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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 May 2003 (01.05.2003)

PCT

(10) International Publication Number
WO 03/036901 A2

(51) International Patent Classification[7]: H04L 29/00

(21) International Application Number: PCT/JP02/10774

(22) International Filing Date: 17 October 2002 (17.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2001-321656 19 October 2001 (19.10.2001) JP

(71) Applicant: MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD. [JP/JP]; 1006, Oaza Kadoma, Kadoma-shi, Osaka 571-8501 (JP).

(72) Inventors: YAMAMOTO, Masaya; 7-41, Higashimakinocho, Hirakata-shi, Osaka 573-1151 (JP). MIURA, Kouji; 4-1, Ueda 3-chome, Matsubara-shi, Osaka 580-0016 (JP). NAKAHARA, Tohru; 4-40, Nonakaminami 1-chome, Yodogawa-ku, Osaka-shi, Osaka 532-0022 (JP).

(74) Agent: NII, Hiromori; c/o NII Patent Firm, 3rd Floor, Shin-Osaka Suehiro Center Bldg., 11-26, Nishinakajima 3-chome, Yodogawa-ku, Osaka-shi, Osaka 532-0011 (JP).

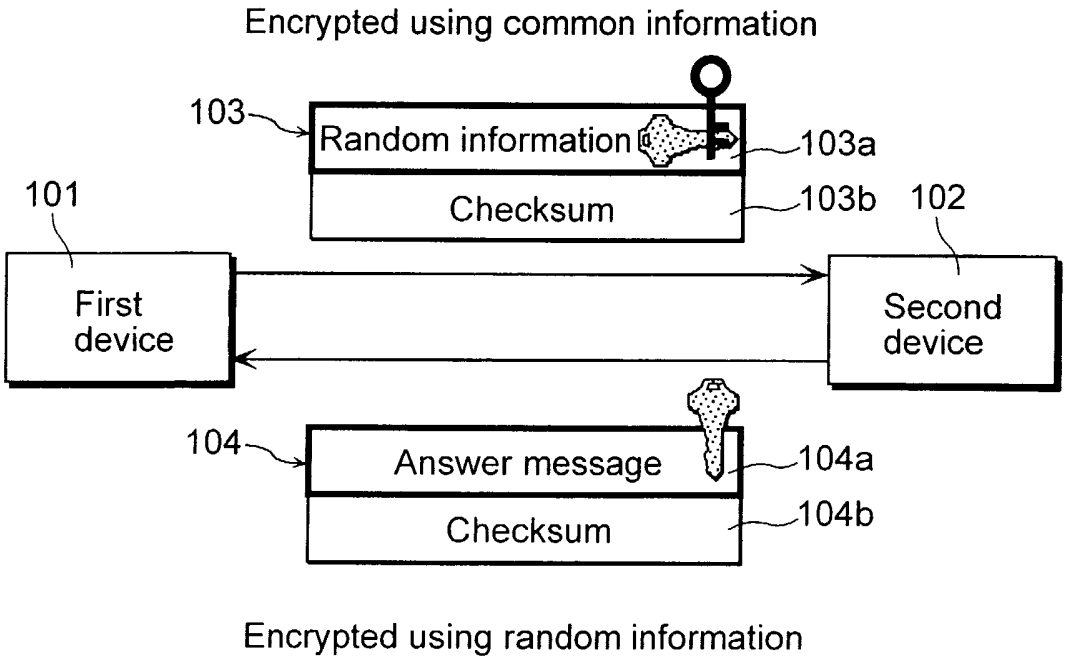
(81) Designated States *(national)*: CN, KR, NO, SG.

(84) Designated States *(regional)*: European patent (DE, ES, FI, FR, GB, IT, NL, SE).

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.

(54) Title: DEVICE AUTHENTICATION SYSTEM AND DEVICE AUTHENTICATION METHOD



(57) Abstract: Transmitting data (103) sent from the first device (101) includes random information (103a), which is encrypted by common information, and checksum (103b), and is sent to the second device (102). The second device (102) receives the transmitting data (103), and sends back answering data (104) that includes answer message (104a), which is encrypted using the random information (103a), and checksum (104b), to the first device (101).

WO 03/036901 A2

DESCRIPTION

DEVICE AUTHENTICATION SYSTEM AND DEVICE AUTHENTICATION METHOD

Technical Field

The present invention relates to a device authentication system that is necessary when each device authenticates other devices within a same network, and the present invention especially relates to a device authentication system used among a plurality of terminals.

Background Art

In recent years, digital content such as music, movies and games can be easily obtained through distribution via the Internet, digital broadcasting or package media. When copying or moving these digital content and their rights between a plurality of terminals, it is usually not allowed to move them limitlessly, but permitted to copy or move only within a certain range.

It is generally considered that copying and moving is permitted only among a plurality of terminals owned by a single user. In order to realize such restriction that allows copying and moving only within a certain range, it is necessary that a group of terminals within which copying and moving among each other is allowed to be formed.

Until now, it has been assumed that this kind of group determination is performed by a server (a group determination terminal). The following is a brief explanation of a group determination processing performed by a server.

The conventional group determination system includes a server, which determines group, and a plurality of terminals that are controlled by and connected with the server so that communication is possible via network. The server holds group lists of terminals

that belong to each group. A group list means, for example, information that associates a group identifier with terminal identifiers.

In a group determination system structured as above, group determination is carried out as follows. First, in order for a controlled terminal to acquire a group list of devices that the terminal itself belongs to, the terminal sends a terminal list requesting data to a server. In this terminal list requesting data, such information as the terminal's own terminal identifier and group identifier are included. According to the information included in the terminal list requesting data, the server sends to the requesting terminal a group list that corresponds to the information. By obtaining group information of the group that it belongs to through these procedures, a controlled terminal is able to realize group determination.

For example, in a conventional member identification method for identifying groups, a host terminal broadcasts packets of data that include the name of all the members as well as a network address unique to the host terminal. Each member terminal, then, analyzes the received packets and identifies the information retrieved from a packet that has its name in it, and sends a packet that includes the names of each member and the network addresses unique to each member terminals as data to the host terminal. The host terminal, then, analyzes the received packets, and if it finds the name of a member that belongs to the same group, it obtains the information included in the packet, corresponds the member name and a terminal address, and saves the corresponding data (for an example, see the Japanese Laid-Open Patent Application No. H10-23028 as reference).

First, to explain problems that this conventional group determination method has, that in this method, a parent-child relationship occurs between a server terminal (group determination

terminal) and terminals that are controlled by the server, and thus the server terminal and the controlled terminals must have different functions.

Next, the situation when a conventional determination method is applied to home electric appliances generally used by end users is considered. In order to apply a conventional determination method, a user must understand the parent-child relationships of home appliances he/she owns, and must consider how to set parent-child relationships between the appliances when he/she purchases any home electric appliance. This is because a server terminal is indispensable in the group determination and it is assumed that server terminals and controlled terminals are different in their functions and prices.

Basically, for terminals such as home electric appliances that are added from time to time and also various usages can be assumed, the relationship between terminals should be equal. However, there is no conventional method known for creating a group when all the terminals are in equal relationships.

Now, in consideration of the foregoing problems, the device authentication system according to the present invention enables terminals to determine other terminals that belong to a same group, when terminals are in equal relationships with each other.

Also in the device authentication system according to the present invention, it is aimed that a terminal is able to obtain a list of devices that belong to a same group in a secure manner, before it carries out processing such as authentication or content transmission that gives heavy load to the terminal. Furthermore, in the device authentication system according to the present invention, it is aimed that by using the aforementioned group list, a terminal is able to determine to which device it will send transmitting data, and realizes efficient utilization of communication channel by not communicating with terminals that are not allowed to

obtain certain content.

The present invention also aims to provide a device authentication system that is capable to contribute to the future popularization of network distribution of charged content.

Disclosure of Invention

In order to achieve the above objects, the present invention is the device authentication system comprising at least a first device and a second device for determining whether or not the first device and the second device belong to a same group, wherein the first device includes: a first common information memory unit operable to memorize common information; a transmitting data generating unit operable to generate transmitting data that includes key information; a first encryption unit operable to encrypt the generated transmitting data using the common information; a first transmission unit operable to send the encrypted transmitting data generated by the first encryption unit to the second device; a first decryption unit operable to decrypt, using the key information, encrypted answering data sent from the second device; and an authentication unit operable to judge whether or not the decrypted answering data has a predetermined rule, and when the decrypted answering data has a predetermined rule, to determine that the first device and the second device belong to a same group, and the second device includes: a second common information memory unit operable to memorize the common information; a second decryption unit operable to decrypt, using the common information, the encrypted transmitting data sent from the first device; a judging unit operable to judge whether or not the decrypted transmitting data has a predetermined rule; an answering data generating unit operable to determine that, when the transmitting data has a predetermined rule, the first device and the second device belong to a same group, and to generate answering data indicating that the

first device and the second device belong to a same group; a second encryption unit operable to encrypt the generated answering data using key information included in the transmitting data decrypted by the second decryption unit; and a second transmission unit operable to send the encrypted answering data generated by the second encryption unit to the first device.

Also, in order to achieve the above objects, the present invention is the device authentication system wherein the transmitting data generating unit generates a random number, and generates transmitting data that includes the generated random number as the key information. Furthermore, the present invention is the device authentication system wherein the first device further includes a checksum generating unit operable to generate a first checksum of the transmitting data, the first transmission unit sends the first checksum, together with the encrypted transmitting data, to the second device, and the judging unit judges whether or not the transmitting data has the predetermined rule by judging whether or not a second checksum of the decrypted transmitting data is equal to the first checksum sent from the first device.

Additionally, in order to achieve the above objects, the present invention is the device authentication system comprising a plurality of the second devices, wherein the first transmission unit broadcasts the transmitting data to a plurality of the second devices.

Moreover, in order to achieve the above objects, the present invention is the device authentication system wherein the transmitting data generating unit generates the transmitting data including search information that specifies a target of searching, the second device further includes a search information judging unit operable to judge whether or not the second device holds a target indicated by the search information that is included in the decrypted

transmitting data, and the answering data generating unit generates the answering data including a result of judgment made by the search information judging unit.

Likewise, in order to achieve the above objects, the present invention is the device authentication system wherein the transmitting data generating unit makes a content ID that specifies digital content to be included in the transmitting data as the search information, and the answering data generating unit makes a license ID that specifies a license to be included in the answering data, when the second device holds the license, which is right information that allows utilization of the digital content indicated by the content ID that is included in the transmitting data.

Furthermore, the present invention can be realized not only as the above-mentioned device authentication system, but also as a device authentication method that has the steps included in the device authentication system, as well as a communication device that realizes said units on a device.

Needless to say, the present invention can also be realized as a program that realizes the device authentication method on a computer etc., or the program can be distributed via recording media such as CD-ROMs or transmission media such as communication network.

Brief Description of Drawings

These and other objects, advantages and features of the invention will become apparent from the following description thereof taken in conjunction with the accompanying drawings that illustrate a specific embodiment of the invention. In the Drawings:

Fig. 1 is an illustration explaining a device authentication system according to the first embodiment.

Fig. 2 is a diagram showing relationships of a plurality of devices and groups according to the first embodiment.

Fig. 3 is a block diagram showing a detailed structure of the first device according to the first embodiment.

Fig. 4 is a block diagram showing a detailed structure of the second device according to the first embodiment.

Fig. 5 is a diagram showing a data structure of transmitting data according to the first embodiment.

Fig. 6 is a diagram showing a data structure of answering data according to the first embodiment.

Fig. 7A is a diagram showing a screen of user interface according to the first embodiment.

Fig. 7B is a diagram showing another screen of user interface according to the first embodiment.

Fig. 8A is a diagram showing information items of a group list created by the first device according to the first embodiment.

Fig. 8B is a diagram showing information items of another group list created by the first device according to the first embodiment.

Fig. 9 is a flowchart showing a group determination processing of a device authentication system according to the first embodiment.

Fig. 10 is a block diagram showing a detailed structure of the third device according to the second embodiment.

Fig. 11 is a block diagram showing a detailed structure of the fourth device according to the second embodiment.

Fig. 12 is a diagram showing a data structure of transmitting data according to the second embodiment.

Fig. 13 is a diagram showing a data structure of answering data according to the second embodiment.

Fig. 14 is a sequence diagram showing transmission procedure taken when the third device carries out license search, using search information, to the fourth device and the fifth device according to the second embodiment.

Fig. 15 is a flowchart showing group determination processing of a device authentication system according to the second embodiment.

Best Mode for Carrying Out the Invention

The following is an explanation of the best mode for carrying out the invention, with reference to the attached figures for understanding of the present invention. However, the following embodiments are only some examples of realizing the present invention and are not to limit the technical field of the invention. Now, the best mode for carrying out the present invention is explained with reference to figures.

Prior to detailed explanations, this is the definition of the "group" in the present invention. If there are terminals that allow such processing as copying or moving contents or the rights of the contents between each other, it is logically possible to "group" the terminals. The unit of these "grouped" terminals is called the "Authorized Domain", and hereinafter referred to as a "group" for simplicity.

(The First Embodiment)

Fig. 1 is an illustration that explains a device authentication system according to the first embodiment of the present invention. In Fig. 1, the first device 101 and the second device 102 are connected so that data transmission through a transmission channel, either wired or wirelessly, is possible. Here, the first device 101 represents a device that determines whether other terminals belong to the same group as itself, and the second device 102 represents a device that responds to the device which inquires whether it belongs to the same group as the inquiring device. In this first embodiment, the explanation is made using the two terminals, the first device 101 and the second device 102, but device authentication is possible

through the same method for all terminals that are within broadcast reachable area.

The first device 101, for example, can be a device used by the end user, such as a PC, a cellular phone, or a set-top box. This first device 101 is the device that carries out grouping and creates group lists. In order to carry out grouping, it creates transmitting data 103, encrypts the transmitting data 103 and sends it out to the second device 102.

The second device 102 is, similar to the first device 101, a terminal such as a PC, a cellular phone or a set-top box, which is within the broadcast reachable area. It receives the transmitting data 103 sent from the first device 101, creates and encrypts answering data 104, and sends the data back to the first device 101.

Transmitting data 103 includes random information 103a and checksum 103b. This random information 103a is encrypted by common information such as passwords that are random byte strings generated by the first device 101. Checksum 103b is the information, where data such as random information 103a is divided, and the data in each block are converted into numeric values and then added up before sending out. In this first embodiment, the checksum 103b is not encrypted before sending, but it is also possible to encrypt checksum 103b by common information etc. before sending out.

Answering data 104 is the data to give response to the information sent out from the first device 101, and it includes answer message 104a and checksum 104b. In answer message 104a, such information as to certify that the device is within the same group is included, and it is encrypted using the random information 103a that has been received. Checksum 104b is, similar to the checksum 103b, the information, where data such as answer message 104a is divided before sending, and the data in each block are converted into numeric values and added up. In the

present embodiment, the information is not encrypted before sending back.

