(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 045 321 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
18.10.2000 Bulletin 2000/42

(51) Int. Cl.[7]: **G06F 17/60**

(21) Application number: **00303049.1**

(22) Date of filing: **11.04.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **12.04.1999 JP 10399199**

(71) Applicant: **Sony Corporation**
Tokyo 141 (JP)

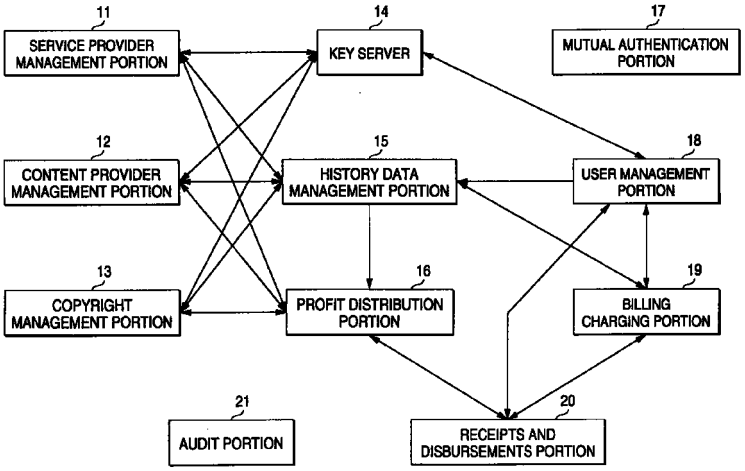
(72) Inventors:
- **Matsuyama, Shinako,**
  c/o Sony Corporation
  Tokyo (JP)
- **Ishibashi, Yoshihito,**
  c/o Sony Corporation
  Tokyo (JP)

(74) Representative:
Robinson, Nigel Alexander Julian
D. Young & Co.,
21 New Fetter Lane
London EC4A 1DA (GB)

(54) Information processing apparatus and method, management apparatus and method, and providing medium

(57) Marketing information can be provided. Fig. 60 shows singers of contents (music) purchased in a predetermined period in decreasing order of purchase count. Such marketing information can be provided to the user, content provider, and service provider.

FIG. 3



EP 1 045 321 A2

Description

[0001] The present invention relates to an information processing apparatus and method, a management apparatus and method, and a providing medium. Particularly, the invention relates to an information processing apparatus and method for decrypting encrypted information, a management apparatus and method, and a providing medium.

[0002] There is a system in which information (hereinafter referred to as "contents") such as music is encrypted, and is transmitted to an information processing apparatus of a user who has made a designated contract, and the user decrypts the contents by the information processing apparatus.

[0003] Naturally, in this system, predetermined billing is caused from the use (purchase) of contents, and the user must settle it. In general, at this time, billing information is transmitted to a management apparatus for managing this system, and the billing is settled through the billing information.

[0004] Although this billing information includes information to specify the purchased contents, and information as to the user as a purchaser, there has been a problem that these pieces of information are not effectively used.

[0005] The present invention has been made in view of these circumstances, and an object of the invention is to enable information included in billing information to be effectively used.

[0006] According to an aspect of the invention, an information processing apparatus comprises preparation means for preparing billing information needed to settle billing of valuable information and including its own ID, transmission means for transmitting the billing information prepared by the preparation means to a management apparatus, and reception means for receiving predetermined marketing information corresponding to a settlement result based on the billing information transmitted by the transmission means and transmitted from the management apparatus.

[0007] According to another aspect of the invention, an information processing method comprises a preparation step of preparing billing information needed to settle billing of valuable information and including its own ID, a transmission step of transmitting the billing information prepared in the preparation step to a management apparatus, and a reception step of receiving predetermined marketing information corresponding to a settlement result based on the billing information transmitted in the transmission step and transmitted from the management apparatus.

[0008] According to a further aspect of the invention, a providing medium provides a computer readable program for making a computer execute a process comprising a preparation step of preparing billing information needed to settle billing of valuable information and including its own ID, a transmission step of transmitting the billing information prepared in the preparation step to a management apparatus, and a reception step of receiving predetermined marketing information corresponding to a settlement result based on the billing information transmitted in the transmission step and transmitted from the management apparatus.

[0009] In the information processing apparatus of the aspect, the information processing method of the second aspect, and the providing medium of the third aspect, billing information needed to settle billing of valuable information and including its own ID is prepared, the prepared billing information is transmitted to a management apparatus, and predetermined marketing information corresponding to a settlement result based on the transmitted billing information and transmitted from the management apparatus is received.

[0010] According to yet further aspect of the invention, a management apparatus comprises storage means for storing predetermined marketing information as to an information processing apparatus correspondingly to ID of the information processing apparatus, settlement means for receiving billing information transmitted from the information processing apparatus and including the ID of the information processing apparatus and for settling billing due to valuable information on the basis of the billing information, readout means for reading the marketing information as to the information processing apparatus stored in the storage means correspondingly to the ID of the information processing apparatus included in the billing information, and first exhibiting means for exhibiting the marketing information read out by the readout means to the information processing apparatus correspondingly to a settlement result by the settlement means.

[0011] According to another aspect of the invention, a management method comprises a storage step of storing predetermined marketing information as to an information processing apparatus correspondingly to ID of the information processing apparatus, a settlement step of receiving billing information transmitted from the information processing apparatus and including the ID of the information processing apparatus and of settling billing due to valuable information on the basis of the billing information, a readout step of reading the marketing information as to the information processing apparatus stored in the storage step correspondingly to the ID of the information processing apparatus included in the billing information, and a first exhibiting step of exhibiting the marketing information read out in the readout step to the information processing apparatus correspondingly to a settlement result in the settlement step.

[0012] According to another aspect of the invention, a providing medium provides a computer readable program for making a computer execute a process comprising a storage step of storing predetermined marketing information as to an information processing apparatus correspondingly to ID of the information processing apparatus, a settlement step of receiving

billing information transmitted from the information processing apparatus and including the ID of the information processing apparatus and of settling billing due to valuable information on the basis of the billing information, a readout step of reading the marketing information as to the information processing apparatus stored in the storage step correspondingly to the ID of the information processing apparatus included in the billing information, and a first exhibiting step of exhibiting the marketing information read out in the readout step to the information processing apparatus correspondingly to a settlement result in the settlement step.

[0013] In the management apparatus of the fourth aspect, the management method of the sixth aspect, and the providing medium of the eighth aspect, predetermined marketing information as to an information processing apparatus is stored correspondingly to ID of the information processing apparatus, billing information transmitted from the information processing apparatus and including the ID of the information processing apparatus is received, billing due to valuable information is settled on the basis of the billing information, the marketing information as to the information processing apparatus stored correspondingly to the ID of the information processing apparatus included in the billing information is read out, and the marketing information read out is exhibited to the information processing apparatus correspondingly to a settlement result.

[0014] Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings in which:

Fig. 1 is a view for explaining an EMD system.
Fig. 2 is a view for explaining the flow of main information in the EMD system.
Fig. 3 is a block diagram showing a functional structure of an EMD service center 1.
Fig. 4 is a view for explaining transmission of a delivery key Kd of the EMD service center 1.
Fig. 5 is another view for explaining transmission of a delivery key Kd of the EMD service center 1.
Fig. 6 is another view for explaining transmission of a delivery key Kd of the EMD service center 1.
Fig. 7 is another view for explaining transmission of a delivery key Kd of the EMD service center 1.
Fig. 8 is another view for explaining transmission of a delivery key Kd of the EMD service center 1.
Fig. 9 is a view for explaining system register information.
Fig. 10 is a view for explaining use point information.
Fig. 11 is a block diagram showing an example of a functional structure of a content provider 2.
Figs. 12A and 12B are views respectively showing an example of UCP.
Figs. 13A and 13B are views for explaining management movement of contents.
Figs. 14A and 14B are views for explaining first generation copying.
Figs. 15A and 15B are views showing examples of code values of a service code and a condition code.
Figs. 16A and 16B are views showing examples of code values set as use conditions of UCP.
Fig. 17 is a view showing an example of content provider secure container.
Fig. 18 is a view showing an example of a certificate of a content provider 2.
Fig. 19 is a block diagram showing a functional structure of a service provider 3.
Figs. 20A and 20B are views showing examples of PT.
Figs. 21A and 21B are views showing examples of code values set as price conditions of PT.
Figs. 22A and 22B are views showing other examples of PT.
Figs. 23A and 23B are views showing examples of code values set as price conditions of other PT.
Fig. 24 is a view showing an example of service provider secure container.
Fig. 25 is a view showing a certificate of a service provider 3.
Fig. 26 is a block diagram showing an example of a functional structure of a receiver 51 of a user home network 5.
Fig. 27 is a view showing an example of a certificate of SAM 62 of the receiver 51.
Fig. 28 is a view showing an example of UCS.
Fig. 29 is a view for explaining the inside of a use information storage portion 63A of an external storage portion 63 of the receiver 51.
Fig. 30 is a view showing an example of billing information.
Fig. 31 is a view showing information stored in a storage module 73 of the receiver 51.
Fig. 32 is a view for explaining reference information 51.
Fig. 33 is a view showing an example of use point information of the reference information 51.
Fig. 34 is a view showing an example of a register list.
Fig. 35 is a block diagram showing an example of a functional structure of a receiver 201 of the user home network 5.
Fig. 36 is a view showing an example of information stored in a storage module 223 of the receiver 201.
Fig. 37 is a view showing an example of reference information 201.
Fig. 38 is a flowchart for explaining use processing of contents.
Fig. 39 is a flowchart for explaining processing for transmitting the delivery key Kd to the content provider 2 by the EMD service center 1.
Fig. 40 is a flowchart for explaining an operation of mutual authentication between the content provider 2 and the EMD service center 1.
Fig. 41 is a flowchart for explaining another opera-

tion of mutual authentication between the content provider 2 and the EMD service center 1.

Fig. 42 is a flowchart for explaining another operation of mutual authentication between the content provider 2 and the EMD service center 1.

Fig. 43 is a flowchart for explaining processing in which the content provider 2 transmits the content provider secure container to the service provider 3.

Fig. 44 is a flowchart for explaining processing in which the service provider 3 transmits the service provider secure container to the receiver 51.

Fig. 45 is a flowchart for explaining processing in which the receiver 51 receives the service provider secure container.

Fig. 46 is a flowchart for explaining processing in which the receiver 51 reproduces contents.

Fig. 47 is a flowchart for explaining processing in which the receiver 201 is registered with the user A as a settlement user.

Fig. 48 is a view showing an example of a registration form.

Fig. 49 is a view showing another example of information stored in a storage module 223 of the receiver 201.

Fig. 50 is a view showing another example of the reference information 201.

Fig. 51 is a view showing another example of information stored in a storage module 223 of the receiver 201.

Fig. 52 is a view showing another example of the reference information 201.

Fig. 53 is another flowchart for explaining processing in which the receiver 201 is registered with the user A as a settlement user.

Fig. 54 is a view showing another example of the system register information.

Fig. 55 is a flowchart for explaining registration processing through credit investigation.

Fig. 56 is a view showing another example of the system registration information.

Fig. 57 is a view showing another example of the system registration information.

Fig. 58 is a flowchart for explaining settlement processing.

Fig. 59 is a view showing an example of marketing information.

Fig. 60 is a view showing an example of summed up information.

Fig. 61 is a view showing another example of summed up information.

Fig. 62 is a view showing another example of summed up information.

Fig. 63 is a view showing another example of summed up information.

Fig. 64 is a view showing another example of summed up information.

[0015] Embodiments of the invention will be described below. In order to clarify the correspondence between respective means recited in the claims and the following examples, the features of the invention are set forth in the following while corresponding examples (however, each of them is merely one example) are respectively added in a parenthesis after the respective means. Of course, this recitation is not intended to limit the means to what is set forth.

[0016] Fig. 1 is a view for explaining an EMD (Electronic Music Distribution) system to which the invention is applied. The EMD system is constituted by an EMD service center 1 for managing registration to the EMD system and for managing respective devices, a content provider 2 for providing contents, a service provider 3 for providing predetermined service corresponding to the contents, and a user home network 5 made of equipment in which the contents are used.

[0017] The content distributed (provided) to the equipment (user) registered in the EMD system is digital data in which information itself has a value, and in the case of this example, one content corresponds to music data of a piece of music. The content is provided to the user while one content is made one unit (single) or a plurality of contents are made one unit (album). The user purchases the content (actually purchases the right to use the content) and uses the provided content.

[0018] As shown in Fig. 2 showing the flow of main information in the EMD system, the EMD service center 1 transmits a distribution key Kd needed to use the contents to the user home network 5 and a plurality of content providers 2 (in the case of this example, two content providers 2-1, 2-2 (hereinafter, in the case where it is not necessary to distinguish the content providers 2-1, 2-2 from each other, the recitation of the content provider 2 is merely made. The same can be said of other devices)). The EMD service center 1 also receives billing information or the like from the equipment of the user home network 5 and settles the fee, receives a UCP from the content provider 2, and receives a PT from the service provider 3.

[0019] The content providers 2-1 and 2-2 hold contents (encrypted by a content key Kco) to be provided, the content key Kco (encrypted by a delivery key Kd) needed to decrypt the contents, and a treatment policy (hereinafter referred to as UCP (Usage Control Policy)) indicating the usage content of the contents or the like, and supply them as a mode called a content provider secure container (described later) to the service provider 3. In the case of this example, it is assumed that there are two service providers 3-1 and 3-2.

[0020] The service providers 3-1 and 3-2 prepare one or plural price information (hereinafter referred to as PT (Price Tag)) corresponding to the UCP supplied from the content provider 2, and hold it. The service provider 3 transmits the prepared PT, together with the contents (encrypted by the content key Kco) supplied from the content provider 2, the content key Kco (encrypted by the delivery key Kd), and the UCP, in a mode called a

service provider secure container, to the user home network 5 through a network 4 constituted by a dedicated cable network, Internet, satellite communication, or the like.

[0021] The user home network 5 prepares usage permissible condition information (hereinafter referred to as UCS (Usage Control Status)) based on the supplied UCP and PT, and executes processing to use the contents based on the prepared UCS. Besides, the user home network 5 prepares billing information at the timing of preparing the UCS, and transmits it, together with the corresponding UCP and PT, to the EMD service center 1 at the timing of, for example, receiving the supply of the delivery key Kd. Incidentally, the user home network 5 can be made not to transmit the UCP and PT to the EMD service center 1.

[0022] In the case of this example, as shown in Fig. 1, the user home network 5 is constituted by a receiver 51 connected to a HDD 52 and including a SAM 62, and a receiver 201 connected to a HDD 202 and including a SAM 212. It is assumed that although the receiver 51 is formally registered in the EMD system, the receiver 201 is not registered in the EMD system at the moment. (SAM (Secure Application Module) is a module which executes, for example, right processing of content, authentication processing, and the like in a content distribution system and has tamper resistance.)

[0023] Fig. 3 is a block diagram showing a functional structure of the EMD service center 1. A service provider management portion 11 supplies information of profit distribution to the service provider 3. A content provider management portion 12 transmits the delivery key Kd to the content provider 2, or supplies information of profit distribution.

[0024] A copyright management portion 13 transmits information indicating the actual results of use of contents in the user home network 5 to an association for managing the copyright, for example, JASRAC (Japanese Society for Rights of Authors, Composers and Publishers).

[0025] A key server 14 stores the delivery key Kd, and supplies it to the content provider 2 through the content provider management portion 12, or supplies it to the user home network 5 through a user management portion 18 or the like.

[0026] The equipment (for example, receiver 51) of the user home network 5 formally registered in the EMD system, and the delivery key Kd supplied to the content provider 2 from the EMD service center 1 will be described with reference to Figs. 4 to 7.

[0027] Fig. 4 is a view showing a delivery key Kd which the EMD service center 1 includes, a delivery key Kd which the content provider 2 includes, and a delivery key Kd which the receiver 51 includes, on January 1998 when the content provider 2 starts to provide the contents and the receiver 51 (Fig. 26) constituting the user home network 5 starts to use the contents.

[0028] In an example of Fig. 4, a delivery key Kd is usable from the first day of a month of a calendar to the last day of the month, and for example, a delivery key Kd of version 1 having a value of "aaaaaaaa" of a random number of a predetermined bit number is usable from January 1, 1998 to January 31, 1998 (that is, a content key Kco for encrypting the contents distributed to the user home network 5 through the service provider 3 from January 1, 1998 to January 31, 1998 is encrypted by the delivery key Kd of the version 1), a delivery key Kd of version 2 having a value of "bbbbbbbb" of a random number of a predetermined bit number is usable from February 1, 1998 to February 28, 1998 (that is, a contents key Kco for encrypting the contents distributed to the user home network 5 through the service provider 3 during the period is encrypted by the delivery key Kd of the version 2). Similarly, a delivery key Kd of version 3 is usable in March, 1998, a delivery key Kd of version 4 is usable in April, 1998, a delivery key Kd of version 5 is usable in May, 1998, and a delivery key Kd of version 6 is usable in June, 1998.

[0029] Before the content provider 2 starts to provide the contents, the EMD service center 1 transmits the six delivery keys Kd of the version 1 to the version 6 usable from January, 1998 to June, 1998 to the content provider 2, and the content provider 2 receives and stores the six delivery keys Kd. The reason why the delivery keys Kd for six months are stored is that it is necessary to take a predetermined period for the content provider 2 to make preparation such as encrypting of contents and the content key prior to providing the contents.

[0030] Before the receiver 51 starts to use the contents, the EMD service center 1 transmits the three delivery keys Kd of the version 1 to the version 3 usable from January, 1998 to March, 1998 to the receiver 51, and the receiver 51 receives and stores the three delivery keys Kd. The delivery keys Kd for three months are stored in order to avoid such a situation that the contents can not be used, in spite of the period of a contract when the contents can be used, because of such a trouble that connection to the EMD service center 1 can not be made, and in order to reduce the load of the user home network 5 by lowering the frequency in connection to the EMD service center 1.

[0031] In the period from January 1, 1998 to January 31, 1998, the delivery key Kd of the version 1 is used in the EMD service center 1, the content provider 2, and the receiver 51 constituting the user home network 5.

[0032] The transmission of the delivery key Kd by the EMD service center 1 to the content provider 2 and the receiver 51 on February 1, 1998 will be described with reference to Fig. 5. The EMD service center 1 transmits six delivery keys Kd of the version 2 to version 7 usable from February, 1998 to July, 1998 to the content provider 2. The content provider 2 receives the six delivery keys Kd, overwrites delivery keys Kd stored before the reception, and stores the new delivery keys

Kd. The EMD service center 1 transmits three delivery keys Kd of the version 2 to version 4 usable from February, 1998 to April, 1998 to the receiver 51. The receiver 51 receives the three delivery keys Kd, overwrites delivery keys Kd stored before the reception, and stores the new delivery keys Kd. The EMD service center 1 stores the delivery key Kd of the version 1 as it is. This is for enabling the delivery key Kd used in the past to be used when an unexpected trouble occurs, or a dishonest act occurs or is found.

[0033] In the period from February 1, 1998 to February 28, 1998, the delivery key Kd of the version 2 is used in the EMD service center 1, the content provider 2, and the receiver 51 constituting the user home network 5.

[0034] The transmission of the delivery key Kd by the EMD service center 1 to the content provider 2 and the receiver 51 on March 1, 1998 will be described with reference to Fig. 6. The EMD service center 1 transmits six delivery keys Kd of the version 3 to version 8 usable from March, 1998 to August, 1998 to the content provider 2. The content provider 2 receives the six delivery keys Kd, overwrites delivery keys Kd stored before the reception, and stores the new delivery keys Kd. The EMD service center 1 transmits three delivery keys Kd of the version 3 to version 5 usable from March, 1998 to May, 1998 to the receiver 51. The receiver 51 receives the three delivery keys Kd, overwrites delivery keys Kd stored before the reception, and stores the new delivery key Kd. The EMD service center 1 stores the delivery key Kd of the version 1 and the delivery key Kd of the version 2 as they are.

[0035] In the period from March 1, 1998 to March 31, 1998, the delivery key Kd of the version 3 is used in the EMD service center 1, the content provider 2, and the receiver 51 constituting the user home network 5.

[0036] The transmission of the delivery key Kd by the EMD service center 1 to the content provider 2 and the receiver 51 on April 1, 1998 will be described with reference to Fig. 7. The EMD service center 1 transmits six delivery keys Kd of the version 4 to version 9 usable from April, 1998 to September, 1998 to the content provider 2. The content provider 2 receives the six delivery keys Kd, overwrites delivery keys Kd stored before the reception, and stores the new delivery keys Kd. The EMD service center 1 transmits three delivery keys Kd of the version 3 to version 5 usable from April, 1998 to June, 1998 to the receiver 51. The receiver 51 receives the three delivery keys Kd, overwrites delivery keys Kd stored before the reception, and stores the new delivery keys Kd. The EMD service center 1 stores the delivery key Kd of the version 1 and the delivery key Kd of the version 2, and the delivery key Kd of the version 3 as they are.

[0037] In the period from April 1, 1998 to April 30, 1998, the delivery key Kd of the version 4 is used in the EMD service center 1, the content provider 2, and the receiver 51 constituting the user home network 5.

[0038] Like this, by distributing the delivery keys Kd of future months in advance, even if the user does not access the EMD service center 1 for 1 or 2 months, the purchase of contents can be made though not quite satisfactorily, and at a suitable time, the user can access the EMD service center 1 to receive the key.

[0039] The delivery keys Kd for three months or six months are distributed, as described above, to the equipment of the user home network 5 formally registered in the EMD system and the content provider 2. On the other hand, instead of the delivery keys Kd for three months, a delivery key Kd for one month as shown in Fig. 8 is distributed to the equipment of the user home network 5 in the state where it is not formally registered in the EMD system but is temporarily registered (the detail will be described later). In this example, in order to formally register the equipment of the user home network 5 in the EMD system, a registration procedure requiring a time of about one month, such as credit investigation processing, becomes necessary. Then, in order to enable the usage of contents even in the period (about one month) from an application for registration to the formal registration, the delivery key Kd usable for one month is distributed to the equipment not formally registered (equipment temporarily registered).

[0040] Reference will be made to Fig. 3 again. A history data management portion 15 stores billing information, PT corresponding to the contents, UCP corresponding to the content, and the like, outputted from the user management portion 18.

[0041] The profit distributing portion 16 calculates the profit of the EMD service center 1, the content providers 2-1, 2-2, and the service providers 3-1, 3-2 on the basis of various pieces of information supplied from the history data management portion 15, and outputs the result to the service provider management portion 11, the content provider management portion 12, a receipts and disbursements portion 20, and the copyright management portion 13. The profit distributing portion 16 calculates a usage point (the more the profit is, that is, the more the user uses, the larger the value is) to each of the content providers 2-1, 2-2 and the service provides 3-1, 3-2 in accordance with the calculated profit, and outputs to the user management portion 18. Incidentally, in the following, the usage point in the content provider 2 will be referred to as a "content usage point", and the usage point in the service provider 3 will be referred to as a "service usage point".

[0042] A mutual authentication portion 17 executes mutual authentication among the content provider 2, the service provider 3, and the equipment of the user network 5.

[0043] The user management portion 18 manages information (hereinafter, referred to as system registration information) with respect to the equipment of the user home network 5 which can be registered in the EMD system. As shown in Fig. 9, the system registration information includes information corresponding to

items of [ID of SAM], [equipment number], [settlement ID], [settlement user information], a plurality of [subordinate user information], and [usage point information]. In the case of this example, [ID of SAM], [equipment number], [settlement ID], and [usage point information] are not made open. However, the predetermined information of [settlement user information] and [subordinate user information] is made open in the case where the user permits. In the drawing, the information shaded is information which is not made open (exhibition is not permitted), and the information not shaded is information which is made open (exhibition is permitted). Incidentally, the exhibition here means that the information is provided to the content provider 2, the service provider 3, or the equipment of the user home network 5.

[0044] In the [ID of SAM], the ID of the SAM of the equipment of the user home network 5, which was manufactured, is stored. In the [ID of SAM] of the system registration information of Fig. 9, the ID of the SAM 62 of the receiver 51 and the ID of the SAM 212 of the receiver 201 are set.

[0045] In the [equipment number], the equipment number previously set for the equipment of the user home network 5 including the SAM is set. In the case where the equipment of the user home network 5 has a function (includes a communication portion) capable of directly communicating with the service provider 3 and the EMD service center 1 through the network 4, and for example, has a function (has a display portion and an operation portion) to output (present) the content of the UCP or PT to the user, and to enable the user to select the use content of the UCP, the equipment (hereinafter, the equipment having such functions will be referred to as main equipment) is given the equipment number of No. 100 or more. In the case where the equipment has not such functions, the equipment (hereinafter, such equipment will be referred to as subordinate equipment) is given the equipment number of No. 99 or less. In the case of this example, although the details will be described later, since both the receiver 51 and the receiver 201 include the foregoing functions, the equipment number (No. 100) of No. 100 or more is given to each, and in the corresponding [equipment number], the equipment number of No. 100 is set.

[0046] In the [settlement ID], a predetermined settlement ID allocated when a receiver is formally registered in the EMD system is stored. In the case of this example, since the receiver 51 is formally registered and the settlement ID is given, in the [settlement ID] corresponding to the ID of the SAM 62 in the system registration information of Fig. 9, the given settlement ID is stored. On the other hand, since the receiver 201 is not registered in the EMD system, and the settlement ID is not given, any information is not set in the [settlement ID] corresponding to the ID of the SAM 212 in the system registration information of Fig. 9.

[0047] In the [settlement user information], the name, address, telephone number, settlement agency information (for example, credit card number, etc.), birth date, age, gender, ID, password, etc. of the user who settles the billing to be added up (hereinafter, such a user will be referred to as a settlement user) are set. In the case of this example, although the settlement agency information, ID and password are made information which is not made open, the other information of the name, address, telephone number, birth date, age, and gender is made information which is made open in the case where the user permits.

[0048] The name, address, telephone number, settlement agency information, birth date, and gender of the settlement user set in the [settlement user information] (hereinafter, in the case where it is not necessary to individually distinguish these pieces of information set in the [settlement user information], the whole will be referred to as user general information) are provided by the user when an application for registration is made and are set. In the case of this example, since credit investigation processing is carried out on the basis of the information of the name, address, telephone number, and settlement agency information, accurate information (for example, information registered in the settlement agency) is necessary. On the other hand, since the birth date, age, and gender of the user general information are not used for the credit investigation processing, in the case of this example, it is not necessary that such information is accurate, and it is not always necessary for the user to provide the information. The ID and password of the settlement user stored in the [settlement user information] are allocated and are set when temporal registration in the EMD system is made.

[0049] In the case of this example, the receiver 51 is registered with the user F as the settlement user, and in the [settlement user information] corresponding to the ID of the SAM 62 in the system registration information of Fig. 9, the user general information provided from the user F, the ID of the user F, and the password of the user F are set. Since an application for registration is not made for the receiver 201, any information is not set in the [settlement user information] corresponding to the ID of the SAM 212.

[0050] In the case of this example, it is assumed that the user F permits exhibition of the name, address, telephone number, birth date, age, and gender (all information which can be made open).

[0051] In the [subordinate user information], the name, address, telephone number, birth date, age, gender, ID, password, etc. of the user who does not settle the billing (hereinafter, such a user will be referred to as a subordinate user) are set. That is, among various pieces of information set in the [settlement user information], those other than the information of the settlement agency are set. In the case of this example, these pieces of information may be made open.

[0052] Incidentally, since the credit investigation processing is not carried out for the subordinate user, it

is not necessary that the name, address, telephone number, birth date, age, and gender of the subordinate user set in the [subordinate user information] are accurate. For example, in the case of the name, a nickname or the like may be used. Although the name is necessary to specify the user, it is not always necessary for the user to provide the other information. The ID and password of the subordinate user set in the [subordinate user information] are allocated and set when temporal registration or formal registration is made.

[0053] In the case of this example, since the subordinate user is not registered in both the receiver 51 and the receiver 201, any information is not set in the [subordinate user information] corresponding to the ID of the SAM 62 in the system registration information of Fig. 9 and in the [subordinate user information] corresponding to the ID of the SAM 212.

[0054] In the [usage point information], the usage point outputted from the profit distributing portion 16 is set. In the case of this example, in the receiver 51, the contents are already used, and in the [usage point information] corresponding to the SAM 62, the usage point information as shown in Fig. 10 is stored. In the example of Fig. 10, the content usage point of the content provider 2-1 given to the user F (settlement user) of the receiver 51 is 222 points, the content usage point of the content provider 2-2 is 123 points, the service usage point of the service provider 3-1 is 345 points, and the service usage point of the service provider 3-2 is 0 point.

[0055] In this example, the total points 345 (= 123 + 222) of the content usage point of the content provider 2-1 and the content provider 2-2 are made equal to the total points 345 (345 + 0) of the service usage point of the service provider 3-1 and the service provider 3-2.

[0056] In the receiver 201, since contents are not used (usage is not permitted) at the moment, any information is not naturally set in the [usage point information] corresponding to the ID of the SAM 212.

[0057] The user management portion 18 manages such system registration information, and further, prepares a registration list (described later) correspondingly to predetermined processing, and transmits it together with the delivery key Kd to the user home network 5.

[0058] Reference will be made to Fig. 3 again. A billing charging portion 19 calculates the billing to the user on the basis of, for example, the billing information, UCP and PT supplied from the history data management portion 15, and supplies the result to the receipts and disbursements portion 20. The receipts and disbursements portion 20 communicates with a not-shown external bank or the like on the basis of the disbursements to the user, the content provider 2, and the service provider 3, and the sum of usage fees to be collected, and executes the settlement processing. The receipts and disbursements portion 20 also notifies the user management portion 18 of the result of the settlement processing.

[0059] The audit portion 21 inspects the correctness (that is, whether a dishonest act is performed or not) of the billing information, PT, and UCP supplied from the equipment of the user home network 5. In this case, the EMD service center 1 receives the UCP from the content provider 2, the PT from the service provider 3, and the UCP and PT from the user home network 5, respectively.

[0060] Fig. 11 is a block diagram showing a functional structure of the content provider 2-1. A content server 31 stores contents to be supplied to the user, and supplies them to a watermark adding portion 32. The watermark adding portion 32 adds a watermark (electronic watermark) to the contents supplied from the content server 31, and supplies them to a compression portion 33.

[0061] The compression portion 33 compresses the contents supplied from the watermark adding portion 32 through a system such as ATRAC2 (Adaptive Transform Acoustic Coding 2) (trade mark) and supplies them to an encrypting portion 34. The encrypting portion 34 encrypts the contents compressed in the compression portion 33 by using a random number supplied from a random number generating portion 35 as a key (hereinafter, this random number will be referred to as a content key Kco) and by a common key encrypting system such as DES (Data Encryption Standard), and outputs the result to a secure container preparing portion 38.

[0062] The random number generating portion 35 supplies the random number of a predetermined bit number, which becomes the content key Kco, to the encrypting portion 34 and an encrypting portion 36. The encrypting portion 36 encrypts the content key Kco by using a delivery key Kd supplied from the EMD service center 1 and by a common key encrypting system such as DES, and outputs the result to the secure container preparing portion 38.

[0063] The DES is an encrypting system in which a common key of 56 bits is used, and processing is carried out while a plain text of 64 bits is made one block. The processing of the DES is composed of a portion (data mixing portion) for mixing the plain text into an encrypted text, and a portion (key processing portion) for generating a key (enlarged key) used by the data mixing portion from a common key. Since all algorism of the DES is open to the public, here, basic processing of the data mixing portion will be described in brief.

[0064] First, 64 bits of the plain text are divided into H_0 of the upper 32 bits and L_0 of the lower 32 bits. An enlarged key K_1 of 48 bits supplied from the key processing portion and L_0 of the lower 32 bits are made input, and the output of an F function obtained by mixing L_0 of the lower 32 bits is calculated. The F function is constituted by two kinds of basic transformations, that is, "substitution" for substituting a numerical value through a predetermined rule and "transposition" for transposing a bit position through a predetermined rule.

Next, H_0 of the upper 32 bits and the output of the F function are subjected to an exclusive OR operation, and its result is made L_1. L_0 is made H_1.

[0065] On the basis of H_0 of the upper 32 bits and L_0 of the lower 32 bits, the above processing is repeated 16 times, and the obtained H_{16} of the upper 32 bits and L_{16} of the lower 32 bits are outputted as an encrypted text. Decrypting is realized by using the common key used for encrypting and by reversely proceeding the above procedure.

[0066] A policy storage portion 37 stores UCP set correspondingly to contents, and outputs it to the secure container preparing portion 38. Fig. 12 shows UCP A and UCP B which are set correspondingly to contents A held in the content server 31 and are stored in the policy storage portion 37. The UCP includes predetermined information corresponding to the respective items of [ID of contents], [content information], [ID of content provider], [ID of UCP], [effective period of UCP], [use condition], and [use content].

[0067] In the [ID of contents], the ID of the contents to which the UCP corresponds is set. In the respective [ID of contents] of the UCP A (Fig. 12A) and UCP B (Fig. 12B), the ID of the contents A is set. In the [content information], predetermined content information as to the contents (music), such as the title of music or the name of a singer, is set. In the respective [content information] of the UCP A and UCP B, the content information of the contents A is set.

[0068] In the [ID of content provider], the ID of the content provider as a supplier of the contents is set. In the [ID of content provider] of each of the UCP A and the UCP B, the ID of the content provider 2-1 is set. In the [ID of UCP], the predetermined ID assigned to each UCP is set, the ID of the UCP A is set in the [ID of UCP] of the UCP A, and the ID of the UCP B is set in the [ID of UCP] of the UCP B. Information indicating the effective period of UCP is set in the [effective period of UCP], the effective period of the UCP A is set in the [effective period of UCP] of the UCP A, and the effective period of the UCP B is set in the [effective period of UCP] of the UCP B.

[0069] Predetermined information corresponding to each item of user condition] and [equipment condition] is set in the [use condition]. Information indicating the condition of the user capable of selecting this UCP is set in the [user condition], and information indicating the condition of the equipment capable of selecting this UCP is set in the [equipment condition].

[0070] In the case of the UCP A, [use condition 10] is set, and information ("200 points or more") indicating that the condition is such that the use point is 200 points or more is set in the [user condition 10] of the [use condition 10]. Information ("no condition") indicating that there is no condition is set in the [equipment condition 10] of the [use condition 10]. That is, only the user having the content use point of 200 points or more for the content provider 2-1 can select the UCP A.

[0071] In the case of the UCP B, [use condition 20] is set, and information ("less than 200 points") indicating that the condition is such that the use point is less than 200 points is set in the [user condition 20] of the [use condition 20]. Besides, information ("no condition") indicating that there is no condition is set in the [equipment condition 20] of the [use condition 20]. That is, only the user having the content use points of less than 200 points for the content provider 2-1 can select the UCP B.

[0072] The [use content] includes predetermined information corresponding to the respective items of [ID], [format], [parameter], and [management movement permissible information]. In the [ID], predetermined ID assigned to information set in the [use content] is set. In the [format], information indicating a use format of contents, such as reproduction or copying, is set. In the [parameter], predetermined information corresponding to the use format set in the [format] is set.

[0073] In the [management movement permissible information], information ("permissible" or "impermissible") indicating whether management movement of contents is possible or not (permitted or not) is set. When the management movement of the contents is made, as shown in Fig. 13A, while the contents are held in the equipment of the management movement origin, the contents are moved to the equipment of the management movement destination. That is, the contents are used in both the equipment of the management movement origin and the equipment of the management movement destination. At this point, it is different from a normal movement, as shown in Fig. 13B, in which the contents are not held in the equipment of the movement origin, but the contents are held only in the movement destination equipment, and the contents are used only in the equipment of the movement destination.

[0074] While the management movement of contents is carried out, the equipment of the management movement origin can not (not permitted) perform the management movement of the contents to another equipment as shown in Fig. 13A. That is, the contents are held only in two devices of the equipment of the management movement origin and the equipment of the management movement destination. At this point, it is different from the first generation copying as shown in Fig. 14A in which a plurality of copies (first generation) can be formed from the original contents. Besides, since it is possible to make the management movement of the contents to another equipment by returning the contents from the equipment of the management movement origin, in this point, it is also different from copying of only one time as shown in Fig. 14B.

[0075] Reference will be made to Fig. 12A again. The UCP A is provided with four [use content 11] to [use content 14]. In the [use content 11], and in its [ID 11], predetermined ID assigned to the [use content 11] is set. In the [format 11], information ("purchased reproduction") indicating the use format in which the contents are purchased and are reproduced is set, and in the

[parameter 11], predetermined information corresponding to the "purchased reproduction" is set. In the [management movement permissible information 11], information ("permissible") indicating that management movement of contents is possible is set.

[0076] In the [use content 12], and in its [ID 12], predetermined ID assigned to the [use content 12] is set. In the [format 12], information ("first generation copying") indicating the use format of carrying out the first generation copying is set. The first generation copying can prepare a plurality of first generation copies from the original contents as shown in Fig. 14A. However, it is not possible (not permissible) to prepare second generation copying from the first generation copying. In the [parameter 12], predetermined information corresponding to the "first generation copying" is set. In the [management movement permissible information 12], information ("impermissible") indicating that the management movement can not be made is set.

