

DESCRIPTION

SERVICE PROVIDING SERVER, INFORMATION PROCESSING
APPARATUS, DATA PROCESSING METHOD, AND COMPUTER PROGRAM

5

[Technical Field]

[0001]

The present invention relates to a service
providing server, an information processing apparatus, a
10 data processing method, and a computer program. More
particularly, the present invention is directed to a
service providing server, an information processing
apparatus, a data processing method, and a computer
program, all implementing provision of content-related
15 services to a user device which executes processing of
playing back an information recording medium, such as a
disc in which content is stored.

[Background Art]

[0002]

20 Various kinds of software data (hereinafter
referred to as content) such as audio data including
music, image data including movies, game programs and
various application programs, are provided to a user as
stored on an information recording medium including, e.g.,
25 a DVD (Digital Versatile Disc), an MD (Mini
Disc)(registered trade mark), a CD (Compact Disc), or a
high-density recordable disc using blue laser (Blu-ray
Disc)(registered trade mark). The user can play back
content for use in a user device including a PC (Personal
30 Computer), a disc player, i.e., in a playback apparatus.

[0003]

Furthermore, in recent years, a service providing

configuration has been in use, in which various services related to content stored in an information recording medium such as a disc are provided from a server networked with user devices.

5 [0004]

For example, when content stored in the disc is a movie in a foreign language, various content-related services including subtitles or dubbing data for its audio, or a disc purchasing discount ticket for a sequel
10 of the content, are provided to the user devices such as PCs from the server connected via a network.

[0005]

How services are provided from the server can take various forms. Some services may have no restricted
15 access, whereas some other services may be under a certain condition that e.g., they can be provided up to once for each disc which has service-related content recorded thereon.

[0006]

20 The rights of distribution or the like of content stored in a disc, that is, various content such as music data and image data, are generally held by their creators or their distributors. Consequently, at the time of the distribution of such content, a configuration for setting
25 a certain restricted access is generally adopted, i.e., only authorized users are permitted to use the content for preventing unauthorized use.

[0007]

Therefore, also the services provided in
30 association with content, a system is desired to be established, in which provision of a service is permitted

on condition that a certain right of use has been validated, i.e., processing of validating that a user is a purchaser of an authentic disc has been performed.

[Disclosure of the Invention]

5 [Problems to be Solved by the Invention]

[0008]

Embodiments of the present invention provide a service providing server, an information processing apparatus, a data processing method, and a computer
10 program, all enabling unauthorized use of services to be excluded by validating a right to use a service, in a configuration in which content is provided as stored on various information recording media including DVDs, CDs, blue laser recording media, and further a networked
15 service providing server performs service providing processing.

[Means for Solving the Problems]

[0009]

In accordance with a first aspect of the present invention, there is provided a service providing server for executing service providing processing in response to a service providing request from an information processing apparatus, characterized by having:

a data reception section which receives a service request accompanied by an information recording medium ID and a service ID, from the information processing apparatus;

a storage section which stores service providing situation data for each of the information recording medium IDs as service management data for each of title-unique values corresponding to titles of content stored on information recording media; and

a data processing section which executes processing of verifying the information recording medium ID and signature data contained in the information recording medium ID received via the data reception section, acquires a title-unique value on the basis of the information recording medium ID on condition that the information recording medium ID and the signature data are validated, acquires from the storage section service providing situation data corresponding to the title-unique value contained in the information recording medium ID or the title-unique value calculated by executing a calculation based on data contained in the information recording medium ID to judge whether or not a service specified by the information recording medium ID and the service ID is providable, and executes the service providing processing on condition that the service is judged to be providable.

[0010]

[0011]

Furthermore, in an embodiment of the service providing server of the present invention, the service

providing server is characterized by having the storage section storing a revocation list being a list of unauthorized information recording medium IDs, and the processing of verifying the information recording medium ID in the data processing section is characterized by being executed as processing of comparing the information recording medium ID received from the information processing apparatus with the IDs recorded in the revocation list.

10 [0012]

Furthermore, in an embodiment of the service providing server of the present invention, the information recording medium ID is characterized by being configured to include a title-unique value corresponding to a title of content stored in an information recording medium, and signature data generated on the basis of a secret key of a management apparatus and differing for each of the information recording media, and the data processing section is characterized by being configured to execute the processing of verifying the information recording medium ID as processing of generating a message to which a public key of the management apparatus is applied, for comparison with the signature data contained in the information recording medium ID, and also execute the processing of acquiring the service providing situation data corresponding to the title-unique value contained in the information recording medium ID, from the storage section.

[0013]

30 Furthermore, in an embodiment of the service providing server of the present invention, the

information recording medium ID is characterized by being configured to include a prime $p(w)$ set in response to a number W of pieces of information recording media manufactured, and data $IDKey(w)$ calculated by a
5 calculation based on the prime $p(w)$ and the title-unique value, and the data processing section is characterized by being configured to execute processing of judging whether or not data contained in the information recording medium ID is the prime, as the ID verifying
10 processing, and also calculate the title-unique value from the data $IDKey(w)$ contained in the information recording medium ID, and acquiring the service providing situation data corresponding to the title-unique value calculated, from the storage section.

15 [0014]

In accordance with a second aspect, there is provided an information processing apparatus for executing a service providing request to a service providing server, characterized by having:

20 a recording medium interface which executes processing of accessing an information recording medium; and

a data processing section which executes processing of verifying an information recording medium ID and
25 signature data contained in the information recording medium ID read from the information recording medium via the recording medium interface, and executes processing of transmitting the information recording medium ID and the signature data to the service providing server on
30 condition that the information recording medium ID and the signature data are validated,

characterized in that the data processing section is

configured to execute the processing of verifying the
information recording medium ID as processing of
verifying the signature data contained in the information
recording medium ID, and execute the processing of
5 acquiring, from the storage section, the service
providing situation data corresponding to the title-
unique value, according to the title-unique value
contained in the information recording medium ID, or the
title-unique value calculated by executing a calculation
10 based on data contained in the information recording
medium ID.

[0015]

[0016]

Furthermore, in an embodiment of the information processing apparatus of the present invention, the processing of verifying the information recording medium ID in the data processing section is characterized by being configured as processing of acquiring a revocation list being a list of unauthorized information recording medium IDs from a storage section or the information recording medium, and comparing the information recording medium ID received from the information processing apparatus with the IDs recorded in the revocation list acquired.

[0017]

In an embodiment of the information processing apparatus of the present invention, the information recording medium ID is characterized by being configured to include a title-unique value corresponding to a title of content stored on the information recording medium, and signature data generated on the basis of a secret key of a management apparatus and differing for each of the information recording media; and the data processing section is characterized by being configured to execute the processing of verifying the information recording medium ID as processing of generating a message to which a public key of the management apparatus is applied, for

comparison with the signature data contained in the
information recording medium ID.

[0018]

Furthermore, in an embodiment of the information
5 processing apparatus of the present invention, the
information recording medium ID is characterized by
being configured to include a prime $p(w)$ set in response
to each of a number W of information recording media
manufactured, and data $IDKey(w)$ calculated by a
10 calculation based on the prime $p(w)$ and a title-unique
value, and the data processing section is configured to
execute processing of judging whether or not data
contained in the information recording medium ID is the
prime, as the ID verifying processing.

15 [0019]

In accordance with a third aspect, there is provided a data processing method for executing service providing processing in response to a service providing request from an information processing apparatus,

5 characterized by having:

a data reception step of receiving a service request accompanied by an information recording medium ID and a service ID, from the information processing apparatus; and

10 a data processing step of executing processing of verifying the information recording medium ID and signature data contained in the information recording medium ID received, acquiring a title-unique value on the basis of the information recording medium ID and
15 signature data on condition that the information recording medium ID and signature data are validated, acquiring service providing situation from a storage section for storing situations data corresponding to the title-unique value contained in the information
20 recording medium ID or the title-unique value calculated by executing a calculation based on data contained in the information recording medium ID acquired, for each of the information recording medium IDs as service management data for each of title-unique
25 values contained in the information recording medium ID or the title-unique value calculated by executing a calculation based on data contained in the information recording medium ID stored on information recording media, judging whether or not a service specified by the
30 information recording medium ID and the service ID is providable, and executing the service providing

processing on condition that the service is judged to be providable.

[0020]

[0021]

5 Furthermore, in an embodiment of the data processing method of the present invention, the processing of verifying the information recording medium ID in the data processing step is characterized by including a step of executing it as processing of
10 comparing the information recording medium ID received

from the information processing apparatus with IDs recorded in a revocation list being a list of unauthorized information recording medium IDs.