Now, using Fig. 2, the flow of how the first device 101 determines whether or not other devices belong to the same group as itself is explained. In the first embodiment, the difference of whether a device belongs to the same group or not depends on whether or not the device holds common information A. This means, in order to carry out the group determination processing using the present invention's method, it is presupposed that all the devices that belong to the same group hold the common information A.

Fig. 2 is a figure showing the relationship of a plurality of devices and groups according to the first embodiment. Here in this device authentication system, there are the first device 101, the second device 102, the sixth device 201 and the seventh device 202. In the first embodiment, the first device 101 represents a device that carries out filtering of other devices that belong to the same group as itself, and via broadcast, it determines whether or not other devices belong to the same group as itself. In Fig. 2, the first device 101 and the second device 102 belong to the same group, Authorized Domain 1, and the seventh device 202 belongs to another group, Authorized Domain 2.

The first device 101 is a terminal such as a PC, and it broadcasts transmitting data that is encrypted using the common information A to the second device 102 and the seventh device 202, both of which are within the broadcast reachable area and allow data transmission. Here, the range that allows transmission includes, for example, a home network used within each house.

The second device 102 holds the common information A, and is able to decrypt the transmitting data that has been encrypted using this common information A. Disregarding any transmission error, the second device 102 is able to send back correct answering

data to the first device 101. And when the first device 101 receives the answering data, it determines that the second device 102 belongs to the same group as itself by carrying out certain prescribed processing.

Since the seventh device 202 holds common information C, which is different from common information A, when it receives transmitting data that has been encrypted using common information A, the result of prescribed processing carried out at the checksum determination unit of the seventh device 202 will be "not equal", and thus does not send back any answering data. Even when the result of checksum determination carried out at the seventh device 202 was "equal" by coincidence, checksum determination carried out at the first device 101 will be "unequal" and thus the seventh device 202 will not be added to the list as a device which belongs to the same group. Meanwhile, the sixth device 201 that is outside the broadcast reachable area will not be determined to be in the same group since transmitting data will not reach the device.

Using the aforementioned determination method, the first device 101 is able to create a list of devices that belong to the same group as itself without sending common information A. It is guaranteed that all the devices that are included in the group list at least hold common information A, and thus is guaranteed that they belong to the same group.

Now, the detailed structures of the first device 101 and the second device 102 will be explained respectively.

Fig. 3 is a block diagram that shows the detailed structure of the first device 101 according to the first embodiment. The first device 101 is a terminal that carries out broadcast and creates a list of devices that belong to the same group as itself. The first device 101 includes random information generating unit 301 where random byte strings are generated, encryption/decryption unit 302,

common information memory unit 303 where common information such as passwords are memorized, checksum generating unit 304, inter-device communication unit 305 and checksum determination unit 306. Checksum is information, where data is divided before sending, and the data in each block are converted into numeric values and then added up.

First, the flow of data when the first device 101 sends out transmitting data T-Data 1 to the second device 102 is explained.

Random information generating unit 301 creates random byte strings and uses them as random information R1 such as session key information and padding data. This random information R1 is held in this unit until time-out comes. Here, the time-out means the waiting time that the device will wait for responses from other devices to come, starting from the generation of random information R1, and is set by the user or the device manufacturer. Meanwhile, random information generating unit 301 sends random information R1 to checksum generating unit 304 and encryption/decryption unit 302.

Encryption/decryption unit 302 encrypts the random information R1 using common information A, and sends this encrypted information E1 to inter-device communication unit 305. Common information memory unit 303 has hard disk etc. to store common information A. This common information A is usually kept by the server side, not to be inputted by the user, and the information will be inputted to common information memory unit 303 by the server side at the time the user signs up for or purchases a device.

Checksum generating unit 304 generates CS1 by adding up the data within each block of checksum target section of the received random information R1, and sends this CS1 to inter-device communication unit 305. Inter-device communication unit 305, then, makes a packet of transmitting data T-Data 1 from the

received checksum CS1 and encrypted information E1, and sends it out as transmitting data T-Data 1 to the second device 102.

Next, the flow of data when the first device 101 receives answering data A-Data 2, which has been sent back from the second device 102, is explained.

First, inter-device communication unit 305 carries out data transmission between another device, the second device 102. When it receives answering data A-Data 2 from the second device 102, inter-device communication unit 305 sends encrypted information E2 to encryption/decryption unit 302 for decryption, and CS3 that is attached to answering data A-Data 2 to checksum determination unit 306.

Encryption/decryption unit 302 decrypts the encrypted information E2 using random information R1, and sends the decrypted answer data DA2 to checksum generating unit 304. Then, checksum generating unit 304 generates CS4 by adding up the numeric values of data within each block of checksum target section of the received decrypted answer data DA2, and sends this CS4 to checksum determination unit 306.

Checksum determination unit 306 maintains a group list, a memory unit which memorizes the devices that belong to the same group. It compares the aforementioned CS3 and CS4, and if the two checksum values are equal, it adds the second device 102 to the group list as a device that belongs to the same group. In case if the two checksum values are not equal, it determines that the second device 102 does not belong to the same group as itself, and thus will not add to the group list.

In the previous sentence, it was stated that decrypted answer data DA2 is sent by encryption/decryption unit 302. It can be made, however, that checksum determination unit 306 sends out an acquisition request.

Fig. 4 is a block diagram that shows the detailed structure of

the second device 102 according to the first embodiment. In addition to encryption/decryption unit 402, common information memory unit 403, checksum generating unit 404, inter-device communication unit 405 and checksum determination unit 406 that are similar to the first device 101, the second device 102 includes answer data generating unit 407, which generates answer data AD that includes such information as to certify that it belongs to the same group. Here, random information generating unit 301 that is included in the first device 101 is not included in the second device 102.

Now, the flow of transmitting data T-Data 1 which has been received by the second device 102 from the first device 101 is explained. When inter-device communication unit 405 receives transmitting data T-Data 1, of the transmitting data T-Data 1, it sends encrypted information E1 to encryption/decryption unit 402 and CS1 to checksum determination unit 406.

Encryption/decryption unit 402 decrypts the encrypted information E1 using common information A that is stored in common information memory unit 403, and it sends the decrypted data DR 1 to checksum generating unit 404.

Checksum generating unit 404 then generates CS2 by adding up the numeric values of data within each block of checksum target section of the decrypted data DR1, and sends this CS2 to checksum determination unit 406. Checksum determination unit 406 compares the aforementioned CS1 with CS2, and if they are equal, checksum determination unit 406 directs answer data generating unit 407 to create answer data AD, since transmitting data T-Data 1 is now confirmed as data sent from a device that belongs to the same group.

Following this direction, answer data generating unit 407 generates answer data AD, which includes such data as to certify that it belongs to the same group, and send this answer data AD to

encryption/decryption unit 402 and checksum generating unit 404. Encryption/decryption unit 402 encrypts the answer data AD using random information R1 that is included in encrypted information E1, and send it to inter-device communication unit 405 as encrypted data E2. Meanwhile, checksum generating unit 404 generates CS3 by adding up the numeric values of data within each block of checksum target section of answer data AD and sends it to inter-device communication unit 405. Instead of using random information R1, the encryption can also be carried out using common information A.

Inter-device communication unit 405, then, generates a packet of answering data A-Data 2 that includes the encrypted data E2 and CS3, and sends it back to the first device 101. And this is the end of a series of data processing carried out in the device authentication system.

Fig. 5 is a figure showing the data structure of transmitting data T-Data 1 according to the first embodiment. Note that this figure is presented as an example to explain the first embodiment.

Transmitting data T-Data 1 is a message sent from the first device 101 to other devices that requests other devices to respond on whether they belong to the same group as the first device 101 or not. It includes message header 501, client ID 502, random information 503, padding data 504 and checksum 505.

Message header 501 includes such message as inquiring whether the receiving device belongs to the same group or not. It is located at the head of transmitting data T-Data 1 and is sent without being encrypted. Client ID 502 holds the client ID of the first device 101, the sender of the message.

Random information 503 is composed of random byte strings and it includes such information as session key that is used when answering data is encrypted. This session key information is maintained in the first device 101 until the time-out time comes and

is used to decrypt the encrypted section of answering data.

Padding data 504 is a spare data. For example, its encryption algorithm is AES, and is attached when the data length of transmitting data T-Data 1 is not a multiple of 8 bytes, a unit of encryption, so that transmitting data T-Data 1 becomes a multiple of 8 bytes. It is encrypted by common information, and encryption target data section ED may be lengthened using padding data 504 in order to increase the encryption strength. Instead of using padding data 504, it may also be possible to set a reserve field of approximately 2 bytes.

Checksum 505 holds the sum of the numeric values of data within each block of checksum target section CT, which includes client ID 502, random information 503 and padding data 504. Also, instead of using checksum algorithm such as CRC32, hash function, for example SHA-1 or MD 5, may be used.

Encryption target data ED includes client ID 502, random information 503 and padding data 504, and random information 503 is at least to be included. Also in this encryption target data ED, device identification information that is to uniquely identify the first device 101 on network may be included. To be specific, this device identification information can be its own IP address or client ID 502, the device's identifier, etc. In case if IP address is necessary, for example when sending back answering data, it is also possible to include IP address in transmitting data T-Data 1.

Now, using Fig. 6, the contents of answering data A-Data 2 is explained. Fig. 6 is a figure showing the data structure of answering data A-Data 2 according to the first embodiment. Note that this figure is presented only as an example to explain the embodiment, and the present invention is not to be limited to this structure.

Answering data A-Data 2 is a reply to transmitting data T-Data 1, an answer requesting message sent from the first device

101. This answering data A-Data 2 includes message header 601, client ID 602, common information 603, padding data 604 and checksum 605.

Message header 601 includes such information as a message on whether the receiving device belongs to the same group or not, and client ID 602 is the client ID of the second device 102, the sender of the answering data A-Data 2. Common information 603 is the common information such as passwords held in common by both the first device 101 and the second device 102, and in this first embodiment, it is common information A.

Padding data 604 is a spare data, and answer data AD can be lengthened using padding data 604 in order to increase encryption strength. Checksum 605 is the sum of the numeric values of data within each block of checksum target section CT, which includes client ID 602, random information 603 and padding data 604.

Answer data AD includes client ID 602, common information 603 and padding data 604, and common information 603 is included in order to confirm that the second device 102 holds common information A. This answer data AD is encrypted using session key etc. that is included in aforementioned random information 503 before sending back.

Also, answer data AD at least includes device identification information for uniquely identifying the second device 102 on network. Here, the device identification information can be, for example, its own IP address or client ID 602, the device's identifier. However, although it is stated in the previous sentences that answer data AD at least includes device identification information, this is not necessarily be the case if the message header that complies with the communications protocols given when a plurality of devices communicate includes information equivalent to device identification information (e.g. its own IP address).

Now, as a preparation to use the present invention's device

authentication system, here are the examples of how to set common information to devices.

Figs. 7A and 7B are illustrations showing the screens of user interface in this first embodiment. The setting range of a group, in this case, is assumed to be a plurality of devices generally owned by a same user. In order to carry out group setting, the user, in one way or another, obtains common information and input the information through UI that is shown in Fig. 7A to devices that belong to the same group. It may also be possible to set up passwords etc. in order to limit users who carry out the setting of common information to devices. The method of obtaining common information by a user can be, for example as shown in Fig. 7B, to make display the common information of a device ("zeppetstore", in this case) and input the information to other devices that are to belong to the same group. It is also possible that the user obtains common information from device manufacturers or sales outlets by post, e-mail etc, or users may create their own common information and set the information to the devices that are to belong to the same group.

Another possibility is that common information is not to be given to users, but is set by device manufacturers or sales outlets at the time when devices are shipped or sold, according to users' request or the policies of manufacturers or sales outlets. Common information can also be stored in IC cards, and the setting may be made on each device by reading in information from the inserted IC card. Every possible means are assumed for the ways in obtaining IC cards, as has been mentioned in the preceding sentences on obtaining common information. Instead of using IC cards, storage medium such as compact flashes, or other storage medium that allows secure data management, such as SD cards, can also be used.

Usually, however, common information is not supposed to be

inputted by users, but is managed by server sides and will automatically be inputted to each terminal through transmission channels at the time when users join groups or purchase PCs. Since there are possibilities that users will intentionally increase the number of devices that belong to a same group if the users know common information, this method will prevent such cases from occurring.

Next, an example of contents regarding the information items of a group list created by the first device 101 is explained.

Figs. 8A and 8B are illustrations of the information items of group lists created by the first device 101 in this embodiment. In Fig. 8A, there is an item of group ID (801a) that identifies the group, and identification information of the devices that belong to the group is described to this group ID (801a). As for the identification information of devices, such information as device ID (802a, 803a) is described. Also in correspondence to the group ID (801a), processing that is allowed within the group may be described. This allowed processing in the case of Fig. 8A is "copying", and other possibilities include "reproducing" or "moving".

Similarly in Fig. 8B, there is an item of group ID (811b) that identifies the group, and to this group ID (811b), such information as device ID (812b, 813b) is described as the identification information of devices that belong to the group. In Fig. 8B, the allowed processing within the group is "moving".

Each device can also belong to a plurality of groups, and in that case, each device holds a plurality of common information that correspond to the plurality of groups, and through prescribed processing, it is possible that each device holds a plurality of group lists.

Once a group list is completed, communication is carried out between the devices that are included in the list and processing that is allowed within the group etc. are performed. Subsequent

processing such as authentication or content acquisition will be carried out using common methods under secure conditions. If a group list is generated every time any processing including copying or moving is carried out and deleted instantly after the processing is completed, then it will be possible to acquire the latest group information each time any processing is carried out.

In this first embodiment, methods for group setting and group determination are explained so as to be user-oriented, but it is also possible that from content holders' viewpoint, it is not desirable to expand the domain of a group. In that case, the maximum value of device identification information that can be described in a group list may be set, and it can be made that at a time a group list is created based on answering data from other terminals, the generation processing of the group list is forcibly terminated when it reaches the maximum value. When these processing is carried out with presupposition that devices always operate properly and also the network structure is invariant, users are able to set the number of devices that belong to a same group only up to the maximum value plus a few. At least, this will make possible to prevent the number of devices within a group to increase limitlessly.

The setting for a same group has been explained above, but it is basically possible to set devices that belong to the same group quite flexibly and easily by newly inputting or deleting common information.

Now, the operation of device authentication system according to the first embodiment that is structured as has been described above is explained.

Fig. 9 is a flowchart showing the procedure of group determination of device authentication system according to the first embodiment. In this first embodiment, the explanation is made on the first device 101 determining whether the second device 102 belongs to the same group or not, but by using the similar device

authentication system, it is also possible to carry out group determination between a plurality of terminals via broadcast etc. Also, in explaining the operation of the device authentication system, reference is made to the codes used in Figs. 3 and 4.

First, random information generating unit 301 that is included in the fist device 101 generates random information R1 and send the information to encryption/decryption unit 302 and checksum generating unit 304 that also are included in the first device 101 (S901). In this first embodiment, random information generating unit 301 must maintain random information R1 until time-out comes. Or, even before time-out comes, random information R1 may be deleted from random information generating unit 301 in accordance with the direction of termination given by the user. Random information R1 is a random byte string of several bytes, and the byte count depends on encryption algorithm etc. used for encryption/decryption processing.