[0077] In the [use content 13], and in its [ID 13], predetermined ID assigned to the [use content 13] is set. In the [format 13], information ("reproduction with limited period") indicating the use format of making reproduction only in a predetermined period (time) is set. In the [parameter 13], correspondingly to the "reproduction with limited period", the start time (hour) of the period and the end time (hour) are set. In the [management movement permissible information 13], "impermissible" is set.

[0078] In the [use content 14], and in its [ID 14], predetermined ID assigned to the [use content 14] is set. In the [format 14], information ("Pay Per Copy 5") indicating the use format of copying 5 times (so-called book of tickets to enable copying to be performed five times) is set. Incidentally, also in this case, as shown in Fig. 14B, a copy from a copy can not be made (permitted). In the [parameter 14], information ("copying 5 times") indicating that copying can be made five times is set. In the [management movement permissible information 14], "impermissible" is set.

[0079] In the UCP B of Fig. 12B, two [use content 21] and [use content 22] are provided. In the [use content 21], and in its [ID 21], a predetermined ID assigned to the [use content 21] is set. In the [format 21], information ("Pay Per Play 4") indicating the use format in which reproduction is performed 4 times is set. In the [parameter 21], information "reproduction 4 times" indicating that reproduction can be made 4 times is set. In the [management movement permissible information 21], "impermissible" is set.

[0080] In the [use content 22], and in its [ID 22], a predetermined ID assigned to the [use content 22] is set. In the [format 22], "Pay Per Copy 2" is set, and in the [parameter 22], "copying 2 times" is set. In the [management movement permissible information 22], "impermissible" is set.

[0081] Here, when the content of the UCP A is compared with that of the UCP B, the user having the use points of 200 points or more can select the use content from the four use content 11 to use content 14, while the user having the use points of less than 200 points can select only the use content from the two use content 21 and use content 22.

[0082] Although Fig. 12 schematically shows the UCP A and the UCP B, for example, the [use condition 10] of the UCP A and the [use condition 20] of the UCP B are actually constituted by a service code shown in Fig. 15A and a condition code shown in Fig. 15B, and further, by a value code indicating numerical values and predetermined kinds corresponding to the service code.

[0083] Fig. 16A shows a code value of each code set as the [user condition 10] and the [equipment condition 10] of the [use condition 10] of the UCP A (Fig. 12A). Since the [user condition 10] of the [use condition 10] of the UCP A is made "200 points or more", the service code (Fig. 15A) of 80xxh meaning "there is condition as to use point", the value code of 0000C8h indicating the numerical value of 200, and the condition code (Fig. 15B) of 06h meaning ">= (equal or more)" are set as the user condition.

[0084] Since the [equipment condition 10] of the UCP A is made [no condition], the service code of 0000h meaning "no condition", the value code of FFFFFFh having no meaning at this time, and the condition code of 00h meaning "without condition" are set as the equipment condition.

[0085] Fig. 16B shows a code value of each code set as the [user condition 20] and the [equipment condition 20] of the [use condition 20] of the UCP B. Since the [user condition 20] is made "less than 200 points", the service code of 80xxh meaning "there is condition as to use point", the value code of 0000C8h indicating the numerical value of 200, and the condition code of 03h meaning "< (less than)" are set as the user condition.

[0086] Since the [equipment condition 20] of the UCP B is made "no condition" similarly to the [equipment condition 10] of the UCP A, and the same code values are set, the description is omitted.

[0087] Reference will be made to Fig. 11 again. The secure container preparing portion 38 prepares a content provider secure container made of, for example, as shown in Fig. 17, contents A (encrypted by content key KcoA), the content key KcoA (encrypted by delivery key Kd), UCP A, UCP B, and a signature. The signature is such that a hash value obtained by applying a hash function to the whole of the data to be transmitted (in this case, contents A (encrypted by the content key KcoA)), the content key KcoA (encrypted by the delivery key Kd), the UCP A and the USP B is encrypted with a secret key (in this case, secret key Kscp of the content provider 2-1) of public key cipher.

[0088] The secure container preparing portion 38 attaches a certificate of the content provider 2-1 as shown in Fig. 18 to the content provider secure container and transmits it to the service provider 3. This certificate is constituted by the version number of the

certificate, the serial number of the certificate allocated to the content provider 2-1 by certificate authority, algorism and parameter used for the signature, the name of the certificate authority, effective period of the certificate, name of the content provider 2-1, public key Kpcp of the content provider 2-1, and its signature (encrypted by secret key Ksca of the certificate authority).

[0089] The signature is data for checking falsifying and for authenticating an author, and is prepared in such a manner that a hash value is taken by a hash function on the basis of the data to be transmitted, and this is encrypted by a secret key of the public key code.

[0090] The hash function and checking of the signature will be described. The hash function is a function which receives predetermined data to be transmitted, compresses it to data of a predetermined bit length, and outputs it as a hash value. The hash function has features that it is difficult to predict an input from a hash value (output), when one bit of data inputted to the hash function is changed, a number of bits of the hash value are changed, and it is difficult to find input data having the same hash value.

[0091] A receiving person having received the signature and data decrypts the signature with the public key of the public key cipher, and obtains the result (hash value). Further, the hash value of the received data is calculated, and it is judged whether the calculated hash value is equal to the hash value obtained by decrypting the signature. In the case where it is judged that the hash value of the transmitted data is equal to the decrypted hash value, it is understood that the received data are not falsified, and are data transmitted from a transmitting person holding the secret key corresponding to the public key. As the hash function of the signature, MD4, MD5, SHA-1, or the like is used.

[0092] Next, the public key cipher will be described. To a common key cipher system in which the same key (common key) is used in encrypting and decrypting, in the public key cipher system, a key used in encrypting and a key used in decrypting are different from each other. In the case of using the public key cipher, even if one of the keys is made open, the other can be made secret, and a key which may be made open is called a public key, and the other key to be kept secret is called a secret key.

[0093] A typical RSA (Rivest-Shamir-Adleman) cipher in the public key cipher will be described in brief. First, p and q, which are two sufficiently large prime numbers, are obtained, and further, n of the product of p and q is obtained. The least common multiple L of (p-1) and (q-1) is calculated, and further, a numeral e, which is not less than 3 and less than L, and is relatively prime to L, is obtained (that is, a number which can commonly divide e and L is only 1).

[0094] Next, a multiplication inverse element d of e with respect to multiplication with L as a divisor is obtained. That is, ed = 1 mod L is established among d, e, and L, and d can be calculated by Euclidean algorithm. At this time, n and e are made public keys, and p, q, and d are made secret keys.

[0095] An encrypted text C is calculated from a plain text M by processing of equation (1).

$$C = M^e \bmod n \quad (1)$$

[0096] The encrypted text C is decrypted to the plain text M by processing of equation (2).

$$M = C^d \bmod n \quad (2)$$

[0097] Although the proof is omitted, it is based on Fermat's small theorem that a plain text is converted into an encrypted text by the RSA cipher, and it can be decrypted, and the base is that equation (3) is established.

$$M = C^d = (M^e)^d = M^{(ed)} = M \bmod n \quad (3)$$

[0098] If the secret keys p and q are known, the secret key d can be calculated from the public key e. However, if a figure number of the public key n is made large so that factorization into prime factors of the public key n is difficult in calculation, the secret key d can not be calculated from the public key e by merely knowing the public key n, and decrypting can not be made. As described above, in the RSA cipher, the key used for encrypting and the key for decrypting can be made different from each other.

[0099] An elliptic curve cipher as another example of the public key cipher will be described in brief. It is assumed that a point on an elliptic curve $y^2 = x^3 + ax + b$ is expressed by B. Addition of points on the elliptic curve is defined, and nB expresses a result where B is added n times. Similarly, subtraction is defined. It is proofed that calculation of n from B and nB is difficult. B and nB are made public keys, and n is made a secret key. Using a random number r, encrypted texts C1 and C2 are calculated from the plain text M with the public key and by the processing of equation (4) and equation (5).

$$C1 = M + rnB \quad (4)$$

$$C2 = rB \quad (5)$$

[0100] The encrypted texts C1 and C2 are decrypted to the plain text M by the processing of equation (6).

$$M = C1 - nC2 \quad (6)$$

[0101] Only those having the secret key n can decrypt. As described above, similarly to the RSA cipher, also in the elliptic curve cipher, the key used for encrypting and the key for decrypting can be made different from each other.

[0102] Reference will be made to Fig. 11 again. A mutual authentication portion 39 of the content provider 2-1 makes mutual authentication with the EMD service center 1 before the delivery key Kd supplied from the EMD service center 1 is received. Besides, the mutual authentication portion 39 can also be made mutual authentication with the service provider 3 before the content provider secure container is transmitted to the service provider 3. In the case of this example, since the content provider secure container does not include information which must be made secret, this mutual authentication is not necessarily required.

[0103] Since the content provider 2-2 basically includes the same structure as the content provider 2-1, its illustration and explanation are omitted.

[0104] Next, with reference to a block diagram of Fig. 19, a functional structure of the service provider 3-1 will be described. A content server 41 stores contents (encrypted by a content key Kco), the content key Kco (encrypted by a delivery key Kd), UCP, and a signature of the content provider 2, which are contained in the content provider secure container supplied from the content provider 2, and supplies them to a secure container preparing portion 44.

[0105] An estimating portion 42 checks the validity of the content provider secure container based on the signature contained in the content provider secure container supplied from the content provider 2. In this case, the certificate of the content provider 2 is checked, and when it is valid, the public key of the content provider 2 is obtained. Then, on the basis of the obtained public key, the validity of the content provider secure container is checked.

[0106] When the validity of the content provider secure container is confirmed, the estimating portion 42 prepares PT corresponding to UCP contained in the content provider secure container, and supplies it to the secure container preparing portion 44. Figs. 20A and 20B show two PT A-1 (Fig. 20A) and PT A-2 (Fig. 20B) prepared correspondingly to the UCP A of Fig. 12A. The PT includes information such as predetermined information corresponding to each item of [ID of contents], [content information], [ID of content provider], [ID of UCP], [ID of service provider], [ID of PT], [effective period of PT], [price condition], and [price content].

[0107] Information of items corresponding to the UCP is set in the [ID of contents], [content information], [ID of content provider], and [ID of UCP] of the PT, respectively. That is, the ID of contents A is set in the [ID of contents] of each of the PT A-1 and PT A-2, the content information of the contents A is set in the [content information] of each, the ID of the content provider 2-1 is set in the [ID of content provider] of each, and the ID of the UCP A is set in the [ID of UCP] of each.

[0108] In the [ID of service provider], the ID of the service provider 3 as the providing origin of the PT is set. In the [ID of service provider] of each of the PT A-1 and PT A-2, the ID of the service provider 3-1 is set. In the [ID of PT], predetermined ID assigned to each PT is set. The ID of the PT A-1 is set in the [ID of PT] of the PT A-1, and the ID of the PT A-2 is set in the [ID of PT] of the PT A-2. In the [effective period of PT], information indicating the effective period of the PT is set. The effective period of the PT A-1 is set in the [effective period of PT] of the PT A-1, and the effective period of the PT A-2 is set in the [effective period of PT] of the PT A-2.

[0109] In the [price condition], similarly to the [use condition] of the UCP, predetermined information corresponding to each item of the [user condition] and [equipment condition] is set. In the [user condition] of the [price condition], information indicating the condition of the user capable of selecting this PT is set, and in the [equipment condition], information indicating the condition of the equipment capable of selecting this PT is set.

[0110] In the case of the PT A-1, [price condition 10] is set, and in the [user condition 10] of the [price condition 10], information ("male") indicating that the user is male is set, and in the [equipment condition 10], "no condition" is set. That is, only the male user can select the PT A-1.

[0111] In the [user condition 10] and [equipment condition 10] of the [price condition 10] of the PT A-1, actually, as shown in Fig. 21A, code values of various codes are set. In the [user condition 10] of the [price condition 10], the service code (Fig. 15A) of 01xxh meaning "with gender condition", the value code of 000000h meaning a male at this time, and the condition code (Fig. 15B) of 01h meaning "=" are set. In the [equipment condition 10], the service code of 0000h meaning "no condition", the value code of FFFFFFh having no meaning in this case, and the condition code of 00h meaning "without condition" are set.

[0112] In the case of the PT A-2, the [price condition 20] is set, and in the [user condition 20] of the [price condition 20], information ("female") indicating that the user is female is set, and in the [equipment condition 20], "no condition" is set. That is, only the female user can select the PT A-2.

[0113] Also in the [user condition 20] and [equipment condition 20] of the [price condition 20] of the PTA-2, actually, as shown in Fig. 21B, code values of various codes are set. The service code (Fig. 15A) of 01xxh meaning "with gender condition ", the value code of 000001h meaning a female in this case, and the condition code (Fig. 15B) of 01h meaning "=" are set in the [user condition 20] of the [price condition 20]. The service code of 0000h meaning "no condition", the value code of FFFFFFh having no meaning in this case, and the condition code of 00h meaning "without condition" are set in the [equipment condition 20].

[0114] Reference will be made to Figs. 20A and 20B again. In the [price content] of the PT, a use fee in the case where the contents are used in the use format set in the [format] of the [use content] of the corresponding UCP is shown. That is, "2000 yen" set in the [price content 11] of the PT A-1, and "1000 yen" set in the

[price content 21] of the PT A-2 indicate the purchase price (fee) of the contents A since the [format 11] of the [use content 11] of the UCP A (Fig. 12A) is "purchase reproduction".

[0115] The expression "600 yen" of the [price content 12] of the PT A-1 and "300 yen" of the [price content 22] of the PT A-2 indicate the fee of the case where the contents A are used in the use format of first generation copy, from the [format 12] of the [use content 12] of the PT A-1. The expression "100 yen" of the [price content 13] of the PT A-1 and "50 yen" of the [price content 23] of the PT A-2 indicate the fee of the case where the contents A are used in the use format of reproduction with a limited period, from the [format 13] of the [use content 13] of the UCP A. The expression "300 yen" of the [price content 14] of the PT A-1 and "150 yen" of the [price content 24] of the PT A-2 indicate the fee of the case where the contents A are used in the use format of copying 5 times, from the [format 14] of the [use content 14] of the UCP A.

[0116] In the case of this example, when the price content of the PT A-1 (applied to the male user) is compared with the price content of the PT A-2 (applied to the female user), the price indicated in the price content of the PT A-1 is set twice the price indicated in the price content of the PT A-2. For example, the [price content 11] of the PT A-1 corresponding to the [use content 11] of the UCP A is made "2000 yen", while the [price content 21] of the PT A-2 similarly corresponding to the [use content 11] of the UCP A is made "1000 yen". Similarly, the price set in each of the [price content 12] to [price content 14] of the PT A-1 is set twice the price set in each of the [price content 22] to [price content 24] of the PT A-2. That is, the contents A are contents which can be used by the female user at a lower price.

[0117] Figs. 22A and 22B show two PT B-1 and PT B-2 prepared correspondingly to the UCP B of Fig. 12B. The PT B-1 of Fig. 22A includes ID of the contents A, content information of the contents A, ID of the content provider 2-1, ID of the UCP B, ID of the service provider 3-1, ID of the PT B-1, effective period of the PT B-1, price condition 30, two price contents 31 and 32, and the like.

[0118] In the [user condition 30] of the [price condition 30] of the PT B-1, "no condition" is set, and in the [equipment condition 30], information ("subordinate equipment") indicating that the equipment is a subordinate equipment is set. That is, the PT B-1 becomes selectable only in the case where the contents A are used in the subordinate equipment.

[0119] Also in the [user condition 30] and the [equipment condition 30] of the [price condition 30] of the PT B-1, actually, as shown in Fig. 23A, code values of respective codes are set. The service code (Fig. 15A) of 0000h meaning "no condition", the value code of FFFFFFh having no meaning in this case, and the condition code (Fig. 15B) of 00h meaning "without condition" are set in the [user condition 30]. Since the [equipment condition 30] is made the "subordinate equipment", the service code of 00xxh meaning "there is condition as to equipment", the value code of 000064h indicating "numerical value of 100" at this time, and the condition code of 03h meaning "< (smaller)" are set. In the case of this example, since an equipment number smaller than No. 100 is set in the subordinate equipment, such a code value is set.

[0120] The expression "100 yen" of the [price content 31] of the PT B-1 indicates the fee of the case where reproduction is made four times, since the [format 21] of the [use content 21] of the UCP B (Fig. 12B) is made "Pay Per Play 4", and "300 yen" of the [price content 32] indicates the fee of the case where copying is made two times, since the [format 22] of the [use content 22] of the UCP B is made "Pay Per Copy 2".

[0121] The other PT B-2 of Fig. 22B prepared correspondingly to the UCP B includes ID of the contents A, content information of the contents A, ID of the content provider 2-1, ID of the UCP B, effective period of the UCP B, ID of the service provider 3-1, ID of the PT B-2, effective period of the PT B-2, price condition 40, two price contents 41 and 42, and the like;

[0122] In the [user condition 40] of the [price condition 40] of the PT B-2, "no condition" is set, and in the [equipment condition 40], information ("main equipment") indicating that the equipment is the main equipment is set. That is, the PT B-2 becomes selectable only in the case where the contents are used in the main equipment.

[0123] Also in the [user condition 40] and the [equipment condition 40] of the [price condition 40] of the PTB-2, actually, as shown in Fig. 23B, code values of respective codes are set. The service code (Fig. 15A) of 0000h meaning "no condition", the value code of FFFFFFh having no meaning in this case, and the condition code (Fig. 15B) of 00h meaning "without condition" are set in the [user condition 40] of the [price condition 40]. The service code of 00xxh meaning "there is condition as to equipment", the value code of 000064h indicating "numerical value of 100" at this time, and the condition code of 06h meaning "= > (equal or more)" are set in the [equipment condition 40].

[0124] The price indicated in each of the [price content 41] and the [price content 42] of the PT B-2 indicates the fee of the case where the contents A are used in the use format shown in each of the [format 21] of the [use content 21] and the [format 22] of the [use content 22] of the UCP B.

[0125] Here, when the price content of the PT B-1 (applied to the subordinate equipment) is compared with the price content of the PT B-2 (applied to the main equipment), the price content of the PT B-1 is set twice the price content of the PT B-2. For example, the [price content 31] of the PT B-1 is made "100 yen" while the [price content 41] of the PT B-2 is made "50 yen", and the [price content 32] is made "300 yen" while the [price content 42] is made "150 yen".

[0126] Reference will be made to Fig. 19 again. A policy storage portion 43 stores UCP of contents supplied from the content provider 2, and supplies it to the secure container preparing portion 44.

[0127] The secure container preparing portion 44 prepares a service provider secure container made of, for example, as shown in Fig. 24, contents A (encrypted by a content key KcoA), the content key KcoA (encrypted by a delivery key Kd), UCP A, UCP B, signature of the content provider 2, PT A-1, A-2, B-1, B-2, and signature of the service provider 3.

[0128] The secure container preparing portion 44 supplies the prepared service provider secure container, together with a certificate of the service provider constituted by, as shown in Fig. 25, the version number of the certificate, the serial number of the certificate allocated to the service provider 3-1 by certificate authority, algorism and parameter used for the signature, the name of the certificate authority, the effective period of the certificate, the name of the service provider 3-1, the public key Kpsp of the service provider 3-1, and the signature, to the user home network 5.

[0129] Reference will be made to Fig. 19 again. Before the content provider secure container supplied from the content provider 2 is received, a mutual authentication portion 45 makes mutual authentication with the content provider 2. Besides, before the service provider secure container is transmitted to the user home network 5, the mutual authentication portion 45 makes mutual authentication with the user home network 5. However, for example, in the case where the network 4 is satellite communication, the mutual authentication between the service provider 3 and the user home network 5 is not executed. In the case of this example, since secret information is not particularly contained in the content provider secure container and the service provider secure container, it is not necessary that the service provider 3 makes mutual authentication with the content provider 2 and the user home network 5.

[0130] Since the structure of the service provider 3-2 is basically the same as the structure of the service provider 3-1, its illustration and description are omitted.

[0131] Next, with reference to a block diagram of Fig. 26, a structural example of the receiver 51 constituting the user home network 5 will be described. The receiver 51 is constituted by a communication portion 61, a SAM 62, an external storage portion 63, an expansion portion 64, a communication portion 65, an interface 66, a display control portion 67, and an input control portion 68. The communication portion 61 communicates with the service provider 3 or the EMD service center 1 through the network 4, and receives or transmits predetermined information.

[0132] The SAM 62 is made up of a mutual authentication module 71, a billing processing module 72, a storage module 73, a decrypting/encrypting module 74, and a data inspection module 75, and is constructed by a single chip cipher processing dedicated IC which has a multi-layer structure, has an inner memory cell sandwiched between dummy layers of aluminum layers or the like, and has such characteristics (tamper resistance) that from the outside, it is hard to dishonestly read out data, for example, the width of an operating voltage or frequency is narrow.

[0133] The mutual authentication module 71 of the SAM 62 transmits a certificate stored in the storage module 73 and shown in Fig. 27 to a mutual authentication partner, and executes mutual authentication, and by this, it supplies a temporary key Ktemp (session key) commonly owned by the authentication partner to the decrypting/encrypting module 74. Since information corresponding to information contained in the certificate (Fig. 18) of the content provider 2-1 and the certificate (Fig. 25) of the service provider 3-1 is contained in the certificate of the SAM, the description is omitted.

[0134] The billing processing module 72 prepares UCS and billing information on the basis of the use content of the selected UCP. Fig. 28 shows UCS A prepared based on the use content 11 of the UCP A shown in Fig. 12A, and the price content 11 of the PT A-1 shown in Fig. 20A. As shown in Fig. 28, predetermined information corresponding to each item of [ID of contents], [content information], [ID of content provided], [ID of UCP], [effective period of UCP], [ID of service provider], [ID of PT], [effective period of PT], [ID of UCS], [ID of SAM], [ID of user], [use content], and [use history] is set in the UCS.

[0135] In each of the [ID of contents], [content information], [ID of content provider], [ID of UCP], [effective period of UCP], [ID of service provider], [ID of PT], and [effective period of PT] of the UCS information of items corresponding to those of PT is set. That is, the ID of the contents A is set in the [ID of contents] of the UCS A of Fig. 28, the content information of the contents A is set in the [content information], the ID of the content provider 2-1 is set in the [ID of content provider], the ID of the UCP A is set in the [ID of UCP], the effective period of the UCP A is set in the [effective period of UCP], the ID of the service provider 3-1 is set in the [ID of service provider], the ID of the PT A-1 is set in the [ID of PT], and the effective period of the PT A-1 is set in the [effective period of PT].

[0136] The predetermined ID allocated to the UCS is set in the [ID of UCS], and the ID of the USC A is set in the [ID of UCS]. The ID of the SAM of the equipment is set in the [ID of SAM], and the ID of the SAM 62 of the receiver 51 is set in the [ID of SAM] of the UCS A. The ID of the user using the contents is set in the [ID of user], and the ID of the user F is set in the [ID of user] of the UCS A.

[0137] The [use content] is made up of respective items of [ID], [format], [parameter], and [management movement state information], and information of items corresponding to those of [use content] of the selected UCP is set in the items of the [ID], [format], and [param-

eter]. That is, information (ID of the use content 11) set in the [ID 11] of the [use content 11] of the UCP A is set in the [ID] of the UCS A, "purchase reproduction" set in the [format 11] of the [use content 11] is set in the [format], and information (information corresponding to "purchase reproduction") set in the [parameter 11] of the [use content 11] is set in the [parameter].

[0138] In the case where "permissible" is set in the [management movement permissible information] of the selected UCP (in the case where management movement can be made), in the [management movement state information] of the [use content], the ID of each of the equipment of the management movement origin (equipment which purchased the contents) and the equipment of the management movement destination is set. Incidentally, in the state where the management movement of contents is not carried out, the ID of the equipment of the management movement origin is set also as the ID of the equipment of the management movement destination. On the other hand, in the case where "impermissible" is set in the [management movement permissible information] of the UCP, "impermissible" is set in the [management movement state information]. That is, in this case, management movement of contents is not carried out (not permissible). In the [management movement state information] of the UCS A, since "permissible" is set in the [management movement permissible information 11] of the [use content 11] of the UCP A, and at this time, since the management movement of the contents A is not made, the ID of the SAM 62 is set as the ID of the equipment of the management movement origin and as the ID of the equipment of the management movement destination.

[0139] The [use history] contains the history of use format to the same contents. In the [use history] of the UCS A, although only the information indicating "purchase reproduction" is stored in the [use history] of the UCS A, for example, in the case where the contents A was previously used in the receiver 51, information indicating the use format at that time is also stored.

[0140] In the foregoing UCS, although the [effective period of UCP] and [effective period of PT] are provided, it is also possible that they are made not to be set in the UCS. In the foregoing UCS, although the [ID of content provider] is provided, in the case where the ID of the UCP is unique, and the content provider can be specified by this, it is also possible not to provide it. Similarly, with respect to the [ID of service provider], in the case where the ID of the PT is unique and the service provider can be specified by this, it is also possible not to provide it.

[0141] The prepared UCS, together with a content key Kco (encrypted by a saving key Ksave) supplied from a decrypting unit 91 of the decrypting/encrypting module 74 of the receiver 51, is transmitted to the external storage portion 63, and is stored in a use information storage portion 63A. As shown in Fig. 29, the use information storage portion 63A of the external storage portion 63 is divided into M blocks Bp-1 to Bp-M (for example, divided every megabyte), and each block Bp is divided into N use information memory regions Rp-1 to Rp-N. The content key Kco (encrypted by the saving key Ksave) supplied from the SAM 62, and the UCS are correspondingly stored in the use information memory region Rp of the predetermined block Bp of the use information storage portion 63A.

[0142] In the example of Fig. 29, the UCS A shown in Fig. 28 and the content key KcoA (encrypted by the saving key Ksave) for decrypting the contents A are correspondingly stored in the use information memory region Rp-3 of the block Bp-1. In the use information memory regions Rp-1 and Rp-2 of the block Bp-1, other content keys Kco1 and Kco2 (respectively encrypted by the saving key Ksave) and the UCS 1 and UCS 2 are respectively stored. In the use information memory region Rp-4 (not shown) to Rp-N of the block Bp-1, and the block Bp-2 (not shown) to Bp-M, the content key Kco and the UCS are not recorded, but predetermined initial information indicating vacancy is stored. In the case where it is not necessary to distinguish the content key Kco (encrypted by the saving key Ksave) and the UCS stored in the use information memory region Rp from each other, they will be referred to as use information together.

[0143] Fig. 30 shows billing information A prepared at the same time as the UCS A shown in Fig. 28. In the billing information, as shown in Fig. 30, predetermined information corresponding to respective items of [ID of contents], [ID of content provider], [ID of UCP], [effective period of UCP], [ID of service provider], [ID of PT], [effective period of PT], [ID of UCS], [ID of SAM], [ID of user], [use content], and [billing information] is set.

[0144] In the [ID of contents], [ID of content provider], [ID of UCP], [effective period of UCP], [ID of service provider], [ID of PT], [effective period of PT], [ID of UCS], [ID of SAM], [ID of user], and [use content] of the billing information, information of the respective items corresponding to them is set. That is, the ID of the contents A is set in the [ID of contents] of the billing information A of Fig. 30, the ID of the content provider 2-1 is set in the [ID of content provider], the ID of the UCP A is set in the [ID of UCP], the effective period of the UCP A is set in the [effective period of UCP], the ID of the service provider 3-1 is set in the [ID of service provider], the ID of the PT A-1 is set in the [ID of PT], the effective period of the PT A-1 is set in the [effective period of PT], the ID of the UCS A is set in the [ID of UCS], the ID of the SAM 62 is set in the [ID of SAM], the ID of the user F is set in the [ID of user], and the content of the [use content 11] of the UCS A is set in the [use content].

[0145] Information indicating the sum of billing added up in the equipment is set in the [billing history] of the billing information. The sum of billing added up in the receiver 51 is set in the [billing history] of the billing information A.

[0146] Incidentally, in the foregoing billing informa-

tion, although the [effective period of UCP] and the [effective period of PT] are provided, they may not be provided in the billing information. Besides, in the foregoing billing information, although the [ID of content provider] is provided, in the case where the ID of the UCP is unique, and the content provider can be specified by this, it is also possible not to provide that. Similarly, with respect to the [ID of service provider], in the case where the ID of the PT is unique, and the service provider can be specified by this, it is also possible not to provide that.

[0147] Reference will be made to Fig. 26 again. In the storage module 73, as shown in Fig. 31, various keys such as the public key Kpu of the SAM 62, the secret key Ksu of the SAM 62, the public key Kpesc of the EMD service center 1, the public key Kpca of the certificate authority, the saving key Ksave, and the delivery key Kd for March, the certificate (Fig. 27) of the SAM 62, billing information (for example, billing information A of Fig. 30), reference information 51, M inspection values Hp-1 to Hp-M, and the like are stored.

[0148] Fig. 32 shows the reference information 51 stored in the storage module 73. The reference information includes predetermined information set in respective items of [ID of SAM], [equipment number], [settlement ID], [upper limit amount of billing], [settlement user information], [subordinate user information], and [use point information].

[0149] In the [ID of SAM], [equipment number], [settlement ID], [settlement user information], [subordinate user information], and [use point information] of the reference information, information of corresponding items of the system registration information (Fig. 9) managed by the user management portion 18 of the EMD service center 1 is set. That is, the ID of the SAM 62, the equipment number (No. 100) of the SAM 62, the settlement ID of the user F, the settlement user information of the user F (general information (name, address, telephone number, settlement agency information, birth date, age, gender) of the user F, the ID of the user F, and the password of the user F), and use point information shown in Fig. 33 (information similar to that shown in Fig. 10) are set in the reference information 51.

[0150] In the [upper limit amount of billing], the upper limit amounts of billing different between the state where the equipment is formally registered in the EMD system and the state where it is temporarily registered are set. In the [upper limit amount of billing] of the reference information 51, since the receiver 51 is formally registered, information ("upper limit amount at the time of formal registration") indicating the upper limit amount of billing in the state where it is formally registered is set. Incidentally, the upper limit amount of billing in the state of the formal registration is larger than the upper limit amount of billing in the state of temporal registration.

[0151] Next, the M inspection values Hp-1 to Hp-M stored in the storage module 73 and shown in Fig. 31 will be described. The inspection value Hp-1 is a hash value calculated by applying a hash function to the whole of data stored in the block Bp-1 of the use information storage portion 63A of the external storage portion 63. Similarly to the inspection value Hp-1, the inspection values Hp-2 to Hp-M are also hash values of data stored in the corresponding blocks Bp-2 to Bp-M of the external storage portion 63.

[0152] Reference will be made to Fig. 26 again. The decrypting/encrypting module 74 of the SAM 62 is constituted by a decrypting unit 91, a random number generating unit 92, and an encrypting unit 93. The decrypting unit 91 decrypts an encrypted content key Kco by a delivery key Kd and outputs it to the encrypting unit 93. The random number generating unit 92 generates a random number of predetermined figures as the need arises (for example, at the time of mutual authentication), generates a temporal key Ktemp, and outputs it to the encrypting unit 93.

[0153] The encrypting unit 93 encrypts the decrypted content key Kco again by the saving key Ksave held in the storage module 73. The encrypted content key Kco is supplied to the external storage portion 63. When transmitting the content key Kco to the expansion portion 64, the encrypting unit 93 encrypts the content key Kco by the temporal key Ktemp generated by the random number generating unit 92.

[0154] The data inspection module 75 compares the inspection value Hp stored in the storage module 73 with the hash value of the data of the corresponding block Bp of the use information storage portion 63A of the external storage portion 63, and inspects whether the data of the block Bp is not falsified. The data inspection module 75 again calculates the inspection value Hp when the purchase, use, management movement, and the like of the contents are carried out, and stores (renews) the value in the storage module 73.

[0155] The expansion portion 64 is constituted by a mutual authentication module 101, a decrypting module 102, a decrypting module 103, an expansion module 104, and a watermark adding module 105. The mutual authentication module 101 performs mutual authentication with the SAM 62, and outputs the temporal key Ktemp to the decrypting module 102. The decrypting module 102 decrypts the content key Kco, which was encrypted by the temporal key Ktemp, by the temporal key Ktemp, and outputs it to the decrypting module 103. The decrypting module 103 decrypts the contents recorded in the HDD 52 by the content key Kco, and outputs it to the expansion module 104. The expansion module 104 further expands the decrypted contents through a system of ATRAC2 or the like, and outputs it to the watermark adding module 105. The watermark adding module 105 inserts a watermark (electronic watermark) of information (for example, ID of the SAM 62) for specifying the receiver 51 to the contents, and outputs it to a not-shown speaker, and reproduces music.

[0156] The communication portion 65 carries out

communication processing with the receiver 201 of the user home network 5. The interface 66 changes a signal from the SAM 62 and the expansion portion 64 into a predetermined format, and outputs it to the HDD 52. Further, the interface changes a signal from the HDD 52 into a predetermined format, and outputs it to the SAM 62 and the expansion portion 64.

[0157] The display control portion 67 controls output to a display portion (not shown). The input control portion 68 controls input from an operation portion (not shown) constituted by various buttons and the like.

[0158] The HDD 52 stores a registration list as shown in Fig. 34, in addition to the contents supplied from the service provider 3, UCP, and PT. This registration list is constituted by a list portion where information is stored in a table form, and an object SAM information portion where predetermined information as to an equipment for holding the registration list is stored.

[0159] In the object SAM information portion, the SAM ID of the equipment holding this registration list, in the case of this example, the ID of the SAM 62 of the receiver 51 is stored (in the column of [object SAM ID]). Further, in the object SAM information portion, the effective period of this registration list is stored (in the column of [effective period]), the version number of the registration list is stored (in the column of [version number]), and the number of the connected equipment (including itself), in the case of this example, since other equipment is not connected to the receiver 51, the value of 1 including itself is stored (in the column of [number of connected equipment]).

[0160] The list portion is constituted by nine items of [SAM ID], [user ID], [purchase processing], [billing processing], [billing equipment], [content supply equipment], [state flag], [signature of registration condition], and [registration list signature], and in the case of this example, as the registration conditions of the receiver 51, predetermined information is stored in the respective items.

[0161] The ID of the SAM of the equipment is stored in the [SAM ID]. In the case of this example, the ID of the SAM 62 of the receiver 51 is stored. In the [user ID], the ID of the user of the corresponding equipment is stored. In the case of this example, the ID of the user F is stored.

[0162] In the [purchase processing], information ("permissible" or "impermissible") indicating whether the corresponding equipment can perform processing for purchasing contents (specifically, purchase of use permissible conditions and content key Kco) is stored. In the case of this example, since the receiver 51 can perform the processing for purchasing contents, "permissible" is stored.

[0163] In the [billing processing], information ("permissible" or "impermissible") indicating whether the corresponding equipment can perform processing for settling the billing to the EMD service center 1 is stored. In the case of this example, since the user F is registered as the settlement user, the receiver 51 can perform processing for settling the billing. Thus, "permissible" is stored in the [billing processing].

[0164] In the [billing equipment], the ID of the SAM of the equipment for performing the billing processing to the billing added up in the corresponding equipment is stored. In the case of this example, since the receiver 51 (SAM 62) can settle the billing of itself, the ID of the SAM 62 is stored.

[0165] In the [content supply equipment], in the case where the corresponding equipment receives the supply of contents from other connected equipment, not the service provider 3, the ID of the SAM of the equipment capable of supplying the contents is stored. In the case of this example, since the receiver 51 receives the supply of contents from the service provider 3, information ("No") indicating that there is no equipment to supply contents is stored.

[0166] In the [state flag], an operation limiting condition of the corresponding equipment is stored. In the case of no limitation, information ("no limitation") indicating that case, in the case where a predetermined limitation is applied, information ("with limitation") indicating that case, and in the case where the operation is stopped, information ("stop") indicating that case are stored, respectively. For example, in the case where the settlement did not succeed, or in the case where credit investigation for formal registration is not completed (in the case of temporal registration), "with limitation" is set in the [state flag] corresponding to the equipment. In the case of this example, in the equipment in which "with limitation" is set in the [state flag], although processing of using already purchased contents is executed, processing for purchasing new contents can not be executed. That is, a specific limitation is imposed on the equipment. In the case where a dishonest act such as illegal copying of contents is found, "stop" is set in the [state flag], and the operation of the equipment is stopped. By this, the equipment comes to be impossible to receive any service from the EMD system.

[0167] In the case of this example, it is assumed that any restriction is not imposed on the receiver 51, and "No" is set in the [state flag].

[0168] In the [registration condition signature], as a registration condition, a signature by the EMD service center 1 to information stored in each of the [SAM ID], [user ID], [purchase processing], [billing processing], [billing equipment], [content supply equipment], and [state flag] is stored. In the case of this example, the signature to the registration condition of the receiver 51 is stored. In the [registration list signature], a signature to the whole of data set in the registration list is set.