[0022]

5 Furthermore, in an embodiment of the data processing method of the present invention, the information recording medium ID is characterized by being configured to include a title-unique value corresponding to a title of content stored on the information recording
10 medium, and signature data generated on the basis of a secret key of a management apparatus and differing for each of the information recording media, and the data processing step is characterized by including a step of executing the processing of verifying the information
15 recording medium ID as processing of generating a message to which a public key of the management apparatus is applied, for comparison with the signature data contained in the information recording medium ID, and also executing the processing of acquiring the service
20 providing situation data corresponding to the title-unique value contained in the information recording medium ID, from the storage section.

[0023]

 Furthermore, in an embodiment of the data
25 processing method of the present invention, the information recording medium ID is characterized by including a prime $p(w)$ set in response to each of a number W of information recording media manufactured, and data $IDKey(w)$ calculated by a calculation based on the
30 prime $p(w)$ and the title-unique value, and the data processing step is characterized by including a step of

executing processing of judging whether or not data contained in the information recording medium ID is the prime as the ID verifying processing, and also calculating the title-unique value from the data

5 IDKey(w) contained in the information recording medium ID, and acquiring the service providing situation data corresponding to the title-unique value calculated, from the storage section.

[0024]

10 In accordance with a fourth aspect, there is provided a data processing method for executing a service providing request to a service providing server, characterized by having:

a recording medium accessing step of executing
15 processing of accessing an information recording medium via a recording medium interface; and

a data processing step of executing processing of verifying an information recording medium ID read from the information recording medium and signature data that
20 are received via the recording medium interface, and executing processing of transmitting the information recording medium ID to the service providing server on condition that the information recording medium ID and signature data are validated,

25 characterized in that the data processing step is configured to execute the processing of verifying the information recording medium ID as processing of verifying the signature data contained in the information recording medium ID, and execute the
30 processing of acquiring, from the storage section, the service providing situation data corresponding to the

title-unique value, according to the title-unique value
contained in the information recording medium ID, or the
title-unique value calculated by executing a calculation
based on data contained in the information recording

5 medium ID.

[0025]

[0026]

Furthermore, in an embodiment of the data processing method of the present invention, the processing of verifying the information recording medium ID in the data processing step is characterized by
5 including a step of acquiring a revocation list being a list of unauthorized information recording medium IDs from a storage section or the information recording medium, and comparing the information recording medium ID received from the information processing apparatus with
10 the IDs recorded in the revocation list acquired.

[0027]

Furthermore, in an embodiment of the data processing method of the present invention, the information recording medium ID is characterized by
15 including a title-unique value corresponding to a title of content stored on the information recording medium, and signature data generated on the basis of a secret key of a management apparatus and differing for each of the information recording media, and the data processing step
20 is characterized by including a step of executing the processing of verifying the information recording medium ID as processing of generating a message to which a public key of the management apparatus is applied, for comparison with the signature data contained in the
25 information recording medium ID.

[0028]

Furthermore, in an embodiment of the data processing method of the present invention, the information recording medium ID is characterized by
30 including a prime $p(w)$ set in response to each of a number W of information recording media manufactured, and

data IDKey(w) calculated by a calculation based on the
prime $p(w)$ and a title-unique value, and the data
processing step is characterized by including a step of
executing processing of judging whether or not data
5 contained in the information recording medium ID is the
prime as the ID verifying processing.

[0029]

In accordance with a fifth aspect, there is provided a computer program for executing processing in response to a service providing request from an information processing apparatus, characterized by

5 having:

a data reception step of receiving a service request accompanied by an information recording medium ID and a service ID, from the information processing apparatus; and

10 a data processing step of executing processing of verifying the information recording medium ID and signature data contained in the information recording medium ID received, acquiring a title-unique value on the basis of the information recording medium ID and
15 signature data on condition that the information recording medium ID and signature data are validated, acquiring service providing situation data from a storage section for storing service providing situation data corresponding to the title-unique value contained
20 in the information recording medium ID or the title-unique value calculated by executing a calculation based on data contained in the information recording medium ID, for each of the information recording medium IDs as service management data for each of title-unique values
25 contained in the information recording medium ID or the title-unique value calculated by executing a calculation based on data contained in the information recording medium ID stored on information recording media, judging whether or not a service specified by the
30 information recording medium ID and the service ID is providable, and executing the service providing

processing on condition that the service is judged to be providable.

[0030]

5 In accordance with a sixth aspect, there is provided a computer program for executing a service providing request to a service providing server, characterized by having:

10 a recording medium accessing step of executing processing of accessing an information recording medium via a recording medium interface; and

15 a data processing step of executing processing of verifying an information recording medium ID and signature data contained in the information recording medium ID read from the information recording medium via the recording medium interface, and executing processing of transmitting the information recording medium ID and signature data to the service providing server on condition that the information recording medium ID and signature data are validated,

20 characterized in that the data processing step is configured to execute the processing of verifying the information recording medium ID as processing of verifying the signature data contained in the information recording medium ID, and execute the processing of acquiring, from the storage section, the service providing situation data corresponding to the title-unique value, according to the title-unique value contained in the information recording medium ID, or the title-unique value calculated by executing a calculation
25 based on data contained in the information recording medium ID.
30

[0031]

Note that the computer program according to
embodiments of the present invention is a computer
program that can be provided by a storage medium, a
5 communication medium, e.g., a storage medium such as a
CD or an FD, an MO, or a communication medium such as a
network, provided in a computer-readable form to, e.g.,
a general-purpose computer system that can execute
various program codes. By providing such a program in a
10 computer-readable form, processing according to the
program is realized on the computer system.

[0032]

Further aspects, features and advantages of the
present invention will become apparent from a more
15 detailed description that is based on a later-described
embodiment of the present invention and accompanying

drawings. Note that the system used in the present specification means a logical set configuration of a plurality of apparatus, and is not limited to one wherein apparatus each having its own configuration are grouped
5 within the same enclosure.

[Effects of the Invention]

[0033]

According to the configuration of the present invention, in a configuration in which content is
10 provided as stored in various information recording media including a DVD, a CD, a blue laser recording medium, and in which service providing processing is performed from a networked service providing server, the service providing server verifies an information recording medium ID
15 transmitted thereto from an information processing apparatus (user device), and provides a service based on service providing situation data for each of the information recording medium IDs. Therefore, only if the information processing apparatus having transmitted a
20 service request is one having read a valid information recording medium ID from an information recording medium, and only if it has been validated that the service is providable on the basis of the service providing situation data, the providing of the service is executed.

25 [0034]

Furthermore, according to the configuration of the present invention, the information recording medium ID stored on the information recording medium includes data whose validity can be checked, such as signature data of
30 a management apparatus, and also either has a title-unique value or includes data from which the title-unique

value is calculable. Therefore, the service providing server can check the validity based on the data included in the information recording medium ID, and additionally can acquire the title-unique value, whereby the server
5 can specify service providing situation data set so as to correspond to the title-unique value.

[0035]

[Fig. 1] It is a diagram for explaining data stored in an information recording medium.

10 [Fig. 2] It is a diagram for explaining a configuration of a revocation list.

[Fig. 3] It is a diagram for explaining MAC (Message Authentication Code) generating/verifying processing when a MAC is used.

15 [Fig. 4] It is a diagram for explaining a hierarchical tree structure applied to processing of encrypting and distributing various keys and data.

[Fig. 5] It is a diagram showing an example in which a content key is distributed and decrypted using an EKB
20 (Enabling Key Block).

[Fig. 6] It is a diagram for explaining a configuration for manufacturing, managing an information recording medium.

[Fig. 7] It is a diagram for explaining a
25 configuration example of a service providing server.

[Fig. 8] It is a diagram for explaining service providing situation data which the service providing server holds.

[Fig. 9] It is a diagram for explaining a
30 configuration example of an information processing apparatus (user device).

[Fig. 10] It is a diagram for explaining disc ID setting examples.

[Fig. 11] It is a flowchart for explaining processing which the information processing apparatus (user device) executes.

[Fig. 12] It is a flowchart for explaining a disc ID verifying sequence which the information processing apparatus (user device) executes.

[Fig. 13] It is a flowchart for explaining a disc ID verifying sequence which the information processing apparatus (user device) executes.

[Fig. 14] It is a flowchart for explaining a disc ID verifying sequence which the information processing apparatus (user device) executes.

[Fig. 15] It is a flowchart for explaining a disc ID verifying sequence which the information processing apparatus (user device) executes.

[Fig. 16] It is a diagram for explaining processing by which the information processing apparatus receives a service from the service providing server.

[Fig. 17] It is a flowchart for explaining processing which the service providing server executes.

[Best Modes for Carrying out the Invention]

[0036]

Below, details of a service providing server, an information processing apparatus, a data processing method, and a computer program according to the present invention are described with reference to the drawings.