When encryption/decryption unit 302 receives random information R1 from random information generating unit 301, it sends common information acquisition request to common information memory unit 303 and then receives common information A from common information memory unit 303. Next, encryption/decryption unit 302 generates encrypted information E1 by encrypting encryption target data ED, which at least includes random information R1, using common information A as a key, and sends the encrypted data to inter-device communication unit 305 (S902). Here, for encryption algorithm, the one that has enough encryption strength to actual usage is usually adopted, such as DES, Triple DES and AES being some examples. In the following explanations, encryption/decryption unit 302 and encryption/decryption unit 402 in Fig. 4 are assumed to hold one same encryption algorithm, but they may also hold a plurality of encryption algorithms. However, in the case that a plurality of

encryption algorithms are held, encryption algorithm identifiers become necessary, and both the first device 101 and the second device 102 must hold the same encryption algorithms that correspond to the aforementioned encryption algorithm identifiers.

Next, checksum generating unit 304 generates CS1 of the aforementioned encryption target data ED, which at least includes random information R1, and sends it to inter-device communication unit 305 (S903).

When inter-device communication unit 305 receives both the encrypted information E1 and CS1, it sends to other devices transmitting data T-Data 1, which at least includes the encrypted information E1 and CS1 and has message header etc. that complies with communication protocol attached (S904).

Now, when inter-device communication unit 405 that is included in the second device 102 receives the transmitting data T-Data 1 from the first device 101, it extracts encrypted information E1 and CS1 from the transmitting data T-Data 1 (S905).

Then, inter-device communication unit 405 sends encrypted information E1 to encryption/decryption unit 402 and CS1 to checksum determination unit 406, both of which are included in the second device 102.

When encryption/decryption unit 402 receives encrypted information E1, it sends common information acquisition request to common information memory unit 403, and receives common information A from common information memory unit 403. Encryption/decryption unit 402 then decrypts encrypted information E1 using common information A as a key and obtains decrypted encrypted information (hereinafter referred to as "decrypted encryption target data") DR1 and sends it to checksum generating unit 404 (S906). Encryption/decryption unit 402 maintains the decrypted encryption target data DR1 until answer data AD will be sent from answer data generating unit 407.

Now, checksum generating unit 404 generates CS2 of the decrypted encryption target data DR1 that was received, and sends it to checksum determination unit 406 (S907). Checksum determination unit 406 then carries out the comparison process of received CS1 and CS2 (S908).

If the result of comparison processing was CS1=CS2, then checksum determination unit 406 sends control code telling that checksums were equal, and if the result was CS1≠CS2, then it sends control code telling that checksums were not equal, in both cases to answer data generating unit 407.

If answer data generating unit 407 receives a control code telling that checksums were not equal, it does not generate any answer data (S909). It can also be made to fill answer data AD by padding data, which is meaningless byte strings, etc., or describe an error code, but in this first embodiment, the explanation is made on an assumption that answer data AD is not generated if checksums were not equal. Or, it is also possible to make that if checksums were not equal, checksum determination unit 406 does not send control code to answer data generating unit 407.

Then, answer data generating unit 407 generates answer data AD in accordance with the control code received, and sends the data to encryption/decryption unit 402 and checksum generating unit 404 (S910).

Because it is determined that a device which has sent back proper answer data AD to the first device 101 at least belongs to the same group, the same determination can be made when the checksums were not equal because of communication errors.

Now, encryption/decryption unit 402 extracts random information R1 from decrypted encryption target data DR1 that it has been maintaining. Using this random information R1 that includes session key etc., encryption/decryption unit 402 encrypts the received answer data AD, generates encrypted information E2,

and sends it to inter-device communication unit 405 (S911). Meanwhile, checksum generating unit 404 generates CS3 of the received answer data AD and sends it to inter-device communication unit 405 (S912). When inter-device communication unit 405 receives both encrypted information E2 and CS2, it sends answering data A-Data 2, which at least includes encrypted information E2 and CS3 and has message header etc. that complies with communication protocol attached, to the first device 101 (S913).

When inter-device communication unit 305 that is included in the first device 101 receives answering data A-Data 2 from the second device 102, it extracts encrypted information E2 and CS3 from the data (S914). Then, inter-device communication unit 305 sends encrypted information E2 to encryption/decryption unit 302, and CS3 to checksum determination unit 306.

When encryption/decryption unit 302 receives encrypted information E2 from inter-device communication unit 305, it sends random information acquisition request to random information generating unit 301 and receives random information R1 from random information generating unit 301. Encryption/decryption unit 302, then, decrypts the received encrypted information E2 using the received random information R1 as a key, obtains decrypted encrypted information (hereinafter referred to as "decrypted answer data") DA2, and sends it to checksum generating unit 304 and checksum determination unit 306 (S915). When sending the data to checksum determination unit 306, it is also possible to extract device identification information from decrypted answer data DA2 and send it as well.

Now, checksum generating unit 304 generates CS4 of the received decrypted answer data DA2 and sends it to checksum determination unit 306 (S916). Checksum determination unit 306 carries out comparison processing of the received CS3 and CS4 (S917).

If the result of the comparison processing is CS3=CS4, then it is determined that the second device 102, which sent the answer data AD, belongs to the same group, and the second device 102 is added to the list as a device that belongs to the same group (S919). Meanwhile, if the result is CS3≠CS4, then it is determined that the device does not belong to the same group and the processing is terminated (S918). For the same reason as in the case when the result of checksum comparison performed by the second device 102 was not equal, the same determination is made if checksums were not equal because of transmission errors. This concludes the detailed explanation of device authentication system between the first device 101 and the second device 102.

Note that in this first embodiment, encryption target sections are, respectively, encryption target data ED and answer data AD for transmitting data T-Data 1 and answering data A-Data 2, and checksum 505 and checksum 605 are not included. It is also possible, however, to carry out encryption including checksum 505 and checksum 605.

To be specific, at the time when transmitting data T-Data 1 is created in the first device 101, both checksum target section CT and checksum 505 can be encrypted using common information A after checksum 505 of checksum target section CT is calculated. And then, transmitting data T-Data 1 that includes checksum target section CT and checksum 505, both being encrypted, can be sent to the second device 102. Meanwhile, at the side of the second device 102, the received transmitting data T-Data 1 is decrypted using common information A and after the prescribed processing is carried out, both encrypted information E2 and checksum CS3 can be encrypted using random information 503 and then sent back as answering data A-Data 2.

As has been explained, in the device authentication system according to this fist embodiment, transmitting data T-Data 1 that is

sent from the first device 101 includes encryption target data ED, which includes random information 503 etc., that is encrypted using common information A, and checksum 505. And the second device 102 decrypts the encryption target data ED using common information A and by carrying out comparison processing of checksum 505, it determines whether the first device 101 belongs to the same group or not. If the first device 101 belongs to the same group, then the second device 102 sends back answering data A-Data 2, which includes encrypted information E2 that has been encrypted using random information 503 and checksum 605, to the first device 101. When the first device 101 receives answering data A-Data 2, it decrypts answer data AD using random information 503 that has been maintained, determines whether the second device 102 belongs to the same group or not by carrying out comparison processing of checksum 605, and if checksums are equal, it adds the second device 102 to the group list.

Consequently, in the device authentication system of this first embodiment, the first device 101 is able to create, by itself, a group list of devices that belong to the same group without sending common information A to other devices, and this allows the first device 101 to securely obtain a group list of devices that belong to the same group before it carries out processing such as authentication processing or content transmission processing, which will give heavy load to the first device 101.

In addition, in the device authentication system of this first embodiment, the first device 101 is able to create, by itself, a group list of devices that belong to the same group independently from a server, and will be effective in carrying out grouping among a plurality of devices via broadcast etc.

Also in the device authentication system according to this first embodiment, in case if each terminal is treated to be at the equal level as a terminal that holds common information A, then by

deciding to which devices it will send data according to the aforementioned group list, each device will not make transmission to devices that are not allowed to acquire the content. Thus, it will be possible to make efficient use of communication network, reduce traffic and so on.

Furthermore, in this first embodiment, by using random information R1, which are random numbers, for the encryption and decryption of answering data A-Data 2, data transmission between the first device 101 and the second device 102 can be made more securely and avoid more effectively such attacks as replay attacks, a way of attacking computers by obtaining the content of prior communications and sending the same content pretending to be the sender of the content.

So far, in this first embodiment, it has been explained that the data transmitted between devices includes message header 501, encryption target data ED that is encrypted, and checksum of this encryption target data ED, and comparison processing of checksum is carried out in the second device 102, the receiving side. It can also be made, however, to include pre-decided fixed information in encryption target data ED, and the receiving side judges whether or not the sending device holds the same common information A by checking whether the fixed information is included or not. In this case, the data transmitted between devices may include message header 501 and encrypted encryption target data ED, which includes fixed information. Including fixed information means, for example, to insert a letter string such as "Hello" at the head of encryption target data ED.

Also in this embodiment, the determination on whether the other device belongs to the same group or not is carried out using common information A by the second device, but it can be made that the determination on whether a device belongs to the same group or not is carried out not by the second device 102, but only by the first

device 101. It is possible, for example, that the second device 102 decrypts received encrypted information E1 using common information A and obtains random information R1. Without carrying out checksum determination (without judging whether the same common information A is held or not), however, the second device 102 encrypts answer data AD using the aforementioned random information R1 and sends it back to the first device 101. The first device 101 then decrypts the data, determines on whether the obtained data is correct as answer data AD, and thus determining whether the sending device belongs to the same group or not.

(The Second Embodiment)

Now, device authentication system according to the second embodiment of the present invention is explained. In this second embodiment, explanations will be made mainly on points that differ from the first embodiment in order to simplify explanations. This second embodiment is regarding about a content distribution system where digital products (content) and right information (license) that enable users to utilize the content are managed in separate forms, and distributed from a server to terminals via networks. In the second embodiment, an example of applying the system for searching license that is memorized in other terminals within the same group.

Fig. 10 is a block diagram that shows a detailed structure of the third device 1001 according to this second embodiment. In this second embodiment, the third device 1001 includes content usage unit 1001a, input unit 1005 and search information attaching unit 1007, in addition to the structure of the aforementioned first device 101.

Content usage unit 1001a is used when downloading contents such as movies or music as well as license from a server via

networks such as broadband. It includes content memory unit 1002 where contents such as movies are memorized, license memory unit 1003 where licenses that are issued by the server upon request from terminals, that are PC users etc., as well as output control unit 1004 which manages the contents memorized in content memory unit 1002 in accordance with the usage rules permitted by license. However, the structure of content usage unit 1001a is only an example for explanation and the structure is not to be limited to this second embodiment.

Content memory unit 1002 memorizes contents downloaded from the server via broadband etc. when the users of the terminals carry out purchase procedure. These contents are usually sent to the third device 1001 after encrypted at the server using content key.

In license memory unit 1003, license obtained by the terminal users etc. that is issued by the server upon the users' request is memorized. License is data that gives usage permission of contents to clients that includes such information as content ID of the contents to which the license is associated with, action ID that states the form of usage of the contents, and content key that decrypts the encrypted contents, and furthermore, it memorizes usage rule data that indicates the usage rules of contents on devices. In the usage rule data, such information as valid period (e.g. from June 1, 2002 to August 31, 2002), maximum number of times that usage is allowed (e.g. allowed to reproduce once), or maximum time length for each continuous reproduction (e.g. ten hours per reproduction is allowed for maximum) are included. Usage rules that are managed by the server are, for example, usage rules included in license and information that can be acquired and managed by the server (e.g. usage record of a user or a list of devices possessed by the user).

Output control unit 1004 has, or is connected to via cables,

such reproduction devices as a television, a speaker or a printer, and the user of the third device 1001 utilizes contents with these reproduction devices within the scope of usage permission of license. By connecting output control unit 1004 to recording devices, it is also possible to record the contents to storage media such as DVD or SD.

Input unit 1005 is connected with the third device 1001 via network, and inputs such data as content, license or user information to content usage unit 1001a that is included in the third device 1001. This input unit 1005 is controlled by the server side that has databases.

Terminal managing unit 1001b includes, in addition to the structure of the first embodiment, search information attaching unit 1007. The flow of data when the third device 1001 sends transmitting data T-Data 3 to other devices is as follows. First, random information generating unit 301 and search information attaching unit 1007 generate random information R2 and search information C. In this search information C, information on content ID and action ID that is allowed to utilize under the license that is subject to searching is included. It is also possible to include other information in this search information C. Then, using common information A, encryption/decryption unit 302 generates encrypted information E3 that includes search information C and random information R2, and sends this encrypted information E3 to inter-device communication unit 305. Checksum generating unit 304, meanwhile, generates CS5 from random information R2 and search information C, and inter-device communication unit 305 sends transmitting data T-Data 3, which includes encrypted information E3 and CS5, to the fourth device 1101.

Now, the flow of data when the third device 1001 receives answering data A-Data 4 from other devices is as follows. First, of answering data A-Data 4 that was received from the fourth device

1101, inter-device communication unit 305 sends encrypted data E4 to encryption/decryption unit 302 for decryption, while sending CS7 to checksum determination unit 306. Encryption/decryption unit 302 then decrypts data E4 using random information R2 that it has been maintaining, and sends this decrypted answer data DA4 to checksum generating unit 304. When checksum determination unit 306 receives CS8 that was generated by checksum generating unit 304, it compares CS7 and CS8 and if the result of the comparison was that CS7 and CS8 are equal, the information of license that applies to search information C and held by the fourth device 1101 is added to the license list created by the third device 1001.

Fig. 11 is a block diagram that shows a detailed structure of the fourth device 1101 according to the second embodiment. Similar to the third device 1001 described above, the fourth device 1101 includes content usage unit 1101a, input unit 1105 and terminal management unit 1101b. The structure of content usage unit 1101a is similar to the aforementioned content usage unit 1001a.

In addition to the structure in the first embodiment, terminal management unit 1101b includes search information determination unit 1106. The flow of data from the time the terminal management unit 1101b receives transmitting data T-Data 3 until it sends out a response is as follows. First, inter-device communication unit 405 receives transmitting data T-Data 3 and sends encrypted information E3 to encryption/decryption unit 402, and CS5 to checksum determination unit 406. Encryption/decryption unit 402 decrypts the encrypted information E3 using common information A, sends the decrypted encryption target data DR2 to checksum generating unit 404, and CS6 generated there is sent to checksum determination unit 406. Checksum determination unit 406 then compares CS5 and CS6. If the result was that checksums were not equal, it ignores

transmitting data T-Data 3, but if checksums were equal, search information determination unit 1106 searches content usage unit 1101a and retrieves license that corresponds to the content that applies to search information C. If no license that satisfies search information C is found, then answer data generating unit 407 does not create any answer data AD, but if license that satisfies search information C is found, then encrypted information E4 that includes license information C2 and answer data AD is created. Then, inter-device communication unit 405 sends answering data A-Data 4, which includes the encrypted information E4 as well as CS7 generated from license information C2 and answer data AD, to the third device 1001.