[0169] Fig. 35 shows a structural example of the receiver 201. Since a communication portion 211 of the receiver 201 to an input control portion 218 have the same function as the communication portion 61 of the receiver 51 to the input control portion 68, their descrip-

tion is suitably omitted.

[0170] In a storage module 223 of the SAM 212, at this point of time, as shown in Fig. 36, a public key Kpu of the SAM 212, a secret key Ksu of the SAM 212, a public key Kpesc of the EMD service center 1, a public key Kpca of certificate authority, a saving key Ksave, certificate of the SAM 212 previously distributed from the certificate authority, and as shown in Fig. 37, reference information 201 in which the ID of the SAM 212 and the equipment number (No. 100) of the receiver 201 are set, are stored. Incidentally, a delivery key Kd expressed with a shadow in the Fig. 36 is not stored at this point of time.

[0171] Since a HDD 202 has the same function as the HDD 52, the description is omitted.

[0172] Next, the processing of the EMD system will be described with reference to the flowchart of Fig. 38. Here, the description will be made on, as an example, a case where contents A held in the content provider 2-1 are supplied to the receiver 51 of the user home network 5 through the service provider 3-1 and are used.

[0173] At step S11, the processing in which the delivery key Kd is supplied from the EMD service center 1 to the content provider 2-1 is carried out. The details of this processing are shown in the flowchart of Fig. 39. That is, at step S31, the mutual authentication portion 17 (Fig. 3) of the EMD service center 1 makes mutual authentication with the mutual authentication portion 39 (Fig. 11) of the content provider 2-1, and after confirms that the content provider 2-1 is a proper provider, the content provider management portion 12 of the EMD service center 1 transmits the delivery key Kd supplied from the key server 14 to the content provider 2-1. The details of the mutual authentication processing will be described later with reference to Figs. 40 to 42.

[0174] Next, at step S32, the encrypting portion 36 of the content provider 2-1 receives the delivery key Kd transmitted from the EMD service center 1, and stores it at step S33.

[0175] Like this, when the encrypting portion 36 of the content provider 2-1 stores the delivery key Kd, the processing is ended, and proceeds to step S12 of Fig. 38. Here, before the processing subsequent to step S12 is explained, with respect to the mutual authentication processing (processing for confirming that deception is not made) at step S31 of Fig. 39, a description will be made on, as examples, a case of using one common key (Fig. 40), a case of using two common keys (Fig. 41), and a case of using a public key cipher (Fig. 42).

[0176] Fig. 40 is a flowchart for explaining an operation of mutual authentication between the mutual authentication portion 39 of the content provider 2 and the mutual authentication portion 17 of the EMD service center 1, by one common key and using DES of common key cipher. At step S41, the mutual authentication portion 39 of the content provider 2 generates a random number R1 of 64 bits (the random number generating portion 35 may generate it). At step S42, the mutual authentication portion 39 of the content provider 2 encrypts the random number R1 by using the DES and by the previously stored common key Kc (encrypting may be made in the encrypting portion 36). At step S43, the mutual authentication portion 39 of the content provider 2 transmits the encrypted random number R1 to the mutual authentication portion 17 of the EMD service center 1.

[0177] At step S44, the mutual authentication portion 17 of the EMD service center 1 decrypts the received random number R1 by the previously stored common key Kc. At step S45, the mutual authentication portion 17 of the EMD service center 1 generates a random number R2 of 32 bits. At step S46, the mutual authentication portion 17 of the EMD service center 1 replaces the lower 32 bits of the decrypted random number R1 of 64 bits by the random number R2, and generates concatenation $R1_H||R2$. Incidentally, here, Ri_H designates the upper bit of Ri, and A||B designates concatenation of A and B (what is composed of (n + m) bits obtained by combining the lower bits of n bits of A with B of m bits). At step S47, the mutual authentication portion 17 of the EMD service center 1 encrypts $R1_H||R2$ by using the DES and by the common key Kc. At step S48, the mutual authentication portion 17 of the EMD service center 1 transmits the encrypted $R1_H||R2$ to the content provider 2.

[0178] At step S49, the mutual authentication portion 39 of the content provider 2 decrypts the received $R1_H||R2$ by the common key Kc. At step S50, the mutual authentication portion 39 of the content provider 2 checks $R1_H$ of the upper 32 bits of the decrypted $R1_H||R2$, and if it is coincident with $R1_H$ of the upper 32 bits of the random number R1 generated at step S41, the mutual authentication portion authenticates that the EMD service center 1 is a proper center. When the generated random number $R1_H$ is not coincident with the received $R1_H$, the processing is ended. When both are coincident with each other, at step S51, the mutual authentication portion 39 of the content provider 2 generates a random number R3 of 32 bits. At step S52, the mutual authentication portion 39 of the content provider 2 sets the received and decrypted random number R2 of 32 bits to the upper bits, and sets the generated random number R3 to the lower bits to make concatenation R2||R3. At step S53, the mutual authentication portion 39 of the content provider 2 encrypts the concatenation R2||R3 by using the DES and by the common key Kc. At step S54, the mutual authentication portion 39 of the content provider 2 transmits the encrypted concatenation R2||R3 to the mutual authentication portion 17 of the EMD service center 1.

[0179] At step S55, the mutual authentication portion 17 of the EMD service center 1 decrypts the received concatenation R2||R3 by the common key Kc. At step S56, the mutual authentication portion 17 of the EMD service center 1 checks the upper 32 bits of the decrypted concatenation R2||R3, and if it is coincident

with the random number R2, the mutual authentication portion authenticates that the content provider 2 is a proper provider, and if not coincident, it regards the provider as an unfair provider and ends the processing.

[0180] Fig. 41 is a flowchart for explaining the operation of mutual authentication between the mutual authentication portion 39 of the content provider 2 and the mutual authentication portion 17 of the EMD service center 1, by two common keys Kc1 and Kc2 and by using the DES of the common key cipher. At step S61, the mutual authentication portion 39 of the content provider 2 generates a random number R1 of 64 bits. At step S62, the mutual authentication portion 39 of the content provider 2 encrypts the random number R1 by using the DES and by the previously stored common key Kc1. At step S63, the mutual authentication portion 39 of the content provider 2 transmits the encrypted random number R1 to the EMD service center 1.

[0181] At step S64, the mutual authentication portion 17 of the EMD service center 1 decrypts the received random number R1 by the previously stored common key Kc1. At step S65, the mutual authentication portion 17 of the EMD service center 1 encrypts the random number R1 by the previously stored common key Kc2. At step S66, the mutual authentication portion 17 of the EMD service center 1 generates a random number R2 of 64 bits. At step S67, the mutual authentication portion 17 of the EMD service center 1 encrypts the random number R2 by the common key Kc2. At step S68, the mutual authentication portion 17 of the EMD service center 1 transmits the encrypted random number R1 and random number R2 to the mutual authentication portion 39 of the content provider 2.

[0182] At step S69, the mutual authentication portion 39 of the content provider 2 decrypts the received random number R1 and random number R2 by the previously stored common key Kc2. At step S70, the mutual authentication portion 39 of the content provider 2 checks the decrypted random number R1, and if it is coincident with the random number R1 (random number R1 before being encrypted) generated at step S61, the mutual authentication portion authenticates that the EMD service center 1 is a proper center, and if not coincident, the mutual authentication portion regards it as an unfair center and ends the processing. At step S71, the mutual authentication portion 39 of the content provider 2 encrypts the decrypted random number R2 by the common key Kc1. At step S72, the mutual authentication portion 39 of the content provider 2 transmits the encrypted random number R2 to the EMD service center 1.

[0183] At step S73, the mutual authentication portion 17 of the EMD service center 1 decrypts the received random number R2 by the common key Kc1. At step S74, the mutual authentication portion 17 of the EMD service center 1 authenticates that the content provider 2 is a proper provider if the decrypted random number R2 is coincident with the random number R2 (random number R2 before being encrypted) generated at step S66, while it regards the provider as an unfair provider and ends the processing if not coincident.

[0184] Fig. 42 is a flowchart for explaining the operation of mutual authentication between the mutual authentication portion 39 of the content provider 2 and the mutual authentication portion 17 of the EMD service center 1, by using an elliptic curve cipher with a length of 160 bits, as the public key cipher. At step S81, the mutual authentication portion 39 of the content provider 2 generates a random number R1 of 64 bits. At step S82, the mutual authentication portion 39 of the content provider 2 transmits a certificate (what is previously obtained from the certificate authority) including its own public key Kpcp and the random number R1 to the mutual authentication portion 17 of the EMD service center 1.

[0185] At step S83, the mutual authentication portion 17 of the EMD service center 1 decrypts the signature (encrypted by the secret key Ksca of the certificate authority) of the received certificate by the previously obtained public key Kpca of the certificate authority, and extracts the hash value of the public key Kpcp of the content provider 2 and the name of the content provider 2, and further extracts the public key Kpcp of the content provider 2 and the name of the content provider 2 stored in the certificate as a plain text. If the certificate is a proper one issued by the certificate authority, it is possible to decrypt the signature of the certificate, and the hash value of the public key Kpcp and the name of the content provider 2 obtained by decrypting coincides with a hash value obtained by applying a hash function to the public key Kpcp of the content provider 2 and the name of the content provider 2 stored in the certificate as the plain text. By this, it is authenticated that the public key Kpcp is a proper one which is not falsified. If the signature can not be decrypted, or even if decrypted, the hash values are not coincident with each other, it is found that the key is not a proper public key or the provider is not a proper provider. At this time, the processing is ended.

[0186] When the proper authentication result is obtained, at step S84, the mutual authentication portion 17 of the EMD service center 1 generates a random number R2 of 64 bits. At step S85, the mutual authentication portion 17 of the EMD service center 1 generates concatenation R1||R2 of the random number R1 and the random number R2. At step S86, the mutual authentication portion 17 of the EMD service center 1 encrypts the concatenation R1||R2 by its own secret key Ksesc. At step S87, the mutual authentication portion 17 of the EMD service center 1 encrypts the concatenation R1||R2 by the public key Kpcp of the content provider 2 obtained at step S83. At step S88, the mutual authentication portion 17 of the EMD service center 1 transmits the concatenation R1||R2 encrypted by the secret key Ksesc, the concatenation R1||R2 encrypted by the public key Kpcp, and the certificate (previously obtained

from the certificate authority) including its own public key Kpesc to the mutual authentication portion 39 of the content provider 2.

[0187] At step S89, the mutual authentication portion 39 of the content provider 2 decrypts the signature of the received certificate by the previously obtained public key Kpca of the certificate authority, and if correct, it extracts the public key Kpesc from the certificate. Since the processing of this case is the same as the case of step S83, the description is omitted. At step S90, the mutual authentication portion 39 of the content provider 2 decrypts the concatenation R1||R2, encrypted by the secret key Ksesc of the EMD service center 1, by the public key Kpesc obtained at step S89. At step S91, the mutual authentication portion 39 of the content provider 2 decrypts the concatenation R1||R2, encrypted by its own public key Kpcp, by its own secret key Kscp. At step S92, the mutual authentication portion 39 of the content provider 2 compares the concatenation R1||R2 decrypted at step S90 with the concatenation R1||R2 decrypted at step S91, and if coincident, the mutual authentication portion authenticates that the EMD service center 1 is a proper one, and if not coincident, the portion regards it as an improper one and ends the processing.

[0188] When a proper authentication result is obtained, at step S93, the mutual authentication portion 39 of the content provider 2 generates a random number R3 of 64 bits. At step S94, the mutual authentication portion 39 of the content provider 2 generates concatenation R2||R3 of the random number R2 obtained at step S90 and the generated random number R3. At step S95, the mutual authentication portion 39 of the content provider 2 encrypts the concatenation R2||R3 by the public key Kpesc obtained at step S89. At step S96, the mutual authentication portion 39 of the content provider 2 transmits the encrypted concatenation R2||R3 to the mutual authentication portion 17 of the EMD service center 1.

[0189] At step S97, the mutual authentication portion 17 of the EMD service center 1 decrypts the encrypted concatenation R2||R3 by its own secret key Ksesc. At step S98, if the decrypted random number R2 is coincident with the random number R2 (random number R2 before being encrypted) generated at step S84, the mutual authentication portion 17 of the EMD service center 1 authenticates that the content provider 2 is a proper provider, and if not coincident, it regards the content provider as an improper provider and ends the processing.

[0190] As described above, the mutual authentication portion 17 of the EMD service center 1 and the mutual authentication portion 39 of the content provider 2 make mutual authentication. The random number used for the mutual authentication is used as a temporal key Ktemp effective for only the processing subsequent to the mutual authentication.

[0191] Next, the processing of step S12 of Fig. 38 will be described. At step S12, the processing in which a content provider secure container is supplied to the service provider 3-1 from the content provider 2-1 is carried out. The details of the processing are shown in the flowchart of Fig. 43. That is, at step 201, the watermark adding portion 32 (Fig. 11) of the content provider 2-1 reads out the contents A from the content server 31, inserts a predetermined watermark (electronic watermark) indicating the content provider 2-1, and supplies it to the compression portion 33.

[0192] At step S202, the compression portion 33 of the content provider 2-1 compresses the contents A inserted with the watermark by a predetermined system such as ATRAC2, and supplies to the encrypting portion 34. At step S203, the random number generating portion 35 generates a random number which becomes a content key KcoA, and supplies it to the encrypting portion 34.

[0193] At step S204, the encrypting portion 34 of the content provider 2-1 uses the random number (content key KcoA) generated in the random number generating portion 35 by the predetermined system of DES or the like, and encrypts the contents A in which the watermark is inserted and which is compressed. Next, at step S205, the encrypting portion 36 encrypts the content key KcoA by the predetermined system such as DES and by the delivery key Kd supplied from the EMD service center 1.

[0194] At step S206, the secure container preparing portion 38 of the content provider 2-1 calculates a hash value by applying a hash function to the whole of the contents A (encrypted by the content key KcoA), the content key KcoA (encrypted by the delivery key Kd), UCP A and UCP B (Fig. 12) stored in the policy storage portion 37 and corresponding to the contents A, and encrypts it by its own secret key Kscp. By this, the signature shown in Fig. 17 is prepared.

[0195] At step S207, the secure container preparing portion 38 of the content provider 2-1 prepares the content provider secure container shown in Fig. 17, which includes the contents A (encrypted by the content key KcoA), the content key KcoA (encrypted by the delivery key Kd), UCP A, UCP B (Fig. 12) and the signature prepared at step S206.

[0196] At step S208, the mutual authentication portion 39 of the content provider 2-1 makes mutual authentication with the mutual authentication portion 45 (Fig. 19) of the service provider 3-1. Since the authentication processing is the same as the case explained with reference to Figs. 40 to 42, the description is omitted. At step S209, the secure container preparing portion 38 of the content provider 2-1 attaches the certificate (Fig. 18) previously issued from the certificate authority to the content provider secure container prepared at step S207, and transmits it to the service provider 3-1.

[0197] When the content provider secure container is supplied to the service provider 3-1 in this way, the

processing is ended, and proceeds to step S13 of Fig. 38.

[0198] At step S13, the service provider secure container is supplied from the service provider 3-1 to the user home network 5 (receiver 51). The details of this processing are shown in the flowchart of Fig. 44. That is, at step S221, the estimating portion 42 (Fig. 19) of the service provider 3-1 confirms the signature contained in the certificate (Fig. 18) attached to the content provider secure container transmitted from the content provider 2-1, and if falsifying of the certificate is not made, it extracts the public key Kpcp of the content provider 2-1 from that. Since the confirmation of the signature of the certificate is the same as the processing at step S83 of Fig. 42, the description is omitted.

[0199] At step S222, the estimating portion 42 of the service provider 3-1 decrypts the signature of the content provider secure container transmitted from the content provider 2-1 by the public key Kpcp of the content provider 2-1, judges whether the obtained hash value is coincident with a hash value obtained by applying a hash function to the whole of the contents A (encrypted by the content key KcoA), the content key KcoA (encrypted by the delivery key Kd), the UCP A and the UCP B, and confirms whether the content provider secure container is not falsified. In the case where values of both are not coincident with each other (in the case where falsifying is found), the processing is ended. In the case of this example, it is assumed that falsifying of the content provider secure container is not carried out, and the processing proceeds to step S223.

[0200] At step S223, the estimating portion 42 of the service provider 3-1 extracts the contents A (encrypted by the content key KcoA), the content key KcoA (encrypted by the delivery key Kd), and the signature from the content provider secure container, and supplies them to the content server 41. The content server 41 stores those. The estimating portion 42 extracts also the UCP A and UCP B from the content provider secure container, and supplies them to the policy storage portion 43 and the secure container preparing portion 44.

[0201] At step S224, the estimating portion 42 of the service provider 3-1 prepares PT A-1, PT A-2 (Fig. 20), and PT B-1, PT B-2 (Fig. 22) on the basis of the extracted UCP A and UCP B, and supplies them to the secure container preparing portion 44.

[0202] At step S225, the secure container preparing portion 44 of the service provider 3-1 prepares the service provider secure container shown in Fig. 24 from the contents A (encrypted by the content key KcoA), the content key KcoA (encrypted by the delivery key Kd), and the signature of the content provider 2-1, which are read out from the content server 41, and the UCP A, B, and the PT A-1, A-2, B-1, B-2, which are supplied from the estimating portion 42.

[0203] At step S226, the mutual authentication portion 45 of the service provider 3-1 makes mutual authentication with the mutual authentication module 71 (Fig. 26) of the receiver 51. Since this authentication processing is the same as the case where the explanation has been made with reference to Figs. 40 to 42, the explanation is omitted.

[0204] At step S227, the secure container preparing portion 44 of the service provider 3-1 attaches the certificate (Fig. 25) of the service provider 3-1 to the service provider secure container prepared at step S225, and transmits it to the receiver 51 of the user home network 5.

[0205] In this way, when the service provider secure container is transmitted from the service provider 3-1 to the receiver 51, the processing is ended, and proceeds to step S14 of Fig. 38.

[0206] At step S14, the service provider secure container transmitted from the service provider 3-1 is received by the receiver 51 of the user home network 5. The details of this processing are shown in the flowchart of Fig. 45. That is, at step S241, the mutual authentication module 71 (Fig. 26) of the receiver 51 makes mutual authentication with the mutual authentication portion 45 (Fig. 19) of the service provider 3-1 through the communication portion 61, and when the mutual authentication can be made, the communication portion 61 receives the service provider secure container (Fig. 24) from the service provider 3-1 with which the mutual authentication was made. In the case where the mutual authentication can not be made, the processing is ended. In the case of this example, it is assumed that the mutual authentication was made, and the processing proceeds to step S242.

[0207] At step S242, the communication portion 61 of the receiver 51 receives a public key certificate from the service provider 3-1 with which the mutual authentication was made at step S241.

[0208] At step S243, the decrypting/encrypting module 74 of the receiver 51 checks the signature contained in the service provider secure container received at step S241, and checks whether falsifying has been made or not. Here, in the case where falsifying is found, the processing is ended. In the case of this example, it is assumed that falsifying is not found, and the processing proceeds to step S244.

[0209] At step S244, the UCP in which the reference information 51 (Fig. 32) stored in the storage module 73 of the receiver 51 satisfies the use condition, and the PT in which it satisfies the price condition are selected, and are displayed on a not-shown display portion through the display control portion 67. The user F refers to the content of the displayed UCP and PT, operates a not-shown operation portion, and selects one use content of the UCP. By this, the input control portion 68 outputs a signal inputted from the operation portion and corresponding to the operation of the user F to the SAM 62.

[0210] In the case of this example, in the [use point information] of the reference information 51 of the

receiver 51, as shown in Fig. 33, the content use point of the content provider 2-1 is made 222 points. That is, according to this reference information 51, between UCP A and UCP B set correspondingly to the contents A, the USP A (Fig. 12A) in which the [user condition 10] of the [use condition 10] is made "200 points or more" is selected. Besides, in the [settlement user information] of the reference information 51, since the user F is made male, the condition set in the [price condition 10] of the PT A-1 (Fig. 20A) is satisfied. As a result, between the PT A-1 and PT A-2 prepared correspondingly to the UCP A, the PT A-1 is selected. Eventually, the content of the UCP A and the PT A-1 is displayed on the display portion. In the case of this example, by this, it is assumed that the user F selects the use content 11 of the UCP A (price content 11 of the PT A-1).

[0211] At step S245, the billing processing module 72 of the SAM 62 of the receiver 51 prepares UCS A (Fig. 28) and billing information A (Fig. 30) on the basis of the content (content of the [price content 11] of the PT A-1) of the [use content 11] of the UCP A selected at step S 244. That is, in this case, the contents A are purchased and reproduced at a charge of 2000 yen.

[0212] At step S246, the contents A (encrypted by the content key KcoA), UCP A, PTA-1, PTA-2, and the signature of the content provider 2, which are contained in the service provider secure container (Fig. 24), are extracted, are outputted to the HDD 52, and are stored. At step S247, the decrypting unit 91 of the decrypting/encrypting unit 74 decrypts the content key KcoA (encrypted by the delivery key Kd) contained in the service provider secure container by the delivery key Kd stored in the storage module 73.

[0213] At step S248, the encrypting unit 93 of the decrypting/encrypting unit 74 encrypts the content key KcoA decrypted at step S247 by the saving key Ksave stored in the storage module 73.

[0214] At step S249, the data inspection module 75 of the receiver 51 detects the block Bp of the use information storage portion 63A (Fig. 29) of the external storage portion 63 in which the content key KcoA encrypted by the saving key Ksave at step S248 and UCS A prepared at step S245 are correspondingly stored. In the case of this example, the block Bp-1 of the use information storage portion 63A is detected. Incidentally, in the use information storage portion 63A of Fig. 29, although the drawing shows as if the content key KcoA and UCS A are stored in the use information memory region Rp-3 of the block Bp-1, in the case of this example, they are not stored in the use information memory region Rp-3 of the block Bp-1 at this point of time, but predetermined initial information indicating vacancy is stored.

[0215] At step S250, the data inspection module 75 of the receiver 51 applies a hash function to the data of the block Bp-1 detected at step S249 (all data stored in the use information memory regions Rp-1 to Rp-N) to obtain a hash value. Next, at step S251, the data inspection module 75 compares the hash value obtained at step S250 with the inspection value Hp-1 (Fig. 31) corresponding to the block Bp-1 stored in the storage module 73, and judges whether they are coincident with each other. In the case where it is judged that they are coincident, since the data of the block Bp-1 are not falsified, the processing proceeds to step S252.

[0216] At step S252, the SAM 62 of the receiver 51 stores the use information (content key KcoA encrypted by the saving key Ksave at step S248, and UCS A (Fig. 28) prepared at step S245) in the use information memory region Rp-3 of the block Bp-1 of the external storage portion 63.

[0217] At step S253, the data inspection module 75 of the receiver 51 applies a hash function to all data stored in the block Bp-1, which includes the use information memory region Rp-3 in which the use information is stored at step S252, of the use information storage portion 63A, and calculates a hash value, and at step S254, overwrites the inspection value Hp-1 stored in the storage module 73. At step S255, the billing processing module 72 stores the billing information A prepared at step S245 in the storage module 73, and the processing is ended.

[0218] At step S251, in the case where it is judged that the calculated hash value is not coincident with the inspection value Hp-1, since the data of the block Bp-1 are falsified, the procedure proceeds to step S256, and it is judged whether the data inspection module 75 has examined all blocks Bp of the use information storage portion 63A of the external storage portion 63. In the case where all blocks Bp of the external storage portion 63 have not been examined, the procedure proceeds to step S257, other blocks Bp having vacancy in the use information storage portion 63A are searched, and then, the procedure returns to step S250, and the subsequent processing is executed.

[0219] At step S256, in the case where all blocks Bp of the use information storage portion 63A of the external storage portion 63 have been examined, since a block Bp (use information memory region Rp) capable of storing use information does not exist, the processing is ended.

[0220] Like this, when the service provider secure container is received by the receiver 51, the processing is ended, and proceeds to step S15 of Fig. 38.

[0221] At step S15, the supplied contents A are used in the receiver 51. In the case of this example, according to the use content 11 of the selected UCP A, the contents A are reproduced and are used. Then, here, the reproduction processing of the contents A will be described. The details of this reproduction processing are shown in the flowchart of Fig. 46.

[0222] At step S261, the data inspection module 75 of the receiver 51 applies a hash function to the content key KcoA (encrypted by the saving key Ksave) and the data of the block Bp-1, which includes the use information memory region Rp-3 in which the UCS A is stored

at step S252 of the Fig. 45, of the use information storage portion 63A of the external storage portion 63, and calculates a hash value.

[0223] At step S262, the data inspection module 75 of the receiver 51 judges whether the hash value calculated at step S261 is coincident with the hash value (inspection value Hp-1) calculated at step S253 of Fig. 45 and stored in the storage module 73 at step S254, and in the case where they are coincident with each other, since the data of the block Bp-1 are not falsified, the procedure proceeds to step S263.

[0224] At step S263, on the basis of the information indicated in the [parameter] of the [use content] of the UCS A (Fig. 28), it is judged whether the contents A can be used. For example, in the UCS in which the [format] of the [use content] is made [reproduction with limited period], since the start period (hour) and end period (hour) are stored in the [parameter], in this case, it is judged whether the present hour is in the range. When the present hour is in the range, it is judged that the use of the contents is possible, and when the hour is in the outside of the range, it is judged that the use is impossible. In the UCS in which the [format] of the [use content] is made the use format where reproduction (copying) is made only a predetermined number of times, the remaining usable number of times is stored in the [parameter]. In this case, when the usable number of times stored in the [parameter] is not 0, it is judged that the use of the corresponding contents is possible, while when the usable number of times is 0, it is judged that the use is impossible.

[0225] Incidentally, since the [format] of the [use content] of the UCS A is made [purchase reproduction], in this case, the contents A are purchased, and are reproduced without limit. That is, information indicating that the contents can be used is set in the [parameter] of the [use content] of the UCS A. Thus, in the case of this embodiment, at step S263, it is judged that the contents A can be used, and the procedure proceeds to step S264.

[0226] At step S264, the billing module 72 of the receiver 51 renews the UCS A. Although information to be renewed is not contained in the UCS A, for example, in the case where the [format] of the [use content] is made the use format in which reproduction is made only a predetermined number of times, the reproducible number of times stored in the [parameter] is decremented by 1.

[0227] Next, at step S265, the SAM 62 of the receiver 51 stores the UCS A (actually, not renewed) renewed at step S264 in the use information memory region Rp-3 of the block Bp-1 of the use information storage portion 63A of the external storage portion 63. At step S266, the data inspection module 75 applies a hash function to the data of the block Bp-1 of the use information storage portion 63A of the external storage portion 63, in which the UCS A is stored at step S265, and calculates a hash value, and overwrites the inspection value Hp-1 stored in the storage module 73.

[0228] At step S267, the mutual authentication module 71 of the SAM 62 and the mutual authentication module 101 of the expansion portion 64 make mutual authentication, and the SAM 62 and the expansion portion 64 have the temporal key Ktemp in common. Since this authentication processing is the same as the case described with reference to Figs. 40 to 42, its description is omitted here. The random numbers R1, R2, and R3 used for the mutual authentication or their combination is used as the temporal key Ktemp.

[0229] At step S268, the decrypting unit 91 of the decrypting/encrypting module 74 decrypts the content key KcoA (encrypted by the saving key Ksave) stored in the block Bp-1 (use information memory region Rp-3) of the use information storage portion 63A of the external storage portion 63 at step S252 of Fig. 45 by the saving key Ksave stored in the storage module 73.

[0230] Next, at step S269, the encrypting unit 93 of the decrypting/encrypting module 74 encrypts the decrypted content key KcoA by the temporal key Ktemp. At step S270, the SAM 62 transmits the content key KcoA encrypted by the temporal key Ktemp to the expansion portion 64.

[0231] At step S271, the decrypting module 102 of the expansion portion 64 decrypts the content key KcoA by the temporal key Ktemp. At step S272, the expansion portion 64 receives the contents A (encrypted by the content key Kco) recorded in the HDD 52 through the interface 66. At step S273, the decrypting module 103 of the expansion portion 64 decrypts the contents A (encrypted by the content key Kco) by the content key KcoA.

[0232] At step S274, the expansion module 104 of the expansion portion 64 expands the decrypted contents A by a predetermined system such as ATRAC2. At step S275, the watermark adding module 105 of the expansion portion 64 inserts a predetermined watermark (electronic watermark) for specifying the receiver 51 to the expanded contents A. At step S276, the contents A are outputted to a not-shown speaker or the like, and the processing is ended.

[0233] At step S262, in the case where it is judged that the hash value calculated at step S261 is not coincident with the hash value stored in the storage module 73 of the receiver 51, or at step S263, in the case where it is judged that the contents can not be used, at step S277, the SAM 62 executes predetermined error processing such as displaying an error message on a not-shown display portion through the display control portion 67, and the processing is ended.

[0234] In this way, in the receiver 51, when the contents A are reproduced (used), the processing is ended, and the processing of Fig. 38 is also ended.

[0235] Next, a description will be made on a processing in which among equipments constituting the user home network 5, the receiver 201 not registered in the EMD system is registered while the user A as a pur-

chaser is made a settlement user. The flowchart of Fig. 47 shows a processing procedure of the receiver 201 in the case of executing this processing.

[0236] At step S401, the user A purchasing the receiver 201 enters predetermined information in a registration form attached to the receiver 201 at the time of purchase, and sends it to a management company for managing the EMD service center 1. As shown in Fig. 48, in this registration form, an expression indicating ID of the SAM of the equipment to be attached (in this case, ID of the SAM 212 of the receiver 201) is recited, and further, there are provided columns in which information such as name, address, telephone number, information of settlement agency (for example, the number of a credit card, etc.), birth date, age, gender, password, user ID, settlement ID, and the like of the user can be entered. Correspondingly to the columns in which the name, address, telephone number, birth date, age, and gender are entered, there are provided columns ([open: permissible or impermissible]) in which the information as to whether or not the respective information is permitted to be made open, is entered. In the case where the user permits the information to be made open, the user encircles "permissible" of the corresponding column. In the case where the exhibition of the information is not permitted, the user encircles "impermissible" of the corresponding column.

[0237] The pass word, ID, and settlement ID of the user are given to the user when he or she is registered (formally registered or temporarily registered) in the EMD system, and these are not made open.

[0238] In the case of this example, at this point of time, since the user A is not registered in the EMD system, he or she does not has the password, user ID, and settlement ID. Then, as shown in Fig. 48, the user A enters the name, address, telephone number, information of settlement agency, birth date, age, and gender (hereinafter, in the case where it is not necessary to individually distinguish the name, address, telephone number, information of settlement agency, birth date, age, and gender, which are entered in the registration form, from one another, the whole will be referred to as "user general information") in the registration form. In the case of this example, since it is assumed that the user A permits the name, birth date, and age to be made open, "permissible" of the corresponding column is encircled by a circle. On the other hand, since it is assumed that the user A does not permit the address, telephone number, and gender to be made open, "impermissible" of the corresponding column is encircled by a circle.

[0239] In this case, since the user A is registered as the settlement user of the receiver 201, a credit investigation processing is carried out to the user A. Then, the user A must always enter the information of the name, address, telephone number, and settlement agency in the user general information, which are used for the credit investigation processing, in the registration form.

[0240] Next, at step S402, the user A carries out an operation to the receiver 201 to transmit a predetermined use start signal indicating the start of use of contents in the receiver 201 to the EMD service center 1. By this, mutual authentication is made between the mutual authentication portion 221 of the receiver 201 and the mutual authentication portion 17 of the EMD service center 1, and then, the use start signal is transmitted to the EMD service center 1 through the communication portion 211 of the receiver 201. Incidentally, this use start signal includes ID of the SAM of the equipment requiring the use start (in this case, ID of the SAM 212 of the receiver 201).

[0241] At step S403, the receiver 201 receives and stores the delivery key Kd (Fig. 8) for January, upper limit amount of billing at the time of temporal registration, ID of the user A, password of the user A, and user general information written in the registration form at step S401, which are transmitted from the EMD service center 1 when it is temporarily registered in the EMD system (hereinafter, in the case where it is not necessary to respectively distinguish these pieces of information from one another, the information transmitted from the EMD service center 1 at this time will be referred to as temporal registration information). Specifically, before the information transmitted from the EMD service center 1 is received, mutual authentication between the mutual authentication module 221 of the receiver 201 and the mutual authentication portion 17 of the EMD service center 1 is carried out, and the temporal key Ktemp is owned in common. The information from the EMD service center 1, received through the communication portion 211 of the receiver 201, is decrypted by the decrypting/encrypting module 224 and by the temporal key Ktemp commonly owned by the EMD service center 1, and is outputted to the storage module 223 to be stored.

[0242] By this, in the storage module 223 of the receiver 201, as shown in Fig. 49, the delivery key Kd for January is stored. At this time, in the reference information 201 stored in the storage module 223, as shown in Fig. 50, in addition to the information (Fig. 37) stored before this processing, "upper limit amount at temporal registration" is set in the [upper limit amount of billing], and the user general information of the user A, the ID of the user A, and the password are set in the [settlement user information]. Incidentally, in the case of this example, since the user A applies registration while only the name, birth date, and age are permitted to be made open, the information of the user A is stored in the [name], [birth date], and [age] of the reference information 201 under the condition that the exhibition is permitted. Incidentally, in the example of Fig. 50, in the drawing, the information displayed with a shadow indicates that its exhibition is not permitted, and the information displayed without a shadow indicates that its exhibition is permitted.

[0243] Next, at step S404, the receiver 201 receives

and stores the delivery key Kd for March, upper limit amount of billing at the time of formal registration, and settlement ID of the user A, which are transmitted from the EMD service center 1 at the time of formal registration in the EMD system (hereinafter, in the case where it is not necessary to respectively distinguish these pieces of information transmitted from the EMD service center 1 at this time, the whole will be referred to as formal registration information). Since the specific processing here is similar to the case at step S403, the description is omitted. By this, in the storage module 223 of the receiver 201, as shown in Fig. 51, instead of the delivery key Kd for January in the information (Fig. 49) stored prior to this processing, the delivery key Kd for March is stored, and in the reference information 201, as shown in Fig. 52, "upper limit amount at the time of formal registration" is set in the [upper limit amount of billing], and the settlement ID of the user A is newly set in the [settlement ID].

[0244] In the manner as described above, the receiver 201 is registered in the EMD system while the user A is made the settlement user. By this, it becomes possible for the user A to use the contents in the receiver 201.

[0245] Next, a processing procedure of the EMD service center 1 in the case of executing the foregoing processing (processing in which the receiver 201 is registered in the EMD system while the user A is made the settlement user) will be described with reference to the flowchart of Fig. 53.

[0246] At step S411, when a management company for managing the EMD service center 1 receives the registration form (step S401 of Fig. 47) sent by the user A, it inputs the content to the EMD service center 1. By this, in the [settlement user information], corresponding to the ID of the SAM 212 of the receiver 201, in the system registration information held by the user management portion 18 of the EMD service center 1, as shown in Fig. 54, the user general information of the user A (name, address, telephone number, information of settlement agency, birth date, age, and gender) is stored.

[0247] In the case of this example, since the user A enters the information in the registration form while only the name, birth date, and age are permitted to be made open, those pieces of information are stored as information permitted to be made open (in the drawing, without a shadow).

[0248] At step S412, a registration processing through credit investigation is started. The details of the registration processing through this credit investigation are shown in the flowchart of Fig. 55. That is, at step S421, the receipts and disbursements portion 20 of the EMD service center 1 communicates, for example, with the settlement agency of the user A on the basis of the information of the name, address, telephone number, and settlement agency of the user A entered in the registration form, and starts the credit investigation processing to the user A.

[0249] At step S422, the user management portion 18 of the EMD service center 1 judges whether the use start signal (step S402 of Fig. 47) transmitted from the receiver 201 is received or not, and in the case where it is judged that the signal is received, the procedure proceeds to step S423, and it is judged whether the credit investigation processing started at step S421 is completed or not.

[0250] In the case where it is judged at step S423 that the credit investigation processing is not completed, the procedure proceeds to step S424, the user management portion 18 of the EMD service center 1 assigns the ID and password of the user A, and sets those as information not permitted to be made open, as shown in Fig. 56, in the [settlement user information] corresponding to the ID of the SAM 212 of the system registration information, and transmits them, together with the delivery key Kd for January prepared by the key server 14 and the information indicating the upper limit amount of billing at the time of temporal registration, to the receiver 201. The receiver 201 receives them (step S403 of Fig. 47). In the case of this example, the temporal registration information is transmitted to the receiver 201 in several hours from the time when the EMD service center 1 received the use start signal.

[0251] Next, at step S425, the user management portion 18 of the EMD service center 1 waits until the credit investigation processing started at step S421 is completed, and when the credit investigation processing is completed, the procedure proceeds to step S426, and on the basis of the result of the credit investigation processing, it is judged whether the receiver 201 can be formally registered in the EMD system.

