. The right for using the content may be a right for using the content certificate of a content, in which the ID information of the content user is contained.

The encryption unit 226 is used to encrypt the right for using the content. The encryption unit 226 may also be used to encrypt the content.

The transmission unit 228 is used to transmit the right for using the content directly to the device of the user within the predetermined short distance. Transmission unit 228 transmits a transmission control signal, so as to transmit, via the short distance communication unit 210, the right for using the content of the encrypted content from the encryption unit 226 to the device of the user.

An application scene is that: while a number of companies are in conference, the representatives of two companies need to exchange some very confidential files. Since the provider and user of the files are in the same conference room, the mutual trust has been setup between them. Meanwhile, the provider of files can catch sight of the user's device of the files, such as computer, cellular phone, PDS, and so on, such that the provider can determine whether the user's device of the files is trusty. The provider of files may use the authorization apparatus of the present invention to perform, in a short distance, the authorization of using the content for the user's device of the files, without being afraid that the files are captured by representatives of other companies. Further, the provider of files can set the right for using the content to be read only, meanwhile, the files will be automatically destroyed when thirty minutes lapse after the files being opened. In this case, the provider of files can authorize, in a short distance, the user of the files to use the content, and the authorization process is secure and convenient in operation.

Although the present invention has been described in conjunction with given embodiments, it will be apparent for the skilled persons in the art that many alternatives, modifications, and changes can be made according to the above description. Therefore, such alternatives, modifications, and changes fall into the spirit and scope of the appended claims, and should be included in the present invention.

CLAIMS:

1. A method for authorizing to use a content, enabling a device of a content provider to authorize a device of a user to use the content, wherein both the device of the content provider and the device of the user are capable of performing short distance communication, comprising the steps of:

(a) establishing a short distance communication with the device of the user when the device of the content provider and the device of the user are located within a predetermined short distance;

(b) authorizing the device of the user to use the content within the predetermined short distance.

2. The method according to claim 1, wherein the short distance communication is NFC, and the predetermined short distance is a distance within which the NFC is able to perform communication.

3. The method according to claim 1, wherein the step (b) comprises:

(b1) acquiring an ID information of the device of the user;

(b2) generating a corresponding right for using the content according to the ID information;

(b3) transmitting the right for using the content directly to the device of the user within the predetermined short distance.

4. The method according to claim 3, wherein the step (b1) comprises the steps of:

sending a request for authorizing the user for using the content to the device of the user;

receiving a reply from the device of the user, the reply includes the ID information of the user;

extracting the ID information from the reply.

5. The method according to claim 3, wherein the step (b1) comprises:

receiving a request for getting authorization to use the content from the device of the user, the request includes the ID information of the user;

extracting the ID information from the request.

6. The method according to claim 3, further comprising the step of:

encrypting the right for using the content,

wherein the transmitting step further comprises the step of: transmitting the encrypted right for using the content directly to the device of the user.

7. The method according to claim 6, wherein the encrypting step further comprises the step of:

encrypting the right for using the content with the ID information.

8. An authorization apparatus for authorizing to use a content, enabling a device of a content provider to authorize a device of a user to use the content, wherein both the device of the content provider and the device of the user are capable of performing short distance communication, comprising:

establishing means for establishing a short distance communication with the device of the user when the device of the content provider and the device of the user are located within a predetermined short distance;

authorizing means for authorizing the device of the user to use the content within the predetermined short distance.

9. The apparatus according to claim 8, wherein the apparatus is capable of performing NFC communication, and the predetermined short distance is a distance within

which the NFC is able to perform communication.

10. The apparatus according to claim 8, wherein the short distance authorization apparatus comprises:

acquiring means for acquiring an ID information of the device of the user;

generating means for generating a corresponding right for using the content according to the ID information; and

transmitting means for transmitting the right for using the content directly to the device of the user within the predetermined short distance.

11. The apparatus according to claim 10, wherein the acquisition apparatus comprises:

sending means for sending a request for authorizing the user for using the content to the device of the user;

receiving means for receiving a reply from the device of the user, the reply includes the ID information of the user;

extracting means for extracting the ID information from the reply.