Fig. 12 is a diagram showing the data structure of transmitting data T-Data 3 according to this second embodiment. Note that Fig. 12 is only an example to explain the second embodiment.

Transmitting data T-Data 3 is a message that requests other devices to determine whether they belong to the same group as the third device 1001, as well as to carry out a search for license that applies to search information. In addition to the structure of transmitting data T-Data 1 explained in the first embodiment, it includes data on content ID 1201 and action ID 1202.

Content ID 1201 indicates the ID of content requested. To any content, at least an identifier is allotted to each content in order to uniquely identify the contents, and usually, this identifier is used as content ID 1201. The content ID 1201 is the ID of content that corresponds to the license that is subject to searching.

Action ID 1202 is an identifier that specifies the form of usage of a content indicated by the aforementioned content ID 1201, and is also an ID for the action allowed under the license that is subject to searching. The action, in this case, includes listening, reproducing, copying, moving or printing.

Content ID 1201 and action ID 1202 are included within encryption target data ED that is encrypted by common information A before sending out. Similar to the first embodiment, it is also possible in the second embodiment to encrypt, using common information A, not only encryption target data ED but also checksum 505 before sending.

Fig. 13 is a diagram showing the data structure of answering data A-Data 4 according to this second embodiment. This answering data A-Data 4 is a response to transmitting data T-Data 3 that has been sent from the third device 1001, and in addition to the structure of answering data A-Data 2 of the first embodiment, it includes license ID 1301 and usage rule data 1302.

License ID 1301 itself is not a license, which is right information, but it is an identification number of a license that can be used for the contents of search information C, and in this second embodiment, it is a number used for identifying a license that was searched in the fourth device 1101, a terminal subject to the searching.

Usage rule data 1302 is data that indicates the usage rules of content permitted by license, and is usually included in the license. In this second embodiment, it includes such information as C rules, which determines whether an action – the operation of contents, e.g. listening – can be commenced under the rules determined by the third device 1001 (e.g. for ten times).

Both license ID 1301 and usage rule data 1302 are included in answer data AD that is encrypted by random information R2.

Fig. 14 is a sequence diagram that shows the transmission procedure when the third device 1001, using search information C, carries out license searching for the fourth device 1101 and the fifth device 1401 according to the second embodiment. Note that in this diagram, it is assumed that the fifth device 1401 does not hold common information A.

The third device 1001 searches license memorized in other terminals that belong to a same group, and creates a license list of devices that hold license of content included in search information C. In order to carry out this processing, the third device 1001 sends transmitting data that includes search information C and encrypted by common information A to the fourth device 1101 and the fifth device 1401 (S1402). In this embodiment, the transmission is made via broadcast.

When the fourth device 1101 and the fifth device 1401 receive the transmitting data, they decrypt the encrypted section of data of the transmitting data using common information A, and carries out checksum comparison (S1403). Although the fifth device 1401 receives the transmitting data, because it does not hold common information A, the decryption of the encrypted transmitting data is not carried out properly causing checksum to be unequal, and thus will not send back any answering data (S1404).

Meanwhile, the fourth device 1101 carries out determination on whether common information A as well as search information C are satisfied (S1405), and if they are satisfied then it will send back answering data with license information attached (S1407), but if they are not satisfied then no response is sent back (S1406). Then, the third device 1001 creates license list 1408 that satisfies search information C, as shown in Fig. 14, and according to this license list 1408, it determines to which devices it will send data.

Fig. 15 is a flowchart showing the procedure of group determination in device authentication system according to the second embodiment. The group determination procedure of the device authentication system according to the first embodiment has been explained using Fig. 9, and for processes that are similar to the first embodiment, the same step numbers as Fig. 9 are used in Fig. 15 as well. A detailed flow of the third device 1001 creating a license list 1408 of devices that belong to the same group as itself

and also satisfies search information C is explained in accordance with Fig. 15.

First, random information generating unit 301 included in the third device 1001 generates random information R2 (S901), and search information attaching unit 1007 generates search information C that includes content ID 1201 and action ID 1202 of contents subject to searching (S1501). Then, the random information R2 and search information C are sent to encryption/decryption unit 302 and checksum generating unit 304.

When encryption/decryption unit 302 receives random information R2 from random information generating unit 301, it sends common information acquisition request to common information memory unit 303 and receives common information A from common information memory unit 303. Then, encryption/decryption unit 302 encrypts encryption target data ED that at least includes random information R2 and search information C using common information A as a key, generates encrypted information E3 and sends it to inter-device communication unit 305 (S902).

Next, checksum generating unit 304 generates CS5 of encryption target data ED that at least includes random information R2 and search information C, and sends it to inter-device communication unit 305 (S903).

When inter-device communication unit 305 receives both encrypted information E3 and CS5, it sends transmitting data T-Data 3, which at least includes the encrypted information E3 and CS5 and also attached with message header etc. that complies with communication protocol, to other devices (S904).

Now, when inter-device communication unit 405 that is included in the fourth device 1101 receives transmitting data T-Data 3 from the third device 1001, it extracts the aforementioned encrypted information E3 and CS5 from the transmitting data T-Data

3 (S905). Then, the inter-device communication unit 405 sends the encrypted information E3 to encryption/decryption unit 402 and CS5 to checksum determination unit 406.

After encryption/decryption unit 402 receives encrypted information E3, it receives common information A from common information memory unit 403. Using this common information A as a key, encryption/decryption unit 402 decrypts the encrypted information E3, obtains decrypted encryption target data DR2, and sends it to checksum generating unit 404 (S906). Next, checksum generating unit 404 generates CS6 of the decrypted encryption target data DR2 that was received and sends it to checksum determination unit 406 (S907). Then, checksum determination unit 406 carries out comparison processing of the received CS5 and CS6 (S908).

As a result of the comparison, checksum determination unit 406 sends control code that tells checksums were equal if CS5=CS6, and sends control code that tells checksums were not equal if CS5 ≠CS6, in both cases to answer data generating unit 407. Then, if answer data generating unit 407 receives control code that tells checksums were not equal, no answer data is generated (S909).

Now, search information determination unit 1106 determines if the device holds any license that can be used for content ID which applies to search information C of transmitting data T-Data 3 sent from the third device 1001, and if there is any relevant license held, then the device sends back answering data A-Data 4 attached with license information C2 (S1502). Meanwhile, in case if search information C is not satisfied, then the explanation will be made in this second embodiment under the assumption that no response is send back (S1503). It is also possible, however, to describe data in answering data A-Data 4 telling that no data that corresponds to search information C was found.

Next, search information determination unit 1106 generates

license information C2 that includes license ID etc. (S1504), and when answer data generating unit 407 receives control code, it generates answer data AD that includes the license information C2 according to the control code, and sends it to encryption/decryption unit 402 and checksum generating unit 404 (S910).

Encryption/decryption unit 402, then, extracts random information R2 from decrypted encryption target data DR2 that it has been maintaining, and using this random information R2 as a key, it encrypts the received license information C2 and answer data AD, generates encrypted information E4, and send it to inter-device communication unit 405 (S911). Meanwhile, checksum generating unit 404 generates CS7 of the received answer data AD and sends it inter-device communication unit 405 (S912). Then, inter-device communication unit 405 sends back answering data A-Data 4, which at least includes the encrypted information E4 and CS7 and attached with message header etc. that complies with communication protocol, to the third device 1001 (S913).

Now, inter-device communication unit 305 that is included in the third device 1001receives A-Data 4 from the fourth device 1101 and extracts encrypted information E4 and CS7 (S914). Then, the inter-device communication unit 305 sends encrypted information E4 to encryption/decryption unit 302 and CS7 to checksum determination unit 306.

When encryption/decryption unit 302 receives encrypted information E4 from inter-device communication unit 305, it receives random information R2 from random information generating unit 301. Encryption/decryption unit 302 then decrypts the received encrypted information E4 using the random information R2 as a key, obtains decrypted encrypted information (hereinafter referred to as "decrypted answer data") DA4 and sends it to checksum generating unit 304 and checksum determination unit 306 (S915). Checksum generating unit 304 generates CS8 of the

received decrypted answer data DA4 and sends it to checksum determination unit 306 (S916). Then, checksum determination unit 306 carries out comparison processing of the received CS7 and CS8 (S917).

If the result of comparison was that CS7=CS8, then checksum determination unit 306 determines that the fourth device 1101, which sent answer data AD, belongs to the same group, and also the device has license that corresponds to the contents subject to searching, and therefore adds the license held by the fourth device 1101 and is subject to searching to license list 1408 (S1505). In case if CS7≠CS8, then it is determined that the sending device either does not belong to the same group or does not satisfies search information C (S918). In this second embodiment, it is explained that encryption target sections of transmitting data T-Data 3 and answering data A-Data 4 are, respectively, encryption target data ED and answer data AD. It is also possible, however, to include checksum 505 and checksum 605 in the encrypted section.

As has been explained, in the device authentication system according to the second embodiment, transmitting data T-Data 3 sent by the third device 1001 includes, in addition to random information 503, content ID 1201 and action ID 1202 that are search information C. The fourth device 1101 decrypts encrypted encryption target data ED using common information A, determines whether the third device 1001 belongs to the same group or not by comparing checksum 505, and if the third device 1001 belongs to the same group, further at search information determination unit 1106, determination is made on whether the device holds license that corresponds to the contents that are subject to the searching of content ID 1201 and action ID 1202. If, as a result of the determination, the device holds license that satisfies search information C, then answering data A-Data 4 that includes such information as license ID 1301 and usage rule data 1302 is sent back

to the third device 1001.

When the third device 1001 receives the answering data A-Data 4, it decrypts answer data AD using random information 503, and by carrying out comparison processing of checksum 605, it determines that the fourth device 1101 belongs to the same group and also holds license that satisfies search information C, and thus creates license list 1408 that satisfies search information C.

Therefore, in addition to the positive effects described in the first embodiment, the device authentication system in this second embodiment makes not all the devices that have received transmitting data T-Data 3 from the third device 1001 via broadcast, but makes only the devices that belong to the same group and also hold license that satisfies search information C to send back answering data A-Data 4. In this way, the third device 1001 creates license list 1408, a list of devices that hold license subject to searching, and by following the license list 1408, it can determine more efficiently on the devices that can, for example, exchange or purchase license. The present invention, therefore, can be applied to license search among devices in content distribution system.

In each of the above-mentioned embodiments, common information A was used to explain on common information. It is also possible, however, to make each device hold a plurality of common information, and by, for example, adding or deleting the plural common information, it will be possible to set the range of a group flexibly and easily.

As is apparent from the above explanations, the device authentication system according to the present invention comprises at least a first device and a second device for determining whether or not the first device and the second device belong to a same group, wherein the first device includes: a first common information memory unit operable to memorize common information; a transmitting data generating unit operable to generate transmitting

data that includes key information; a first encryption unit operable to encrypt the generated transmitting data using the common information; a first transmission unit operable to send the encrypted transmitting data generated by the first encryption unit to the second device; a first decryption unit operable to decrypt, using the key information, encrypted answering data sent from the second device; and an authentication unit operable to judge whether or not the decrypted answering data has a predetermined rule, and when the decrypted answering data has a predetermined rule, to determine that the first device and the second device belong to a same group, and the second device includes: a second common information memory unit operable to memorize the common information; a second decryption unit operable to decrypt, using the common information, the encrypted transmitting data sent from the first device; a judging unit operable to judge whether or not the decrypted transmitting data has a predetermined rule; an answering data generating unit operable to determine that, when the transmitting data has a predetermined rule, the first device and the second device belong to a same group, and to generate answering data indicating that the first device and the second device belong to a same group; a second encryption unit operable to encrypt the generated answering data using key information included in the transmitting data decrypted by the second decryption unit; and a second transmission unit operable to send the encrypted answering data generated by the second encryption unit to the first device.

In this way, the device authentication system according to the present invention enables a terminal to determine other terminals that belong to a same group when terminals are in equal relationships with each other, and also enables a terminal to obtain a list of devices that belong to a same group in a secure manner, before it carries out processing such as authentication or content transmission that gives heavy load to the terminal. Furthermore,

by using the aforementioned group list, the device authentication system enables a terminal to determine to which device it will send transmitting data, and realizes efficient utilization of communication channel etc. by not communicating with terminals that are not allowed to obtain certain content.

Also, in the device authentication system according to the present invention, the transmitting data generating unit generates the transmitting data including search information that specifies a target of searching, the second device further includes a search information judging unit operable to judge whether or not the second device holds a target indicated by the search information that is included in the decrypted transmitting data, and the answering data generating unit generates the answering data including a result of judgment made by the search information judging unit. Furthermore, the transmitting data generating unit makes a content ID that specifies digital content to be included in the transmitting data as the search information, and the answering data generating unit makes a license ID that specifies a license to be included in the answering data, when the second device holds the license, which is right information that allows utilization of the digital content indicated by the content ID that is included in the transmitting data.

In this way, the device authentication system according to the present invention enables a terminal to create a license list, a list of devices that hold license subject to searching, and by following the license list, the system enables a terminal to determine more efficiently on the devices that can, for example, exchange or purchase license, and thus enabling the system to be applied to license search among devices in content distribution system.

Industrial Applicability

The device authentication system according to the present invention

can be applicable to a content distribution system that distributes content from a server to a terminal via network, using a personal computer with communication facility.

CLAIMS

1. A device authentication system comprising at least a first device and a second device for determining whether or not the first device and the second device belong to a same group,

wherein the first device includes:

a first common information memory unit operable to memorize common information;

a transmitting data generating unit operable to generate transmitting data that includes key information;

a first encryption unit operable to encrypt the generated transmitting data using the common information;

a first transmission unit operable to send the encrypted transmitting data generated by the first encryption unit to the second device;

a first decryption unit operable to decrypt, using the key information, encrypted answering data sent from the second device; and

an authentication unit operable to judge whether or not the decrypted answering data has a predetermined rule, and when the decrypted answering data has a predetermined rule, to determine that the first device and the second device belong to a same group, and

the second device includes:

a second common information memory unit operable to memorize the common information;

a second decryption unit operable to decrypt, using the common information, the encrypted transmitting data sent from the first device;

a judging unit operable to judge whether or not the decrypted transmitting data has a predetermined rule;

an answering data generating unit operable to determine that, when the transmitting data has a predetermined rule, the first

device and the second device belong to a same group, and to generate answering data indicating that the first device and the second device belong to a same group;

a second encryption unit operable to encrypt the generated answering data using key information included in the transmitting data decrypted by the second decryption unit; and

a second transmission unit operable to send the encrypted answering data generated by the second encryption unit to the first device.

2. The device authentication system according to Claim 1,

wherein the transmitting data generating unit generates a random number, and generates transmitting data that includes the generated random number as the key information.

3. The device authentication system according to Claim 1,

wherein the first device further includes a checksum generating unit operable to generate a first checksum of the transmitting data,

the first transmission unit sends the first checksum, together with the encrypted transmitting data, to the second device, and

the judging unit judges whether or not the transmitting data has the predetermined rule by judging whether or not a second checksum of the decrypted transmitting data is equal to the first checksum sent from the first device.