[0252] At step S426, in the case where it is judged that the receiver 201 can be formally registered in the EMD system, the user management portion 18 of the EMD service center 1 proceeds to step S427, assigns the settlement ID to the user A, and after setting it, as one not permitted to be made open, in the [settlement ID] corresponding to the ID of the SAM 212 in the system registration information as shown in Fig. 57, the user management portion transmits it to the receiver 201, together with the delivery key Kd for March prepared by the key server 14 and the information indicating the upper limit amount of billing at the time of formal registration. The receiver 201 receives them (step S404 of Fig. 47). Incidentally, in the case of this example, the credit investigation processing started at step S401 is completed in about one week. That is, the formal registration information is transmitted to the receiver 201 after one week has passed since the registration form was sent to the management company.

[0253] At step S422, in the case where it is judged that the use start signal is not received, the procedure proceeds to step S428, and it is judged whether the credit investigation processing is completed. In the case where it is judged that the credit investigation process-

ing is not completed, the processing returns to step S422, and the subsequent processing is carried out.

[0254] At step S428, in the case where it is judged that the credit investigation processing is completed, that is, in the case where the credit investigation processing is completed before the use start signal is received, or at step S423, in the case where it is judged that the credit investigation processing is completed, that is, in the case where the credit investigation processing is completed before the temporal registration information is transmitted, the procedure proceeds to step S429.

[0255] At step S429, the user management portion 18 of the EMD service center 1 assigns the ID, password, and settlement ID of the user A, and sets them in the [settlement user information] corresponding to the ID of the SAM 212, and then, transmits them to the receiver 201, together with the delivery key Kd for March prepared by the key server 14, the information indicating the upper limit amount of billing at the time of formal registration, and the user general information. Incidentally, in the case corresponding to the processing shown in the flowchart of Fig. 47, after the temporal registration information is transmitted to the receiver 201, the credit investigation processing is completed.

[0256] At step S426, in the case where it is judged that the receiver 201 is not formally registered in the EMD system, the processing at step S427 is skipped, and the processing is ended. Incidentally, at this time, at step S424, the user ID, password, and user general information set in the system registration information are deleted.

[0257] In this way, after purchasing the receiver 201, the user A becomes possible to use the contents in several hours.

[0258] Next, a processing procedure in the case where billing is settled will be described with reference to the flowchart of Fig. 58. In the case of this example, a description will be made on, as an example, a case where billing added up in the receiver 51 is settled.

[0259] That is, at step S501, mutual authentication between the receiver 51 and the EMD service center 1 is carried out. Since this mutual authentication is the same processing as the case where the description has been made with reference to Figs. 40 to 42, its description is omitted.

[0260] Next, at step S502, the SAM 62 of the receiver 51 transmits a certificate to the user management portion 18 of the EMD service center 1. At step S503, the SAM 62 of the receiver 51 encrypts the billing information stored in the storage module 73 by the temporal key Ktemp commonly owned by the EMD service center 1 at step S501, and transmits it to the EMD service center 1, together with the version of the delivery key Kd, the corresponding UCP and PT stored in the HDD 52, and the registration list.

[0261] At step S504, the user management portion 18 of the EMD service center 1 receives the information transmitted from the receiver 51 at step S503, and decrypts it, and then, the user management portion 18 of the EMD service center 1 confirms whether an unfair act by which "stop" is set in the [state flag] of the registration list exists in the receiver 51.

[0262] At step S505, the billing charging portion 19 of the EMD service center 1 analyzes the billing information received at step S503, and carries out processing of calculating the payment sum of the user (for example, user F) and the like. Next, at step S506, the user management portion 18 confirms whether the settlement was successful by the processing at step S505.

[0263] Next, at step S507, the user management portion 18 of the EMD service center 1 sets the registration conditions of the receiver 51 on the basis of the confirmation result at step S504 and the confirmation result at step S506, and attaches a signature to them and prepares a registration list of the receiver 51.

[0264] For example, at step S504, in the case where an unfair act is confirmed, "stop" is set in the [state flag], and in this case, after this, all processing is stopped. That is, it becomes impossible to receive any service from the EMD system. At step S506, in the case where it is confirmed that the settlement was not successful, "with limitation" is set in the [state flag], and in this case, although the processing of reproducing the contents already purchased is made possible, it becomes impossible to execute processing of newly purchasing contents.

[0265] Next, the procedure proceeds to step S508, and the user management portion 18 of the EMD service center 1 encrypts the delivery key Kd of the newest version (delivery key Kd of the newest version for March) by the temporal key Ktemp, and transmits it, together with the registration list prepared at step S507, to the receiver 51.

[0266] At step S509, the SAM 62 of the receiver 51 receives the delivery key Kd and the registration list transmitted from the EMD service center 1 through the communication portion 61, and after decrypting them, the SAM stores them in the storage module 73. At this time, the billing information stored in the storage module 73 is erased, and the registration list and the delivery key Kd are renewed.

[0267] This processing is started in the case where the billing added up exceeds a predetermined upper limit amount (upper limit amount at the time of formal registration or upper limit amount at the time of temporal registration), or in the case where the version of the delivery key Kd becomes old, and for example, at step S247 of Fig. 45, it becomes impossible to decrypt the content key Kco (encrypted by the delivery key Kd) (in the case where it becomes impossible to receive the service provider secure container).

[0268] Next, marketing information provided by the EMD service center 1 will be described. As described above, when the billing is settled, the billing information is transmitted to the EMD service center 1 (step S503),

and is stored in the history data management portion 15 of the EMD service center 1. That is, the EMD service center 1 includes information (for example, ID of contents, content information, user general information of the user purchasing the contents) relating to the purchased contents, so-called marketing information.

[0269] Fig. 59 shows information which can be made open to the content provider 2, the service provider 3, or the user home network 5, in the information owned by the EMD service center 1 and relating to the purchased contents. In the case of this example, the ID of contents, content information, use format, and selling price (use price) in which "open" is correspondingly shown in the drawing, are made open (provided) to the content provider 2, the service provider 3, and the user home network 5 particularly with no registration. Incidentally, the ID of contents, content information, and use format are information included in the billing information, and the selling price is information specified by the ID of UCP included in the billing information, the ID of use content, and the ID of PT and read out from the price content of the PT.

[0270] In the drawing, the name, address, telephone number, birth date, age, and gender of the user purchasing the contents, in which "required" is correspondingly indicated in the drawing, are information read out from the system registration information managed by the user management portion 18 of the EMD service center 1, and in the case where the exhibition is permitted by the user, those are made open to the content provider 2, the service provider 3, or the user home network 5. That is, in this example, the name, address, telephone number, birth date, age, and gender of the user F are made open. Besides, the name, birth date, and age of the user A are made open.

[0271] The EMD service center 1 can provide the pieces of information of Fig. 59 separately to the content provider 2, the service provider 3, and the user home network 5, and can also provide information of the total of these pieces of information as shown in Figs. 60 to 62.

[0272] Fig. 60 is a bar graph showing singers (artists) of contents used in a predetermined period in decreasing order of use count. Fig. 61 is a bar graph showing use formats of predetermined contents (contents S) in decreasing order of use count. Fig. 62 is a bar graph showing a use count of users (purchasers) of predetermined contents (contents S) in respective age. The added up information shown in Figs. 60 to 62 is provided to the content provider 2, the service provider 3, and the user home network 5 in response to the request. For example, the user can get these pieces of information by using a password.

[0273] Fig. 63 is a bar graph showing a sales state of each content server 2 in a predetermined period. Such information added up for every content provider 2 is provided to the content provider 2 in response to the request. Fig. 64 is a bar graph showing a sales state of each service provider 3 in a predetermined period. Such information added up for every service provider 3 is provided to the service provider 3 in response to the request.

[0274] Incidentally, in the present specification, a system is defined as the whole of an apparatus constituted by a plurality of devices.

[0275] As a providing medium for providing a computer program for carrying out the foregoing processing to the user, in addition to a recording medium such as a magnetic disk, a CD-ROM, or a solid memory, a communication medium such as a network or a satellite can also be used.

[0276] As described above, according to the information processing apparatus of the first aspect, the information processing method of the second aspect, and the providing medium of the third aspect, billing information including the ID of the information processing apparatus is transmitted to the management apparatus, so that marketing information corresponding to the settlement result can be received.

[0277] According to the management apparatus of the fourth aspect, the management method of the sixth aspect, and the providing medium of the eighth aspect, billing information including the ID of the information processing apparatus is received and the settlement processing is carried out, so that marketing information corresponding to the settlement result can be made open

[0278] In so far as the embodiments of the invention described above are implemented, at least in part, using software-controlled data processing apparatus, it will be appreciated that a computer program providing such software control and a storage medium by which such a computer program is stored are envisaged as aspects of the present invention.

Claims

1. An information processing apparatus managed by a management apparatus and using encrypted valuable information through decrypting, comprising:

   preparation means for preparing billing information including its own ID and needed to settle billing of the valuable information;
   transmission means for transmitting the billing information prepared by the preparation means to the management apparatus; and
   reception means for receiving predetermined marketing information corresponding to a settlement result based on the billing information transmitted by the transmission means and transmitted from the management apparatus.

2. An information processing method of an information processing apparatus managed by a management apparatus and using encrypted valuable

information through decrypting, comprising:

a preparation step of preparing billing information including its own ID and needed to settle billing of valuable information;
a transmission step of transmitting the billing information prepared in the preparation step to the management apparatus; and
a reception step of receiving predetermined marketing information corresponding to a settlement result based on the billing information transmitted in the transmission step and transmitted from the management apparatus.

3. A providing medium for providing a computer readable program for making an information processing apparatus, which is managed by a management apparatus and uses encrypted valuable information through decrypting, execute a process comprising:

a preparation step of preparing billing information including its own ID and needed to settle billing of valuable information;
a transmission step of transmitting the billing information prepared in the preparation step to the management apparatus; and
a reception step of receiving predetermined marketing information corresponding to a settlement result based on the billing information transmitted in the transmission step and transmitted from the management apparatus.

4. A management apparatus for managing an information processing apparatus using encrypted valuable information through decrypting, comprising:

storage means for storing predetermined marketing information as to the information processing apparatus correspondingly to an ID of the information processing apparatus;
settlement means for receiving billing information transmitted from the information processing apparatus and including the ID of the information processing apparatus and for settling billing due to the valuable information on the basis of the billing information;
readout means for reading the marketing information as to the information processing apparatus stored in the storage means correspondingly to the ID of the information processing apparatus included in the billing information; and
first exhibition means for exhibiting the marketing information read out by the readout means to the information processing apparatus correspondingly to a settlement result by the settlement means.

5. A management apparatus according to claim 4, wherein the management apparatus is connected to a valuable information providing device for providing the valuable information, and to a service providing device for providing predetermined service correspondingly to the valuable information, and

the management apparatus further comprises second exhibition means for exhibiting the marketing information corresponding to the settlement result by the settlement means to the valuable information providing device and the service providing device.

6. A management method of a management apparatus for managing an information processing apparatus using encrypted valuable information through decrypting, comprising:

a storage step of storing predetermined marketing information as to the information processing apparatus correspondingly to an ID of the information processing apparatus;
a settlement step of receiving billing information transmitted from the information processing apparatus and including the ID of the information processing apparatus, and of settling billing due to the valuable information on the basis of the billing information;
a readout step of reading the marketing information as to the information processing apparatus stored in the storage step correspondingly to the ID of the information processing apparatus included in the billing information; and
a first exhibition step of exhibiting the marketing information read out in the readout step to the information processing apparatus correspondingly to a settlement result in the settlement step.

7. A management method according to claim 6, wherein the management apparatus is connected to a valuable information providing device for providing the valuable information and to a service providing device for providing predetermined service correspondingly to the valuable information; and

the method further comprises a second exhibition step for exhibiting the marketing information corresponding to the settlement result in the settlement step to the valuable information providing device and the service providing device.

8. A providing medium for providing a computer readable program for making a management apparatus, which manages an information processing appara-

tus using encrypted valuable information through decrypting, execute a process comprising:

a storage step of storing predetermined marketing information as to the information processing apparatus correspondingly to an ID of the information processing apparatus;
a settlement step of receiving billing information transmitted from the information processing apparatus and including the ID of the information processing apparatus, and of settling billing due to the valuable information on the basis of the billing information;
a readout step of reading the marketing information as to the information processing apparatus stored in the storage step correspondingly to the ID of the information processing apparatus included in the billing information; and
a first exhibiting step of exhibiting the marketing information read out in the readout step to the information processing apparatus correspondingly to a settlement result in the settlement step.

9. A providing medium according to claim 8, wherein the management apparatus is connected to a valuable information providing device for providing the valuable information, and to a service providing device for providing predetermined service correspondingly to the valuable information, and

the process further comprises a second exhibition step of exhibiting the marketing information corresponding to the settlement result in the settlement step to the valuable information providing device and the service providing device.

FIG. 1

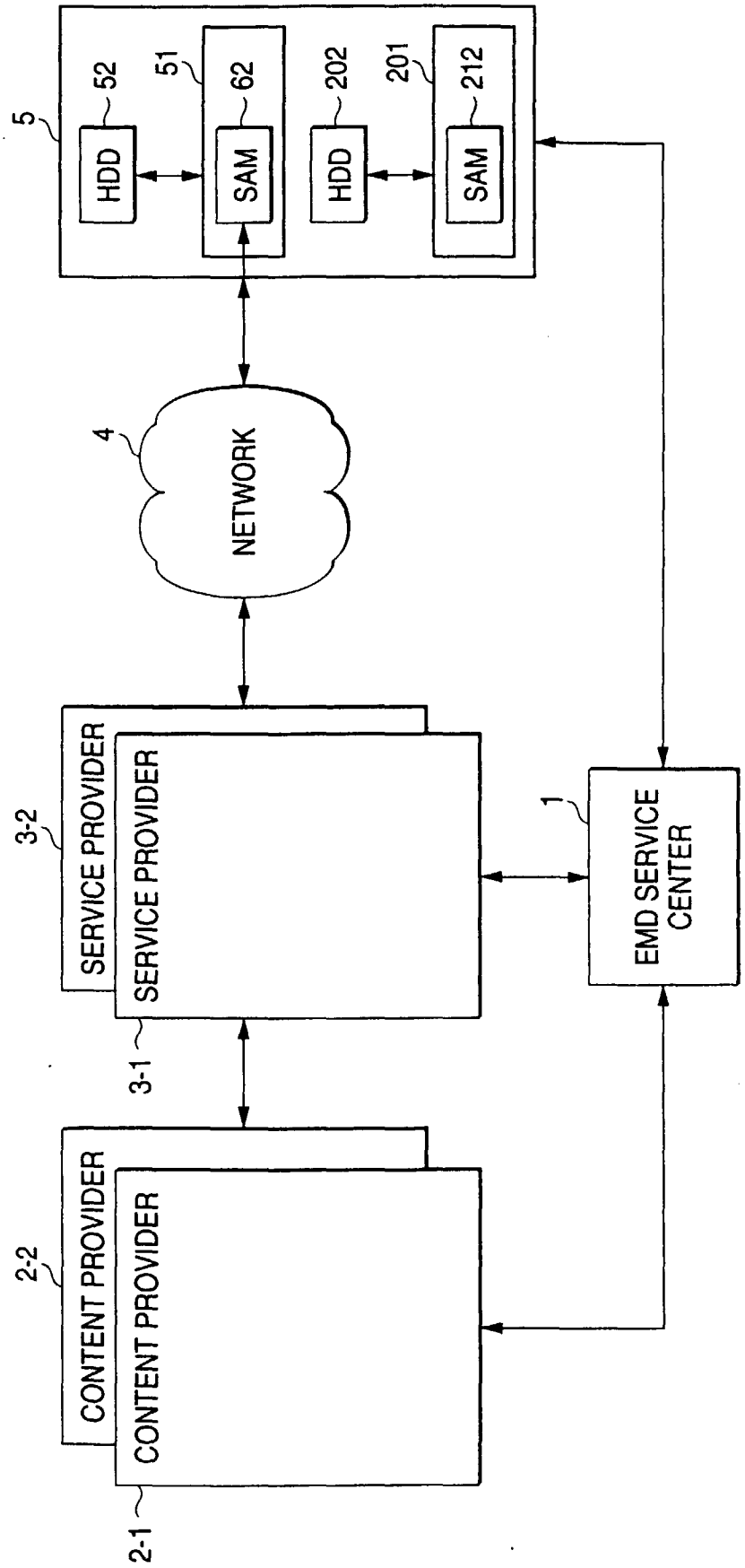

5
52
HDD
51
62
SAM
202
HDD
201
212
SAM
4
NETWORK
3-2
SERVICE PROVIDER
SERVICE PROVIDER
3-1
1
EMD SERVICE CENTER
2-2
CONTENT PROVIDER
CONTENT PROVIDER
2-1

FIG. 2

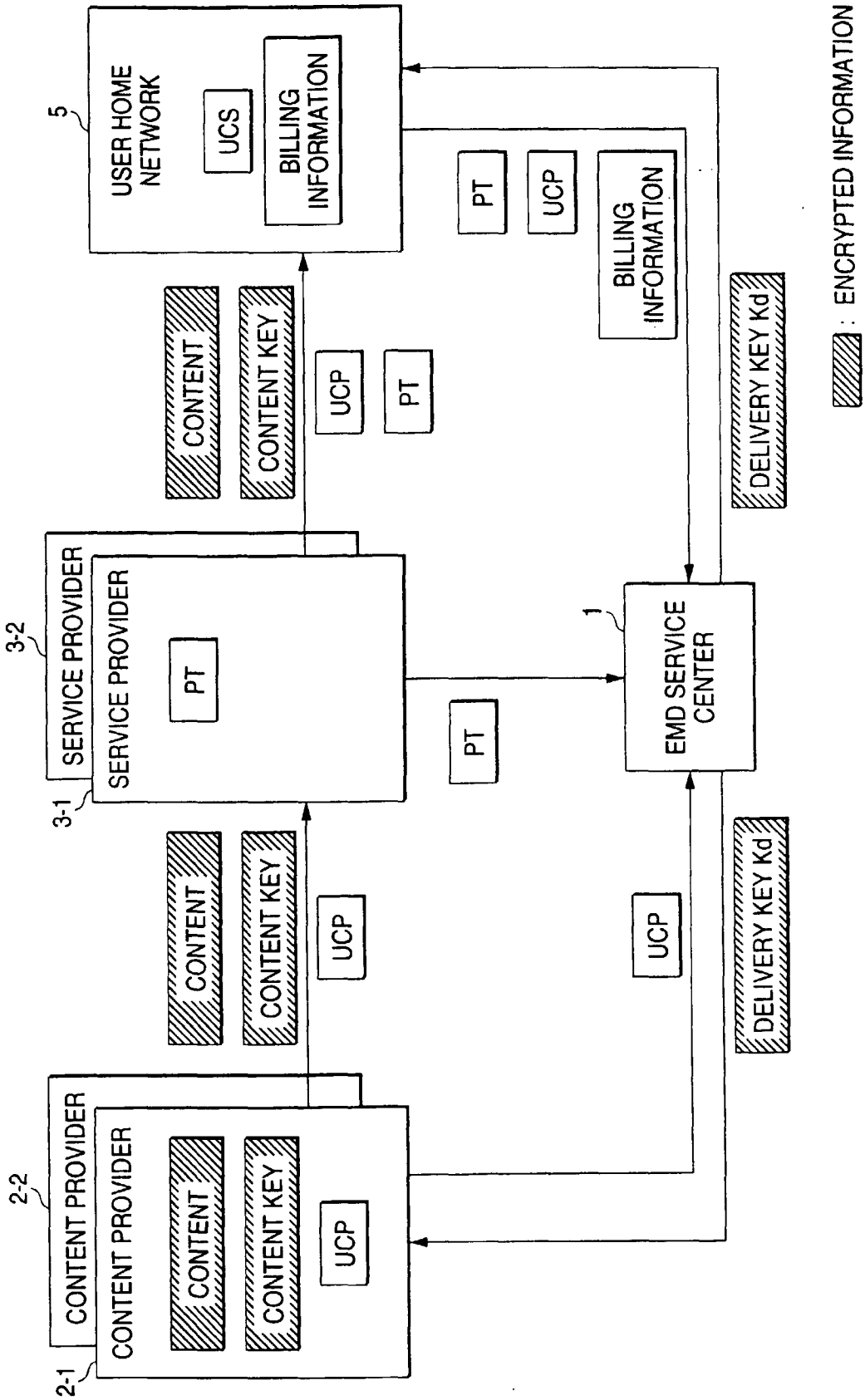

5
USER HOME NETWORK
UCS
BILLING INFORMATION
PT
UCP
BILLING INFORMATION
CONTENT
CONTENT KEY
UCP
PT
DELIVERY KEY Kd
: ENCRYPTED INFORMATION
3-2
SERVICE PROVIDER
SERVICE PROVIDER
PT
3-1
1
EMD SERVICE CENTER
PT
CONTENT
CONTENT KEY
UCP
UCP
DELIVERY KEY Kd
2-2
CONTENT PROVIDER
CONTENT PROVIDER
CONTENT
CONTENT KEY
UCP
2-1

FIG. 3

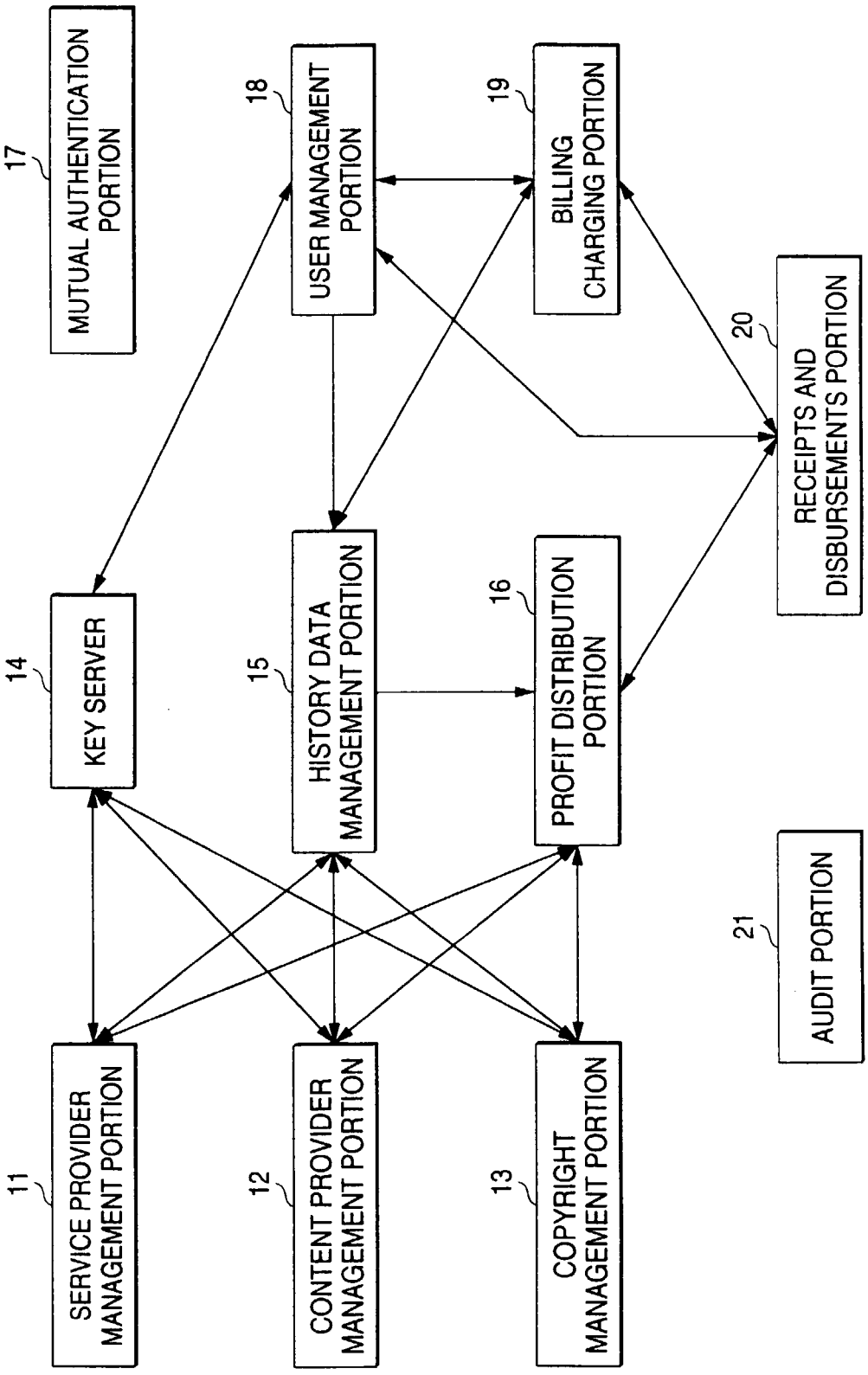

MUTUAL AUTHENTICATION PORTION
17
USER MANAGEMENT PORTION
18
BILLING CHARGING PORTION
19
RECEIPTS AND DISBURSEMENTS PORTION
20
KEY SERVER
14
HISTORY DATA MANAGEMENT PORTION
15
PROFIT DISTRIBUTION PORTION
16
AUDIT PORTION
21
SERVICE PROVIDER MANAGEMENT PORTION
11
CONTENT PROVIDER MANAGEMENT PORTION
12
COPYRIGHT MANAGEMENT PORTION
13

FIG. 4

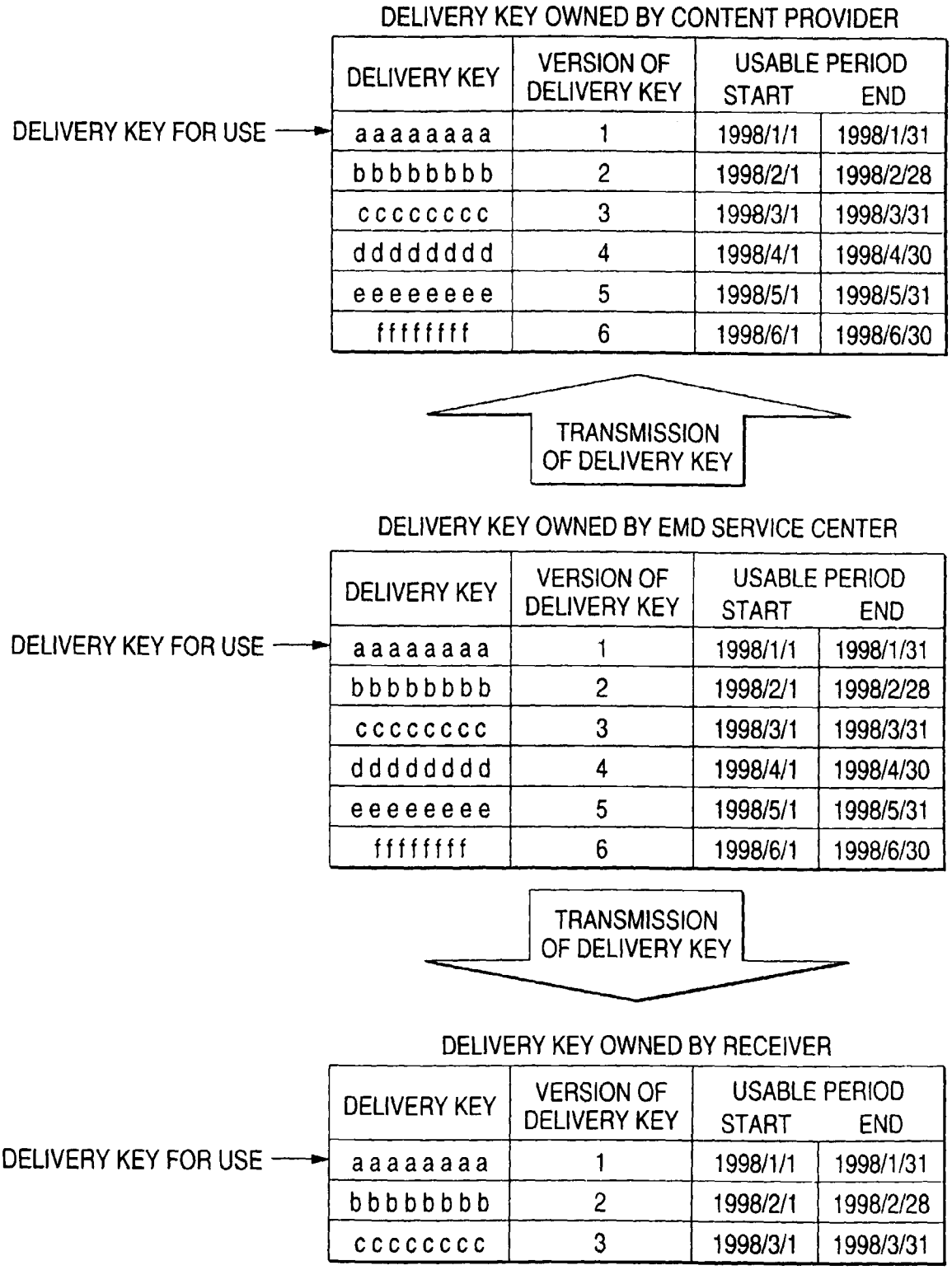

DELIVERY KEY OWNED BY CONTENT PROVIDER
DELIVERY KEY
VERSION OF DELIVERY KEY
USABLE PERIOD START
END
DELIVERY KEY FOR USE
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
TRANSMISSION OF DELIVERY KEY
DELIVERY KEY OWNED BY EMD SERVICE CENTER
DELIVERY KEY
VERSION OF DELIVERY KEY
USABLE PERIOD START
END
DELIVERY KEY FOR USE
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
TRANSMISSION OF DELIVERY KEY
DELIVERY KEY OWNED BY RECEIVER
DELIVERY KEY
VERSION OF DELIVERY KEY
USABLE PERIOD START
END
DELIVERY KEY FOR USE
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31

FIG. 5

DELIVERY KEY OWNED BY CONTENT PROVIDER

DELIVERY KEY	VERSION OF DELIVERY KEY	USABLE PERIOD START	USABLE PERIOD END
DELIVERY KEY FOR USE → bbbbbbbb	2	1998/2/1	1998/2/28
cccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31
ffffffff	6	1998/6/1	1998/6/30
gggggggg	7	1998/7/1	1998/7/31

TRANSMISSION OF DELIVERY KEY

DELIVERY KEY OWNED BY EMD SERVICE CENTER

DELIVERY KEY	VERSION OF DELIVERY KEY	USABLE PERIOD START	USABLE PERIOD END
aaaaaaaa	1	1998/1/1	1998/1/31
DELIVERY KEY FOR USE → bbbbbbbb	2	1998/2/1	1998/2/28
cccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31
ffffffff	6	1998/6/1	1998/6/30
gggggggg	7	1998/7/1	1998/7/31

TRANSMISSION OF DELIVERY KEY

DELIVERY KEY OWNED BY RECEIVER

DELIVERY KEY	VERSION OF DELIVERY KEY	USABLE PERIOD START	USABLE PERIOD END
DELIVERY KEY FOR USE → bbbbbbbb	2	1998/2/1	1998/2/28
cccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30

FIG. 6

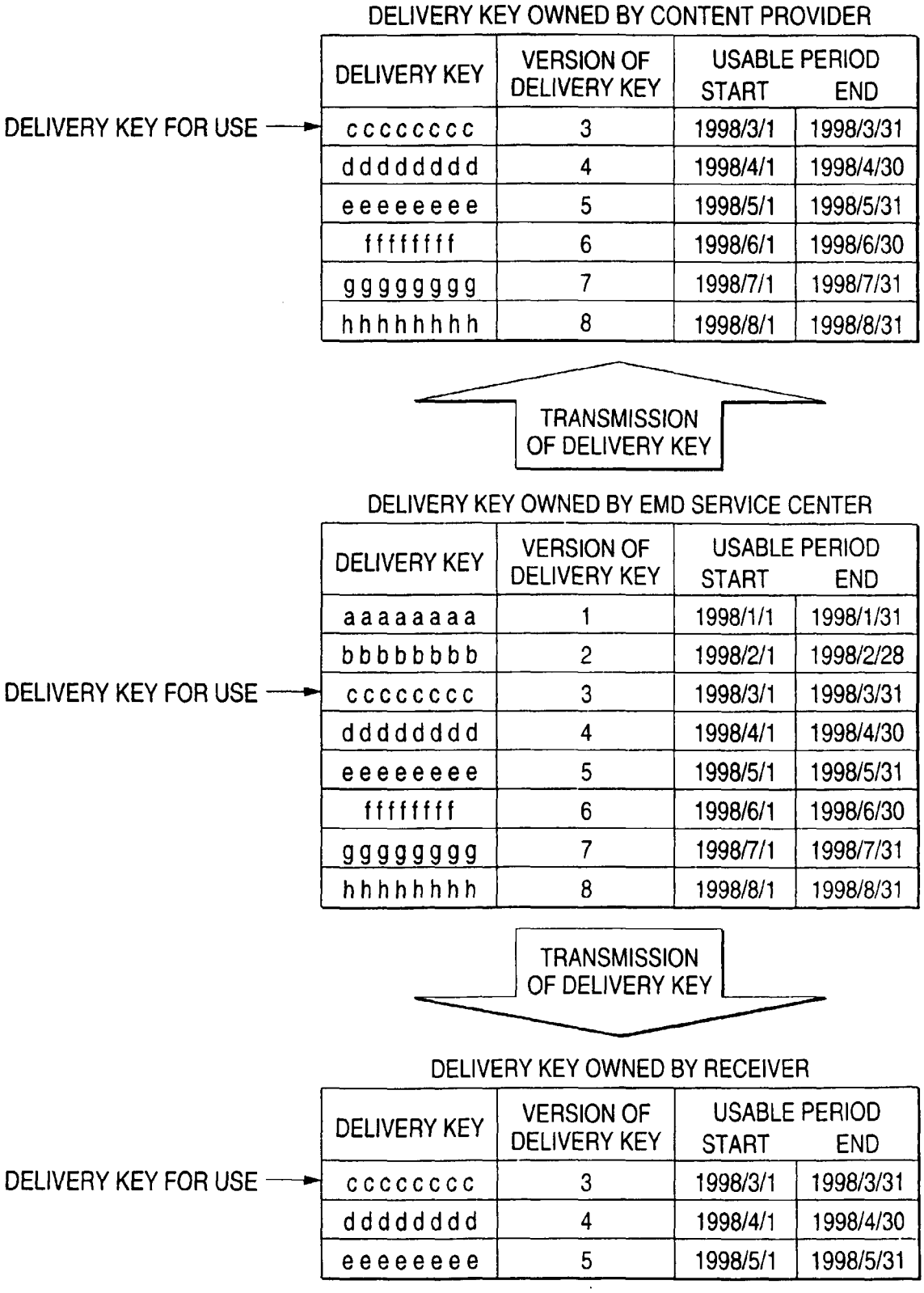

DELIVERY KEY OWNED BY CONTENT PROVIDER
DELIVERY KEY
VERSION OF DELIVERY KEY
USABLE PERIOD START
END
DELIVERY KEY FOR USE
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
TRANSMISSION OF DELIVERY KEY
DELIVERY KEY OWNED BY EMD SERVICE CENTER
DELIVERY KEY
VERSION OF DELIVERY KEY
USABLE PERIOD START
END
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
DELIVERY KEY FOR USE
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
TRANSMISSION OF DELIVERY KEY
DELIVERY KEY OWNED BY RECEIVER
DELIVERY KEY
VERSION OF DELIVERY KEY
USABLE PERIOD START
END
DELIVERY KEY FOR USE
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31