Note that the description is given according to the following items:

1. Data stored in information recording medium
2. Configuration for providing and using/managing content-stored information recording medium
- 5 3. Configuration of information processing apparatus constituting service providing server and user device
4. Details of processing in user device
5. Details of processing in service providing

10 server

[0037]

[1. Data stored in information recording medium]

A configuration example of data recorded on an information recording medium is shown in Fig. 1. Fig. 1
 15 is a diagram for explaining data stored on various information recording medium 100 including a CD (Compact Disc), a DVD (Digital Versatile Disc), an MD (Mini Disc), a Blue laser optical disc (Blu-ray Disc), a flash memory. While a disc-shaped medium is shown as an example in Fig.
 20 1, the present invention is applicable not only to such disc-shaped media, but also to various information recording media including a flash memory.

[0038]

On the information recording medium 100, there is
 25 stored information shown in Fig. 1, i.e., a disc ID 101, content 102, a Disc ID Revocation List (DIRL) 103, an encryption key information (EKB: Enabling Key Block) 104.

[0039]

The disc ID 101 is, e.g., an identifier unique to
 30 the disc, and is stored such that it is hard to erase or rewrite. Note that the disc ID 101 includes a unique

value (title-unique value) for each title corresponding to the content 102 stored on the information recording medium 100, a unique value (disc-unique value) for each information recording medium 100, and information
5 indicative of its validity, e.g., information (validity verification value), such as a signature. Details of the disc ID are described later.

[0040]

Note that since a disc-shaped medium is shown as an
10 example of a content-stored information recording medium in a below-described embodiment, its identifier is described as the disc ID. If any other information recording medium such as a flash memory is used as the content-stored information recording medium, an
15 information recording medium ID corresponding to the disc ID is set.

[0041]

The content 102 is also stored on the information recording medium 100. The content is stored as, e.g.,
20 encrypted content. In a case of the encrypted content, key information for decrypting the content is either stored on the information recording medium 100 or provided via a network.

[0042]

25 The Disc ID Revocation List (DIRL) 103 is also stored on the information recording medium 100. The Disc ID Revocation List (DIRL) 103 is data in which, when any disc recognized as having been copied without authorization or the like, e.g., a CD-R storing
30 unauthorized copied content is found in the market, a disc ID copied on the unauthorized CD-R together with the

content is extracted and listed. The generation and management of the Disc ID Revocation List (DIRL) 103, the providing of the list information to disc manufacturers, and the like are executed by a Central Authority (CA).

5 [0043]

Referring to Fig. 2, a data configuration of the Disc ID Revocation List (DIRL) is described. A Disc ID Revocation List (DIRL) 150 includes, as shown in Fig. 2, a version number 151 monotonously increased according to a time on which the list has been created, a revoked disc ID list 152 enumerating disc IDs of discs for exclusion, and an authenticator as a tampering verification value 153 for the version number 151 and the revoked disc ID list 152. The tampering verification value 153 is data applied to determine whether or not the data for verification, i.e., the version number 151 and the revoked disc ID list 152 in this case has been tampered. A digital signature using a public-key encryption technique, and a Message Authentication Code (MAC) using a symmetric-key encryption technique are applied thereto.

10
15
20

[0044]

If a digital signature using a public-key encryption technique is used as the tampering verification value 153, playback apparatuses acquire a signature verification key (public key) of a reliable entity, e.g., the above-mentioned Central Authority (CA), and verify the signature created with a signature generation key (secret key) of the Central Authority (CA), using the signature verification key (public key) which each of the playback machines has acquired, whereby to determine the version number 151 and the revoked disc ID

25
30

list 152 have been tampered or not.

[0045]

Referring to Fig. 3, Message Authentication Code (MAC) generating/verifying processing using a MAC as the
5 tampering verification value 153 is described. The Message Authentication Code (MAC) is generated as data for tampering verification. While various modes are available for MAC generating/verifying processing, an example of MAC value generation using a DES encryption
10 processing configuration is shown in Fig. 3.

[0046]

As shown in Fig. 3, a message for processing, i.e., the version number 151 and the revoked disc ID list 152 shown in Fig. 2 in this case, is divided into 8-byte
15 blocks (the divided messages are hereinafter referred to as M1, M2, ..., MN). First, an Initial Value (hereinafter referred to as IV) is XORed with M1 (the result is I1). Next, I1 is inputted to a DES (Data Encryption Standard) encrypting section using a key (hereinafter referred to
20 as K1) (its output is E1). Successively, E1 is XORed with M2, and its output I2 is inputted to the DES encrypting section using the key K1 (an output E2). Thereafter, this processing is repeated to encrypt all the messages. The last output EN is the Message
25 Authentication Code (MAC).

[0047]

A MAC value takes a different value once its generator data has been altered. Thus, if a comparison between a MAC generated on the basis of data (message)
30 for verification and a MAC recorded indicates that both coincide, it is proved that the data (message) for verification has not been altered or tampered.

[0048]

Returning to Fig. 1, the description of the data stored in the information recording medium 100 is continued. The encryption key information (EKB: Enabling
 5 Key Block) 104 is also stored on the information recording medium 100.

[0049]

Referring to a drawing, a configuration for providing secret information using the encryption key
 10 information (EKB) is described. Numbers 0-15 shown at the lowermost layer of Fig. 4 are user devices as information processing apparatus for, e.g., using content. Namely, leaves in a hierarchical tree structure shown in Fig. 4 correspond to the devices, respectively.

15 [0050]

Each of the devices 0-15 stores a key set (device keys (DNKs: Device Node Keys)) in a memory at the time of its manufacture or shipment, or thereafter. The key set (DNKs) includes keys (node keys) assigned to nodes in a
 20 path from its own leaf to a root in the hierarchical tree structure, and a leaf key of its own leaf. Symbols K0000-K1111 shown in the lowermost layer in Fig. 4 are the leaf keys assigned to the devices 0-15, respectively, and keys KR-K111 indicated from a KR (root key) at the
 25 uppermost layer to nodes at the second layer from the lowermost layer are the node keys.

[0051]

In the tree structure shown in Fig. 4, e.g., the device 0 owns the leaf key K0000, and the node keys K000,
 30 K00, K0, KR, as device keys. The device 5 owns K0101, K010, K01, K0, KR. The device 15 owns K1111, K111, K11,

K1, KR. Note that only sixteen devices 0-15 are shown in the tree of Fig. 4, and the tree structure is symmetrical having four layers. However, other configurations including more devices within the tree, and also
5 different layers in parts of the tree may be applicable.
[0052]

Moreover, the devices in the tree structure of Fig. 4 include various recording media, such as, e.g., a DVD, a CD, an MD, a flash memory embedded in the device or
10 releasable from the device. Furthermore, various application services can coexist. It is over such a configuration in which different devices and different applications coexist to which the hierarchical tree structure shown in Fig. 4 being content or key
15 distribution configuration is applied.
[0053]

In a system in which such various devices and applications coexist, devices in a part enclosed by a broken line in Fig. 4, i.e., the devices 0, 1, 2, 3 are
20 set as a group. For example, only these devices enclosed by the broken line and included in the group hold authorized rights, i.e., licenses to use encrypted content stored on information recording media. In this case, an EKB is set such that only the devices 0, 1, 2, 3
25 can acquire a key applied to decrypting the content, and the set EKB is stored on the information recording media each storing the encrypted content.
[0054]

As is apparent from Fig. 4, the four devices 0, 1,
30 2, 3 included in one group hold shared keys K00, K0, KR as the device keys (DNKs: Device Node Keys) stored on

their devices.

[0055]

At this point, an EKB configuration for enabling only the devices 0, 1, 2 to acquire a content key Kcon applied to decrypting the content is as shown in, e.g.,
 5 Fig. 5. Namely, an EKB is set as follows:

Index Encrypted data

000 Enc (K000, Kcon)

0010 Enc (K0010, Kcon)

10 [0056]

Note that Enc (Kx, Ky) denotes data Ky encrypted with a key Kx. At this point, the devices 0, 1 can decrypt the encrypted data indexed as [000] using the device key [K000] they hold, and also the device 2 can
 15 decrypt the encrypted data indexed as [0010] in the EKB using the device key [K0010] it holds. They can acquire the content key Kcon through their processing of decrypting the respective encrypted data. The other device holds none of the device keys [K000], [K0010], and
 20 thus cannot acquire the content key by decryption of the EKB even if having received the EKB so configured as shown in Fig. 5.