4. The device authentication system according to Claim 1,

wherein the second device does not send the answering data to the first device when judging unit judges that the decrypted transmitting data does not have a predetermined rule.

5. The device authentication system according to Claim 1,

wherein the first encryption unit combines and encrypts the transmitting data and the first checksum,

the first transmission unit sends encrypted data generated by the first encryption unit to the second device,

the second decryption unit decrypts, using the common information, the encrypted data sent from the first device into the transmitting data and the first checksum, and

the judging unit judges whether or not the transmitting data has the predetermined rule by judging whether or not the second checksum of the decrypted transmitting data is equal to the decrypted first checksum.

6. The device authentication system according to Claim 1,

wherein the transmitting data generating unit generates transmitting data that includes pre-decided fixed information, and

the judging unit judges whether or not the transmitting data has the predetermined rule by judging whether or not fixed information included in the decrypted transmitting data has a pre-decided data pattern.

7. The device authentication system according to Claim 1 comprising a plurality of the second devices,

wherein the first transmission unit broadcasts the transmitting data to a plurality of the second devices.

8. The device authentication system according to Claim 1 comprising a plurality of the second devices,

wherein the first transmission unit sends the transmitting data to a plurality of the second devices, and

the first device further includes:

a group list generating unit operable to generate a group list indicating a list of the second device that belongs to a same group as

the first device based on a determination made on a plurality of the second devices by the authentication unit; and

a group communication unit operable to perform a predetermined communication with the second device according to the generated group list.

9. The device authentication system according to Claim 8,

wherein the first device further controls at least one of the transmitting data generating unit, the first transmission unit and the group list generating unit, so that a number of the second device registered on the group list does not exceed a predetermined number.

10. The device authentication system according to Claim 1,

wherein the transmitting data generating unit makes padding data to be included in the transmitting data so that the size of the transmitting data is of a predetermined length, and

the answering data generating unit makes padding data to be included in the answering data so that the size of the answering data is of a predetermined length.

11. The device authentication system according to Claim 1,

wherein the transmitting data generating unit generates the transmitting data including search information that specifies a target of searching,

the second device further includes a search information judging unit operable to judge whether or not the second device holds a target indicated by the search information that is included in the decrypted transmitting data, and

the answering data generating unit generates the answering data including a result of judgment made by the search information judging unit.

12. The device authentication system according to Claim 11,

wherein the transmitting data generating unit makes a content ID that specifies digital content to be included in the transmitting data as the search information, and

the answering data generating unit makes a license ID that specifies a license to be included in the answering data, when the second device holds the license, which is right information that allows utilization of the digital content indicated by the content ID that is included in the transmitting data.

13. The device authentication system according to Claim 12,

wherein the first device further includes:

a license list generating unit operable to generate a license list indicating a list of the license ID that is included in the answering data sent from the second device; and

a license transmission unit operable to perform communication for sending and receiving a license with the second device based on the generated license list.

14. The device authentication system according to Claim 1,

wherein each of the first common information memory unit and the second common information memory unit memorizes a plurality of different common information,

the first encryption unit encrypts the transmitting data using a single common information selected from a plurality of the common information memorized in the first common information unit, and

the second decryption unit decrypts the transmitting data using a single common information selected from a plurality of the common information memorized in the second common information memory unit.

15. The device authentication system according to Claim 14,

wherein the transmitting data generating unit generates the transmitting data including search information that specifies digital content and a form of usage of the content,

the second device further includes a search information judging unit operable to judge whether or not the second device holds a license, which is right information that allows utilization of the digital content in the form of usage, indicated by the search information included in the decrypted transmitting data,

the answering data generating unit generates the answering data including a result of judgment made by the search information judging unit,

the first encryption unit selects a single common information that corresponds to the form of usage from a plurality of the common information memorized in the first common information memory unit, and encrypts the transmitting data using the selected common information, and

the second decryption unit selects a single common information that corresponds to the form of usage from a plurality of the common information memorized in the second common information memory unit, and decrypts the transmitting data using the selected common information.

16. The device authentication system according to Claim 15,

wherein the first device further includes a first common information editing unit operable to perform adding and deleting of the common information memorized in the first common information memory unit, and

the second device further includes a second common information editing unit operable to perform adding and deleting of the common information memorized in the second common

information memory unit.

17. A device authentication method for a system comprising at least a first device and a second device for determining whether or not the first device and the second device belong to a same group,

wherein each of the first device and the second device includes, respectively, a first common information memory unit and a second common information memory unit that memorize common information,

the device authentication method includes a first step performed by the first device and a second step performed by the second device, and

the first step includes:

a transmitting data generating step for generating transmitting data that includes key information;

a first encryption step for encrypting generated transmitting data using the common information;

a first transmission step for sending encrypted transmitting data generated in the first encryption step to the second device;

a first decryption step for decrypting, using the key information, encrypted answering data sent from the second device; and

an authentication step for judging whether or not the decrypted answering data has a predetermined rule, and when the decrypted answering data has a predetermined rule, for determining that the first device and the second device belong to a same group, and

the second step includes:

a second decryption step for decrypting, using the common information, encrypted transmitting data sent from the first device;

a judging step for judging whether or not the decrypted transmitting data has a predetermined rule;

an answering data generating step for determining that, when the transmitting data has a predetermined rule, the first device and the second device belong to a same group, and for generating answering data indicating that the first device and the second device belong to a same group;

a second encryption step for encrypting the generated answering data using key information that is included in transmitting data decrypted in the decryption step; and

a second transmission step for sending encrypted answering data generated in the second encryption step to the first device.

18. The device authentication method according to Claim 17,

wherein in the transmitting data generating step, a random number is generated and transmitting data that includes the generated random number as the key information is generated.

19. The device authentication method according to Claim 17 further comprising a checksum generating step for generating a first checksum of the transmitting data in the first device,

wherein in the first transmission step, the first checksum is sent, together with the encrypted transmitting data, to the second device; and

in the judging step, whether or not the decrypted transmitting data has the predetermined rule is judged by judging whether or not a second checksum of the decrypted transmitting data is equal to the first checksum sent from the first device.

20. The device authentication method according to Claim 17,

wherein in the first encryption step, the transmitting data and the first checksum are combined and encrypted,

in the first transmission step, encrypted data generated in the first encryption step is sent to the second device,

in the second decryption step, the encrypted data sent from the first device is decrypted into transmitting data and the first checksum, using the common information; and

in the judging step, whether or not the decrypted transmitting data has the predetermined rule is judged by judging whether or not a second checksum of the decrypted transmitting data is equal to the first checksum that is decrypted.

21. The device authentication method according to Claim 17,

wherein the system includes a plurality of the second devices,

in the first transmission step, the transmitting data is sent to a plurality of the second devices, and

the first step further includes:

a group list generating step for generating a group list that indicates a list of the second device that belong to a same group as the first device, based on a determination made on a plurality of the second devices in the authentication step; and

a group communication step for performing a predetermined communication with the second device according to the generated group list.

22. The device authentication method according to Claim 17,

wherein in the transmitting data generating step, the transmitting data including search information that specifies a target of searching is generated,

in the device authentication method, the second step further includes a search information judging step for judging whether or not the second device holds a target indicated by the search information that is included in the decrypted transmitting data, and

in the answering data generating step, answering data including a result of judgment made in the search information judging step is generated.

23. The device authentication method according to Claim 22,

wherein in the transmitting data generating step, a content ID that specifies digital content is to be included in the transmitting data as the search information, and

in the answering data generating step, a license ID that specifies the license is to be included in the answering data, when the second device holds the license, which is right information that allows utilization of the digital content indicated by the content ID included in the transmitting data.

24. The device authentication method according to Claim 17,

wherein each of the first common information memory unit and the second common information memory unit memorize a plurality of different common information,

in the first encryption step, the transmitting data is encrypted using a single common information selected from a plurality of the common information memorized in the first common information memory unit, and

in the second decryption step, the transmitting data is decrypted using a single common information selected from a plurality of the common information memorized in the second common information memory unit.

25. A communication device for determining whether or not a partner device and the device itself belong to a same group by mutually authenticating with the partner device and comprising:

an authentication unit operable to authenticate a partner device; and

an authentication target unit operable to be authenticated by the partner device, and

wherein the authentication unit includes:

a common information memory unit operable to memorize common information;

a transmitting data generating unit operable to generate transmitting data that includes key information;

a first encryption unit operable to encrypt the generated transmitting data using the common information;

a first transmission unit operable to send the encrypted transmitting data generated by the first encryption unit to the partner device;

a first decryption unit operable to decrypt, using the key information, encrypted answering data sent from the partner device; and

an authentication unit operable to judge whether or not the decrypted answering data has a predetermined rule, and when the decrypted answering data has a predetermined rule, to determine that the partner device belong to a same group as the device itself, and

the authentication target unit includes:

a second decryption unit operable to decrypt, using the common information, the encrypted transmitting data sent from the partner device;

a judging unit operable to judge whether or not the decrypted transmitting data has a predetermined rule;

an answering data generating unit operable to determine that, when the transmitting data has a predetermined rule, the partner device belongs to a same group as the device itself, and to generate answering data that indicates that the partner device belongs to a same group as the device itself;

a second encryption unit operable to encrypt the generated answering data using key information that is included in transmitting data decrypted by the decryption unit; and

a second transmission unit operable to send the encrypted

answering data generated by the second encryption unit to the partner device.

26. The communication device according to Claim 25,

wherein the transmitting data generating unit generates a random number, and generates transmitting data that includes the generated random number as the key information.

27. The communication device according to Claim 25,

wherein the partner device further includes a checksum generating unit operable to generate a first checksum of the transmitting data,

the first transmission unit sends the first checksum, together with the encrypted transmitting data, to the partner device, and

the judging unit judges whether or not the decrypted transmitting data has the predetermined rule by judging whether or not a second checksum of the decrypted transmitting data is equal to the first checksum sent from the partner device.

28. A program for a communication device that determines whether or not a partner device and the device itself belong to a same group by mutually authenticating with a partner device, the program comprising:

an authentication step for authenticating a partner device; and

an authentication target step for being authenticated by the partner device,

wherein the authentication step includes:

a transmitting data generating step for generating transmitting data that includes key information;

a first encryption step for encrypting the generated transmitting data using common information that is memorized

beforehand;

a first transmission step for sending the encrypted transmitting data generated in the first encryption step to the partner device;

a first decryption step for decrypting, using the key information, encrypted answering data sent from the partner device; and

an authentication step for judging whether or not the decrypted answering data has a predetermined rule, and when the decrypted answering data has a predetermined rule, for determining that the partner device belongs to a same group as the device itself, and

the authentication target step includes:

a second decryption step for decrypting, using the common information, the encrypted transmitting data sent from the partner device;

a judging step for judging whether or not the decrypted transmitting data has a predetermined rule;

an answering data generating step for determining that, when the transmitting data has a predetermined rule, the partner device and the device itself belong to a same group, and for generating answering data indicating that the partner device and the device itself belong to a same group;

a second encryption step for encrypting the generated answering data using key information that is included in transmitting data decrypted in the decryption step; and

a second transmission step for sending encrypted answering data generated in the second encryption step to the partner device.

29. The program according to Claim 28,

wherein the transmitting data generating step generates a random number, and then generates transmitting data that includes

the generated random number as key information.

30. The program according to Claim 28 further comprising a checksum generating step for generating a first checksum of the transmitting data,

wherein in the first transmission step, the first checksum is sent to the partner device, together with the encrypted transmitting data, and

in the judging step, whether or not the decrypted transmitting data has the predetermined rule is judged by judging whether or not a second checksum of the decrypted transmitting data is equal to the first checksum sent from the partner device.

31. A computer-readable recording medium for a device authentication system comprising at least a first device and a second device for determining whether or not the first device and the second device belong to a same group,

wherein the authentication data is recorded in the computer-readable recording medium, and includes:

encrypted transmitting data that includes key information and is encrypted using common information; and

a checksum of the transmitting data,

the authentication data is data sent from the first device to the second device,

the key information is used for encrypting answering data sent from the second device to the first device, when the second device determines that the first device belongs to a same group as the second device, and

the common information is information held beforehand by a device that belongs to the same group.

32. The recording medium according to Claim 31,

wherein the key information is a random number generated by the first device.

33. The recording medium according to Claim 31,

wherein the transmitting data includes a content ID that specifies a digital content, and

the answering data includes a license ID that specifies a license, which is right information that allows utilization of the digital content indicated by the content ID that is included in the transmitting data.

Fig. 1

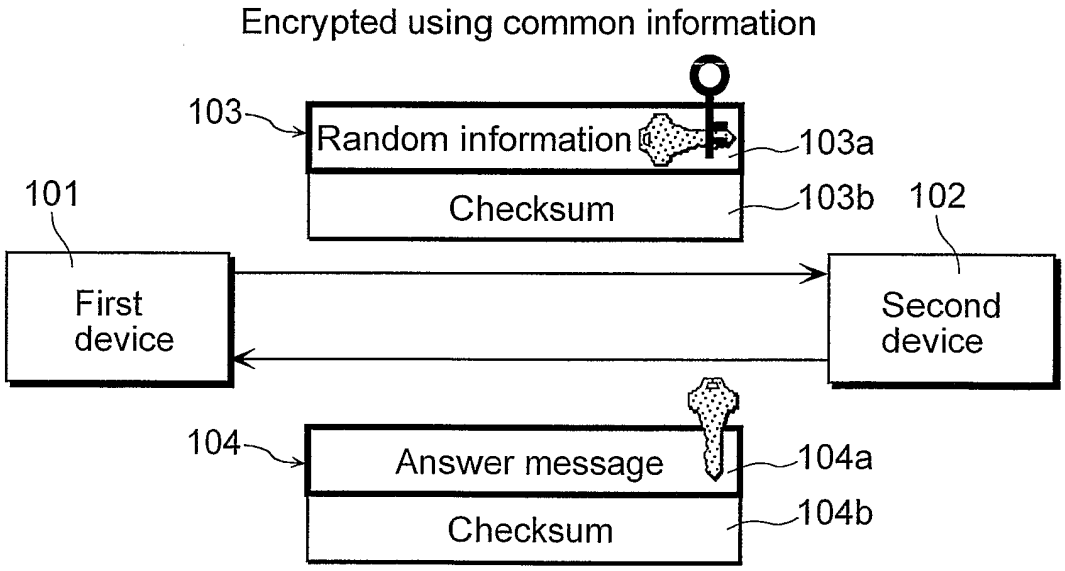

Encrypted using common information
103
Random information
103a
Checksum
103b
101
102
First device
Second device
104
Answer message
104a
Checksum
104b
Encrypted using random information