FIG. 7

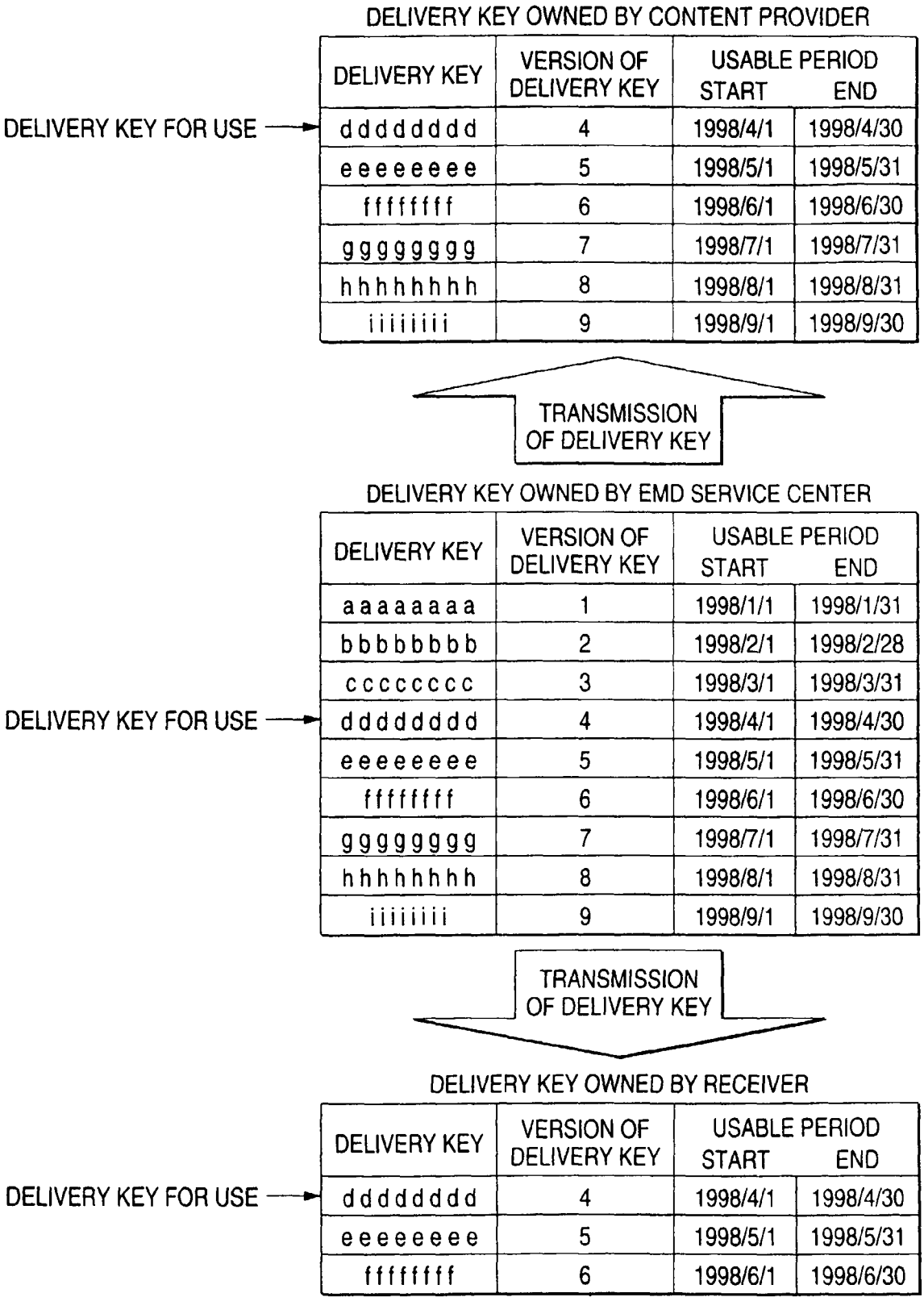

DELIVERY KEY OWNED BY CONTENT PROVIDER
DELIVERY KEY
VERSION OF DELIVERY KEY
USABLE PERIOD START
END
DELIVERY KEY FOR USE
ddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiii 9 1998/9/1 1998/9/30
TRANSMISSION OF DELIVERY KEY
DELIVERY KEY OWNED BY EMD SERVICE CENTER
DELIVERY KEY
VERSION OF DELIVERY KEY
USABLE PERIOD START
END
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
DELIVERY KEY FOR USE
ddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiii 9 1998/9/1 1998/9/30
TRANSMISSION OF DELIVERY KEY
DELIVERY KEY OWNED BY RECEIVER
DELIVERY KEY
VERSION OF DELIVERY KEY
USABLE PERIOD START
END
DELIVERY KEY FOR USE
ddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30

FIG. 8

TEMPORAL DELIVERY KEY Kd

DELIVERY KEY	VERSION OF DELIVERY KEY	USABLE PERIOD	
		START	END
aaaaaaaaaa	1	1998/1/1	1998/1/31

FIG. 9

SYSTEM REGISTRATION INFORMATION

ID OF SAM		ID OF SAM 62	ID OF SAM 212
EQUIPMENT NUMBER		EQUIPMENT NUMBER (NO. 100) OF RECEIVER 51	EQUIPMENT NUMBER (NO. 100) OF RECEIVER 201
SETTLEMENT ID		SETTLEMENT ID OF USER F	
SETTLEMENT USER INFORMATION	NAME	NAME OF USER F	
	ADDRESS	ADDRESS OF USER F	
	TELEPHONE NUMBER	TELEPHONE NUMBER OF USER F	
	SETTLEMENT AGENCY INFORMATION	SETTLEMENT AGENCY INFORMATION OF USER F	
	BIRTH DATE	BIRTH DATE OF USER F	
	AGE	AGE (21) OF USER F	
	GENDER	GENDER (MALE) OF USER F	
	ID OF USER	ID OF USER F	
	PASSWORD	PASSWORD OF USER F	
SUBORDINATE USER INFORMATION	NAME	NAME OF USER F	
	ADDRESS	ADDRESS OF USER F	
	TELEPHONE NUMBER	TELEPHONE NUMBER OF USER F	
	BIRTH DATE	BIRTH DATE OF USER F	
	GENDER	GENDER (MALE) OF USER F	
	ID OF USER	ID OF USER F	
	PASSWORD	PASSWORD OF USER F	
⋮			
USE POINT INFORMATION		USE POINT INFORMATION OF RECEIVER 51	

▨ INFORMATION WHICH IS NOT PERMITTED TO BE MADE OPEN
□ INFORMATION WHICH IS PERMITTED TO BE MADE OPEN

FIG. 10

USE POINT INFORMATION

USER	PROVIDER	USE POINT
SETTLEMENT USER	CONTENT PROVIDER 2-1	222 POINTS
	CONTENT PROVIDER 2-2	123 POINTS
	SERVICE PROVIDER 3-1	345 POINTS
	SERVICE PROVIDER 3-2	0 POINT

FIG. 11

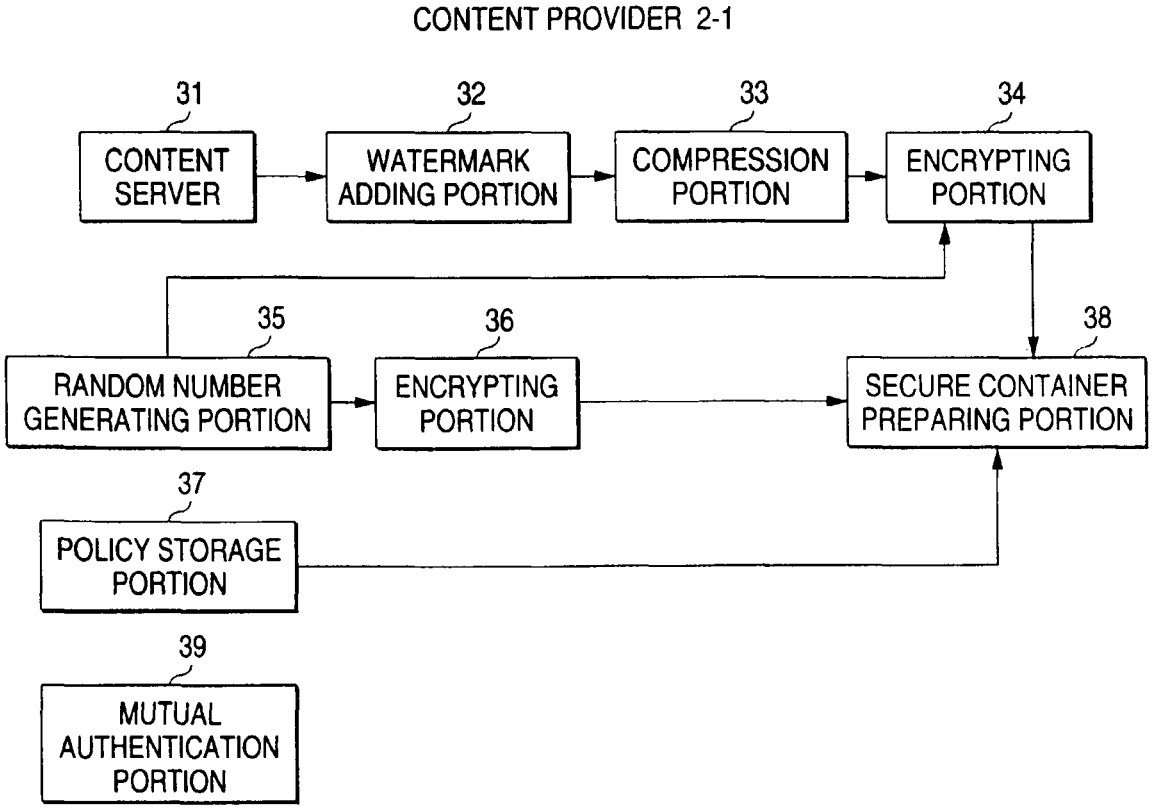


FIG. 12A

UCPA

ID OF CONTENT	ID OF CONTENT A	
CONTENT INFORMATION	CONTENT INFORMATION OF CONTENT A	
ID OF CONTENT PROVIDER	ID OF CONTENT PROVIDER 2-1	
ID OF UCP	ID OF UCPA	
EFFECTIVE PERIOD OF UCPA	EFFECTIVE PERIOD OF UCPA	
USE CONDITION 10	USER CONDITION 10	200 POINTS OR MORE
	EQUIPMENT CONDITION 10	NO CONDITION
USE CONDITION 11	ID 11	ID OF USE CONTENT 11
	FORMAT 11	PURCHASED REPRODUCTION
	PARAMETER 11	x x x x
	MANAGEMENT MOVEMENT PERMISSIBLE INFORMATION 11	PERMISSIBLE
USE CONDITION 12	ID 12	ID OF USE CONTENT 12
	FORMAT 12	FIRST GENERATION COPY
	PARAMETER 12	x x x x
	MANAGEMENT MOVEMENT PERMISSIBLE INFORMATION 12	IMPERMISSIBLE
USE CONDITION 13	ID 13	ID OF USE CONTENT 13
	FORMAT 13	REPRODUCTION WITH LIMITED PERIOD
	PARAMETER 13	x x x x
	MANAGEMENT MOVEMENT PERMISSIBLE INFORMATION 13	IMPERMISSIBLE
USE CONDITION 14	ID 14	ID OF USE CONTENT 14
	FORMAT 14	PAY PER COPY 5
	PARAMETER 14	COPYING 5 TIMES
	MANAGEMENT MOVEMENT PERMISSIBLE INFORMATION 14	IMPERMISSIBLE

FIG. 12B

UCPB

ID OF CONTENT	ID OF CONTENT A	
CONTENT INFORMATION	CONTENT INFORMATION OF CONTENT A	
ID OF CONTENT PROVIDER	ID OF CONTENT PROVIDER 2-1	
ID OF UCP	ID OF UCPB	
EFFECTIVE PERIOD OF UCP	EFFECTIVE PERIOD OF UCPB	
USE CONDITION 20	USER CONDITION 20	LESS THAN 200 POINTS
	EQUIPMENT CONDITION 20	NO CONDITION
USE CONDITION 21	ID 21	ID OF USE CONTENT 21
	FORMAT 21	PAY PER PLAY 4
	PARAMETER 21	REPRODUCTION 4 TIMES
	MANAGEMENT MOVEMENT PERMISSIBLE INFORMATION 21	IMPERMISSIBLE
USE CONDITION 22	ID 22	ID OF USE CONTENT 22
	FORMAT 22	PAY PER COPY 2
	PARAMETER 22	COPYING 2 TIMES
	MANAGEMENT MOVEMENT PERMISSIBLE INFORMATION 22	IMPERMISSIBLE

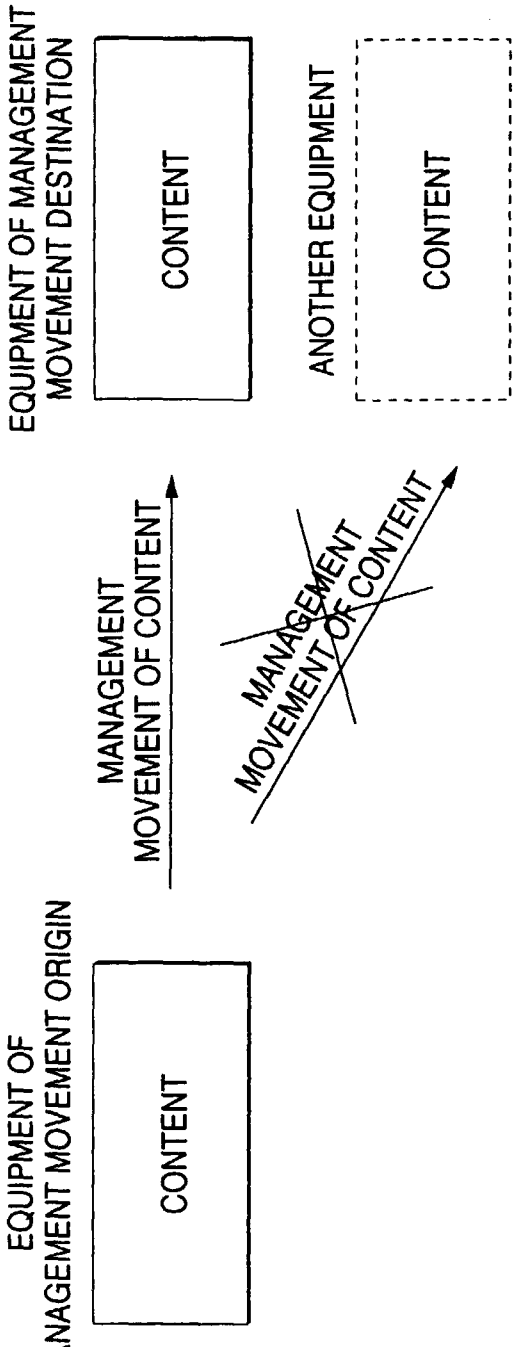


FIG. 13A

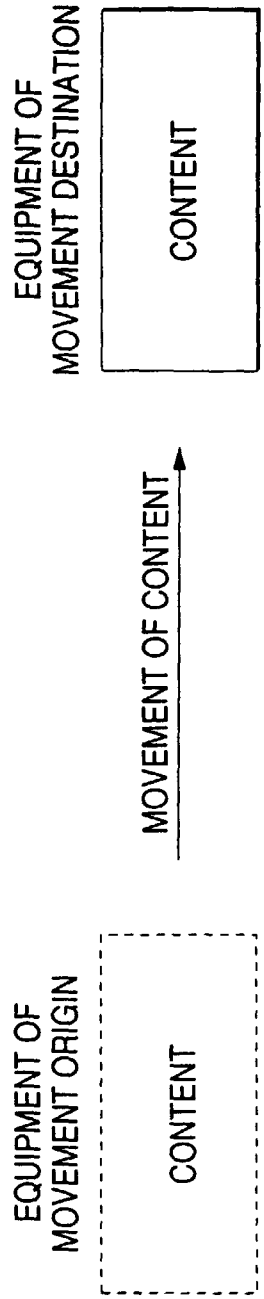


FIG. 13B

FIG. 14B

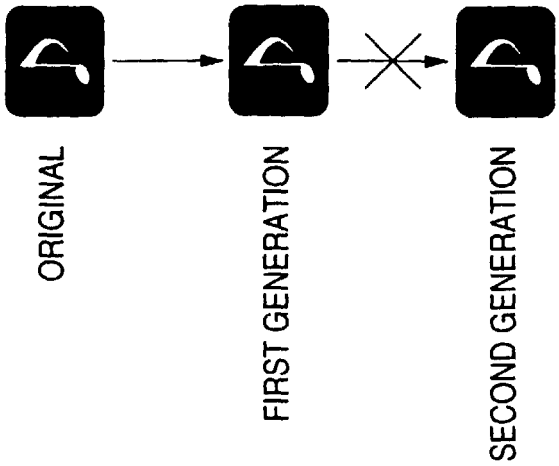


FIG. 14A

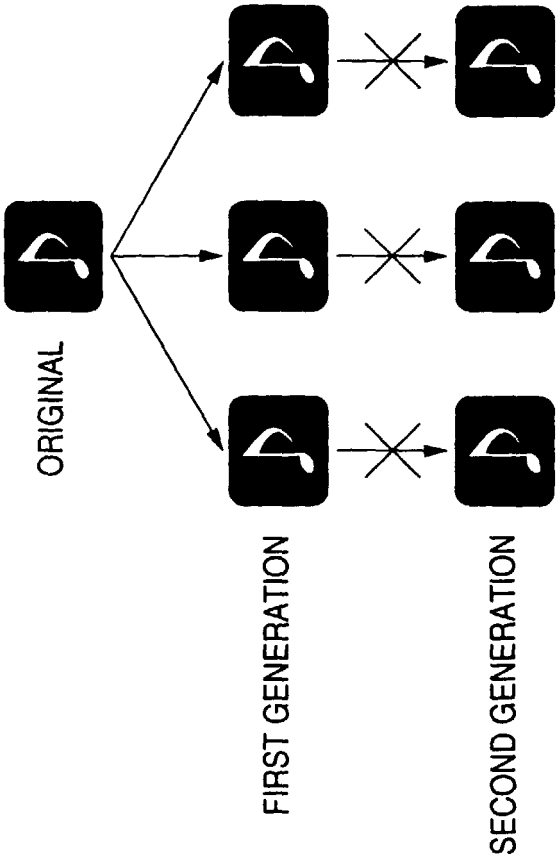


FIG. 15A

SERVICE CODE	MEANING
0000h	NO CONDITION
0001h TO 00FFh	WITH CONDITION AS TO EQUIPMENT
0100h TO 01FFh	WITH GENDER CONDITION
0200h TO 02FFh	WITH AGE CONDITION
0300h TO 7FFFh	WITH ANOTHER CONDITION
8000h TO FFFFh	WITH CONDITION AS TO USE POINT

FIG. 15B

CONDITION CODE	MEANING
00h	NO CONDITION
01h	=
02h	≠
03h	< (LESS THAN)
04h	> (LARGER THAN)
05h	≤ (NOT LARGER THAN)
06h	≥ (NOT LESS THAN)
07h TO FFh	VACANT

FIG. 16A

USE CONDITION 10 OF UCPA

USER CONDITION 10	SERVICE CODE	VALUE CODE	CONDITION CODE
	80 x x h	0000C8h	06h
EQUIPMENT CONDITION 10	SERVICE CODE	VALUE CODE	CONDITION CODE
	0000h	FFFFFFh	00h

FIG. 16B

USE CONDITION 20 OF UCPB

USER CONDITION 20	SERVICE CODE	VALUE CODE	CONDITION CODE
	80 x x h	0000C8h	03h
EQUIPMENT CONDITION 20	SERVICE CODE	VALUE CODE	CONDITION CODE
	0000h	FFFFFFh	00h

FIG. 17

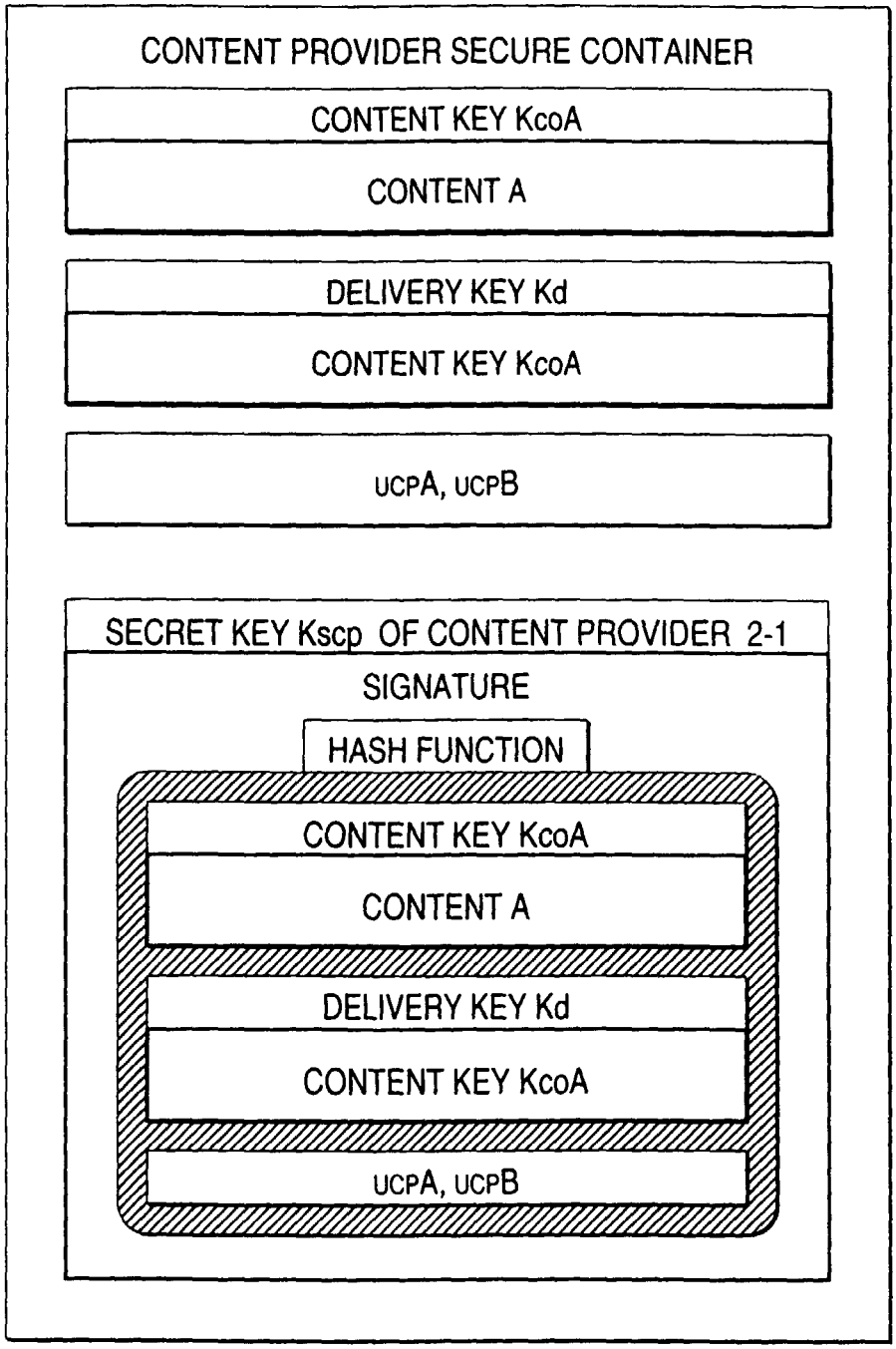

CONTENT PROVIDER SECURE CONTAINER
CONTENT KEY KcoA
CONTENT A
DELIVERY KEY Kd
CONTENT KEY KcoA
UCPA, UCPB
SECRET KEY Kscp OF CONTENT PROVIDER 2-1
SIGNATURE
HASH FUNCTION
CONTENT KEY KcoA
CONTENT A
DELIVERY KEY Kd
CONTENT KEY KcoA
UCPA, UCPB

FIG. 18

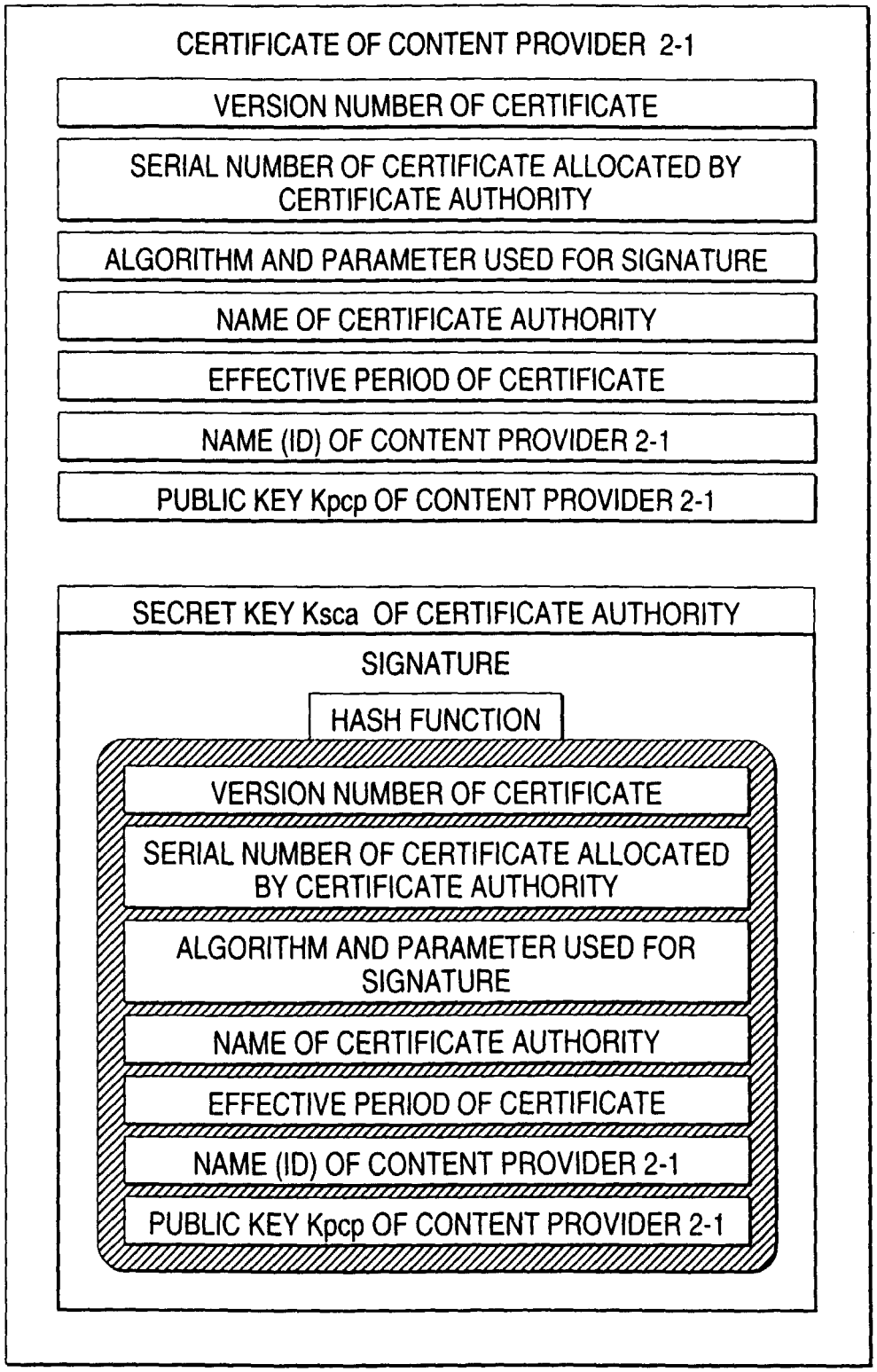

CERTIFICATE OF CONTENT PROVIDER 2-1
VERSION NUMBER OF CERTIFICATE
SERIAL NUMBER OF CERTIFICATE ALLOCATED BY CERTIFICATE AUTHORITY
ALGORITHM AND PARAMETER USED FOR SIGNATURE
NAME OF CERTIFICATE AUTHORITY
EFFECTIVE PERIOD OF CERTIFICATE
NAME (ID) OF CONTENT PROVIDER 2-1
PUBLIC KEY Kpcp OF CONTENT PROVIDER 2-1
SECRET KEY Ksca OF CERTIFICATE AUTHORITY
SIGNATURE
HASH FUNCTION
VERSION NUMBER OF CERTIFICATE
SERIAL NUMBER OF CERTIFICATE ALLOCATED BY CERTIFICATE AUTHORITY
ALGORITHM AND PARAMETER USED FOR SIGNATURE
NAME OF CERTIFICATE AUTHORITY
EFFECTIVE PERIOD OF CERTIFICATE
NAME (ID) OF CONTENT PROVIDER 2-1
PUBLIC KEY Kpcp OF CONTENT PROVIDER 2-1

FIG. 19

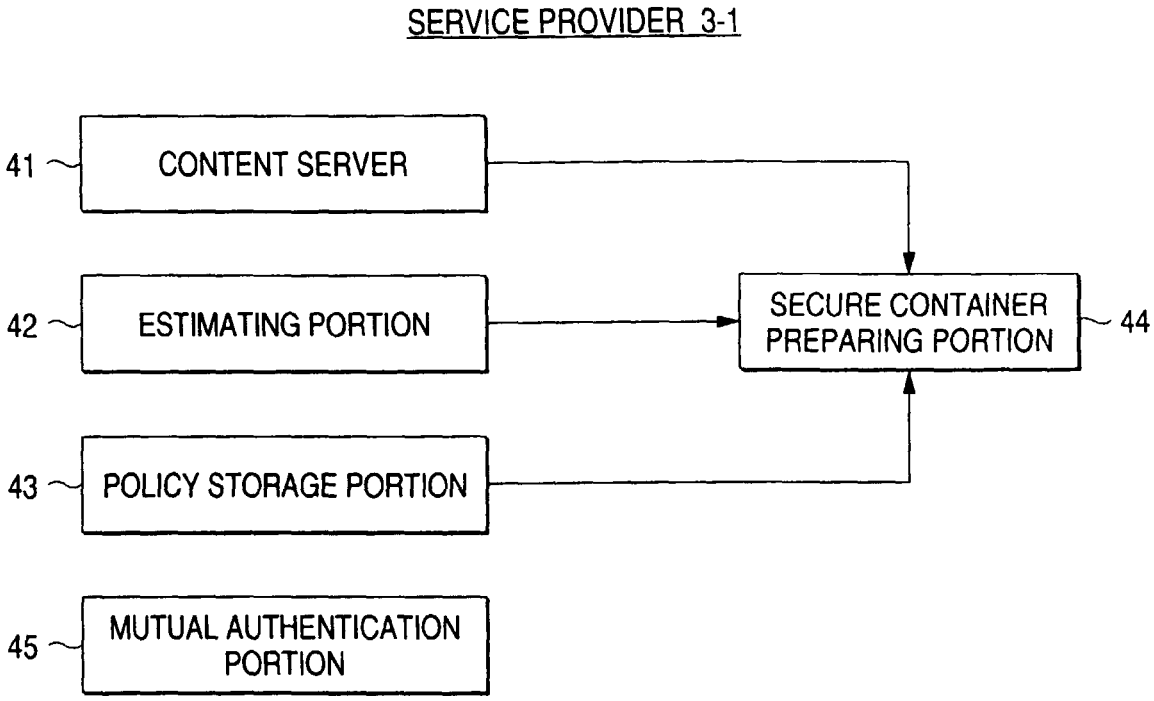

SERVICE PROVIDER 3-1
41
CONTENT SERVER
42
ESTIMATING PORTION
43
POLICY STORAGE PORTION
45
MUTUAL AUTHENTICATION PORTION
SECURE CONTAINER PREPARING PORTION
44

FIG. 20A

PTA-1

ID OF CONTENT	ID OF CONTENT A	
CONTENT INFORMATION	CONTENT INFORMATION OF CONTENT A	
ID OF CONTENT PROVIDER	ID OF CONTENT PROVIDER 2-1	
ID OF UCP	ID OF UCPA	
ID OF SERVICE PROVIDER	ID OF SERVICE PROVIDER 3-1	
ID OF PT	ID OF PTA-1	
EFFECTIVE PERIOD OF PT	EFFECTIVE PERIOD OF PTA-1	
PRICE CONDITION 10	USER CONDITION 10	MALE
	EQUIPMENT CONDITION 10	NO CONDITION
PRICE CONTENT 11	2000 YEN	
PRICE CONTENT 12	600 YEN	
PRICE CONTENT 13	100 YEN	
PRICE CONTENT 14	300 YEN	

FIG. 20B

PTA-2

ID OF CONTENT	ID OF CONTENT A	
CONTENT INFORMATION	CONTENT INFORMATION OF CONTENT A	
ID OF CONTENT PROVIDER	ID OF CONTENT PROVIDER 2-1	
ID OF UCP	ID OF UCPA	
ID OF SERVICE PROVIDER	ID OF SERVICE PROVIDER 3-1	
ID OF PT	ID OF PTA-2	
EFFECTIVE PERIOD OF PT	EFFECTIVE PERIOD OF PTA-2	
PRICE CONDITION 20	USER CONDITION 20	FEMALE
	EQUIPMENT CONDITION 20	NO CONDITION
PRICE CONTENT 21	1000 YEN	
PRICE CONTENT 22	300 YEN	
PRICE CONTENT 23	50 YEN	
PRICE CONTENT 24	150 YEN	

FIG. 21A

PRICE CONDITION 10 OF PTA-1

USER CONDITION 10	SERVICE CODE	VALUE CODE	CONDITION CODE
	01xxh	000000h	01h
EQUIPMENT CONDITION 10	SERVICE CODE	VALUE CODE	CONDITION CODE
	0000h	FFFFFFh	00h

FIG. 21B

PRICE CONDITION 20 OF PTA-2

USER CONDITION 20	SERVICE CODE	VALUE CODE	CONDITION CODE
	01xxh	000001h	01h
EQUIPMENT CONDITION 20	SERVICE CODE	VALUE CODE	CONDITION CODE
	0000h	FFFFFFh	00h

FIG. 22A

PTB-1

ID OF CONTENT	ID OF CONTENT A	
CONTENT INFORMATION	CONTENT INFORMATION OF CONTENT A	
ID OF CONTENT PROVIDER	ID OF CONTENT PROVIDER 2-1	
ID OF UCP	ID OF UCPB	
ID OF SERVICE PROVIDER	ID OF SERVICE PROVIDER 3-1	
ID OF PT	ID OF PTB-1	
EFFECTIVE PERIOD OF PT	EFFECTIVE PERIOD OF PTB-1	
PRICE CONDITION 30	USER CONDITION 30	NO CONDITION
	EQUIPMENT CONDITION 30	SUBORDINATE EQUIPMENT
PRICE CONTENT 31	100 YEN	
PRICE CONTENT 32	300 YEN	

FIG. 22B

PTB-2

ID OF CONTENT	ID OF CONTENT A	
CONTENT INFORMATION	CONTENT INFORMATION OF CONTENT A	
ID OF CONTENT PROVIDER	ID OF CONTENT PROVIDER 2-1	
ID OF UCP	ID OF UCPB	
ID OF SERVICE PROVIDER	ID OF SERVICE PROVIDER 3-1	
ID OF PT	ID OF PTB-2	
EFFECTIVE PERIOD OF PT	EFFECTIVE PERIOD OF PTB-2	
PRICE CONDITION 40	USER CONDITION 40	NO CONDITION
	EQUIPMENT CONDITION 40	MAIN EQUIPMENT
PRICE CONTENT 41	50 YEN	
PRICE CONTENT 42	150 YEN	

FIG. 23A

PRICE CONDITION 30 OF PTB-1

USER CONDITION 30	SERVICE CODE	VALUE CODE	CONDITION CODE
	0000h	FFFFFFh	00h
EQUIPMENT CONDITION 30	SERVICE CODE	VALUE CODE	CONDITION CODE
	00 x x h	000064h	03h

FIG. 23B

PRICE CONDITION 40 OF PTB-2

USER CONDITION 40	SERVICE CODE	VALUE CODE	CONDITION CODE
	0000h	FFFFFFh	00h
EQUIPMENT CONDITION 40	SERVICE CODE	VALUE CODE	CONDITION CODE
	00 x x h	000064h	06h

FIG. 24

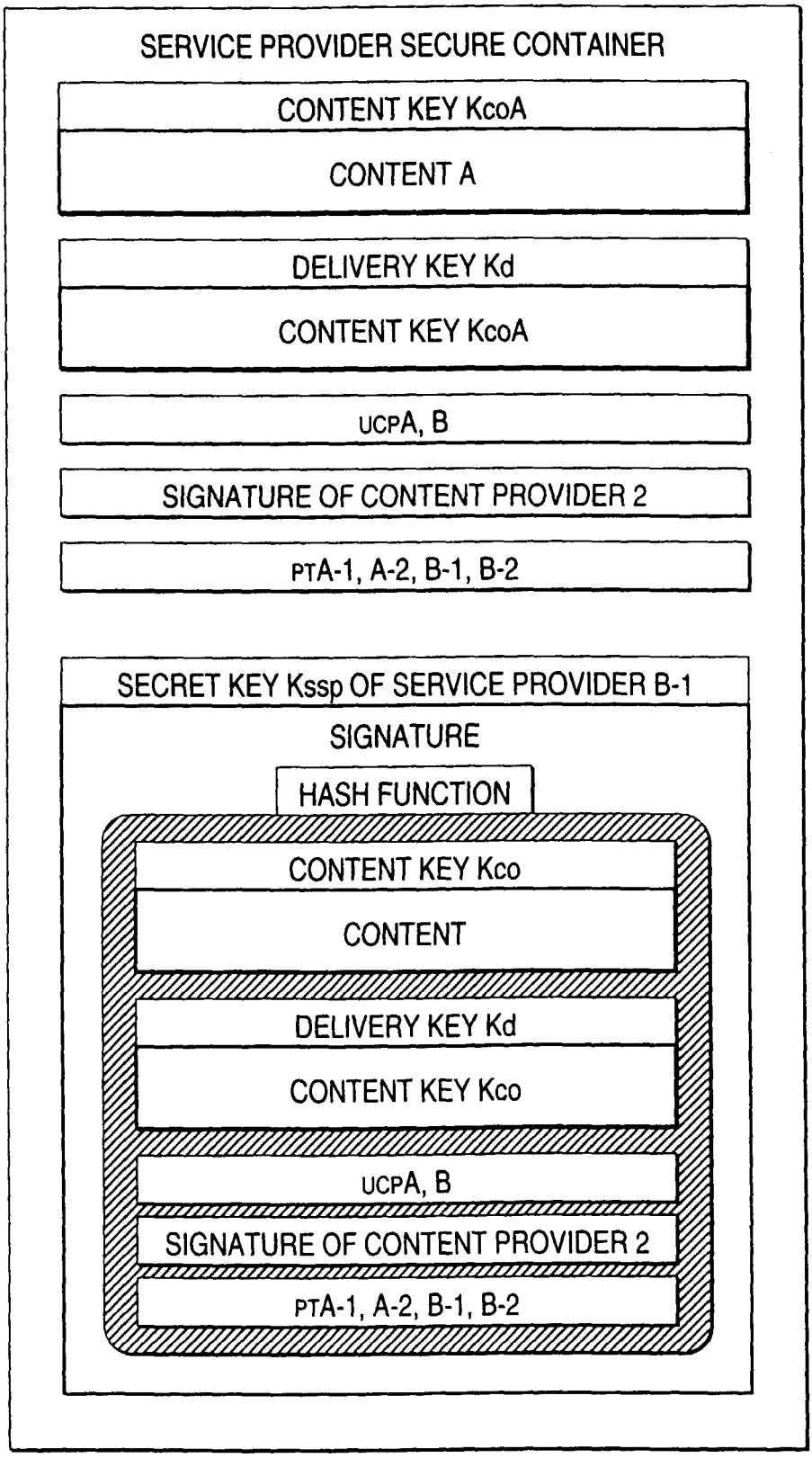

SERVICE PROVIDER SECURE CONTAINER
CONTENT KEY KcoA
CONTENT A
DELIVERY KEY Kd
CONTENT KEY KcoA
UCPA, B
SIGNATURE OF CONTENT PROVIDER 2
PTA-1, A-2, B-1, B-2
SECRET KEY Kssp OF SERVICE PROVIDER B-1
SIGNATURE
HASH FUNCTION
CONTENT KEY Kco
CONTENT
DELIVERY KEY Kd
CONTENT KEY Kco
UCPA, B
SIGNATURE OF CONTENT PROVIDER 2
PTA-1, A-2, B-1, B-2