[0057]

In this way, an EKB is set as data having a
 25 configuration corresponding to licensed devices, whereby the EKB is configured as a key information block which is processable only by any selected device, and through which secret information such as a content key can be provided to only specific devices. The key information
 30 (EKB) issuing center 104 generates an EKB processable only by devices to which it permits use of content, and

provides the EKB to the information recording medium manufacturing entity 103. The information recording medium manufacturing entity 103 stores the EKB in an information recording medium 110 together with the encrypted content, and provides the media to the users.
[0058]

[2. Configuration for providing and using/managing content-stored information recording medium]

Fig. 6 is a diagram for explaining a configuration for providing and using/managing an information recording medium 200 storing the above-mentioned various data.
[0059]

As shown in Fig. 6, in a configuration for providing and managing content, there are a management apparatus 201 that the Central Authority (CA) uses, a content providing apparatus 203 that a content provider uses, a disc manufacturing apparatus 202 that a disc manufacturer uses, an information processing apparatus (user device) 400 that a user uses for executing content playback processing, and a service providing server 300 for executing, e.g., processing of providing services, such as, e.g., subtitles, corresponding to content stored on the information recording medium 200, with respect to the information processing apparatus (user device) 400.
[0060]

The management apparatus 201 generates the aforementioned disc ID and Disc ID Revocation List (DIRL), and provides them to the disc manufacturing apparatus 202. Moreover, the content providing apparatus 203 provides encrypted content and an Enabling Key Block (EKB) to the disc manufacturing apparatus 202.

[0061]

The disc manufacturing apparatus 202 manufactures the information recording medium 200 in which the disc ID and Disc ID Revocation List (DIRL) received from the management apparatus 201 and the encrypted content data and the Enabling Key Block (EKB) received from the content providing apparatus 203 are recorded.

[0062]

A user, e.g., purchases the information recording medium 200, and sets it in the information processing apparatus (user device) 400. The information processing apparatus (user device) 400 can verify that the disc ID recorded in the information recording medium 200 is valid, check that the disc ID is not found in the Revocation List DIRL, and acquire appropriate content key data from the Enabling Key Block EKB on the basis of its own device node key data DNK, whereby he/she can decrypt and play back the encrypted content data.

[0063]

Furthermore, the information processing apparatus (user device) 400 transmits the disc ID recorded on the information recording medium 200 and a service ID as a service identifier, to the service providing server 300. Then, in the service providing server 300, the validity of the disc ID is verified, and further, whether or not the service is providable is determined on the basis of service providing situation data which the service providing server 300 holds. If it is determined that the disc ID is valid and that the service is providable on the basis of the service providing situation data, the server 300 executes its service providing processing for

the information processing apparatus (user device) 400.
[0064]

[3. Configuration of information processing apparatus
constituting service providing server and user device]

5 Next, a configuration of the information processing
apparatus as the service providing server and the user
device is described.
[0065]

10 Fig. 7 is a diagram showing a configuration of the
service providing server shown in Fig. 6. As shown in
Fig. 7, the service providing server 300 has, e.g., a
controller 302 including a CPU, a calculation unit 303
for executing various calculating processing, an
input/output interface (I/F) 304 as an interface for
15 input/output of data from data input devices and to data
output devices, and for input/output of data via a
network, a secure memory 305, a main memory 306. These
components are interconnected via a bus 301.
[0066]

20 The main memory 306 stores data of a low security
level, among various data used for processing by the
calculation unit 303 and the controller 302. The secure
memory 305 stores data of a high security level, among
the various data used for processing by the calculation
25 unit 303 and the controller 302. The secure memory 305
stores, e.g., the disc ID and the like received from the
management apparatus 201 shown in Fig. 6.
[0067]

30 The input/output interface 304 is connected to,
e.g., a control means or a network, not shown, and
receives various data from the management apparatus 201

and the content providing apparatus 203 shown in Fig. 6.
The interface 304 further implements communication with
the information processing apparatus (user device) 400,
which is to receive a service, so as to provide the
5 service.

[0068]

The calculation unit 303 executes various
calculations including generation of verification data
for signature data, on the basis of control from the
10 controller 302. The controller 302 executes various
programs, such as, e.g., a checking program as to whether
or not a service is providable to a user device, a
service providing program.

[0069]

15 The service providing server 300 receives the Disc
ID Revocation List from the management apparatus 201, the
content providing apparatus 203, or other apparatus via
the input/output interface (I/F) 304, periodically or for
each event, and constantly stores the latest version in
20 the secure memory 305.

[0070]

Moreover, the server 300 also receives title-based
title-unique values and service identification
information for identifying services to be provided, from
25 the content providing apparatus 203 or other apparatus,
via the input/output interface (I/F) 304, and stores a
service providing situation database in which title-based
service providing situation information is managed, in
the secure memory 305.

30 [0071]

"Title" means a title corresponding to content

stored on the information recording medium 200 which is attached to the information processing apparatus (user device) 400.

[0072]

5 An example of a data configuration of the service providing situation database is shown in Fig. 8. The service providing situation database includes, as shown in Fig. 8, title identification information about content, which corresponds to services that the service providing
10 server 300 provides, and service providing situations as to the services set for each title-unique value and corresponding to the disc IDs of discs storing the content having that title.

[0073]

15 For example, service providing situation data shown in Fig. 8 is service providing situation data as to:

 title identification information: aaaa; and

 title-unique value: bbbb,

and is a recording of how many times a Service 1 and a
20 Service 2 associated with content corresponding to this title have so far been provided in response to service providing requests based on discs having a disc ID 1 and a disc ID 2, respectively.

[0074]

25 Note that in the service providing situation data shown in Fig. 8 (a),

 the Service 1 is a service specified to be providable only one time to the disc ID 1, and

 the Service 2 is a service specified to be
30 providable up to 5 times to the disc ID 1.

[0075]

The service providing server 300 stores the service providing situation data shown in Fig. 8 in, e.g., the secure memory 305 and holds them therein, and checks, in response to a service providing request accompanied by a disc ID from the information processing apparatus (user device) 400, if the service providing requesting device is making the service providing request based on a valid disc ID, and further, provides the service only if an upper service providable limit is not reached on the basis of the service providing situation data shown in Fig. 8.

[0076]

When having received the service providing request accompanied by the disc ID from the information processing apparatus (user device) 400, the service providing server 300 validates the disc ID having been transmitted thereto from the information processing apparatus (user device) 400, and also checks that the disc ID having been transmitted thereto from the information processing apparatus (user device) 400 is not revoked in the Revocation List held by the service providing server 300.

[0077]

Furthermore, the service providing server 300 executes processing, such as checking or extracting the title-unique value based on the validated disc ID, extracting the disc-unique value. Then, the server 300 specifies, on the basis of the acquired title-unique value, service providing situation data as to the corresponding title by referring to the database storing the service providing situation data shown in Fig. 8, and

checks if the server 300 can provide the service on the basis of the specified data. Namely, the server 300 provides the service only if the upper service providable limit is not reached on the basis of the service
5 providing situation data shown in Fig. 8.

[0078]

Note that in the configuration example of the service providing situation data shown in Fig. 8, the service providing situation data is stored for each disc
10 ID. However, an alternative configuration may be adopted, in which the disc-unique value for identifying an individual disc is used, instead of the disc ID.

[0079]

Note that the service providing server 300 updates
15 the service providing situation data shown in Fig. 8 when having provided the service to the information processing apparatus (user device) 400.

[0080]

Referring next to Fig. 9, a configuration of the
20 information processing apparatus (user device) 400 is described.

[0081]

As shown in Fig. 9, the information processing apparatus (user device) 400 has, e.g., an input/output
25 interface 402, a codec 403 for executing generation and decoding of various coded data such as MPEG (Moving Picture Experts Group), an input/output interface 404 provided with an A/D and D/A converter 405, a encryption processing section 406, a ROM (Read Only Memory) 407, a
30 controller 408, a memory 409, and a recording medium interface for accessing the information recording medium

200. These components are interconnected to a bus 401.

[0082]

The input/output interface 402 receives a digital signal supplied from an external source, such as a
5 network, for output onto the bus 401, and also receives a digital signal on the bus 401 for output to the external source.

[0083]

The codec 403 decodes, e.g., MPEG-coded data
10 supplied via the bus 401 for output to the input/output interface 404, and also encodes a digital signal supplied from the input/output interface 404 for output onto the bus 401.

[0084]

15 The input/output interface 404 incorporates therein the A/D and D/A converter 405. The input/output interface 404 receives an analog signal supplied from an external source, and subjects the signal to analog-to-digital converting processing using the A/D and D/A
20 converter 405, for output to the codec 403 as a digital signal, and also subjects a digital signal from the codec 403 to digital-to-analog converting processing using the A/D and D/A converter 405 for output to the external source as an analog signal.

25 [0085]

The encryption processing section 406 is, e.g., formed of a one-chip LSI, and has a configuration for encrypting or decrypting a digital signal such as, e.g., content supplied thereto via the bus 401, for output onto
30 the bus 401. Note that the encryption processing section 406 is not limited to the one-chip LSI, but may

alternatively be realized by a configuration in which various software or hardware is combined.