Fig. 2

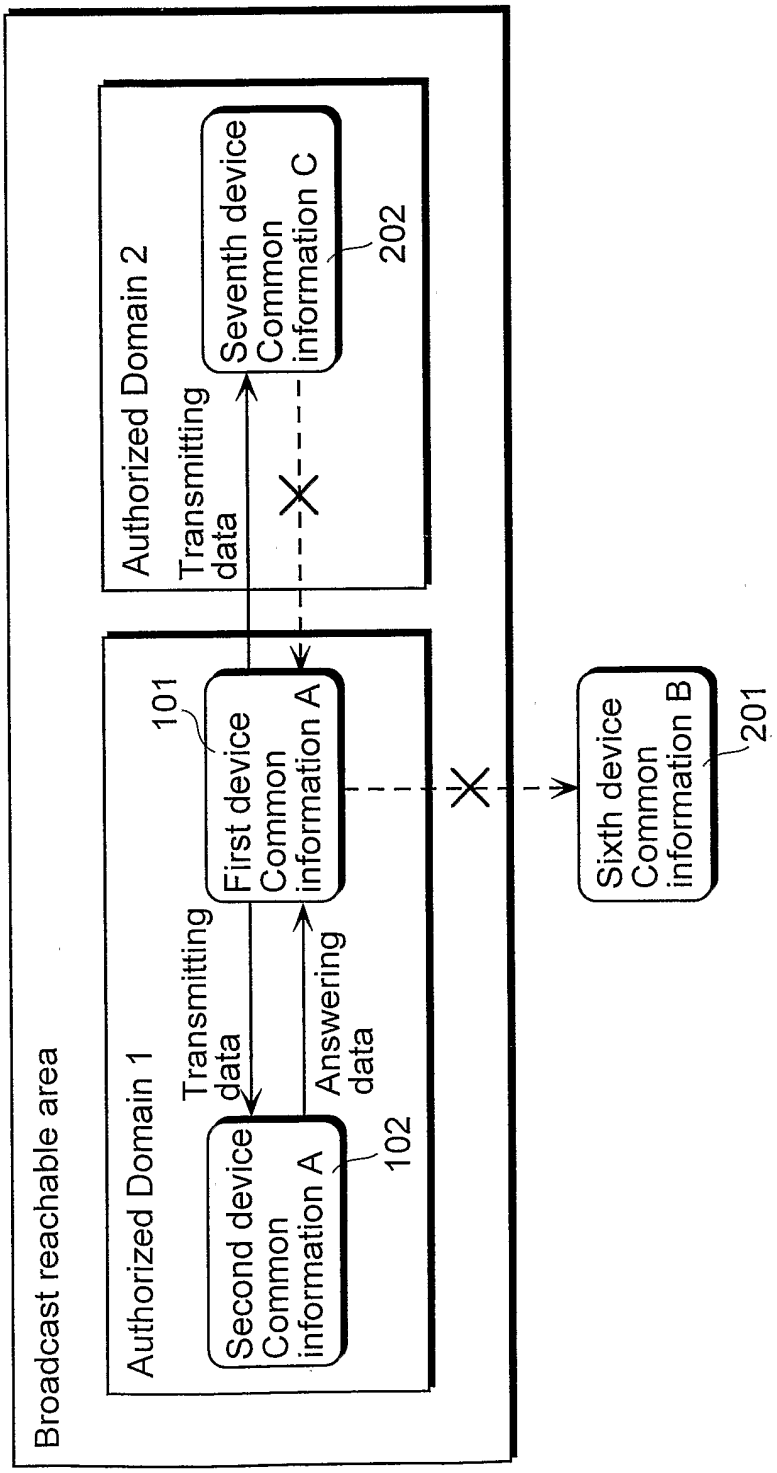

Broadcast reachable area
Authorized Domain 1
Second device Common information A
102
Transmitting data
Answering data
First device Common information A
101
Authorized Domain 2
Transmitting data
Seventh device Common information C
202
Sixth device Common information B
201

Fig. 3

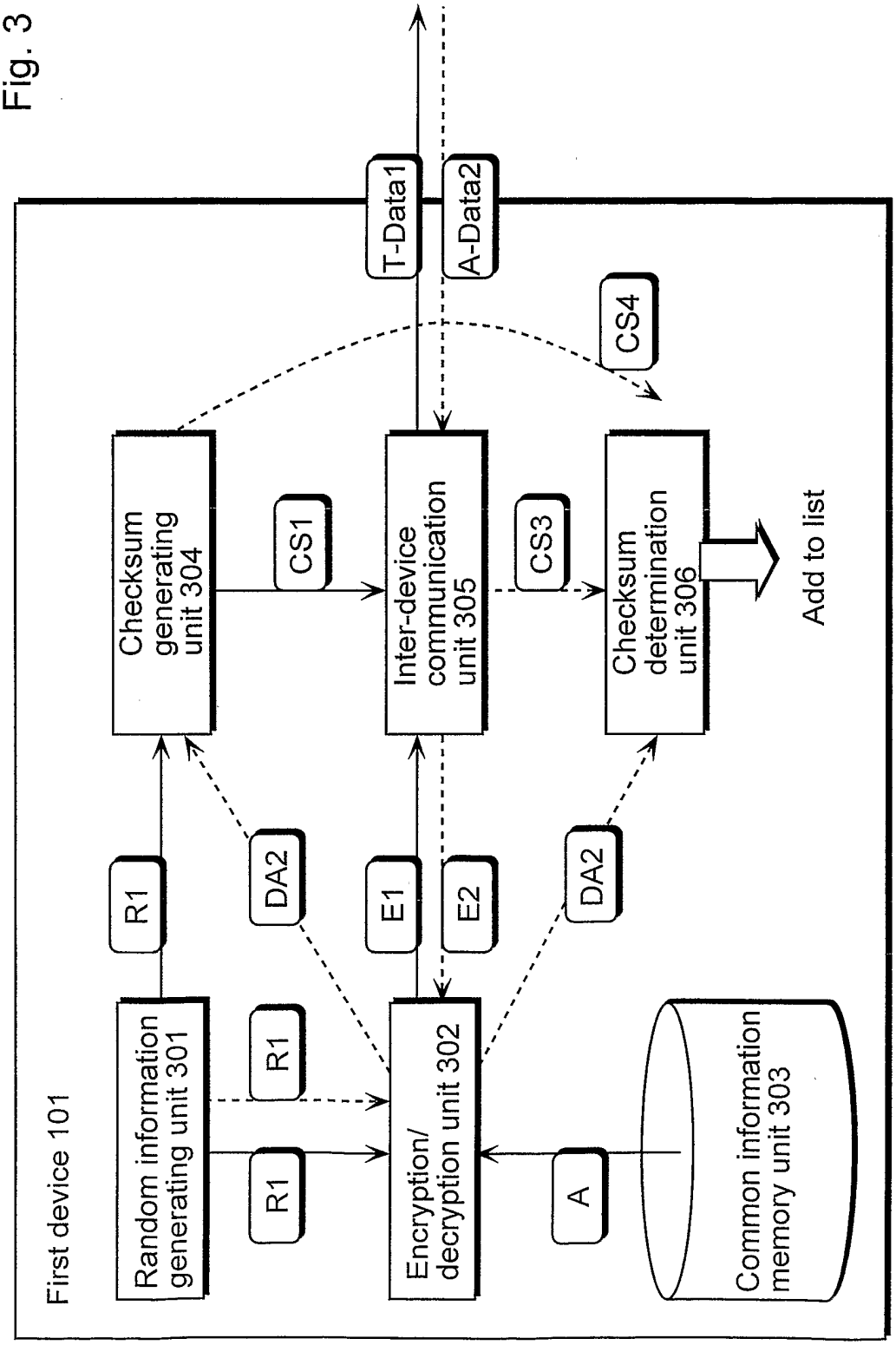

First device 101
Random information generating unit 301
Encryption/ decryption unit 302
Common information memory unit 303
Checksum generating unit 304
Inter-device communication unit 305
Checksum determination unit 306
Add to list
T-Data1
A-Data2
CS1
CS3
CS4
R1
R1
R1
DA2
DA2
E1
E2
A

Fig. 4

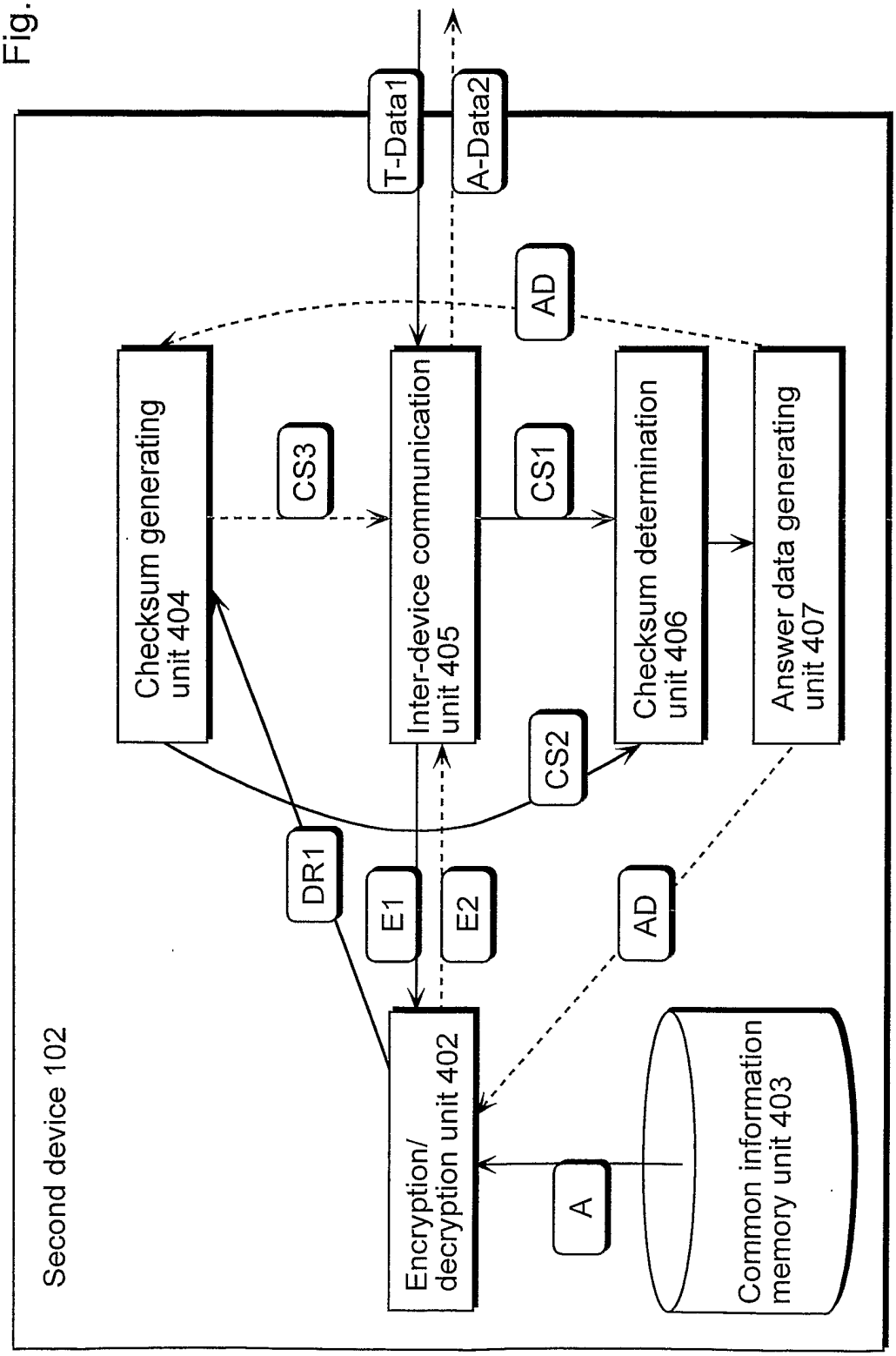

Second device 102
T-Data1
A-Data2
AD
Checksum generating unit 404
CS3
Inter-device communication unit 405
CS1
Checksum determination unit 406
Answer data generating unit 407
CS2
DR1
E1
E2
AD
Encryption/ decryption unit 402
A
Common information memory unit 403

Fig. 5

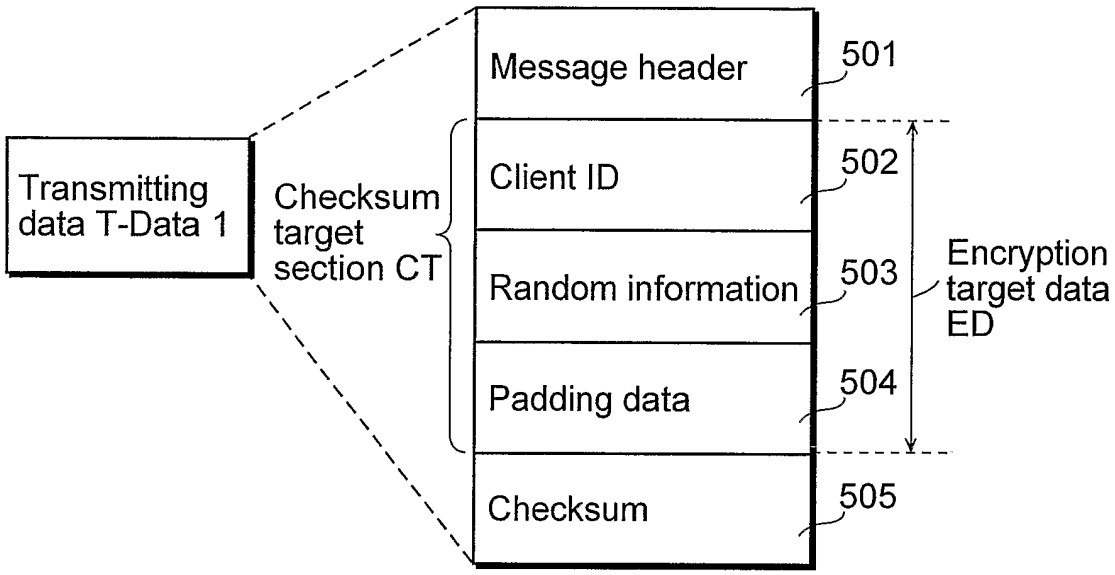

Transmitting data T-Data 1
Checksum target section CT
Message header
501
Client ID
502
Random information
503
Padding data
504
Checksum
505
Encryption target data ED

Fig. 6

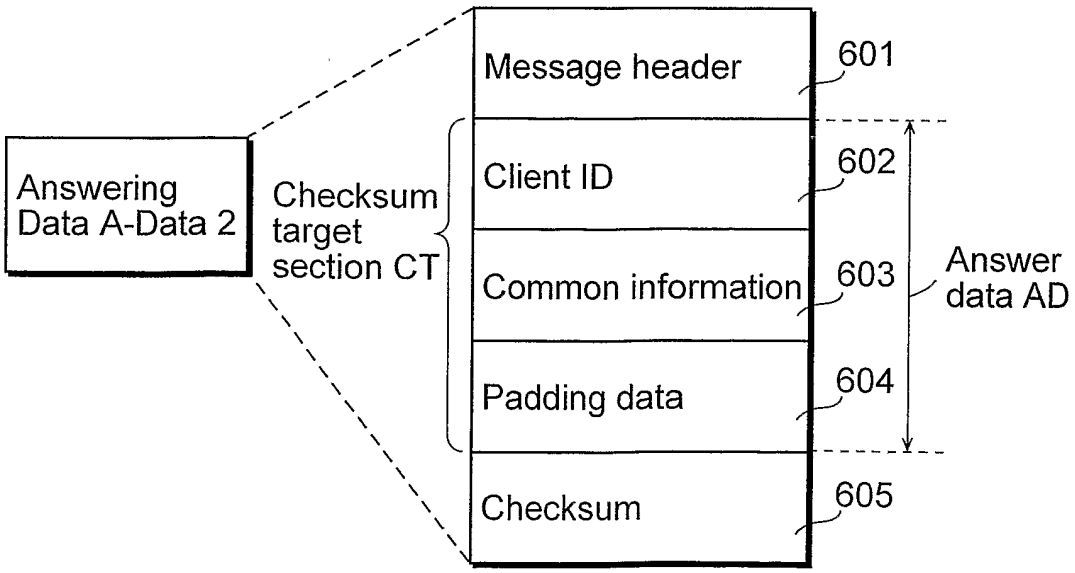

Answering Data A-Data 2
Checksum target section CT
Message header
601
Client ID
602
Common information
603
Padding data
604
Checksum
605
Answer data AD

Fig. 7A

Example of common information setting screen

Setting the common information
Please input the newly set common information and the password for the setting for this device.