FIG. 25

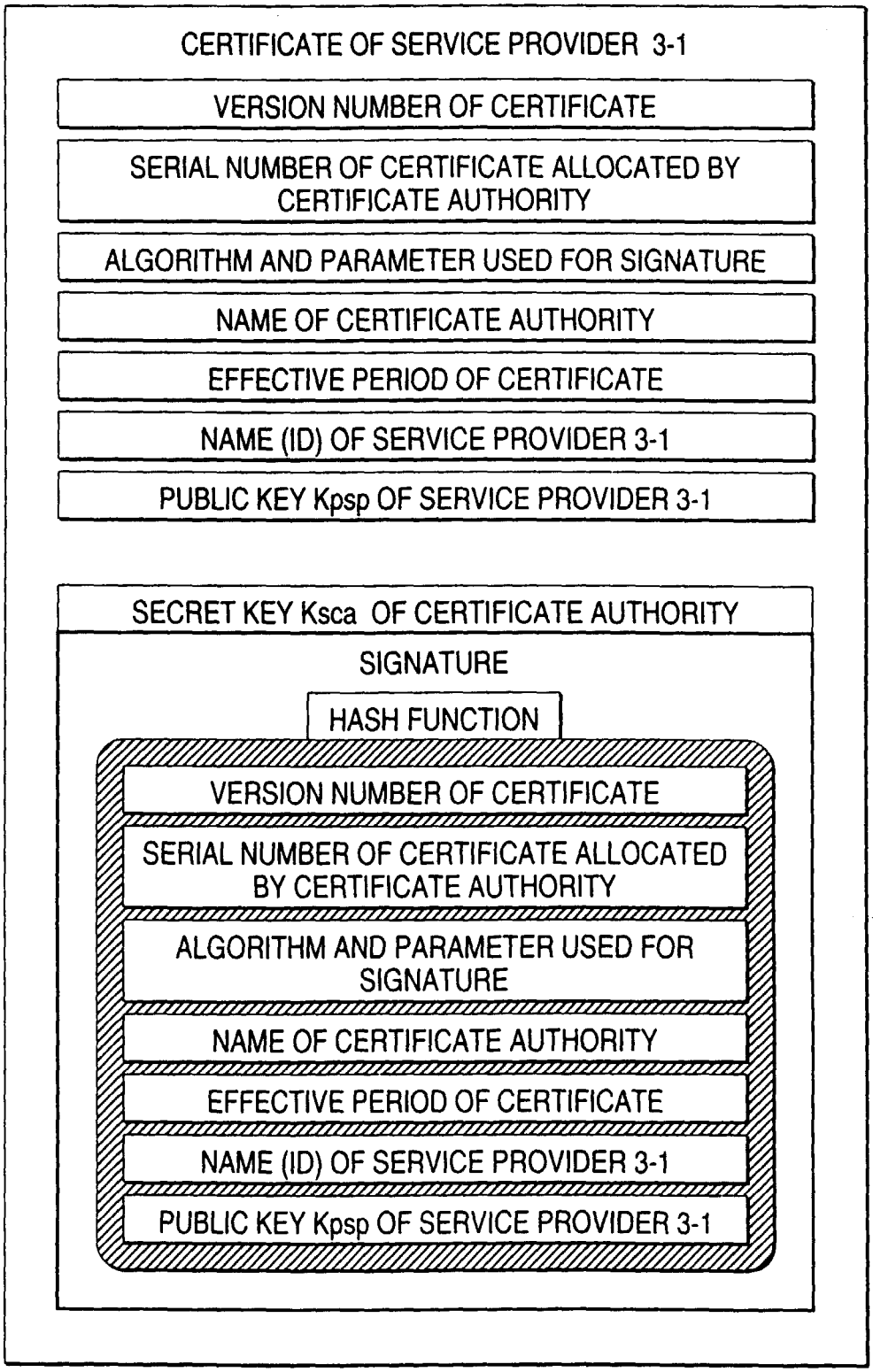

CERTIFICATE OF SERVICE PROVIDER 3-1
VERSION NUMBER OF CERTIFICATE
SERIAL NUMBER OF CERTIFICATE ALLOCATED BY CERTIFICATE AUTHORITY
ALGORITHM AND PARAMETER USED FOR SIGNATURE
NAME OF CERTIFICATE AUTHORITY
EFFECTIVE PERIOD OF CERTIFICATE
NAME (ID) OF SERVICE PROVIDER 3-1
PUBLIC KEY Kpsp OF SERVICE PROVIDER 3-1
SECRET KEY Ksca OF CERTIFICATE AUTHORITY
SIGNATURE
HASH FUNCTION
VERSION NUMBER OF CERTIFICATE
SERIAL NUMBER OF CERTIFICATE ALLOCATED BY CERTIFICATE AUTHORITY
ALGORITHM AND PARAMETER USED FOR SIGNATURE
NAME OF CERTIFICATE AUTHORITY
EFFECTIVE PERIOD OF CERTIFICATE
NAME (ID) OF SERVICE PROVIDER 3-1
PUBLIC KEY Kpsp OF SERVICE PROVIDER 3-1

FIG. 26

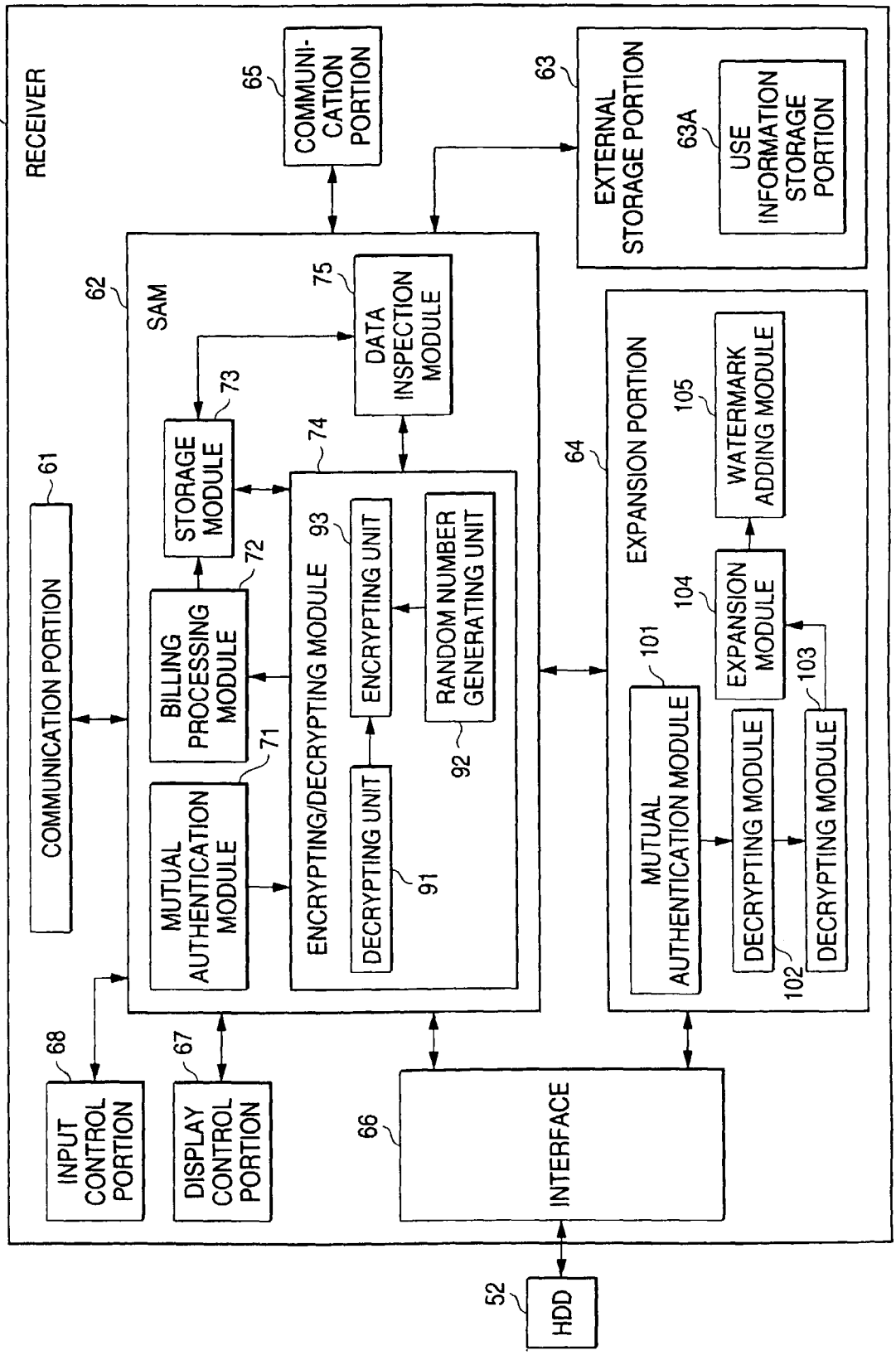

51
RECEIVER
65
COMMUNI-
CATION
PORTION
63
EXTERNAL
STORAGE PORTION
63A
USE
INFORMATION
STORAGE
PORTION
62
SAM
75
DATA
INSPECTION
MODULE
73
STORAGE
MODULE
74
61
COMMUNICATION PORTION
BILLING
PROCESSING
MODULE
72
MUTUAL
AUTHENTICATION
MODULE
71
ENCRYPTING/DECRYPTING MODULE
93
ENCRYPTING UNIT
DECRYPTING UNIT
91
RANDOM NUMBER
GENERATING UNIT
92
64
EXPANSION PORTION
105
WATERMARK
ADDING MODULE
104
EXPANSION
MODULE
101
MUTUAL
AUTHENTICATION MODULE
DECRYPTING MODULE
102
103
DECRYPTING MODULE
68
INPUT
CONTROL
PORTION
67
DISPLAY
CONTROL
PORTION
66
INTERFACE
52
HDD

FIG. 27

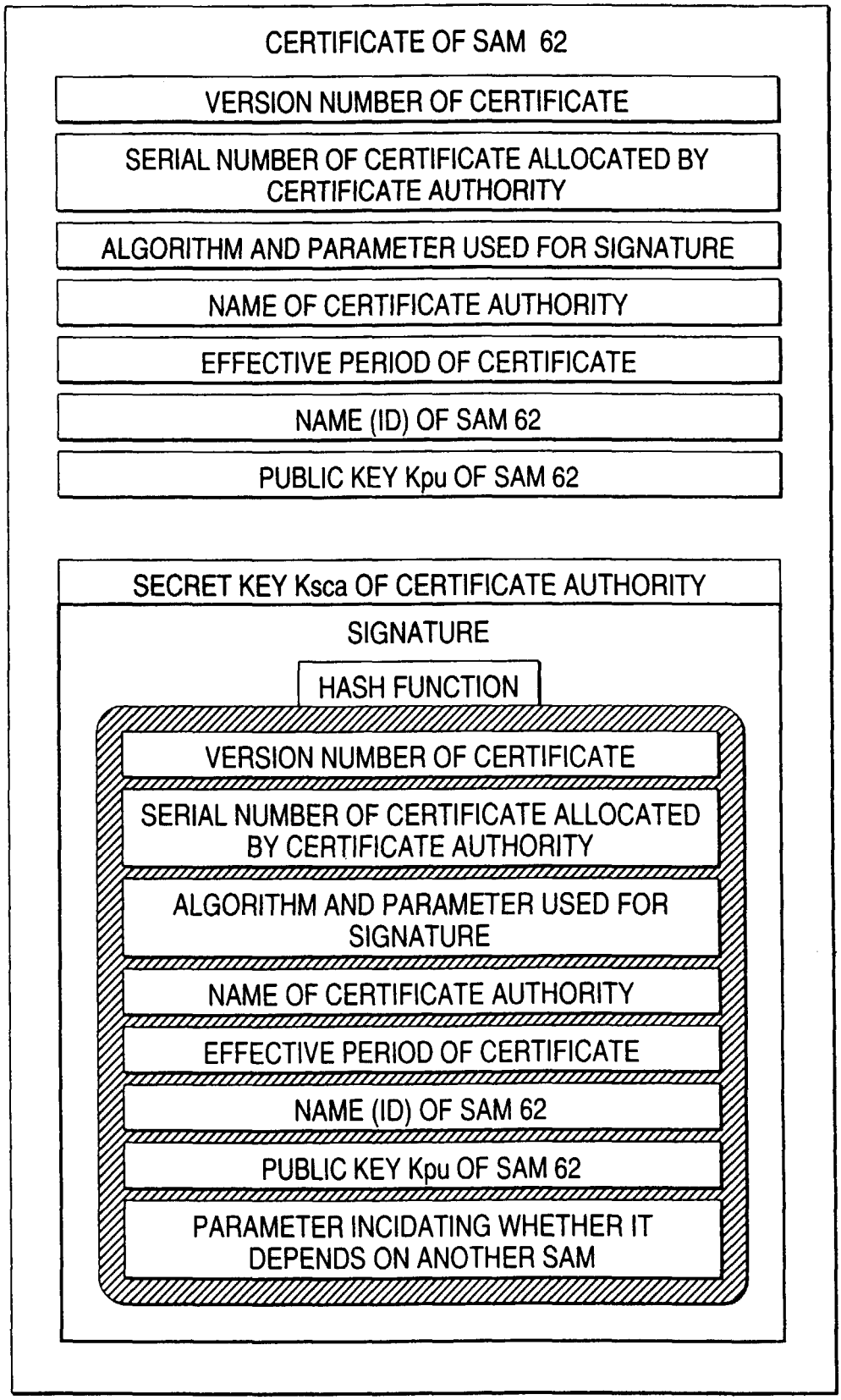

CERTIFICATE OF SAM 62
VERSION NUMBER OF CERTIFICATE
SERIAL NUMBER OF CERTIFICATE ALLOCATED BY CERTIFICATE AUTHORITY
ALGORITHM AND PARAMETER USED FOR SIGNATURE
NAME OF CERTIFICATE AUTHORITY
EFFECTIVE PERIOD OF CERTIFICATE
NAME (ID) OF SAM 62
PUBLIC KEY Kpu OF SAM 62
SECRET KEY Ksca OF CERTIFICATE AUTHORITY
SIGNATURE
HASH FUNCTION
VERSION NUMBER OF CERTIFICATE
SERIAL NUMBER OF CERTIFICATE ALLOCATED BY CERTIFICATE AUTHORITY
ALGORITHM AND PARAMETER USED FOR SIGNATURE
NAME OF CERTIFICATE AUTHORITY
EFFECTIVE PERIOD OF CERTIFICATE
NAME (ID) OF SAM 62
PUBLIC KEY Kpu OF SAM 62
PARAMETER INCIDATING WHETHER IT DEPENDS ON ANOTHER SAM

FIG. 28

UCSA

ID OF CONTENT		ID OF CONTENT A
CONTENT INFORMATION		CONTENT INFORMATION OF CONTENT A
ID OF CONTENT PROVIDER		ID OF CONTENT PROVIDER 2-1
ID OF UCP		ID OF UCPA
EFFECTIVE PERIOD OF UCP		EFFECTIVE PERIOD OF UCPA
ID OF SERVICE PROVIDER		ID OF SERVICE PROVIDER 3-1
ID OF PT		ID OF PTA-1
EFFECTIVE PERIOD OF PT		EFFECTIVE PERIOD OF PTA-1
ID OF UCS		ID OF UCSA
ID OF SAM		ID OF SAM 62
ID OF USER		ID OF USER F
USE CONTENT	ID	ID OF USE CONTENT 11
	FORMAT	PURCHASED REPRODUCTION
	PARAMETER	X X X
	MANAGEMENT MOVEMENT INFORMATION	MANAGEMENT MOVEMENT ORIGIN: ID OF SAM 62 MANAGEMENT MOVEMENT DESTINATION: ID OF SAM 62
USE HISTORY		X X X

EP 1 045 321 A2

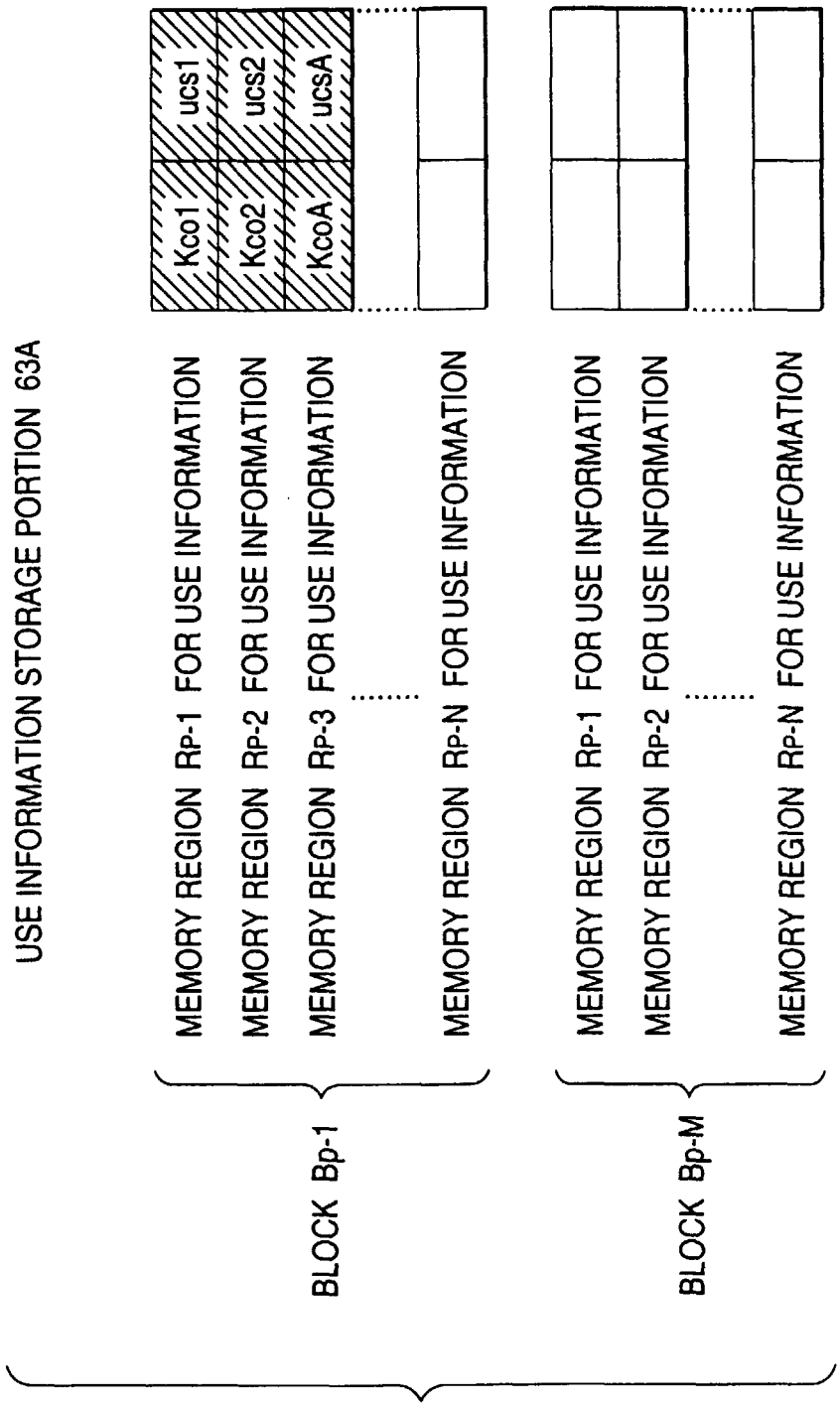

USE INFORMATION STORAGE PORTION 63A
BLOCK Bp-1
BLOCK Bp-M
MEMORY REGION Rp-1 FOR USE INFORMATION
MEMORY REGION Rp-2 FOR USE INFORMATION
MEMORY REGION Rp-3 FOR USE INFORMATION
MEMORY REGION Rp-N FOR USE INFORMATION
MEMORY REGION Rp-1 FOR USE INFORMATION
MEMORY REGION Rp-2 FOR USE INFORMATION
MEMORY REGION Rp-N FOR USE INFORMATION
Kco1
Kco2
KcoA
ucs1
ucs2
ucsA

FIG. 29

FIG. 30

BILLING INFORMATION A

ID OF CONTENT		ID OF CONTENT A
CONTENT INFORMATION		CONTENT INFORMATION OF CONTENT A
ID OF CONTENT PROVIDER		ID OF CONTENT PROVIDER 2-1
ID OF UCP		ID OF UCPA
EFFECTIVE PERIOD OF UCP		EFFECTIVE PERIOD OF UCPA
ID OF SERVICE PROVIDER		ID OF SERVICE PROVIDER 3-1
ID OF PT		ID OF PTA-1
EFFECTIVE PERIOD OF PT		EFFECTIVE PERIOD OF PTA-1
ID OF UCS		ID OF UCSA
ID OF SAM		ID OF SAM 62
ID OF USER		ID OF USER F
USE CONTENT	ID	ID OF USE CONTENT 11
	FORMAT	PURCHASED REPRODUCTION
	PARAMETER	x x x
	MANAGEMENT MOVEMENT INFORMATION	MANAGEMENT MOVEMENT ORIGIN: ID OF SAM 62 MANAGEMENT MOVEMENT DESTINATION: ID OF SAM 62
BILLING HISTORY		x x x

EP 1 045 321 A2

FIG. 31

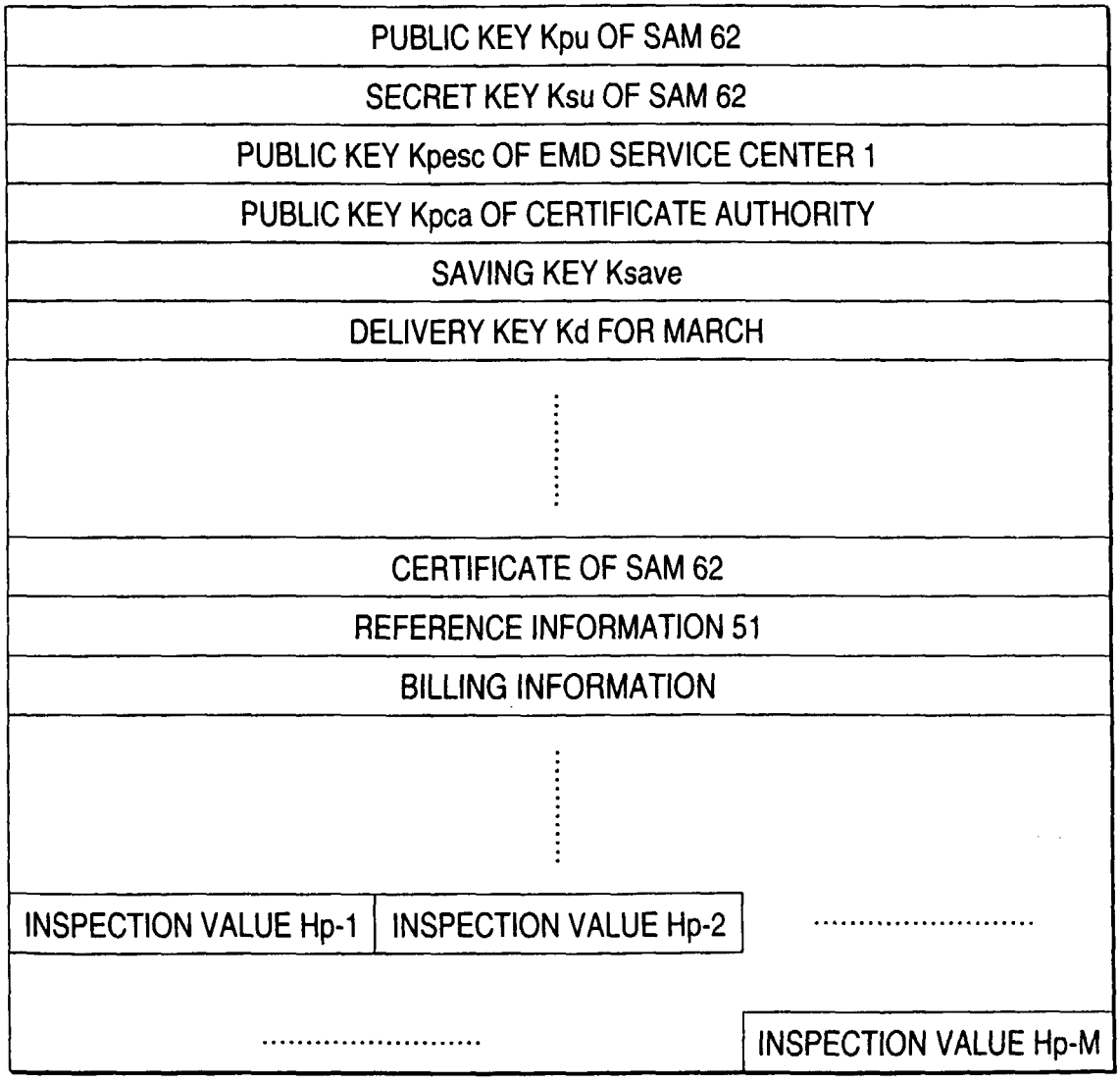

PUBLIC KEY Kpu OF SAM 62
SECRET KEY Ksu OF SAM 62
PUBLIC KEY Kpesc OF EMD SERVICE CENTER 1
PUBLIC KEY Kpca OF CERTIFICATE AUTHORITY
SAVING KEY Ksave
DELIVERY KEY Kd FOR MARCH
CERTIFICATE OF SAM 62
REFERENCE INFORMATION 51
BILLING INFORMATION
INSPECTION VALUE Hp-1
INSPECTION VALUE Hp-2
INSPECTION VALUE Hp-M

FIG. 32

REFERENCE INFORMATION 51

ID OF SAM		ID OF SAM 62
EQUIPMENT NUMBER		EQUIPMENT NUMBER (NO. 100) OF RECEIVER 51
SETTLEMENT ID		SETTLEMENT ID OF USER F
UPPER LIMIT AMOUNT OF BILLING		UPPER LIMIT AMOUNT OF BILLING AT REGISTRATION
SETTLEMENT USER INFORMATION	NAME	NAME OF USER F
	ADDRESS	ADDRESS OF USER F
	TELEPHONE NUMBER	TELEPHONE NUMBER OF USER F
	SETTLEMENT AGENCY INFORMATION	SETTLEMENT AGENCY INFORMATION OF USER F
	BIRTH DATE	BIRTH DATE OF USER F
	AGE	AGE (21) OF USER F
	GENDER	GENDER (MALE) OF USER F
	ID OF USER	ID OF USER F
	PASSWORD	PASSWORD OF USER F
SUBORDINATE USER INFORMATION	NAME	
	ADDRESS	
	TELEPHONE NUMBER	
	BIRTH DATE	
	GENDER	
	ID OF USER	
	PASSWORD	
⋮		
USE POINT INFORMATION		USE POINT INFORMATION OF RECEIVER 51

▨ INFORMATION WHICH IS NOT PERMITTED TO BE MADE OPEN
□ INFORMATION WHICH IS PERMITTED TO BE MADE OPEN

FIG. 33

USE POINT INFORMATION OF REFERENCE INFORMATION 51

USER	PROVIDER	USE POINT
SETTLEMENT USER	CONTENT PROVIDER 2-1	222 POINTS
	CONTENT PROVIDER 2-2	123 POINTS
	SERVICE PROVIDER 3-1	345 POINTS
	SERVICE PROVIDER 3-2	0 POINT

FIG. 34

REGISTRATION CONDITION OF RECEIVER 51

SAM ID	USER ID	PURCHASE PROCESSING	BILLING PROCESSING	BILLING EQUIPMENT	CONTENT SUPPLY EQUIPMENT	STATE FLAG	REGISTRATION CONDITION SIGNATURE	REGISTRATION LIST SIGNATURE
ID OF SAM 62	ID OF USER F	PERMISSIBLE	PERMISSIBLE	ID OF SAM 62	NO	NO LIMITATION	xxxx	xxxx

LIST PORTION

OBJECTIVE SAM ID	ID OF SAM 62
EFFECTIVE PERIOD	xxxx
VERSION NUMBER	xxxx
THE NUMBER OF CONNECTED EQUIPMENT	1

OBJECTIVE SAM INFORMATION

EP 1 045 321 A2

FIG. 35

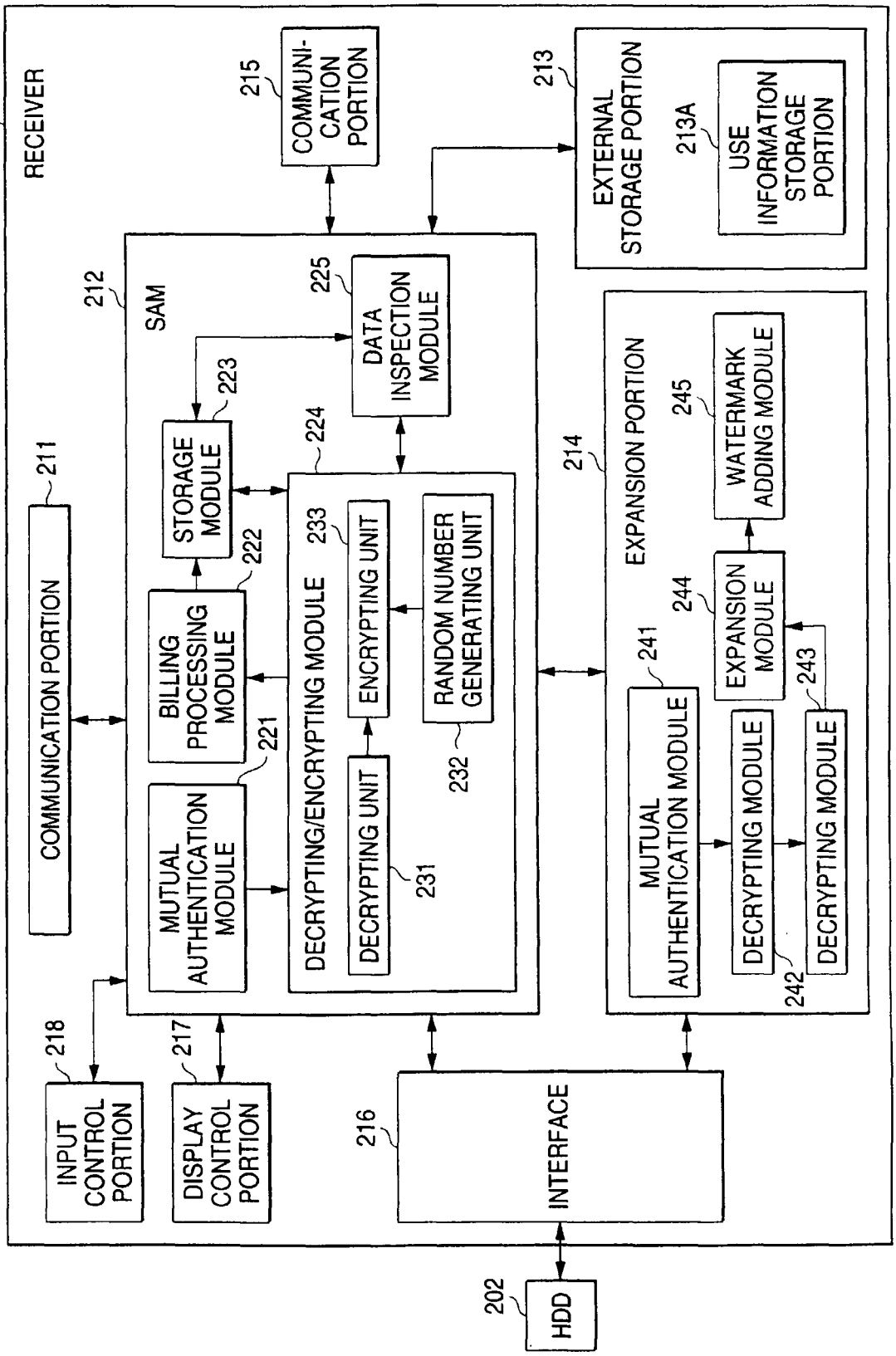

201
RECEIVER
COMMUNICATION PORTION
211
INPUT CONTROL PORTION
218
DISPLAY CONTROL PORTION
217
INTERFACE
216
HDD
202
212
SAM
MUTUAL AUTHENTICATION MODULE
221
BILLING PROCESSING MODULE
222
STORAGE MODULE
223
DECRYPTING/ENCRYPTING MODULE
224
DECRYPTING UNIT
231
ENCRYPTING UNIT
233
RANDOM NUMBER GENERATING UNIT
232
DATA INSPECTION MODULE
225
COMMUNI-CATION PORTION
215
214
EXPANSION PORTION
MUTUAL AUTHENTICATION MODULE
241
DECRYPTING MODULE
242
EXPANSION MODULE
244
DECRYPTING MODULE
243
WATERMARK ADDING MODULE
245
213
EXTERNAL STORAGE PORTION
213A
USE INFORMATION STORAGE PORTION

FIG. 36

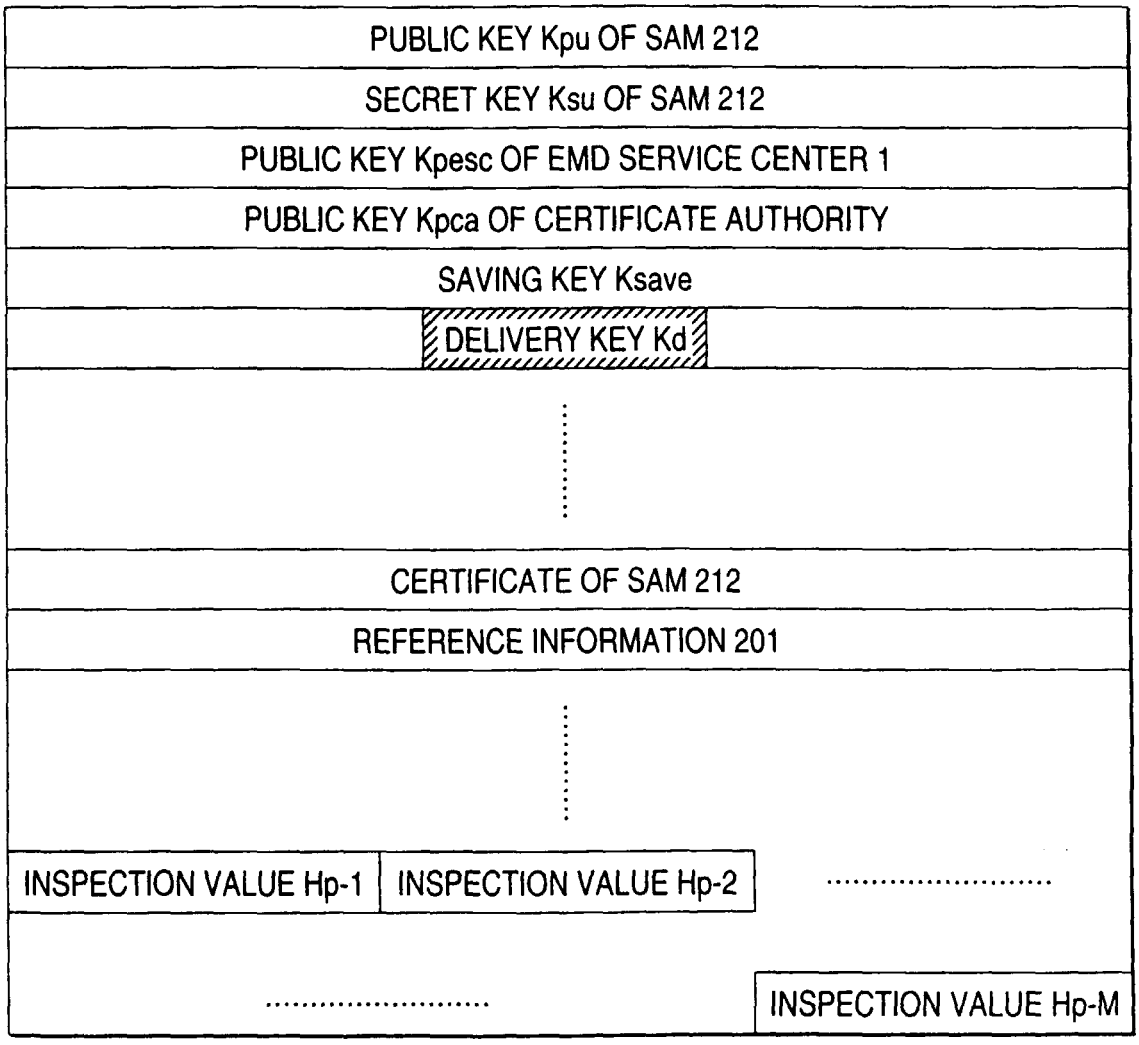

PUBLIC KEY Kpu OF SAM 212
SECRET KEY Ksu OF SAM 212
PUBLIC KEY Kpesc OF EMD SERVICE CENTER 1
PUBLIC KEY Kpca OF CERTIFICATE AUTHORITY
SAVING KEY Ksave
DELIVERY KEY Kd
CERTIFICATE OF SAM 212
REFERENCE INFORMATION 201
INSPECTION VALUE Hp-1
INSPECTION VALUE Hp-2
INSPECTION VALUE Hp-M