[0086]

The ROM 407 stores, e.g., leaf key data being a
5 device key either unique to each information processing
apparatus as a user device or unique to each group of a
plurality of information processing apparatus (user
devices), and node key data being device key data shared
among a plurality of playback apparatus or a plurality of
10 groups. These are applied to processing of decrypting
the aforementioned Enabling Key Block (EKB) as the
encryption key information.

[0087]

The controller 408 includes, e.g., a CPU for
15 executing a program stored in the memory 409. The
controller 408 centrally controls processing of the
information processing apparatus (user device) 400.
Namely, the function (processing) of the information
processing apparatus (user device) 400 is regulated by
20 the program executed by the controller 408.

[0088]

The memory 409 reads the above-mentioned Disc ID
Revocation List (DIRL) from the information recording
medium 200, for secure storage. For example, it is
25 preferable to keep the data tamper-resistant by, e.g.,
storing the data in the memory as encrypted on the basis
of the ID set to each information processing apparatus
(user device) 400. In this way, the Disc ID Revocation
List (DIRL) is stored such that it is not readily
30 feasible to externally erase, tamper, or replace with any
old version. The recording medium interface 410 is used

to access the information recording medium 200.

[0089]

[4. Details of processing in user device]

Next, details of processing are described, which
5 the information processing apparatus 400 as a user device
performs when receiving a service from the service
providing server 300.

[0090]

Fig. 10 is a flowchart for explaining a sequence
10 according to which the information processing apparatus
(user device) 400 shown in Fig. 9 having the information
recording medium attached thereto executes processing
when receiving a service from the service providing
server.

15 [0091]

In step S101, the information processing apparatus
(user device) 400, when having the information recording
medium 200 set thereto in a predetermined access position,
reads the disc ID from the information processing medium
20 200 via the recording medium interface 410, and stores it
in the memory 409.

[0092]

In step S102, the controller 408 of the information
processing apparatus (user device) 400 reads the disc ID
25 stored in the memory 409, to verify whether or not it has
been tampered and whether or not it is valid. This
verifying processing is described later.

[0093]

In step S103, the controller 408, having judged in
30 step S102 that the above disc ID is valid, proceeds to
step S105; otherwise, the controller 408 proceeds to step

S104. In step S104, the controller 408 stops (prohibits) decryption and playback of the encrypted content recorded on the information recording medium 200.

[0094]

5 If having judged that the disc ID is valid, the controller 408 reads, in step S105, the Disc ID Revocation List (DIRL) from the information recording medium 200 via the recording medium interface 410. And if a digital signature using a public-key encryption
10 technique is put thereto as the tampering verification value for the Revocation List read, the controller 408 verifies the List DIRL using a signature verification key (public key). If a Message Authentication Code MAC is
15 verifying processing described earlier with reference to Fig. 3 is executed.

[0095]

 On condition that the Disc ID Revocation List (DIRL) has been judged to be untampered, the controller
20 408 makes a comparison between a version of that Disc ID Revocation List (DIRL) and a version of a Disc ID Revocation List (DIRL) already stored in the memory 409.

[0096]

 If the version of the Disc ID Revocation List (DIRL) read is newer than the version of the Disc ID
25 Revocation List (DIRL) already stored in the memory 409, the controller 408 updates the Revocation List DIRL in the memory 409 with the Disc ID Revocation List (DIRL) read.

30 [0097]

 In step S106, the controller 408 judges whether or

not the disc ID read in step S101 is present in the Revocation List DURL, and proceeds to step S107 when having determined that it is present; otherwise it proceeds to step S108. In step S107, the controller 408
 5 stops (prohibits) decryption and playback of the encrypted content recorded in the information recording medium 200.

[0098]

If the disc ID is not present in the Revocation
 10 List, the controller 408, proceeding to step S108, transmits the disc ID read in step S101 to the service providing server, and further, in step S109, receives the service from the service providing server. Note that the service providing server verifies the disc ID received
 15 from the information processing apparatus (user device) 400 in step S108, and executes the service providing processing only if the disc ID has been validated.

[0099]

Below, disc ID verifying processing executed in
 20 step S102 is described. (The disc ID stored on the information recording medium is set as highly counterfeit-resistant identification information.) An example of a disc ID format is shown in Fig. 11.

[0100]

25 Fig. 11 show six types of disc ID setting example each indicating correspondence between an information recording medium ID (disc ID) as an information recording medium identifier, the title-unique value being a unique value set to the title of content stored on the
 30 information recording medium, and the disc-unique value set as a unique value for the information recording

medium. Note that both the disc ID and the disc-unique value are generated by the management apparatus 201. A title-unique value M may be a part of information constituting the content stored on the information recording medium, or may be configured to be generated by the management apparatus 201, the content providing apparatus 203. A title-unique value S is generated by the management apparatus 201 on the basis of the title-unique value M.

10 [0101]

Symbols shown in Fig. 11 have the following meanings:

M: A unique value corresponding to a title of content stored on an information recording medium;

15 w: $w = 1, 2, \dots, W$, where W is the number of information recording media to be manufactured;

Sig(w): Signature data based on a secret key (e.g., a secret key set on the basis of a public-key encryption technique) of the management apparatus, which is generated according to the number W of information recording media to be manufactured and is thus different for each of the information recording media. Sig(w) means that signatures of the discs are set as Sig(1), Sig(2), ..., Sig(W);

25 p(w): Primes set so as to correspond to the number W of information recording media to be manufactured. Different prime data is set for each of the information recording media generated according to the number W of information recording media to be manufactured; and

30 S: A unique value corresponding to a title of content stored on an information recording medium, and S

$= K^T \bmod M$, where T is a value given by the following equation:

[Math 1]

$$T = \prod_{w=1}^W p_w$$

5 [0102]

IDKey(w): IDKey(w) $= K^{T/p(w)} \bmod M$

where K is a value set to each title, and satisfies $K \in Z_M^*$ (K is a generator of a cyclic group $K \in Z_M^*$. Note that for each $X \in Z_M^*$, there exists an element $X^{-1} \in Z_M^*$ modulo x in integers x being 1 to $X-1$).

[0103]

$e(w)$: Different values corresponding to the number W of discs to be manufactured, which satisfy $e(w) \in Z_M^*$, where $e(w)$ and $\lambda(M)$ are disjoint, i.e., the greatest common divisor of $e(w)$ and $\lambda(M)$ is 1. Note that $\lambda(M)$ is the least common multiple of primes $(q_1 - 1)$ and $(q_2 - 1)$, where q_1, q_2 are primes large enough to be applied to an RSA encryption.

[0104]

20 $I(w)$: $I(w) = S^{d(w)} \bmod M$

where $d(w)$ is the inverse of $e(w)$ modulo $\lambda(M)$.

Σw : Data obtained by encrypting a message $M(w)$ being connected data obtained by connecting data S and data $e(w)$, with a secret key of the management apparatus (CA) 201.

[0105]

Below, disc ID verifying processing sequences in the information processing apparatus (user device) 400, are described, which correspond to the six different disc ID setting examples shown in Fig. 11.

30

[0106]

Referring to Fig. 12, a disc ID verifying processing sequence in the information processing apparatus (user device) 400, which corresponds to a

5 Setting Example 1, is described.

In the Setting Example 1,
disc ID = M, Sig(w),
title-unique value = M, and
disc-unique value = Sig(w)

10 are set.

[0107]

In step S201, the controller 408 of the information recording apparatus (user device) 400 extracts signature data Sig(w) in disc ID (w). Note that the disc ID is
15 denoted a disc ID(w) since it takes a value specific to each of individual discs (w) where $w = 1, 2, \dots, W$, given the number of discs to be manufactured being W.

[0108]

In step S202, the controller 408 generates M(w)'
20 from the signature data Sig(w) read in step S201, on the basis of a public key and published parameters of the management apparatus 201 (Central Authority CA). The message is also denoted similarly to the disc ID(w). A message M(w) indicates that the message is made to
25 correspond to each of the discs.

[0109]

In step S203, the controller 408 compares a message M(w) contained in the disc ID(w) with the message M(w)' generated in step S202.

30 [0110]

In step S204, the controller 408, when having

judged that both coincide in the comparing processing in step S203, proceeds to step S205; otherwise, it proceeds to step S206.

[0111]

5 In step S205, the controller 408 judges that the disc ID(w) extracted in step S201 is valid. In step S206, the controller 408 judges that the disc ID(w) extracted in step S201 is invalid.

[0112]

10 In a Setting Example 2,
 disc ID = S, Sig(w),
 title-unique value = S, and
 disc-unique value = Sig(w)
 are set.

15 This Setting Example 2 is different from the Setting Example 1 only in the title-unique value S in place of M. Thus, its disc ID verifying processing sequence in the information processing apparatus (user device) 400 is similar to that in the Setting Example 1,
 20 except that data generated from the signature data in step S202 is a message $S(w)'$ and that data for comparison in step S203 is data $S(w)$ contained in the disc ID.