12. The apparatus according to claim 10, wherein the short distance authorization apparatus comprises:

encrypting means for encrypting the right for using the content,

wherein the transmitting means is arranged to transmitting the encrypted right for using the content directly to the device of the user.

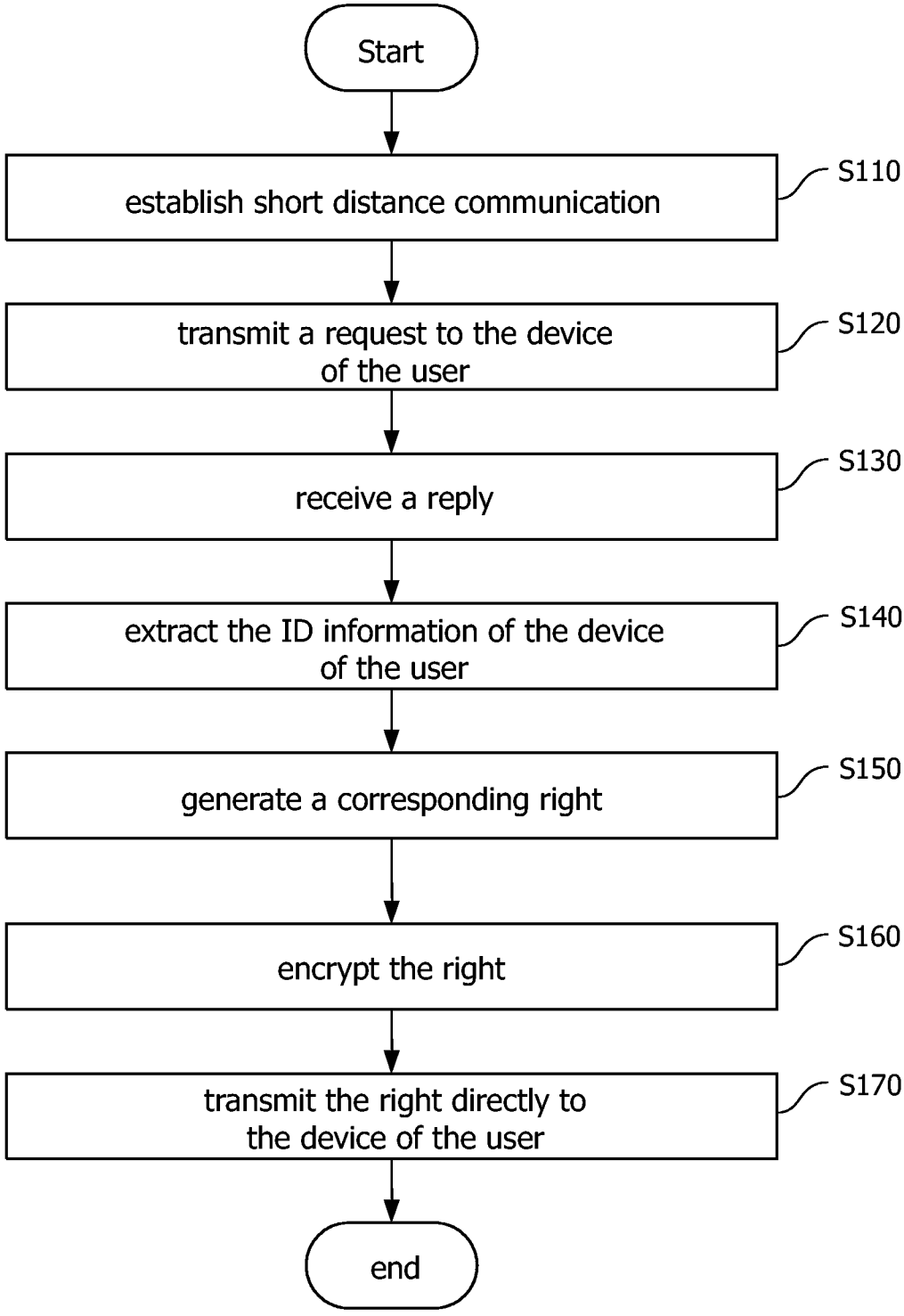

Start
establish short distance communication
S110
transmit a request to the device of the user
S120
receive a reply
S130
extract the ID information of the device of the user
S140
generate a corresponding right
S150
encrypt the right
S160
transmit the right directly to the device of the user
S170
end