FIG. 37

REFERENCE INFORMATION 201

ID OF SAM		ID OF SAM 212
EQUIPMENT NUMBER		EQUIPMENT NUMBER (NO. 100) OF RECEIVER 201
SETTLEMENT ID		
UPPER LIMIT AMOUNT OF BILLING		
SETTLEMENT USER INFORMATION	NAME	
	ADDRESS	
	TELEPHONE NUMBER	
	SETTLEMENT AGENCY INFORMATION	
	BIRTH DATE	
	AGE	
	GENDER	
	ID OF USER	
	PASSWORD	
SUBORDINATE USER INFORMATION	NAME	
	ADDRESS	
	TELEPHONE NUMBER	
	BIRTH DATE	
	GENDER	
	ID OF USER	
	PASSWORD	
⋮		
USE POINT INFORMATION		

▨ INFORMATION WHICH IS NOT PERMITTED TO BE MADE OPEN
□ INFORMATION WHICH IS PERMITTED TO BE MADE OPEN

FIG. 38

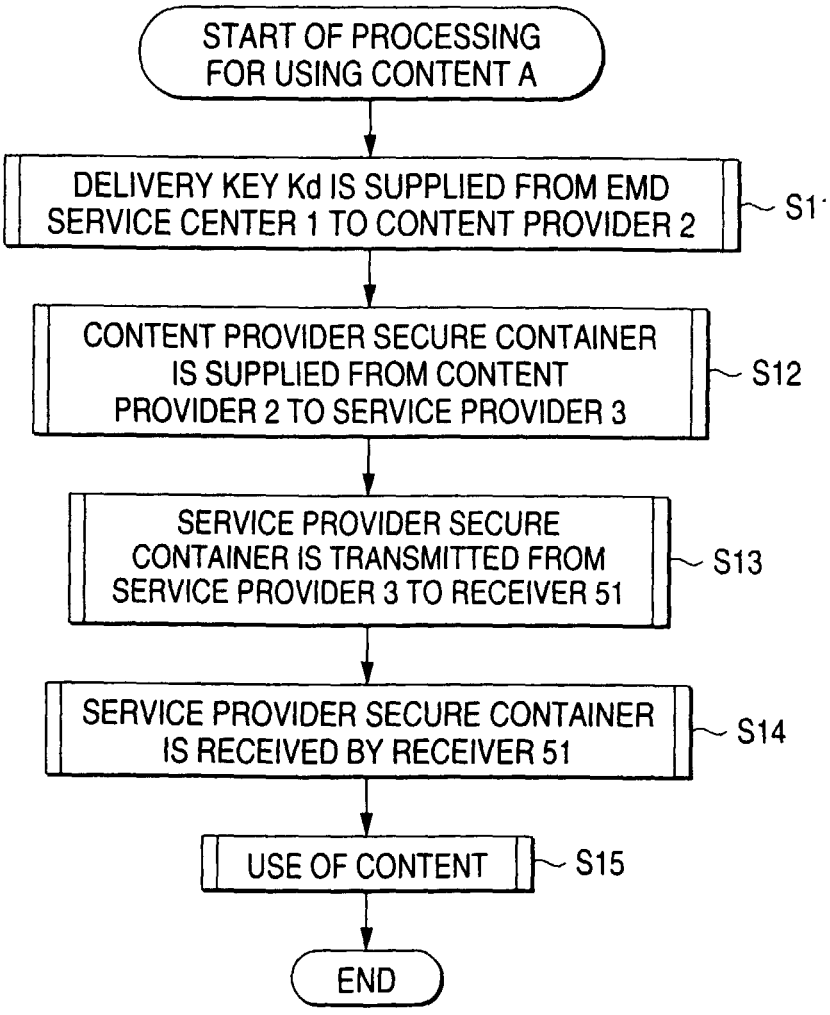

START OF PROCESSING FOR USING CONTENT A
DELIVERY KEY Kd IS SUPPLIED FROM EMD SERVICE CENTER 1 TO CONTENT PROVIDER 2
S11
CONTENT PROVIDER SECURE CONTAINER IS SUPPLIED FROM CONTENT PROVIDER 2 TO SERVICE PROVIDER 3
S12
SERVICE PROVIDER SECURE CONTAINER IS TRANSMITTED FROM SERVICE PROVIDER 3 TO RECEIVER 51
S13
SERVICE PROVIDER SECURE CONTAINER IS RECEIVED BY RECEIVER 51
S14
USE OF CONTENT
S15
END

FIG. 39

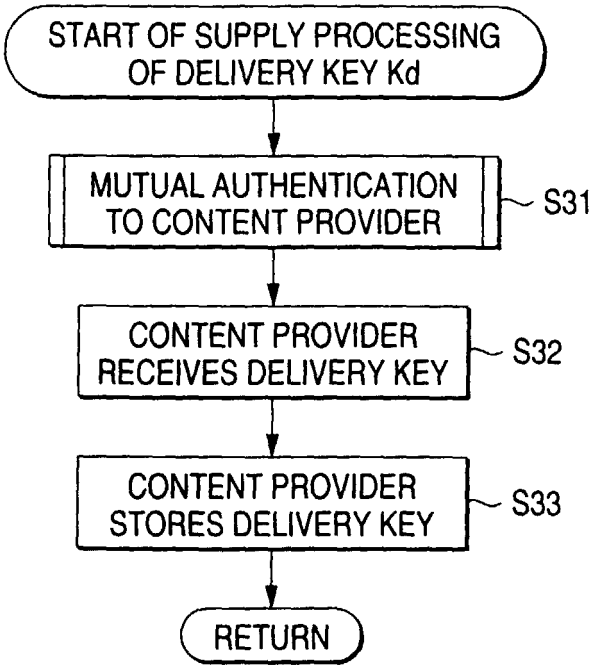

START OF SUPPLY PROCESSING OF DELIVERY KEY Kd
MUTUAL AUTHENTICATION TO CONTENT PROVIDER
S31
CONTENT PROVIDER RECEIVES DELIVERY KEY
S32
CONTENT PROVIDER STORES DELIVERY KEY
S33
RETURN

FIG. 40

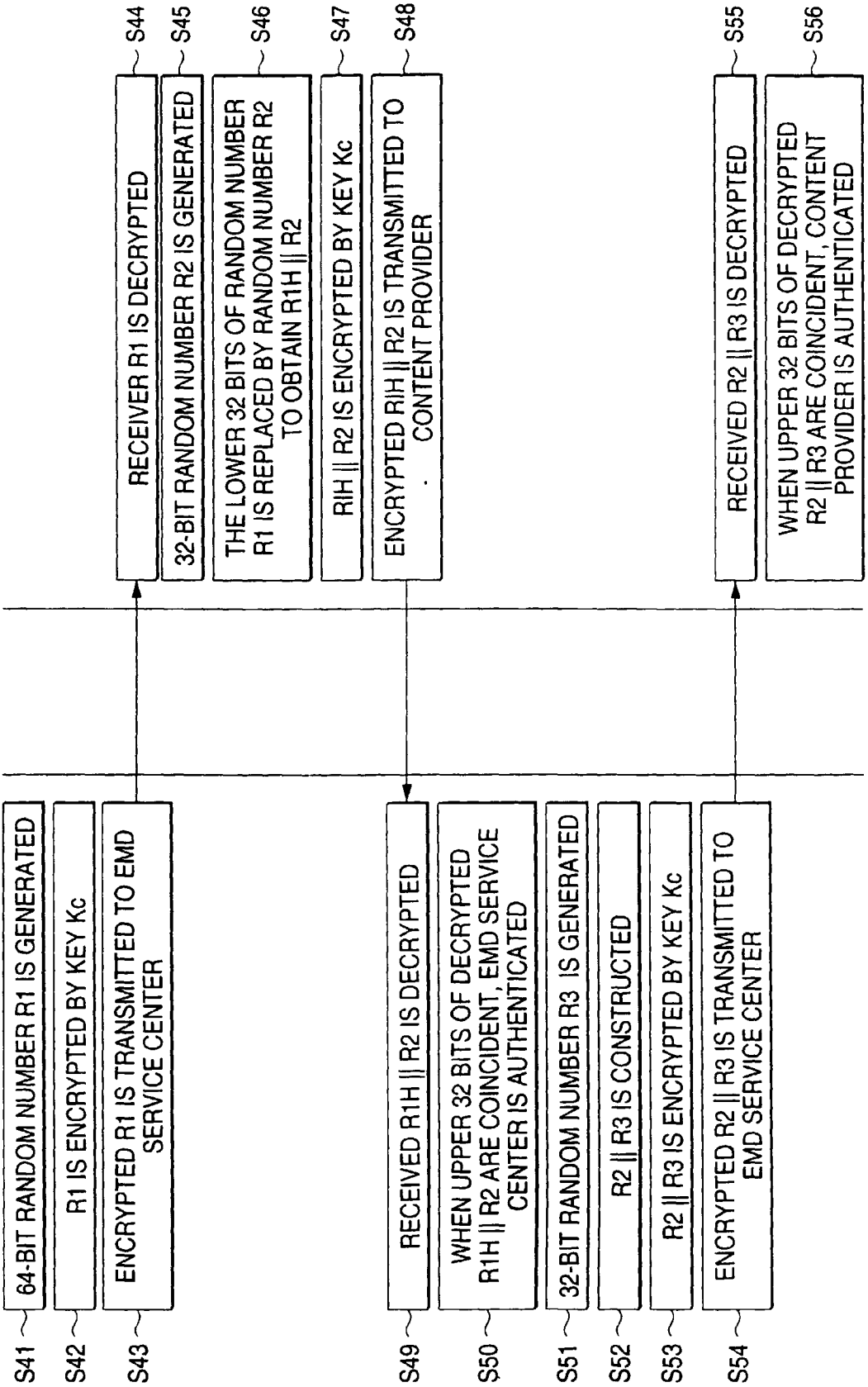

CONTENT PROVIDER
EMD SERVICE CENTER
S41
64-BIT RANDOM NUMBER R1 IS GENERATED
S42
R1 IS ENCRYPTED BY KEY Kc
S43
ENCRYPTED R1 IS TRANSMITTED TO EMD SERVICE CENTER
S44
RECEIVER R1 IS DECRYPTED
S45
32-BIT RANDOM NUMBER R2 IS GENERATED
S46
THE LOWER 32 BITS OF RANDOM NUMBER R1 IS REPLACED BY RANDOM NUMBER R2 TO OBTAIN R1H || R2
S47
R1H || R2 IS ENCRYPTED BY KEY Kc
S48
ENCRYPTED R1H || R2 IS TRANSMITTED TO CONTENT PROVIDER
S49
RECEIVED R1H || R2 IS DECRYPTED
S50
WHEN UPPER 32 BITS OF DECRYPTED R1H || R2 ARE COINCIDENT, EMD SERVICE CENTER IS AUTHENTICATED
S51
32-BIT RANDOM NUMBER R3 IS GENERATED
S52
R2 || R3 IS CONSTRUCTED
S53
R2 || R3 IS ENCRYPTED BY KEY Kc
S54
ENCRYPTED R2 || R3 IS TRANSMITTED TO EMD SERVICE CENTER
S55
RECEIVED R2 || R3 IS DECRYPTED
S56
WHEN UPPER 32 BITS OF DECRYPTED R2 || R3 ARE COINCIDENT, CONTENT PROVIDER IS AUTHENTICATED

FIG. 41

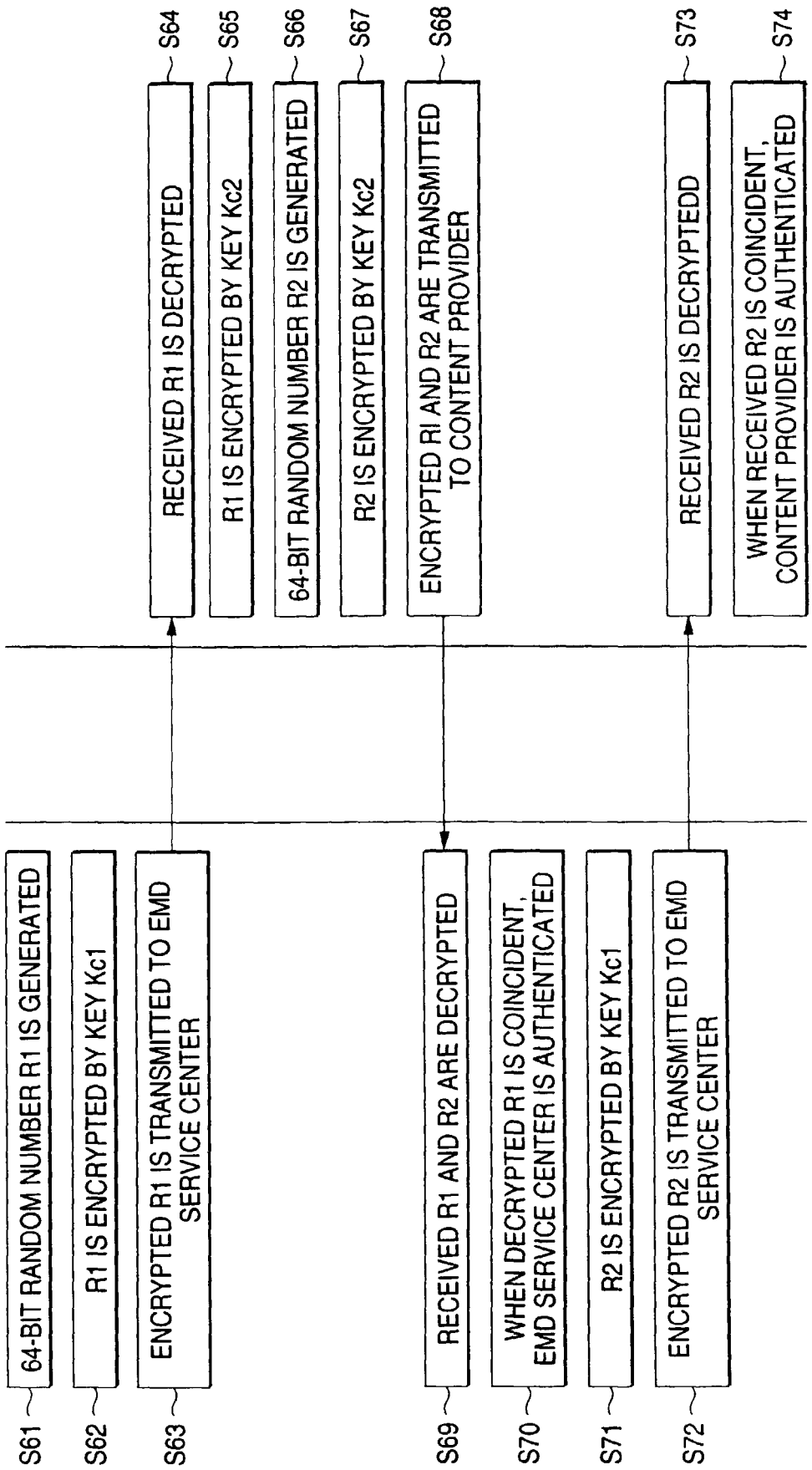

CONTENT PROVIDER
EMD SERVICE CENTER
S61
64-BIT RANDOM NUMBER R1 IS GENERATED
S62
R1 IS ENCRYPTED BY KEY Kc1
S63
ENCRYPTED R1 IS TRANSMITTED TO EMD SERVICE CENTER
S64
RECEIVED R1 IS DECRYPTED
S65
R1 IS ENCRYPTED BY KEY Kc2
S66
64-BIT RANDOM NUMBER R2 IS GENERATED
S67
R2 IS ENCRYPTED BY KEY Kc2
S68
ENCRYPTED RI AND R2 ARE TRANSMITTED TO CONTENT PROVIDER
S69
RECEIVED R1 AND R2 ARE DECRYPTED
S70
WHEN DECRYPTED R1 IS COINCIDENT, EMD SERVICE CENTER IS AUTHENTICATED
S71
R2 IS ENCRYPTED BY KEY Kc1
S72
ENCRYPTED R2 IS TRANSMITTED TO EMD SERVICE CENTER
S73
RECEIVED R2 IS DECRYPTEDD
S74
WHEN RECEIVED R2 IS COINCIDENT, CONTENT PROVIDER IS AUTHENTICATED

FIG. 42

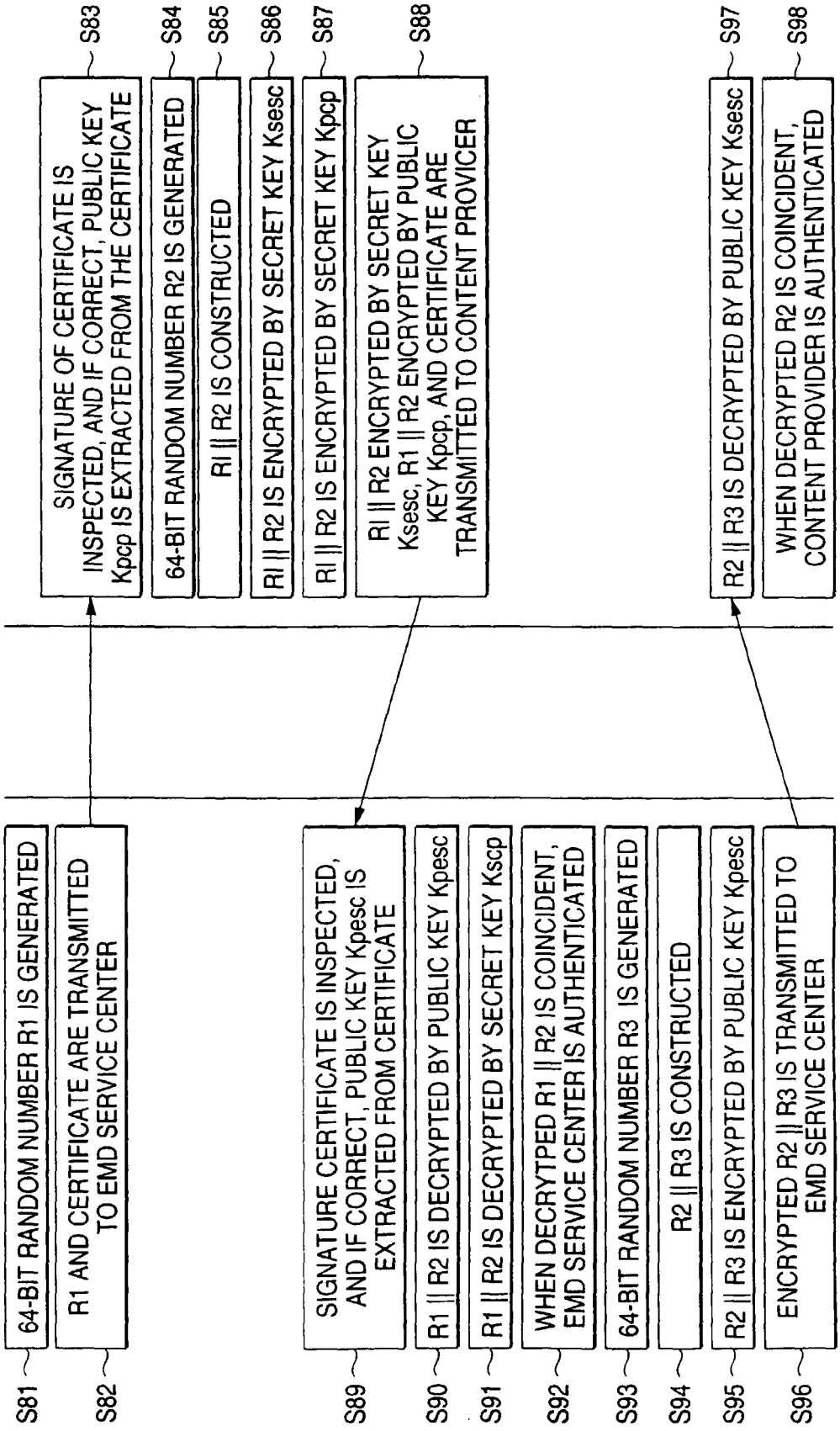

CONTENT PROVIDER
EMD SERVICE CENTER
64-BIT RANDOM NUMBER R1 IS GENERATED
S81
R1 AND CERTIFICATE ARE TRANSMITTED TO EMD SERVICE CENTER
S82
SIGNATURE OF CERTIFICATE IS INSPECTED, AND IF CORRECT, PUBLIC KEY Kpcp IS EXTRACTED FROM THE CERTIFICATE
S83
64-BIT RANDOM NUMBER R2 IS GENERATED
S84
RI || R2 IS CONSTRUCTED
S85
RI || R2 IS ENCRYPTED BY SECRET KEY Ksesc
S86
RI || R2 IS ENCRYPTED BY SECRET KEY Kpcp
S87
RI || R2 ENCRYPTED BY SECRET KEY Ksesc, R1 || R2 ENCRYPTED BY PUBLIC KEY Kpcp, AND CERTIFICATE ARE TRANSMITTED TO CONTENT PROVICER
S88
SIGNATURE CERTIFICATE IS INSPECTED, AND IF CORRECT, PUBLIC KEY Kpesc IS EXTRACTED FROM CERTIFICATE
S89
R1 || R2 IS DECRYPTED BY PUBLIC KEY Kpesc
S90
R1 || R2 IS DECRYPTED BY SECRET KEY Kscp
S91
WHEN DECRYTPED R1 || R2 IS COINCIDENT, EMD SERVICE CENTER IS AUTHENTICATED
S92
64-BIT RANDOM NUMBER R3 IS GENERATED
S93
R2 || R3 IS CONSTRUCTED
S94
R2 || R3 IS ENCRYPTED BY PUBLIC KEY Kpesc
S95
ENCRYPTED R2 || R3 IS TRANSMITTED TO EMD SERVICE CENTER
S96
R2 || R3 IS DECRYPTED BY PUBLIC KEY Ksesc
S97
WHEN DECRYPTED R2 IS COINCIDENT, CONTENT PROVIDER IS AUTHENTICATED
S98

FIG. 43

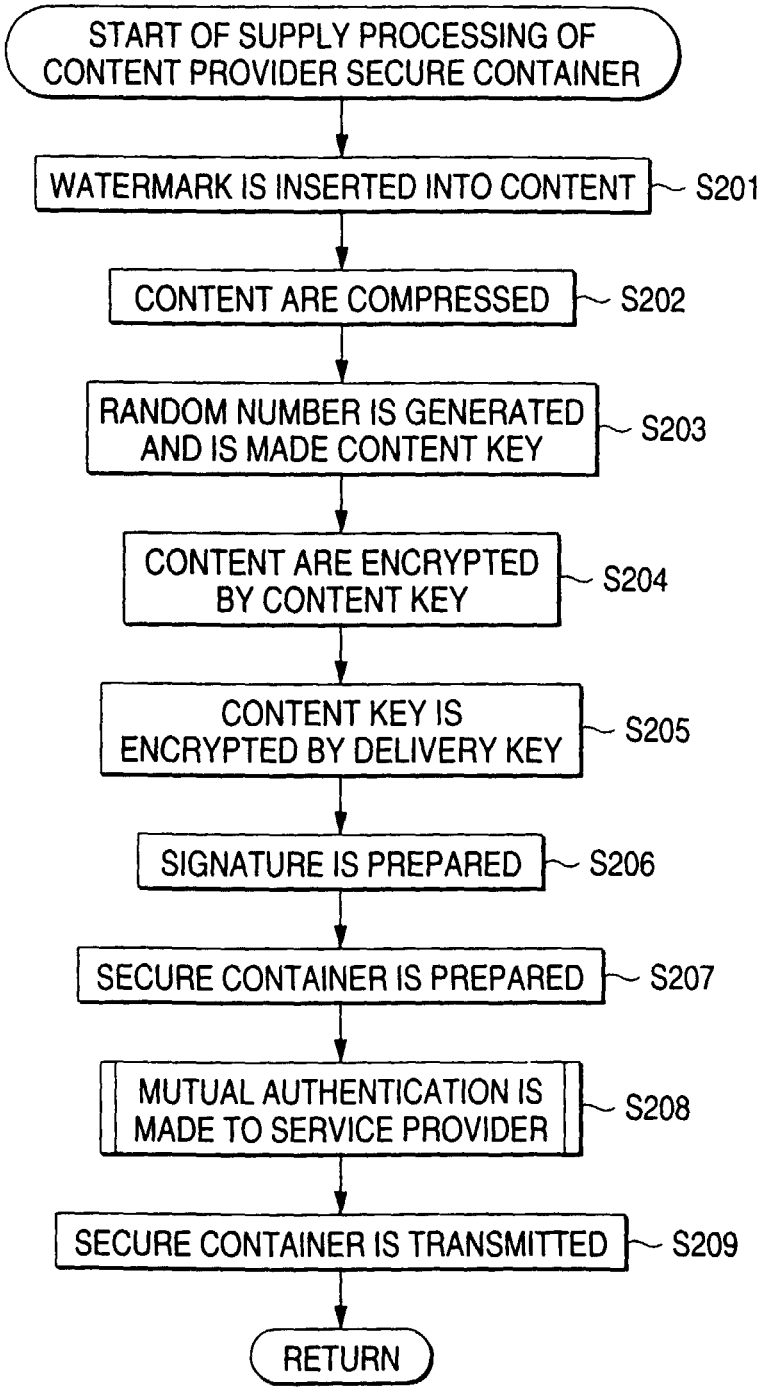

START OF SUPPLY PROCESSING OF CONTENT PROVIDER SECURE CONTAINER
WATERMARK IS INSERTED INTO CONTENT
S201
CONTENT ARE COMPRESSED
S202
RANDOM NUMBER IS GENERATED AND IS MADE CONTENT KEY
S203
CONTENT ARE ENCRYPTED BY CONTENT KEY
S204
CONTENT KEY IS ENCRYPTED BY DELIVERY KEY
S205
SIGNATURE IS PREPARED
S206
SECURE CONTAINER IS PREPARED
S207
MUTUAL AUTHENTICATION IS MADE TO SERVICE PROVIDER
S208
SECURE CONTAINER IS TRANSMITTED
S209
RETURN

FIG. 44

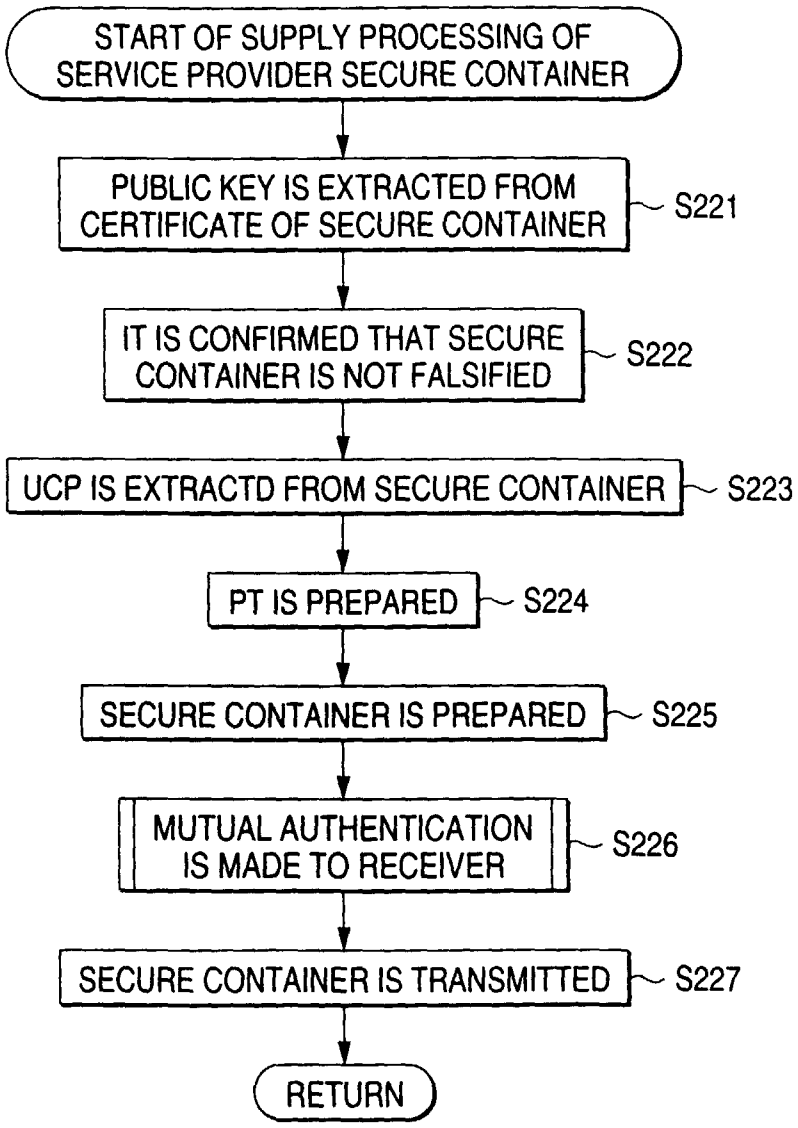

START OF SUPPLY PROCESSING OF SERVICE PROVIDER SECURE CONTAINER
PUBLIC KEY IS EXTRACTED FROM CERTIFICATE OF SECURE CONTAINER
S221
IT IS CONFIRMED THAT SECURE CONTAINER IS NOT FALSIFIED
S222
UCP IS EXTRACTD FROM SECURE CONTAINER
S223
PT IS PREPARED
S224
SECURE CONTAINER IS PREPARED
S225
MUTUAL AUTHENTICATION IS MADE TO RECEIVER
S226
SECURE CONTAINER IS TRANSMITTED
S227
RETURN

FIG. 45

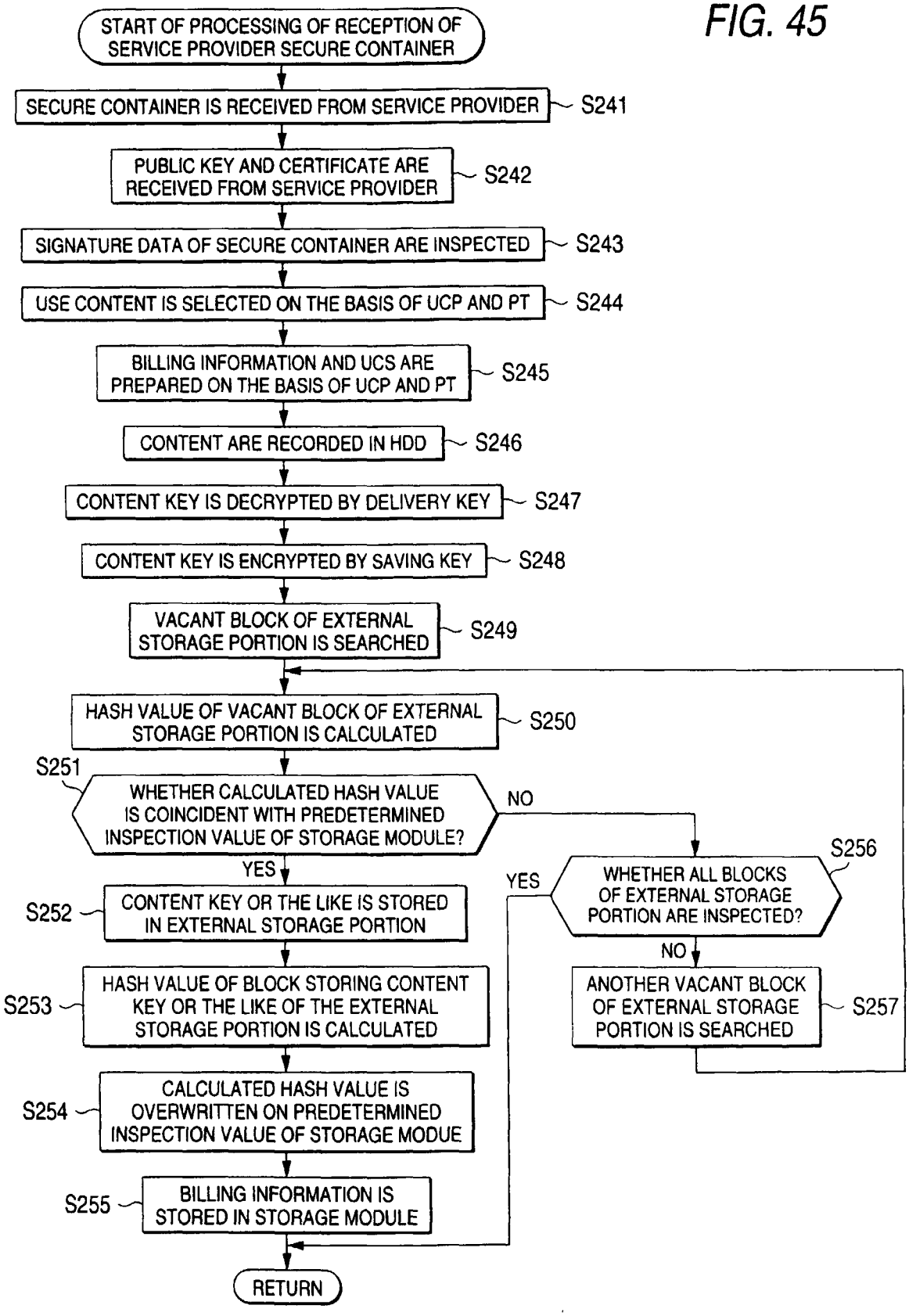

START OF PROCESSING OF RECEPTION OF SERVICE PROVIDER SECURE CONTAINER
SECURE CONTAINER IS RECEIVED FROM SERVICE PROVIDER
S241
PUBLIC KEY AND CERTIFICATE ARE RECEIVED FROM SERVICE PROVIDER
S242
SIGNATURE DATA OF SECURE CONTAINER ARE INSPECTED
S243
USE CONTENT IS SELECTED ON THE BASIS OF UCP AND PT
S244
BILLING INFORMATION AND UCS ARE PREPARED ON THE BASIS OF UCP AND PT
S245
CONTENT ARE RECORDED IN HDD
S246
CONTENT KEY IS DECRYPTED BY DELIVERY KEY
S247
CONTENT KEY IS ENCRYPTED BY SAVING KEY
S248
VACANT BLOCK OF EXTERNAL STORAGE PORTION IS SEARCHED
S249
HASH VALUE OF VACANT BLOCK OF EXTERNAL STORAGE PORTION IS CALCULATED
S250
S251
WHETHER CALCULATED HASH VALUE IS COINCIDENT WITH PREDETERMINED INSPECTION VALUE OF STORAGE MODULE?
NO
YES
S252
CONTENT KEY OR THE LIKE IS STORED IN EXTERNAL STORAGE PORTION
S253
HASH VALUE OF BLOCK STORING CONTENT KEY OR THE LIKE OF THE EXTERNAL STORAGE PORTION IS CALCULATED
S254
CALCULATED HASH VALUE IS OVERWRITTEN ON PREDETERMINED INSPECTION VALUE OF STORAGE MODUE
S255
BILLING INFORMATION IS STORED IN STORAGE MODULE
RETURN
S256
WHETHER ALL BLOCKS OF EXTERNAL STORAGE PORTION ARE INSPECTED?
YES
NO
ANOTHER VACANT BLOCK OF EXTERNAL STORAGE PORTION IS SEARCHED
S257