[0113]

 Referring next to Fig. 13, a disc ID verifying
 25 processing sequence in the information processing apparatus (user device) 400, which corresponds to a Setting Example 3, is described.

 In the Setting Example 3,
 disc ID = $p(w)$, IDKey(w),
 30 title-unique value = S, and
 disc-unique value = $p(w)$ or IDKey(w)

are set.

[0114]

In step S301, the controller 408 of the information processing apparatus (user device) 400 extracts data $p(w)$ in the disc ID(w) read from the information recording medium 200.

[0115]

In step S302, the controller 408 judges whether or not the data $p(w)$ extracted in step S301 is a prime. The controller 408, when having judged that the data $p(w)$ is a prime, proceeds to step S303; otherwise, it proceeds to step S304.

[0116]

In step S303, the controller 408 judges that the disc ID(w) extracted in step S301 is valid. In step S304, the controller 408 judges that the disc ID(w) extracted in step S301 is invalid.

[0117]

Referring next to Fig. 14, a disc ID verifying processing sequence in the information processing apparatus (user device) 400, which corresponds to a Setting Example 4, is described.

In the Setting Example 4,
disc ID = $e(w)$, $I(w)$,
title-unique value = S , and
disc-unique value = $e(w)$ or $I(w)$
are set.

[0118]

In step S401, the information processing apparatus (user device) 400, when having the information recording medium 200 set thereto in a predetermined access position,

reads a disc ID from the information recording medium 200 via the recording medium interface 410, and stores this in the memory 409.

[0119]

5 In step S402, the controller 408 of the information processing apparatus (user device) 400 calculates $I(w)^{e(w)} \bmod M$ using the data $e(w)$ and $I(w)$ in the disc ID recorded in the memory 409, and the result is set as data S' . Namely,

10 $S' = I(w)^{e(w)} \bmod M$

[0120]

 In step S403, the controller 408 reads a Disc ID Revocation List (DIRL) from the information recording medium 200 via the recording medium interface 410. In a case where a digital signature using a public-key encryption technique is put thereto as the tampering verification value for the Revocation List read, the controller 408 verifies the List DIRL using a signature verification key (public key). In a case where a Message Authentication Code MAC is given as the tampering verification value, the MAC verifying processing described earlier with reference to Fig. 3 is executed.

[0121]

 On condition that the Disc ID Revocation List (DIRL) has been judged to be untampered, the controller 408 makes a comparison between a version of that Disc ID Revocation List (DIRL) and a version of a Disc ID Revocation List (DIRL) already stored in the memory 409. In a case where the version of the Disc ID Revocation List (DIRL) read is newer than the version of the Disc ID Revocation List (DIRL) already stored in the memory 409,

the controller 408 updates the Revocation List DIRM in the memory 409 with the Disc ID Revocation List (DIRL) read.

[0122]

5 In step S404, the controller 408 judges whether or not the disc ID read in step S401 is present in the Revocation List, and proceeds to step S405 when having determined that it is present; otherwise it proceeds to step S406.

10 [0123]

 In step S405, the controller 408 stops (prohibits) decryption and playback of the encrypted content recorded in the information recording medium 200. In step S406, the controller 408 transmits the disc ID read in step
15 S401 to the service providing server, and further, in step S407, receives a service from the service providing server. Note that the service providing server verifies the disc ID received from the information processing apparatus (user device) 400 in step S406, and then
20 executes the service providing processing only in a case where the disk ID has been validated.

[0124]

 Referring next to Fig. 15, a disc ID verifying processing sequence in the information processing
25 apparatus (user device) 400, which corresponds to a Setting Example 5, is described.

 In the Setting Example 5,
 disc ID = Σw ,
 title-unique value = S, and
30 disc-unique value = $e(w)$
are set.

[0125]

In step S501, the controller 408 of the information processing apparatus (user device) 400 decrypts a disc ID(w) read from the information recording medium 200 on the basis of public key data of the management apparatus 201 (Central Authority CA), to generate a message M(w). The message M(w) is, as aforementioned, is data in which the data S and the data e(w) are connected.

[0126]

10 In step S502, the information processing apparatus (user device) 400 extracts the data S from the message M(w) decrypted in step S501, on the basis of a size |S|, a size |e(w)|, and a combination pattern of the data S and the data e(w), which are published by the management apparatus 201.

[0127]

The information processing apparatus (user device) 400, subsequent to the above-mentioned processing shown in Fig. 15, performs steps S105-S109 shown in Fig. 10. In this case, the information processing apparatus (user device) 400 uses the disc ID(w) read from the information recording medium 200 in step S501 as a disc ID, in the disc ID comparing processing with the Revocation List in steps S105, S106 shown in Fig. 10.

25 [0128]

The information processing apparatus (user device) 400 decrypts content data, using the data S extracted in step S502 as content key data. Therefore, the content data cannot be decrypted properly in a case where the proper data S cannot be acquired via the above processing of steps S501, S502.

[0129]

In a Setting Example 6,
disc ID = $p(w)$, IDKey(w),
title-unique value = S , and
5 disc-unique value = $p(w)$

are set. This has a disc ID configuration similar to that in the Setting Example 3, and thus disc ID verifying processing similar to the processing described earlier with reference to Fig. 13 is executed.

10 [0130]

[5. Details of processing in service providing server]

Next, processing is described, which the service providing server 300 performs when having received a service providing request from the information processing
15 apparatus (user device) 400.

[0131]

As shown in Fig. 16, the service providing server 300 receives a disc ID from the information processing apparatus (user device) 400. This disc ID is a disc ID
20 the validity of which has been verified through the verifying processing in the information processing apparatus (user device) 400 which, after having attached thereto the information recording medium 200, has executed the processing of reading the disc ID from the
25 information recording medium 200.

[0132]

The service providing server 300, when having received the disc ID along with a service providing request from the information processing apparatus (user
30 device) 400, verifies the validity of the disc ID, and thereafter provides a service on condition that the disc

ID has been validated.

[0133]

Note that the information processing apparatus (user device) 400 transmits a service ID as a service identifier, together with the disc ID, along with the service providing request.

[0134]

The service providing server 300 receives the Disc ID Revocation List from the management apparatus 201, the content providing apparatus 203, or other apparatus via the input/output interface (I/F) 304 shown in Fig. 7, periodically or for each event, and performs processing of storing the latest version in the secure memory 305 constantly. Moreover, the server 300 also receives title-based title-unique values and service identification information for identifying a service which the server 300 provides, from the content providing apparatus 203 or other apparatus via the input/output interface (I/F) 304, and stores the service providing situation database described earlier with reference to Fig. 8, in which title-based service providing situation information is managed, in the secure memory 305.

[0135]

The service providing server 300 stores and holds the service providing situation data shown in Fig. 8 in, e.g., the secure memory 305, and checks, in response to the service providing request accompanied by the disc ID from the information processing apparatus (user device) 400, if the service providing requesting device is making the service providing request based on a valid disc ID, and further, provides the service only in a case where an

upper service providable limit is not reached on the basis of the service providing situation data shown in Fig. 8.

[0136]

5 Referring to Fig. 17, a processing sequence is described, which the service providing server 300 performs when having received a service providing request from the information processing apparatus (user device) 400.

10 [0137]

In step S701, the service providing server 300 receives a service providing request from the information processing apparatus (user device) 400 via the input/output interface (I/F) 304 shown in Fig. 7. This
15 service providing request from the information processing apparatus (user device) 400 includes a disc ID which the information processing apparatus (user device) 400 has acquired from the information recording medium 200, and an identifier for a requested service (service
20 identifier). The disc ID is any of the disc IDs in the Setting Examples 1-6 described earlier with reference to Fig. 11.

[0138]

In step S702, the service providing server 300
25 executes processing of verifying the disc ID received. This verifying processing is performed according to a verification sequence similar to that for the verifying processing executed in the information processing
apparatus (user device) 400, i.e., a verification
30 sequence according to any of the Disc ID Setting Examples 1-6 described with reference to FIGS. 12-15.

[0139]

When the disc ID is validated by the disc ID verifying processing in step S703, the process proceeds to step S705. When the disc ID is judged to be invalid, 5 the process proceeds to step S704, to stop providing the service. Note that for this stopping processing, a message saying that the service providing processing is stopped may be transmitted to the information processing apparatus (user device) 400.

10 [0140]

In a case where the disc ID is validated and the process proceeds to step S705, the server 300 reads the Disc ID Revocation List (DIRL) stored in the secure memory 305 (see Fig. 7).