FIG. 1

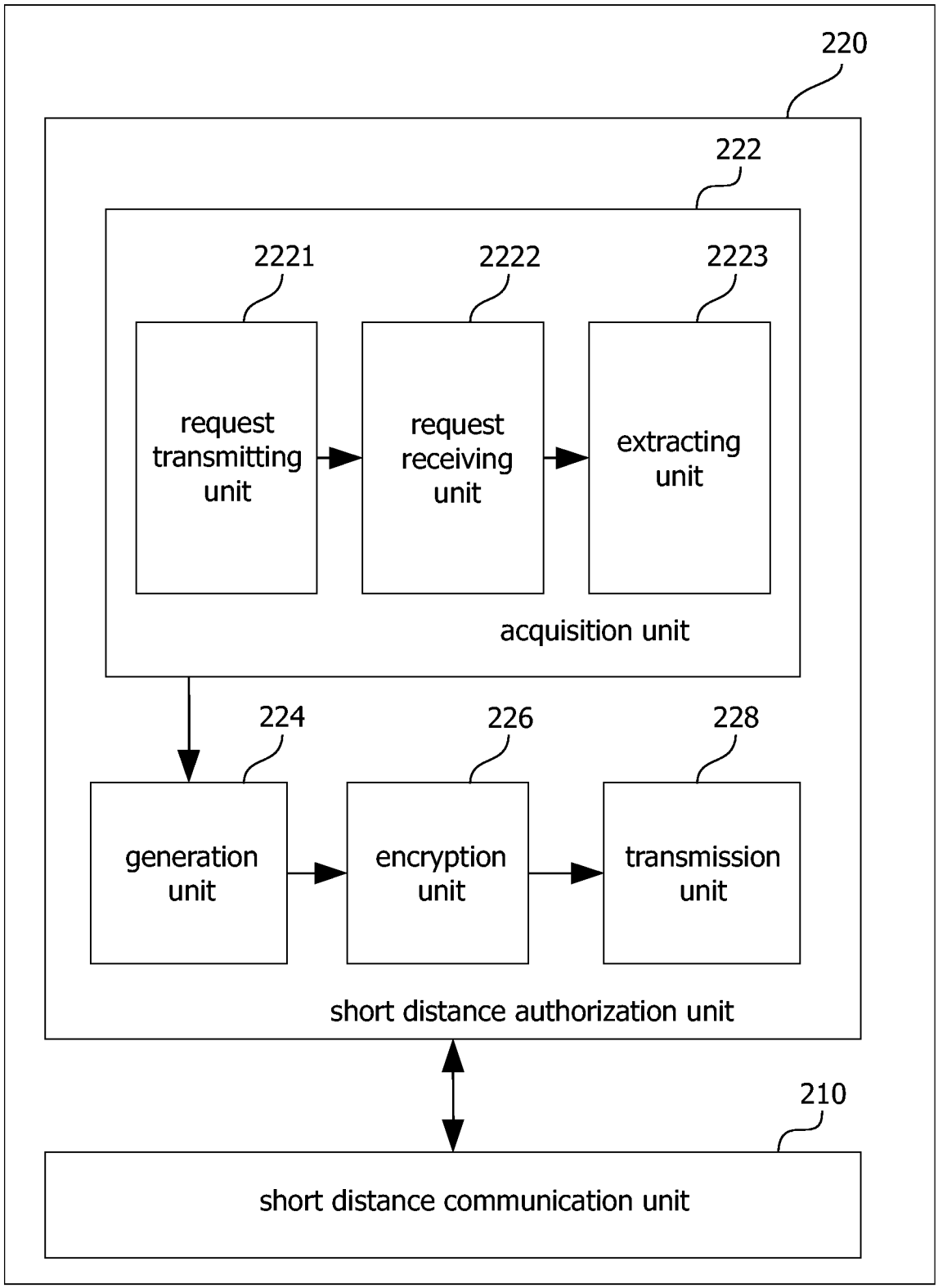

200
220
222
2221
2222
2223
request transmitting unit
request receiving unit
extracting unit
acquisition unit
224
226
228
generation unit
encryption unit
transmission unit
short distance authorization unit
210
short distance communication unit

FIG. 2