Common information

Password

OK

Fig. 7B

Example of displaying common information

Displaying common information
The common information set for this device is:
"zeppetstore"

Fig. 8A

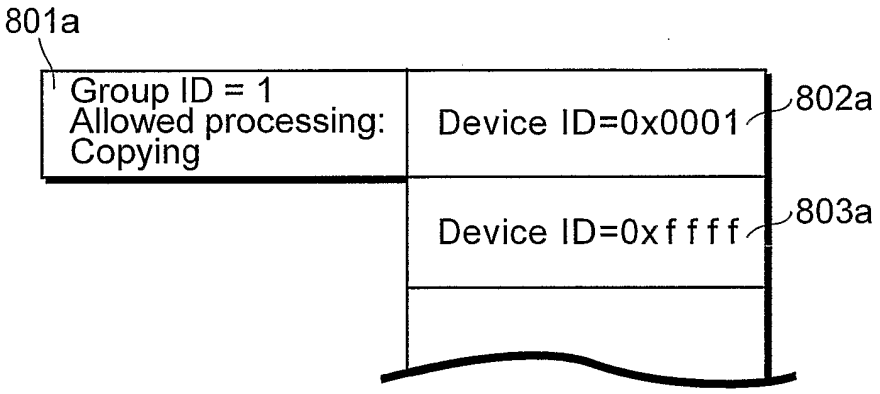

801a
Group ID = 1
Allowed processing:
Copying
Device ID=0x0001
802a
Device ID=0xffff
803a

Fig. 8B

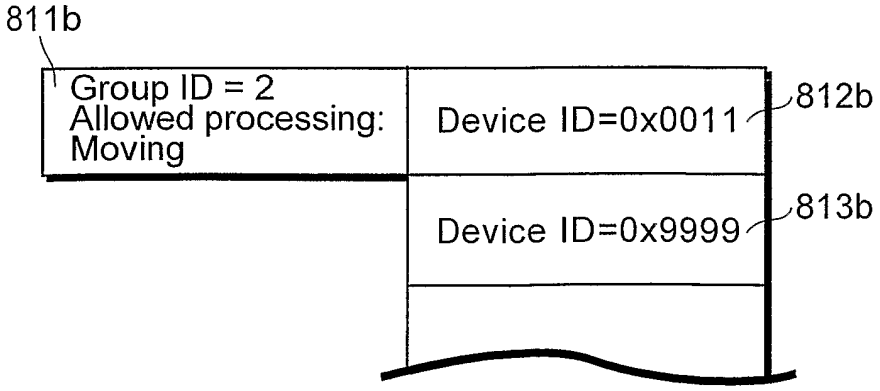

811b
Group ID = 2
Allowed processing:
Moving
Device ID=0x0011
812b
Device ID=0x9999
813b

Fig. 9

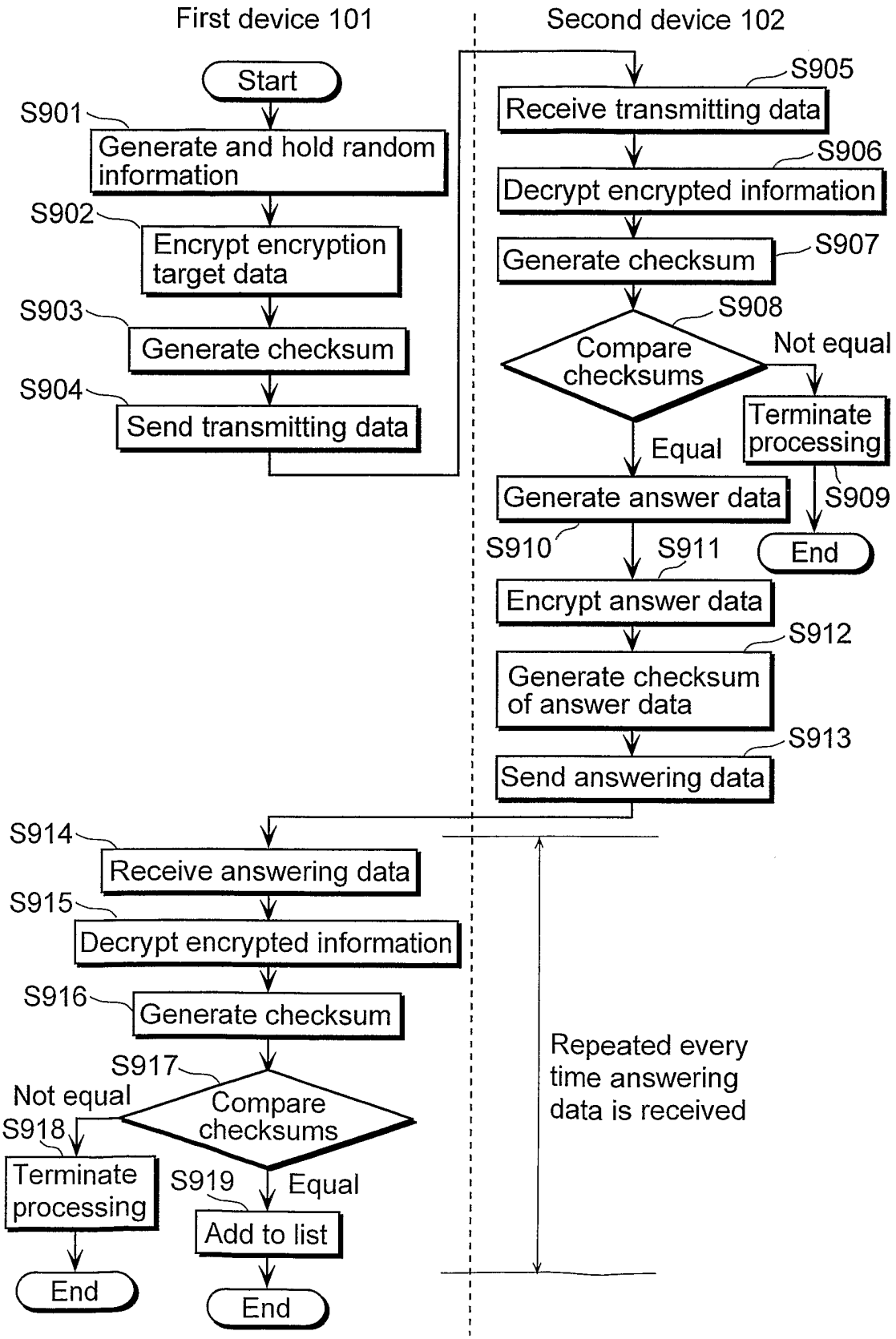

First device 101
Second device 102
Start
S901
Generate and hold random information
S902
Encrypt encryption target data
S903
Generate checksum
S904
Send transmitting data
S905
Receive transmitting data
S906
Decrypt encrypted information
S907
Generate checksum
S908
Compare checksums
Not equal
Terminate processing
Equal
Generate answer data
S909
End
S910
S911
Encrypt answer data
S912
Generate checksum of answer data
S913
Send answering data
S914
Receive answering data
S915
Decrypt encrypted information
S916
Generate checksum
S917
Compare checksums
Not equal
S918
Terminate processing
End
S919
Equal
Add to list
End
Repeated every time answering data is received

Fig. 10

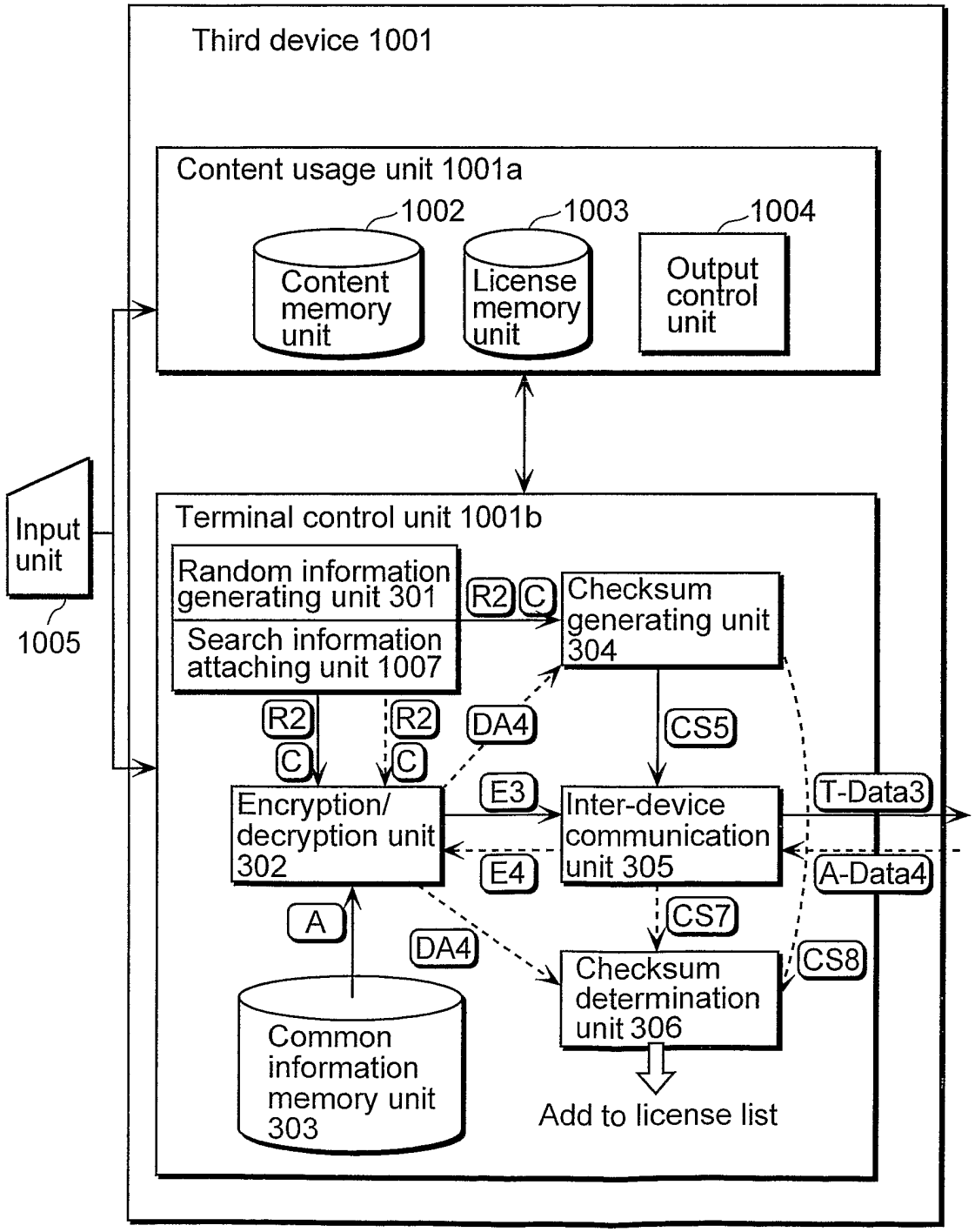

Third device 1001
Content usage unit 1001a
1002
1003
1004
Content memory unit
License memory unit
Output control unit
Input unit
1005
Terminal control unit 1001b
Random information generating unit 301
Search information attaching unit 1007
R2
C
Checksum generating unit 304
DA4
CS5
E3
E4
Encryption/ decryption unit 302
Inter-device communication unit 305
T-Data3
A-Data4
A
CS7
CS8
Checksum determination unit 306
Common information memory unit 303
Add to license list

Fig. 11

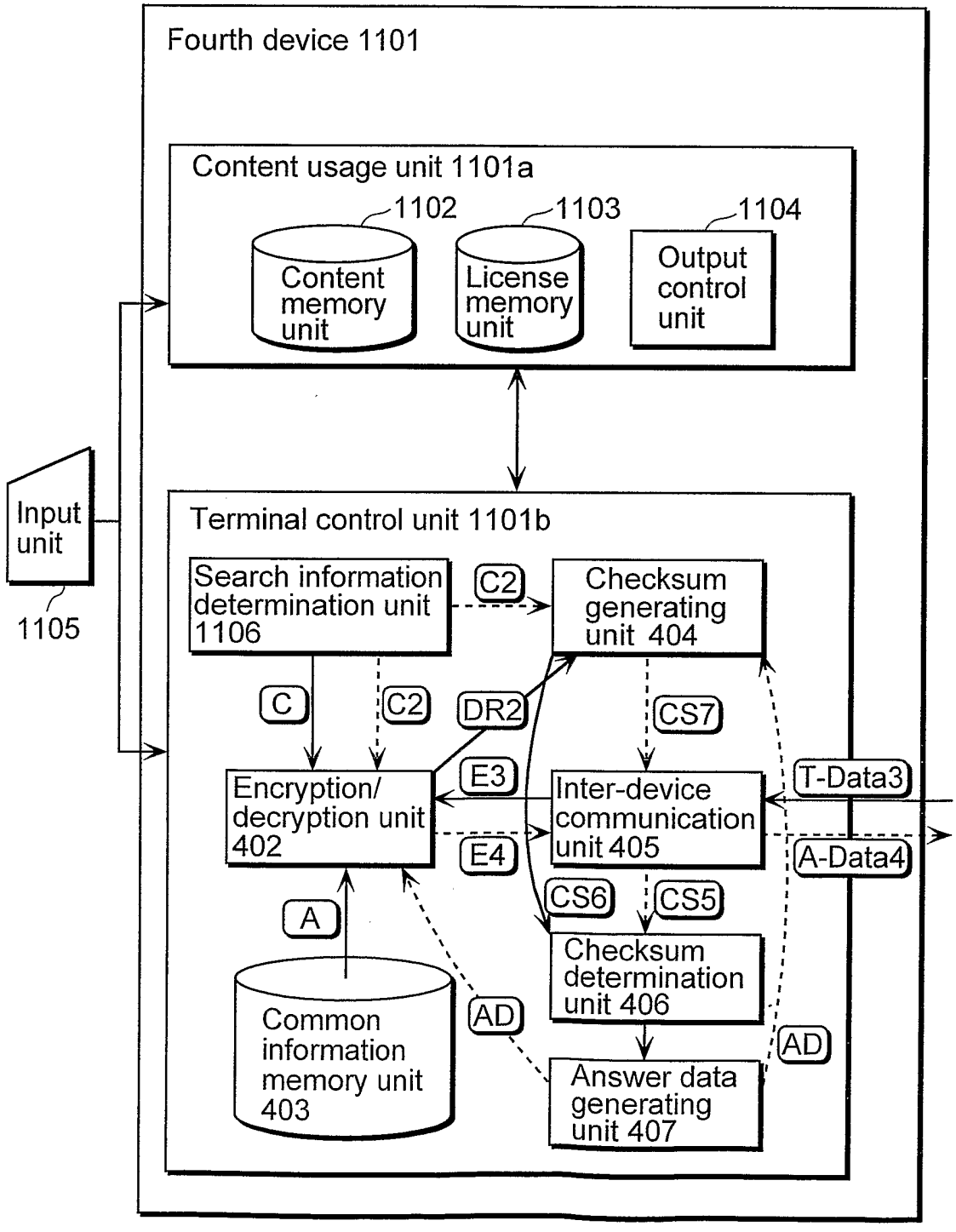

Fourth device 1101
Content usage unit 1101a
1102
1103
1104
Content memory unit
License memory unit
Output control unit
Input unit
1105
Terminal control unit 1101b
Search information determination unit 1106
C2
Checksum generating unit 404
C
C2
DR2
CS7
E3
Encryption/ decryption unit 402
Inter-device communication unit 405
T-Data3
E4
A-Data4
CS6
CS5
A
Checksum determination unit 406
Common information memory unit 403
AD
AD
Answer data generating unit 407