15 [0141]

In step S706, the server 300 judges whether or not the received disc ID which has been validated is recorded in the Revocation List.

[0142]

20 In a case where the received disc ID is recorded in the Revocation List, the server 300 judges that the disc ID is invalid, and the process proceeds to step S711, to stop the service providing processing. Note that for this stopping processing, a message saying that the 25 service providing processing is stopped may be transmitted to the information processing apparatus (user device) 400.

[0143]

30 In a case where the disc ID received is not recorded in the Revocation List, then, in step S707, the server 300 calculates the title-unique value on the basis

of the disc ID. The disc ID is configured as data containing the title-unique value M or S or data from which the title-unique value M or S is calculable, which has been described earlier with reference to Fig. 11.

5 The service providing server 300 acquires the title-unique value M or S contained in the disc ID received, or calculates the title-unique value M or S from the disc ID received by calculating processing performed by the calculation unit 303. This processing of acquiring,
10 calculating the title-unique value M or S is executed as processing which differs according to the Setting Examples 1-6 described earlier with reference to Fig. 11.
[0144]

In step S707, the server further acquires service
15 providing situation data corresponding to the title from the database, on the basis of the title-unique value M or S acquired from the disc ID. Namely, this is the service providing situation data described with reference to Fig. 8, and data in which various service providing situations
20 corresponding to disc IDs are set.
[0145]

In step S707, the server 300 extracts data corresponding to the disc ID and the service identifier received from the information processing apparatus (user
25 device) 400, from the service providing situation data, and checks whether or not the service is providable.
[0146]

Let a description be given therefor using the service providing situation data shown in Fig. 8 as an
30 example. For example, in a case where the disc ID received from the information processing apparatus (user

device) 400 is (Disc ID 1), and the service identifier is (Service 1), it is judged that the service is providable, since an upper limit is set to one time for the Service 1, and its service providing situation indicates

5 "unprovided".

[0147]

When having judged in step S708 that the service is providable on the basis of the service providing situation data, the process proceeds to step S709, whereas when having judged in step S708 that the service is unprovidable on the basis of the service providing situation data, the process proceeds to step S711.

[0148]

In step S711, the server 300 stops its service providing processing. Note that for this stopping processing, a message saying that the service providing processing is stopped may be transmitted to the information processing apparatus (user device) 400.

[0149]

20 If having judged that the service is providable on the basis of the service providing situation data, the server updates the database in step S709.

[0150]

Let a description be given therefor again using the service providing situation data shown in Fig. 8 as an example. For example, in a case where the disc ID received from the information processing apparatus (user device) 400 is (Disc ID 1), and the service identifier is (Service 1), the service providing situation which is "unprovided" is changed to "provided one time".

30 [0151]

In step S710, the service providing server 300 executes its service providing processing to the information processing apparatus (user device) 400 having transmitted the service providing request.

5 [0152]

For example, when content stored in the disc is a foreign movie, various content-related services including subtitles or dubbing data for its audio, or a disc purchasing discount ticket for a sequel of the content, are provided to the information processing apparatus (user device) 400 from the service providing server 300 via a network.

[0153]

Note that communication between the information processing apparatus (user device) 400 and the service providing server 300 is preferably implemented by establishing a secured communication channel where mutual authentication using cryptography is provided and a session key is shared.

20 [0154]

Moreover, the server 300 checks the Disc ID Revocation List (DIRL) in steps S705, S706 every time a service providing request is received in the above-mentioned example. However, it may be configured such that the Disc ID Revocation List is periodically checked beforehand to keep the database updated for any disc ID listed there so as to stop providing the service involving that disc ID any more. In such a configuration, the checking of the Disc ID Revocation List (DIRL) at the time when a service providing request is received can be omitted, to reduce the time for providing a service.

[0155]

Furthermore, the disc ID has been described as differing from one disc to another . However, the disc ID may be common to a unit of, e.g., 10 discs, 100 discs, 5 or 1,000 discs, and the service providing limit set for a single disc ID may be determined in consideration of the number of discs in a group.

[0156]

The present invention has been described above in great detail with reference to the specific embodiment. 10 However, it is self-explanatory that those skilled in the art can make modifications to and substitutions for the embodiment without departing from the scope and spirit of the present invention. That is, the present invention 15 has been disclosed by way of examples, and thus should not be construed in a restrictive sense. In order to judge the scope and spirit of the present invention, the claims set forth at the beginning should be taken into consideration.

20 [0157]

Note that the series of processes described in the specification can be performed by hardware, software, or a configuration in which both are combined. In a case where a process based on software is executed, the 25 processes could be executed by installing a program having recorded processing sequences therein in a memory within a computer incorporated into dedicated hardware, or by installing the program in a general-purpose computer that can execute various processing.

30 [0158]

For example, the program can be recorded on a hard disk or a ROM (Read Only Memory) as a recording medium beforehand. Alternatively, the program can be stored (recorded) temporarily or permanently in a removable recording medium, such as a flexible disk, a CD-ROM (Compact Disc Read Only Memory), a MO (Magneto Optical) disk, a DVD (Digital Versatile Disc), a magnetic disk, a semiconductor memory. Such a removable recording medium can be provided as so-called package software.

10 [0159]

Note that the program can be installed in a computer not only from a removable recording medium such as those mentioned above, but also through wireless transfer to the computer from a downloading site, wired transfer to the computer via a network such as a LAN, the Internet to allow the computer to receive the thus transferred program for installation in a storage medium such as a hard disk incorporated therein.

[0160]

20 Note that the various processes described in the specification are executed not only time-sequentially according to the description, but may also be executed parallelly or individually, according to the processing capability of apparatus assigned to execute the processes or as necessary. In addition, the system used in the present specification means a logical set configuration of a plurality of apparatus, and is not limited to one wherein apparatus each having its own configuration are grouped within the same enclosure.

30 [Industrial Applicability]

[0161]

As described in the foregoing, according to the configuration of the present invention, in a configuration in which content is provided as stored in various information recording media including a DVD, a CD, a blue laser recording medium, and in which service providing processing is performed from a networked service providing server, the service providing server verifies an information recording medium ID transmitted thereto from an information processing apparatus (user device), and provides a service based on service providing situation data for each of the information recording medium IDs. Therefore, only in a case where the information processing apparatus having transmitted a service request is one having read a valid information recording medium ID from an information recording medium, and it has been validated that the service is providable on the basis of the service providing situation data, the providing of the service is executed. Thus, the configuration of the present invention allows various service information corresponding to content to be provided after strictly examining a service receiver and checking his/her having an authorized right, in, e.g., a system in which the service information corresponding to content, such as various content-associated services including subtitles or dubbing data when the content stored on a disc is a foreign movie, is provided from a server.

[0162]

Furthermore, according to the configuration of the present invention, the information recording medium ID stored on the information recording medium includes data

through which its validity can be checked, such as signature data of a management apparatus, and also either has a title-unique value or includes data from which the title-unique value is calculable. Therefore, the service providing server can check the validity based on the data included in the information recording medium ID, and additionally can acquire the title-unique value, whereby the server can specify service providing situation data set so as to correspond to the title-unique value.

5

10 Therefore, various service information corresponding to content can be provided after strictly examining a service receiver and checking his/her having an authorized right.

Claims

1. A service providing server for executing service providing processing in response to a service providing request from an information processing apparatus,

5 characterized by having:

a data reception section which receives a service request accompanied by an information recording medium ID and a service ID, from the information processing apparatus;

10 a storage section which stores service providing situation data for each of the information recording medium IDs as service management data for each of title-unique values corresponding to titles of content stored on information recording media; and

15 a data processing section which executes processing of verifying the information recording medium ID and signature data contained in the information recording medium ID received via the data reception section, acquires a title-unique value on the basis of the information recording medium ID on condition that the information recording medium ID and the
20 signature data are validated, acquires from the storage section service providing situation data corresponding to the title-unique value contained in the information recording medium ID or the title-unique value calculated by executing a calculation based on data contained in the information
25 recording medium ID to judge whether or not a service specified by the information recording medium ID and the service ID is providable, and executes the service providing processing on condition that the service is judged to be providable.

2. The service providing server according to Claim 1, characterized in that:

the service providing server has the storage section which stores a revocation list being a list of unauthorized information recording medium IDs; and

the processing of verifying the information recording medium ID in the data processing section is executed as processing of comparing the information recording medium ID received from the information processing apparatus with the IDs recorded in the revocation list.

3. The service providing server according to Claim 1, characterized in that:

the information recording medium ID is configured to include a title-unique value corresponding to a title of content stored in an information recording medium, and signature data generated on the basis of a secret key of a management apparatus and differing for each of the information recording media; and

the data processing section is configured to execute the processing of verifying the information recording medium ID as processing of generating a message to which a public key of the management apparatus is applied, for comparison with the signature data contained

in the information recording medium ID, and also execute the processing of acquiring the service providing situation data corresponding to the title-unique value contained in the information recording medium ID, from the storage section.