Fig. 12

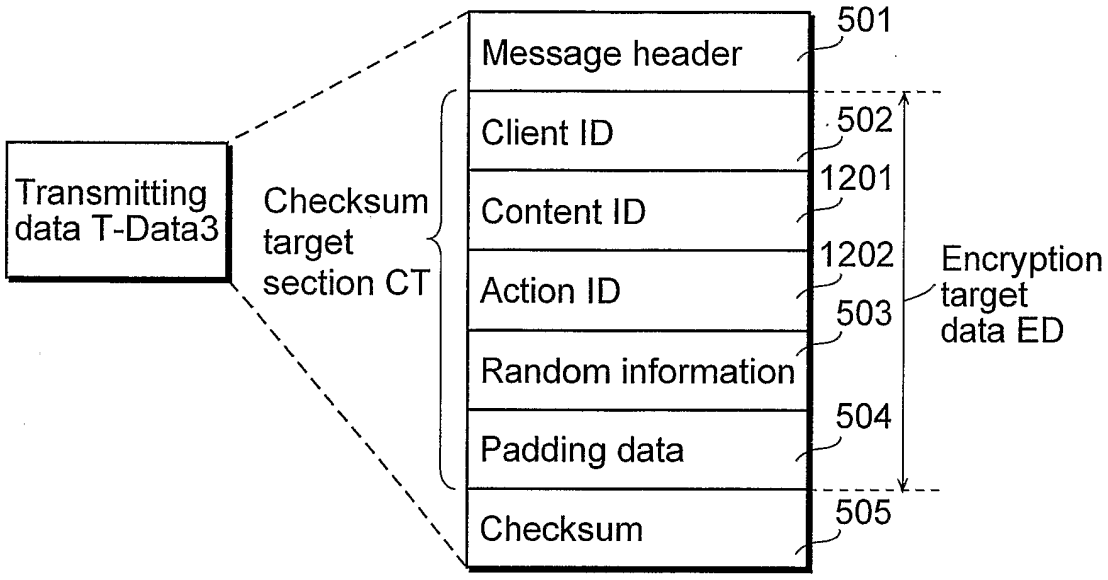

Transmitting data T-Data3
Checksum target section CT
Message header
Client ID
Content ID
Action ID
Random information
Padding data
Checksum
501
502
1201
1202
503
504
505
Encryption target data ED

Fig. 13

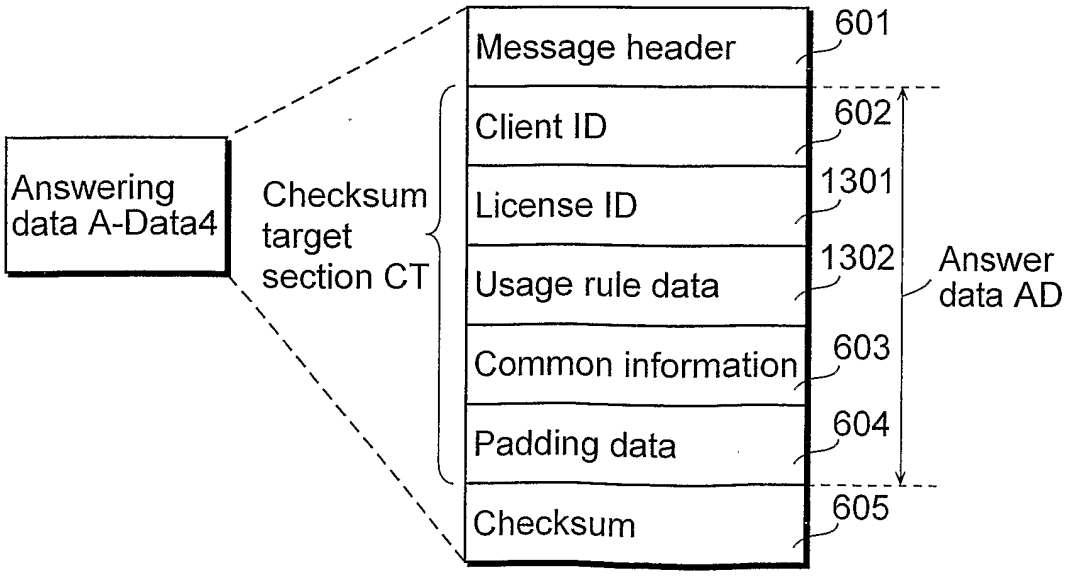

Answering data A-Data4
Checksum target section CT
Message header
Client ID
License ID
Usage rule data
Common information
Padding data
Checksum
601
602
1301
1302
603
604
605
Answer data AD

Fig. 14

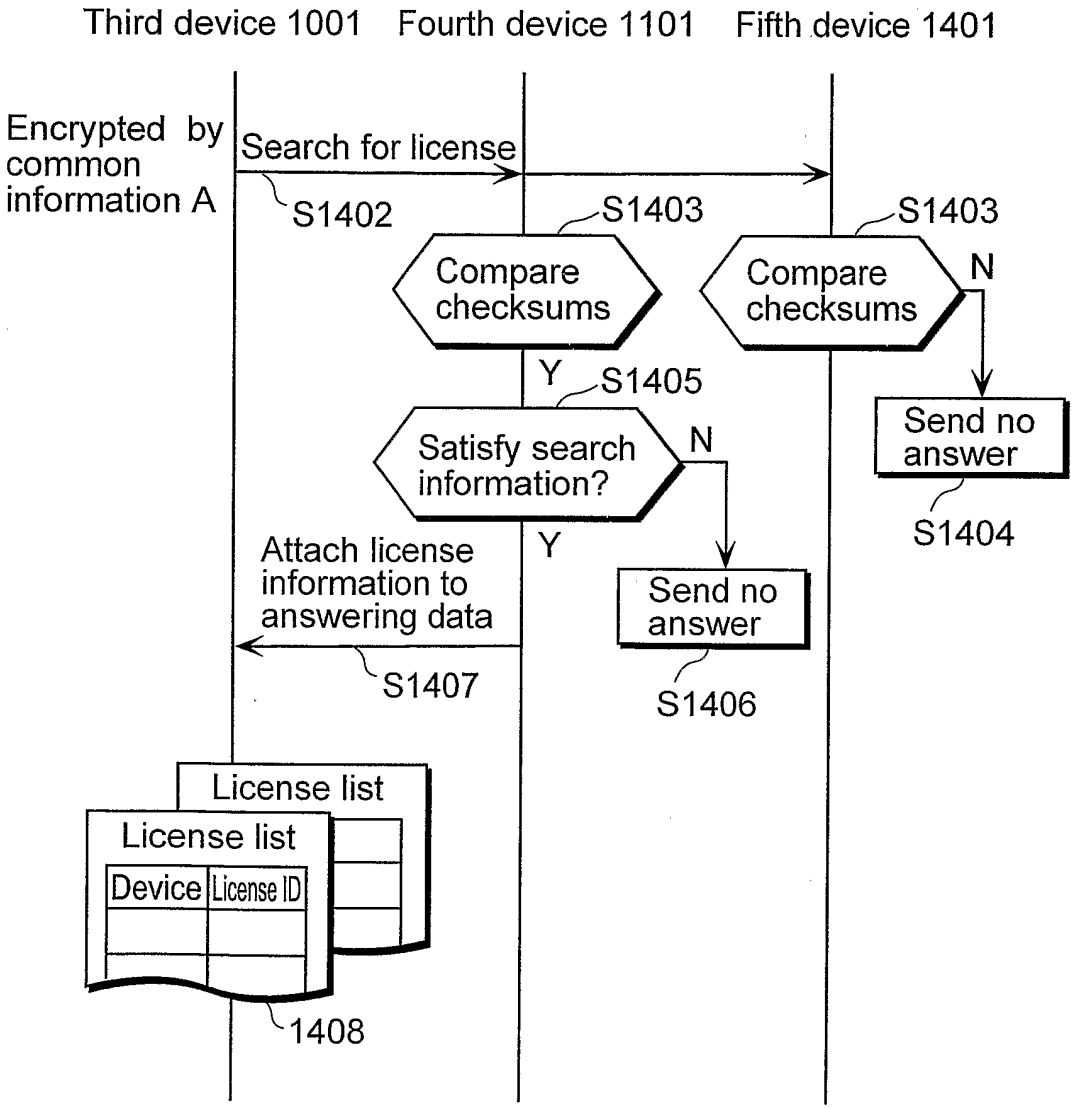
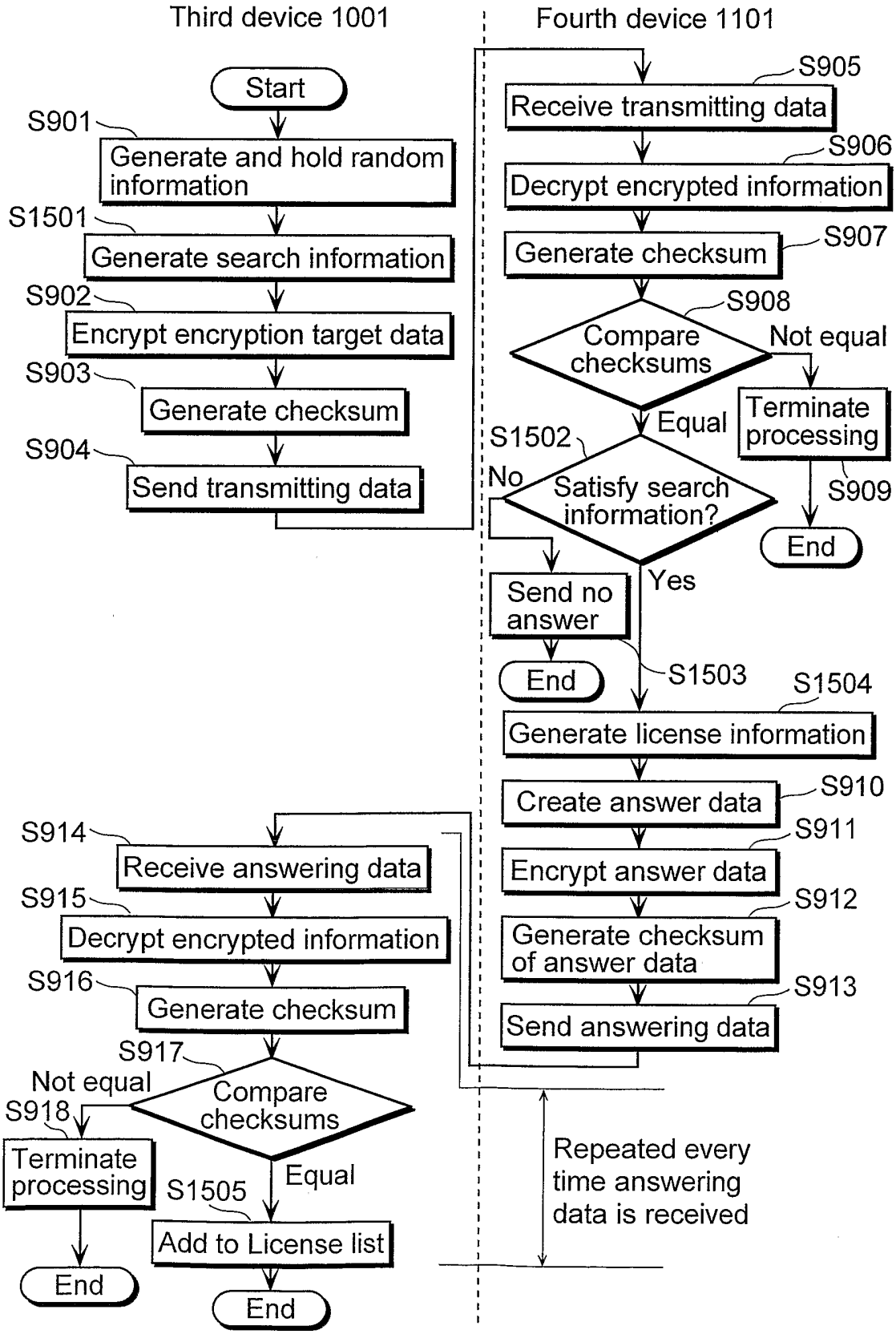

Third device 1001
Fourth device 1101
Fifth device 1401
Encrypted by common information A
Search for license
S1402
S1403
Compare checksums
S1403
Compare checksums
N
Send no answer
S1404
Y
S1405
Satisfy search information?
N
Send no answer
S1406
Y
Attach license information to answering data
S1407
License list
License list
Device
License ID
1408

Fig. 15


Third device 1001
Fourth device 1101
Start
S901
Generate and hold random information
S1501
Generate search information
S902
Encrypt encryption target data
S903
Generate checksum
S904
Send transmitting data
S905
Receive transmitting data
S906
Decrypt encrypted information
S907
Generate checksum
S908
Compare checksums
Not equal
Terminate processing
S909
End
Equal
S1502
Satisfy search information?
No
Send no answer
End
Yes
S1503
S1504
Generate license information
S910
Create answer data
S911
Encrypt answer data
S912
Generate checksum of answer data
S913
Send answering data
S914
Receive answering data
S915
Decrypt encrypted information
S916
Generate checksum
S917
Compare checksums
Not equal
S918
Terminate processing
End
Equal
S1505
Add to License list
End
Repeated every time answering data is received