5

4. The service providing server according to Claim 1, characterized in that:

the information recording medium ID includes:

10 a prime $p(w)$ set in response to each of a number W of information recording media manufactured; and

data IDKey(w) calculated by a calculation based on the prime $p(w)$ and the title-unique value; and

15 the data processing section is configured to execute processing of judging whether or not data contained in the information recording medium ID is the prime, as the ID verifying processing, and also calculate the title-unique value from the data IDKey(w) contained in the information recording medium ID, and acquiring the service providing situation data corresponding to the title-unique value
20 calculated, from the storage section.

5. An information processing apparatus for executing a service providing request to a service providing server, characterized by having:

25 a recording medium interface which executes processing of accessing an information recording medium; and

a data processing section which executes processing of verifying an information recording medium ID and signature data contained in the information recording medium ID read
30 from the information recording medium via the recording medium interface, and executes processing of transmitting the information recording medium ID and the signature data to the service providing

server on condition that the information recording medium ID and the signature data are validated,

characterized in that the data processing section is configured to execute the processing of verifying the
5 information recording medium ID as processing of verifying the signature data contained in the information recording medium ID, and execute the processing of acquiring, from the storage section, the service providing situation data corresponding to the title-unique value, according to the title-unique value
10 contained in the information recording medium ID, or the title-unique value calculated by executing a calculation based on data contained in the information recording medium ID.

6. The information processing apparatus according to Claim
15 5, characterized in that:

the processing of verifying the information recording medium ID in the data processing section is configured as processing of acquiring a revocation list being a list of unauthorized information recording medium IDs from a storage
20 section or the information recording medium, and comparing the information recording medium ID received from the information processing apparatus with the IDs recorded in the revocation list acquired.

25 7. The information processing apparatus according to Claim 5, characterized in that:

the information recording medium ID includes a title-unique value corresponding to a title of content stored on the information recording medium, and signature data generated on
30 the basis of a secret key of a management apparatus and differing for each of the information recording media; and

the data processing section is configured to execute the processing of verifying the information recording medium ID as

processing of generating a message to which a public key of the management apparatus is applied, for comparison with the signature data contained

in the information recording medium ID.

8. The information processing apparatus according to Claim 5, characterized in that:

5 the information recording medium ID includes:

a prime $p(w)$ set in response to each of a number W of information recording media manufactured; and

data $IDKey(w)$ calculated by a calculation based on the prime $p(w)$ and a title-unique value; and

10 the data processing section is configured to execute processing of judging whether or not data contained in the information recording medium ID is the prime, as the ID verifying processing.

15 9. A data processing method for executing service providing processing in response to a service providing request from an information processing apparatus, characterized by having:

a data reception step of receiving a service request accompanied by an information recording medium ID and a

20 service ID, from the information processing apparatus; and

a data processing step of executing processing of verifying the information recording medium ID and signature data contained in the information recording medium ID received, acquiring a title-unique value on the basis of the information recording medium ID and signature data on condition that the information recording medium ID and signature data are validated, acquiring service providing situation from a storage section for storing situations data corresponding to the title-unique value contained in the information recording medium ID or the title-unique value calculated by executing a calculation based on data contained in the information recording medium ID acquired, for each of the information recording medium IDs as service management data for each of

25

30

title-unique values contained in the information recording medium ID or the title-unique value calculated by executing a calculation based on data contained in the information recording medium ID stored on information recording media,

judging whether or not a service specified by the information recording medium ID and the service ID is providable, and executing the service providing processing on condition that the service is judged to be providable.

5

10. The data processing method according to Claim 9, characterized in that:

the processing of verifying the information recording medium ID in the data processing step is configured to include
10 a step of executing it as processing of comparing the information recording medium ID received from the information processing apparatus with IDs recorded in a revocation list being a list of unauthorized information recording medium IDs.

15 11. The data processing method according to Claim 9, characterized in that:

the information recording medium ID is configured

to include a title-unique value corresponding to a title of content stored on the information recording medium, and signature data generated on the basis of a secret key of a management apparatus and differing for each of the information recording media; and

the data processing step is configured to include a step of executing the processing of verifying the information recording medium ID as processing of generating a message to which a public key of the management apparatus is applied, for comparison with the signature data contained in the information recording medium ID, and also executing the processing of acquiring the service providing situation data corresponding to the title-unique value contained in the information recording medium ID, from the storage section.

12. The data processing method according to Claim 9, characterized in that:

the information recording medium ID includes:

a prime $p(w)$ set in response to each of a number W of information recording media manufactured; and

data $IDKey(w)$ calculated by a calculation based on the prime $p(w)$ and the title-unique value; and

the data processing step is configured to include a step of executing processing of judging whether or not data contained in the information recording medium ID is the prime as the ID verifying processing, and also calculating the title-unique value from the data $IDKey(w)$ contained in the information recording medium ID, and acquiring the service providing situation data corresponding to the title-unique value calculated, from the storage section.

13. A data processing method for executing a service providing request to a service providing server, characterized by having:

a recording medium accessing step of executing processing of accessing an information recording medium via a recording medium interface; and

a data processing step of executing processing of verifying an information recording medium ID read from the information recording medium and signature data that are received via the recording medium interface, and executing processing of transmitting the information recording medium ID to the service providing server on condition that the information recording medium ID and signature data are validated,

characterized in that the data processing step is configured to execute the processing of verifying the information recording medium ID as processing of verifying the signature data contained in the information recording medium ID, and execute the processing of acquiring, from the storage section, the service providing situation data corresponding to the title-unique value, according to the title-unique value contained in the information recording medium ID, or the title-unique value calculated by executing a calculation based on data contained in the information recording medium ID.

14. The data processing method according to Claim 13, characterized in that:

the processing of verifying the information recording medium ID in the data processing step is configured to include a step of acquiring a revocation list being a list of unauthorized information recording medium IDs from a storage section or the information recording medium, and comparing the information recording medium ID received from the information

processing apparatus with the IDs recorded in the revocation list acquired.

15. The data processing method according to Claim 13,

characterized in that:

the information recording medium ID is configured to include a title-unique value corresponding to a title of content stored on the information recording medium, and
5 signature data generated on the basis of a secret key of a management apparatus and differing for each of the information recording media; and

the data processing step is configured to include a step of executing the processing of verifying the information
10 recording medium ID as processing of generating a message to which a public key of the management apparatus is applied, for comparison with the signature data contained in the information recording medium ID.

15 16. The data processing method according to Claim 13, characterized in that:

the information recording medium ID includes:

a prime $p(w)$ set in response to each of a number W of information recording media manufactured; and

20 data IDKey(w) calculated by a calculation based on the prime $p(w)$ and a title-unique value; and

the data processing step is configured to include a step of executing processing of judging whether or not data contained in the information recording medium ID is the prime,
25 as the ID verifying processing.

17. A computer program for executing processing in response to a service providing request from an information processing apparatus, characterized by having:

30 a data reception step of receiving a service request accompanied by an information recording medium ID

and a service ID, from the information processing apparatus;
and

5 a data processing step of executing processing of
verifying the information recording medium ID and signature
data contained in the information recording medium ID received,
acquiring a title-unique value on the basis of the information
recording medium ID and signature data on condition that the
information recording medium ID and signature data are
validated, acquiring service providing situation data from a
10 storage section for storing service providing situation data
corresponding to the title-unique value contained in the
information recording medium ID or the title-unique value
calculated by executing a calculation based on data contained
in the information recording medium ID , for each of the
15 information recording medium IDs as service management data
for each of title-unique values contained in the information
recording medium ID or the title-unique value calculated by
executing a calculation based on data contained in the
information recording medium ID stored on information
20 recording media, judging whether or not a service specified by
the information recording medium ID and the service ID is
providable, and executing the service providing processing on
condition that the service is judged to be providable.

25 18. A computer program for executing a service providing
request to a service providing server, characterized by
having:

a recording medium accessing step of executing
processing of accessing an information recording medium via a
30 recording medium interface; and

a data processing step of executing processing of
verifying an information recording medium ID and signature
data contained in the information recording medium ID read

from the information recording medium via the recording medium interface, and executing processing of transmitting the information recording medium ID and signature data to the service providing server on condition that the information

5 recording medium ID and signature data are validated,

characterized in that the data processing step is configured to execute the processing of verifying the information recording medium ID as processing of verifying the signature data contained in the information recording medium

10 ID, and execute the processing of acquiring, from the storage section, the service providing situation data corresponding to the title-unique value, according to the title-unique value contained in the information recording medium ID, or the title-unique value calculated by executing a calculation based
15 on data contained in the information recording medium ID.