FIG. 46

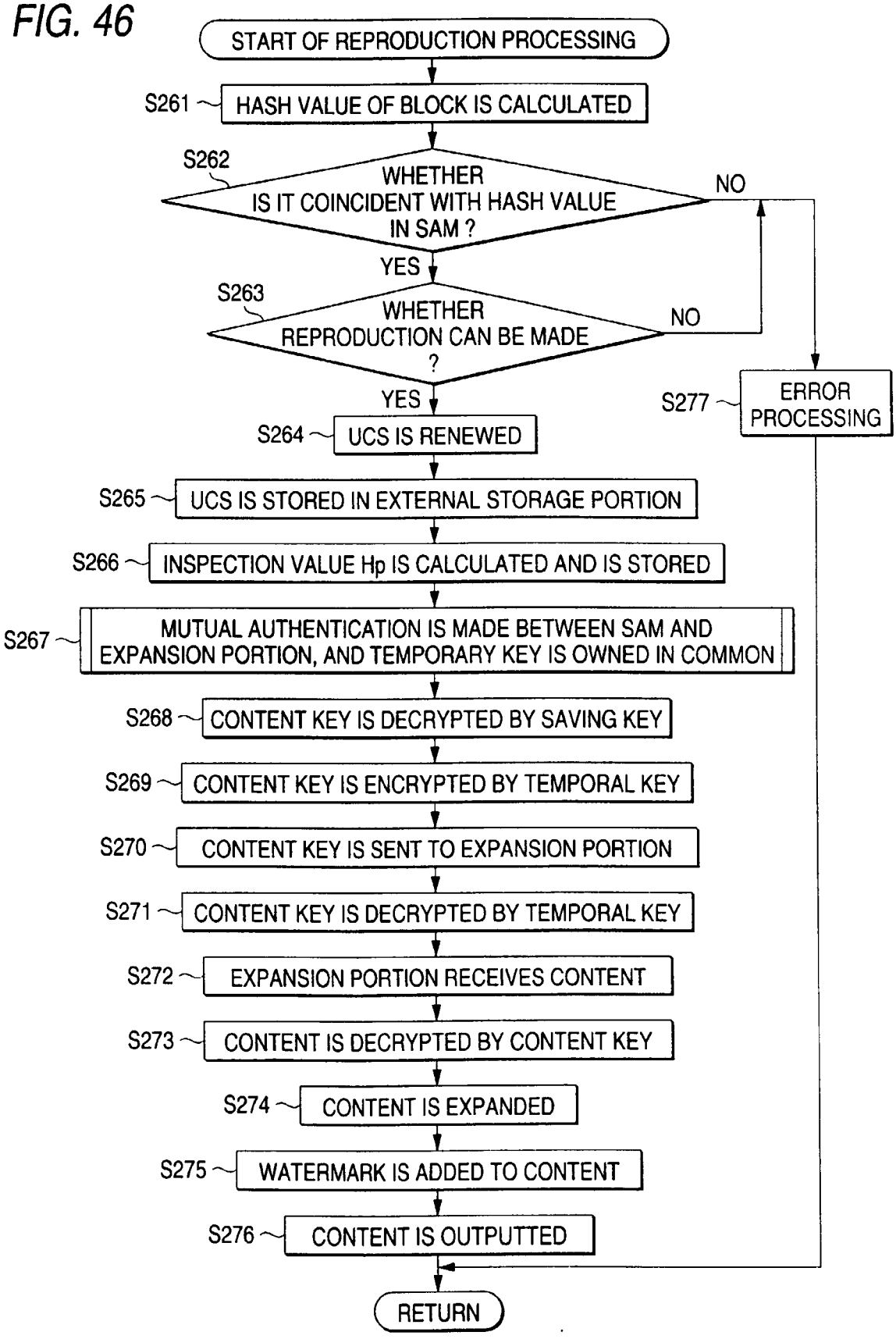

START OF REPRODUCTION PROCESSING
S261
HASH VALUE OF BLOCK IS CALCULATED
S262
WHETHER IS IT COINCIDENT WITH HASH VALUE IN SAM ?
NO
YES
S263
WHETHER REPRODUCTION CAN BE MADE ?
NO
YES
S277
ERROR PROCESSING
S264
UCS IS RENEWED
S265
UCS IS STORED IN EXTERNAL STORAGE PORTION
S266
INSPECTION VALUE Hp IS CALCULATED AND IS STORED
S267
MUTUAL AUTHENTICATION IS MADE BETWEEN SAM AND EXPANSION PORTION, AND TEMPORARY KEY IS OWNED IN COMMON
S268
CONTENT KEY IS DECRYPTED BY SAVING KEY
S269
CONTENT KEY IS ENCRYPTED BY TEMPORAL KEY
S270
CONTENT KEY IS SENT TO EXPANSION PORTION
S271
CONTENT KEY IS DECRYPTED BY TEMPORAL KEY
S272
EXPANSION PORTION RECEIVES CONTENT
S273
CONTENT IS DECRYPTED BY CONTENT KEY
S274
CONTENT IS EXPANDED
S275
WATERMARK IS ADDED TO CONTENT
S276
CONTENT IS OUTPUTTED
RETURN

FIG. 47

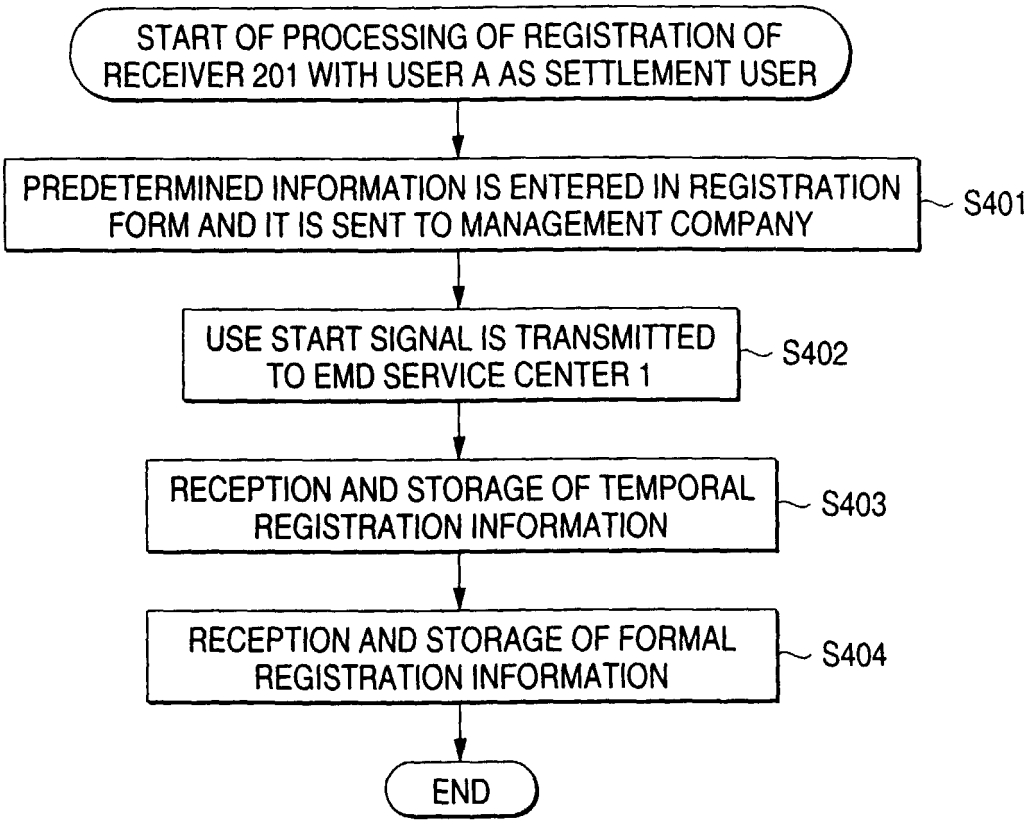

START OF PROCESSING OF REGISTRATION OF RECEIVER 201 WITH USER A AS SETTLEMENT USER
PREDETERMINED INFORMATION IS ENTERED IN REGISTRATION FORM AND IT IS SENT TO MANAGEMENT COMPANY
S401
USE START SIGNAL IS TRANSMITTED TO EMD SERVICE CENTER 1
S402
RECEPTION AND STORAGE OF TEMPORAL REGISTRATION INFORMATION
S403
RECEPTION AND STORAGE OF FORMAL REGISTRATION INFORMATION
S404
END

FIG. 48

REGISTRATION FORM OF RECEIVER 201

		ID OF SAM 212
NAME	NAME OF USER A	OPEN: (PERMISSIBLE) OR IMPERMISSIBLE
ADDRESS	ADDRESS OF USER A	OPEN: PERMISSIBLE OR (IMPERMISSIBLE)
TELEPHONE NUMBER	TELEPHONE NUMBER OF USER A	OPEN: PERMISSIBLE OR (IMPERMISSIBLE)
INFORMATION OF SETTLEMENT AGENCY	NUMBER OF CREDIT CARD OF USER A	
BIRTH DATE	BIRTH DATE OF USER A	OPEN: (PERMISSIBLE) OR IMPERMISSIBLE
AGE	35	OPEN: (PERMISSIBLE) OR IMPERMISSIBLE
GENDER	MALE	OPEN: PERMISSIBLE OR (IMPERMISSIBLE)
PASSWORD	_____	
USER ID	_____	
SETTLEMENT ID	_____	

EP 1 045 321 A2

FIG. 49

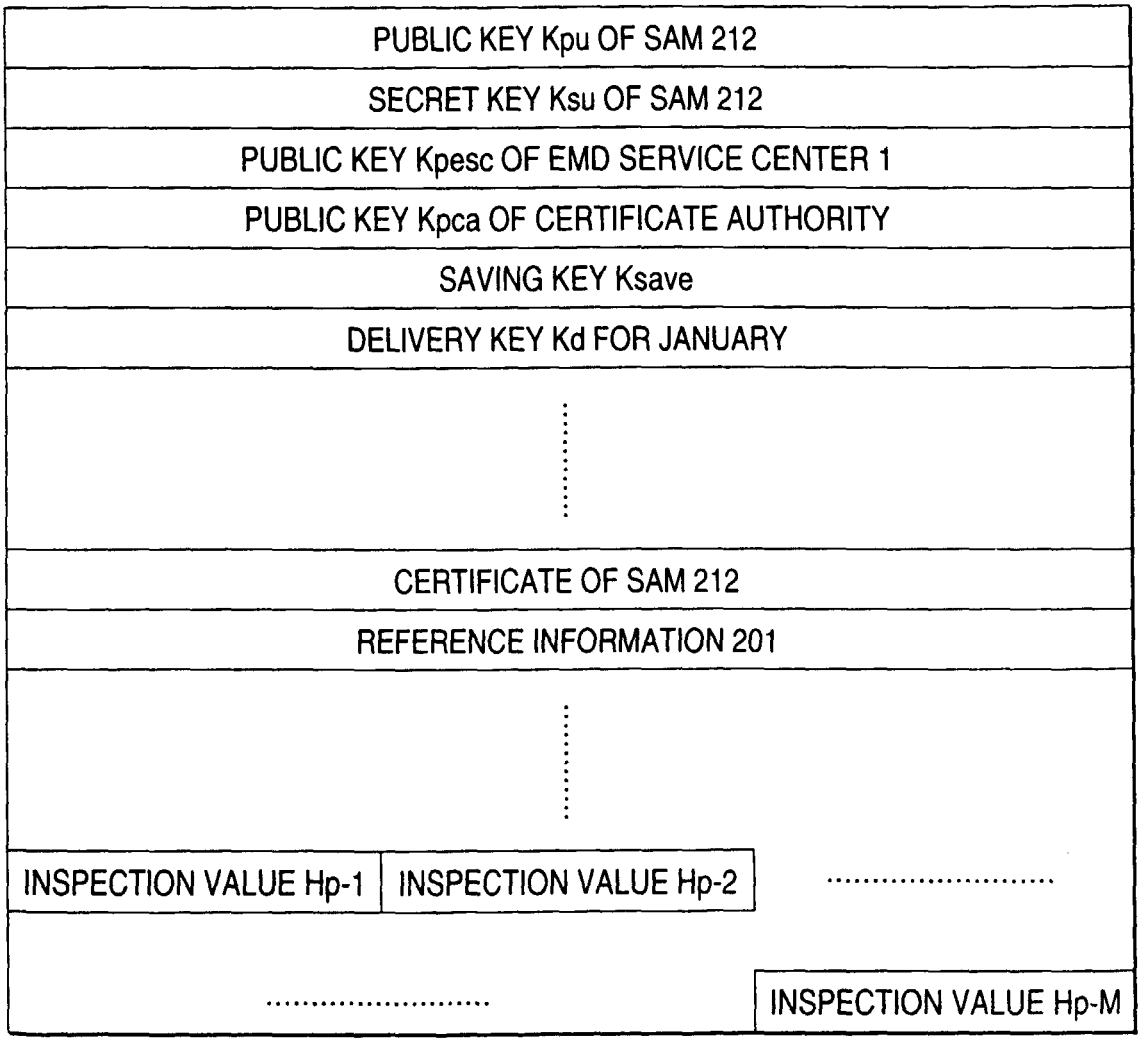

PUBLIC KEY Kpu OF SAM 212
SECRET KEY Ksu OF SAM 212
PUBLIC KEY Kpesc OF EMD SERVICE CENTER 1
PUBLIC KEY Kpca OF CERTIFICATE AUTHORITY
SAVING KEY Ksave
DELIVERY KEY Kd FOR JANUARY
CERTIFICATE OF SAM 212
REFERENCE INFORMATION 201
INSPECTION VALUE Hp-1
INSPECTION VALUE Hp-2
INSPECTION VALUE Hp-M

FIG. 50

REFERENCE INFORMATION 201

ID OF SAM		ID OF SAM 212
EQUIPMENT NUMBER		EQUIPMENT NUMBER (NO. 100) OF RECEIVER 201
SETTLEMENT ID		
UPPER LIMIT AMOUNT OF BILLING		UPPER LIMIT AMOUNT AT TEMPORAL REGISTRATION
SETTLEMENT USER INFORMATION	NAME	NAME OF USER A
	ADDRESS	ADDRESS OF USER A
	TELEPHONE NUMBER	TELEPHONE NUMBER OF USER A
	SETTLEMENT AGENCY INFORMATION	SETTLEMENT AGENCY INFORMATION OF USER A
	BIRTH DATE	BIRTH DATE OF USER A
	AGE	AGE OF USER A
	GENDER	GENDER OF USER A
	ID OF USER	ID OF USER A
	PASSWORD	PASSWORD OF USER A
SUBORDINATE USER INFORMATION	NAME	
	ADDRESS	
	TELEPHONE NUMBER	
	BIRTH DATE	
	GENDER	
	ID OF USER	
	PASSWORD	
USE POINT INFORMATION		

INFORMATION WHICH IS NOT PERMITTED TO BE MADE OPEN
INFORMATION WHICH IS PERMITTED TO BE MADE OPEN

FIG. 51

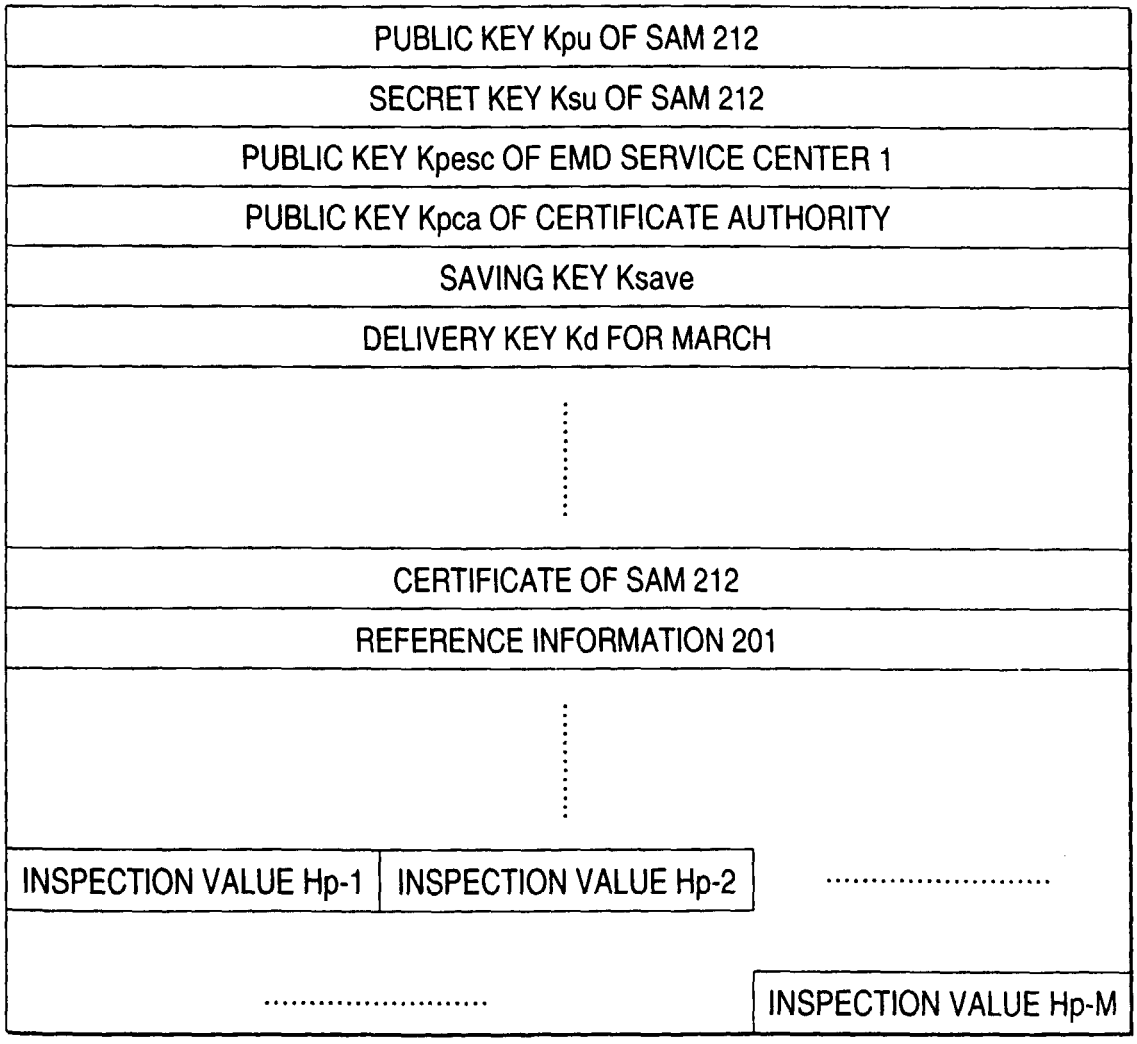

PUBLIC KEY Kpu OF SAM 212
SECRET KEY Ksu OF SAM 212
PUBLIC KEY Kpesc OF EMD SERVICE CENTER 1
PUBLIC KEY Kpca OF CERTIFICATE AUTHORITY
SAVING KEY Ksave
DELIVERY KEY Kd FOR MARCH
CERTIFICATE OF SAM 212
REFERENCE INFORMATION 201
INSPECTION VALUE Hp-1
INSPECTION VALUE Hp-2
INSPECTION VALUE Hp-M

FIG. 52

REFERENCE INFORMATION 201

ID OF SAM		ID OF SAM 212
EQUIPMENT NUMBER		EQUIPMENT NUMBER (NO. 100) OF RECEIVER 201
SETTLEMENT ID		SETTLEMENT ID OF USER A
UPPER LIMIT AMOUNT OF BILLING		UPPER LIMIT AMOUNT AT FORMAL REGISTRATION
SETTLEMENT USER INFORMATION	NAME	NAME OF USER A
	ADDRESS	ADDRESS OF USER A
	TELEPHONE NUMBER	TELEPHONE NUMBER OF USER A
	SETTLEMENT AGENCY INFORMATION	SETTLEMENT AGENCY INFORMATION OF USER A
	BIRTH DATE	BIRTH DATE OF USER A
	AGE	AGE OF USER A
	GENDER	GENDER OF USER A
	ID OF USER	ID OF USER A
	PASSWORD	PASSWORD OF USER A
SUBORDINATE USER INFORMATION	NAME	
	ADDRESS	
	TELEPHONE NUMBER	
	BIRTH DATE	
	GENDER	
	ID OF USER	
	PASSWORD	
USE POINT INFORMATION		

INFORMATION WHICH IS NOT PERMITTED TO BE MADE OPEN
INFORMATION WHICH IS PERMITTED TO BE MADE OPEN

FIG. 53

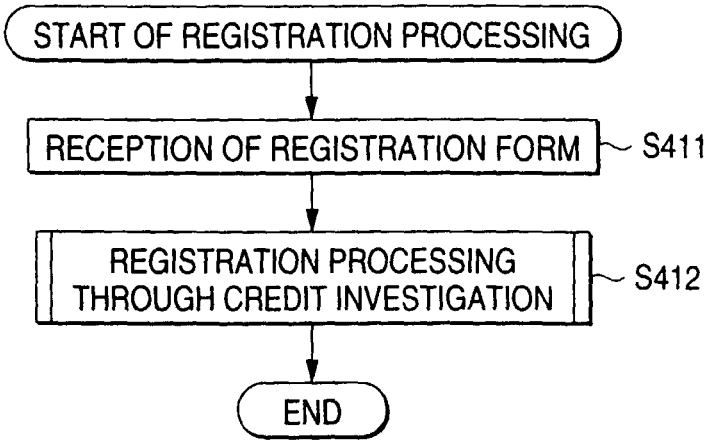

START OF REGISTRATION PROCESSING
RECEPTION OF REGISTRATION FORM
S411
REGISTRATION PROCESSING THROUGH CREDIT INVESTIGATION
S412
END

FIG. 54

SYSTEM REGISTRATION INFORMATION

ID OF SAM		ID OF SAM 62	ID OF SAM 212
EQUIPMENT NUMBER		EQUIPMENT NUMBER (NO. 100) OF RECEIVER 51	EQUIPMENT NUMBER (NO. 100) OF RECEIVER 201
SETTLEMENT ID		SETTLEMENT ID OF USER F	
SETTLEMENT USER INFORMATION	NAME	NAME OF USER F	NAME OF USER A
	ADDRESS	ADDRESS OF USER F	ADDRESS OF USER A
	TELEPHONE NUMBER	TELEPHONE NUMBER OF USER F	TELEPHONE NUMBER OF USER A
	SETTLEMENT AGENCY INFORMATION	SETTLEMENT INFORMATION OF USER F	SETTLEMENT INFORMATION OF USER A
	BIRTH DATE	BIRTH DATE OF USER F	BIRTH DATE OF USER A
	AGE	AGE (21) OF USER F	AGE (35) OF USER A
	GENDER	GENDER (MALE) OF USER F	GENDER (MALE) OF USER A
	ID OF USER	ID OF USER F	
	PASSWORD	PASSWORD OF USER F	
SUBORDINATE USER INFORMATION	NAME		
	ADDRESS		
	TELEPHONE NUMBER		
	BIRTH DATE		
	GENDER		
	ID OF USER		
	PASSWORD		
USE POINT INFORMATION		USE POINT INFORMATION OF RECEIVER 51	

INFORMATION WHICH IS NOT PERMITTED TO BE MADE OPEN

INFORMATION WHICH IS PERMITTED TO BE MADE OPEN

FIG. 55

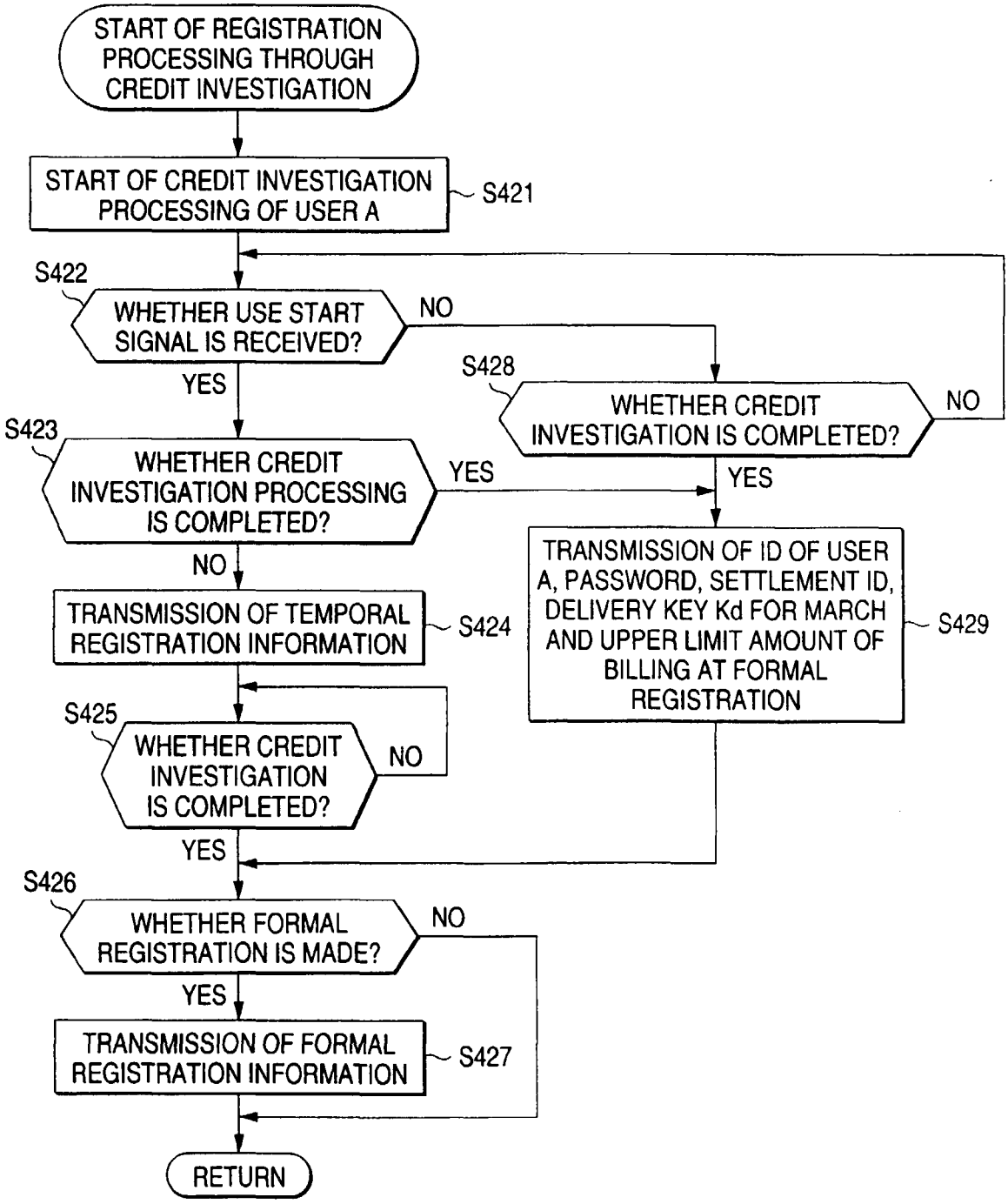

START OF REGISTRATION PROCESSING THROUGH CREDIT INVESTIGATION
START OF CREDIT INVESTIGATION PROCESSING OF USER A
S421
S422
WHETHER USE START SIGNAL IS RECEIVED?
NO
YES
S428
WHETHER CREDIT INVESTIGATION IS COMPLETED?
NO
S423
WHETHER CREDIT INVESTIGATION PROCESSING IS COMPLETED?
YES
YES
NO
TRANSMISSION OF TEMPORAL REGISTRATION INFORMATION
S424
TRANSMISSION OF ID OF USER A, PASSWORD, SETTLEMENT ID, DELIVERY KEY Kd FOR MARCH AND UPPER LIMIT AMOUNT OF BILLING AT FORMAL REGISTRATION
S429
S425
WHETHER CREDIT INVESTIGATION IS COMPLETED?
NO
YES
S426
WHETHER FORMAL REGISTRATION IS MADE?
NO
YES
TRANSMISSION OF FORMAL REGISTRATION INFORMATION
S427
RETURN

FIG. 56

SYSTEM REGISTRATION INFORMATION

ID OF SAM		ID OF SAM 62	ID OF SAM 212
EQUIPMENT NUMBER		EQUIPMENT NUMBER (NO. 100) OF RECEIVER 51	EQUIPMENT NUMBER (NO. 100) OF RECEIVER 201
SETTLEMENT ID		SETTLEMENT ID OF USER F	
SETTLEMENT USER INFORMATION	NAME	NAME OF USER F	NAME OF USER A
	ADDRESS	ADDRESS OF USER F	ADDRESS OF USER A
	TELEPHONE NUMBER	TELEPHONE NUMBER OF USER F	TELEPHONE NUMBER OF USER A
	SETTLEMENT AGENCY INFORMATION	SETTLEMENT INFORMATION OF USER F	SETTLEMENT INFORMATION OF USER A
	BIRTH DATE	BIRTH DATE OF USER F	BIRTH DATE OF USER A
	AGE	AGE (21) OF USER F	AGE (35) OF USER A
	GENDER	GENDER (MALE) OF USER F	GENDER (MALE) OF USER A
	ID OF USER	ID OF USER F	ID OF USER A
	PASSWORD	PASSWORD OF USER F	PASSWORD OF USER A
SUBORDINATE USER INFORMATION	NAME		
	ADDRESS		
	TELEPHONE NUMBER		
	BIRTH DATE		
	GENDER		
	ID OF USER		
	PASSWORD		
USE POINT INFORMATION		USE POINT INFORMATION OF RECEIVER 51	

INFORMATION WHICH IS NOT PERMITTED TO BE MADE OPEN

INFORMATION WHICH IS PERMITTED TO BE MADE OPEN

FIG. 57

SYSTEM REGISTRATION INFORMATION

ID OF SAM		ID OF SAM 62	ID OF SAM 212
EQUIPMENT NUMBER		EQUIPMENT NUMBER (NO. 100) OF RECEIVER 51	EQUIPMENT NUMBER (NO. 100) OF RECEIVER 201
SETTLEMENT ID		SETTLEMENT ID OF USER F	SETTLEMENT ID OF USER A
SETTLEMENT USER INFORMATION	NAME	NAME OF USER F	NAME OF USER A
	ADDRESS	ADDRESS OF USER F	ADDRESS OF USER A
	TELEPHONE NUMBER	TELEPHONE NUMBER OF USER F	TELEPHONE NUMBER OF USER A
	SETTLEMENT AGENCY INFORMATION	SETTLEMENT INFORMATION OF USER F	SETTLEMENT INFORMATION OF USER A
	BIRTH DATE	BIRTH DATE OF USER F	BIRTH DATE OF USER A
	AGE	AGE OF USER F	AGE OF USER A
	GENDER	GENDER OF USER F	GENDER OF USER A
	ID OF USER	ID OF USER F	ID OF USER A
	PASSWORD	PASSWORD OF USER F	PASSWORD OF USER A
SUBORDINATE USER INFORMATION	NAME		
	ADDRESS		
	TELEPHONE NUMBER		
	BIRTH DATE		
	GENDER		
	ID OF USER		
	PASSWORD		
USE POINT INFORMATION		USE POINT INFORMATION OF RECEIVER 51	

INFORMATION WHICH IS NOT PERMITTED TO BE MADE OPEN

INFORMATION WHICH IS PERMITTED TO BE MADE OPEN

FIG. 58

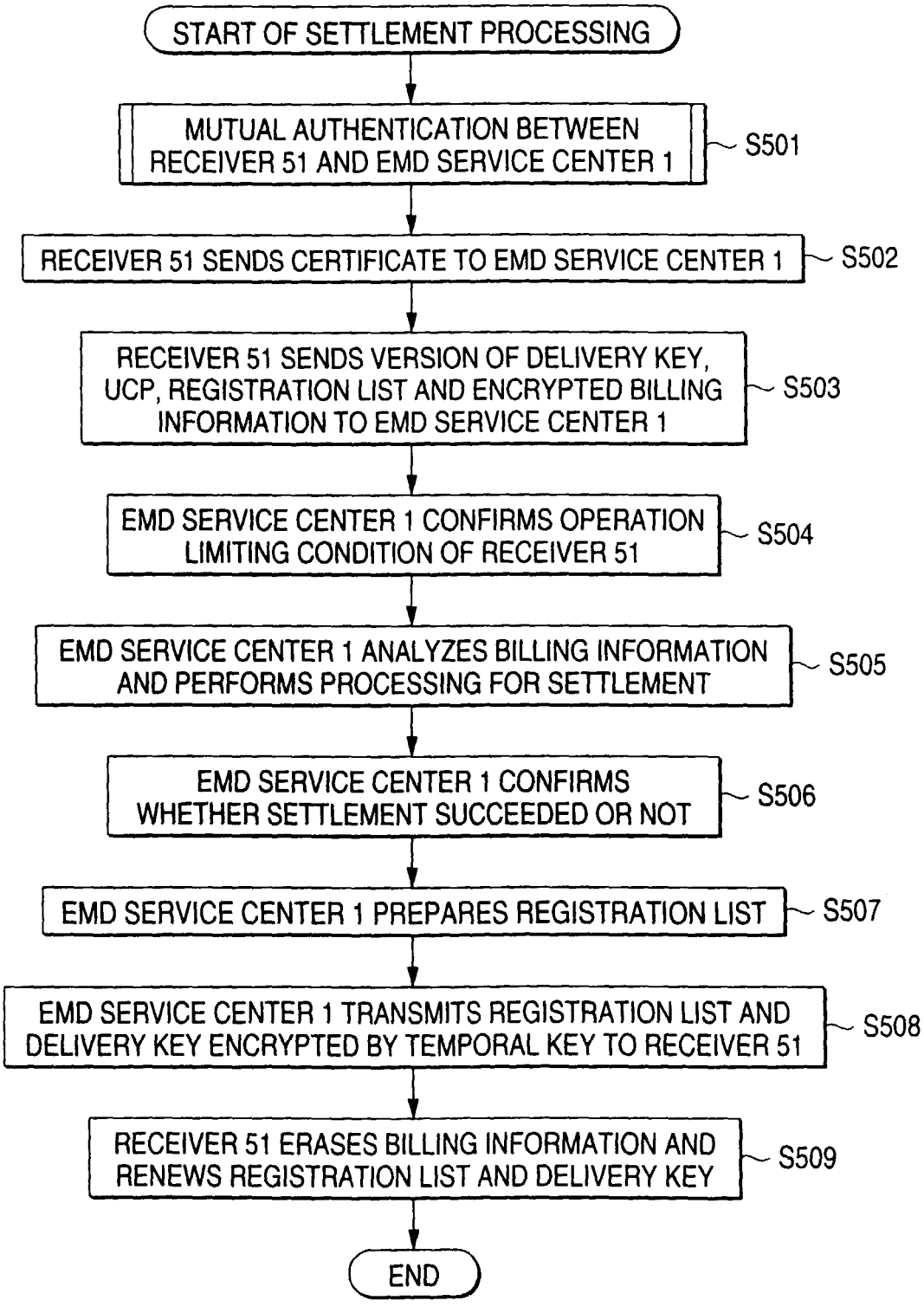

START OF SETTLEMENT PROCESSING
MUTUAL AUTHENTICATION BETWEEN RECEIVER 51 AND EMD SERVICE CENTER 1
S501
RECEIVER 51 SENDS CERTIFICATE TO EMD SERVICE CENTER 1
S502
RECEIVER 51 SENDS VERSION OF DELIVERY KEY, UCP, REGISTRATION LIST AND ENCRYPTED BILLING INFORMATION TO EMD SERVICE CENTER 1
S503
EMD SERVICE CENTER 1 CONFIRMS OPERATION LIMITING CONDITION OF RECEIVER 51
S504
EMD SERVICE CENTER 1 ANALYZES BILLING INFORMATION AND PERFORMS PROCESSING FOR SETTLEMENT
S505
EMD SERVICE CENTER 1 CONFIRMS WHETHER SETTLEMENT SUCCEEDED OR NOT
S506
EMD SERVICE CENTER 1 PREPARES REGISTRATION LIST
S507
EMD SERVICE CENTER 1 TRANSMITS REGISTRATION LIST AND DELIVERY KEY ENCRYPTED BY TEMPORAL KEY TO RECEIVER 51
S508
RECEIVER 51 ERASES BILLING INFORMATION AND RENEWS REGISTRATION LIST AND DELIVERY KEY
S509
END

FIG. 59

OPEN INFORMATION

ID OF CONTENT	OPEN
CONTENT INFORMATION (NAME OF MUSIC, NAME OF SINGER)	OPEN
USE FORMAT	OPEN
SELLING PRICE	OPEN

NAME	REQUIRED
ADDRESS	REQUIRED
TELEPHONE NUMBER	REQUIRED
BIRTH DATE	REQUIRED
AGE	REQUIRED
GENDER	REQUIRED

FIG. 60

ARTIST SALE INFORMATION

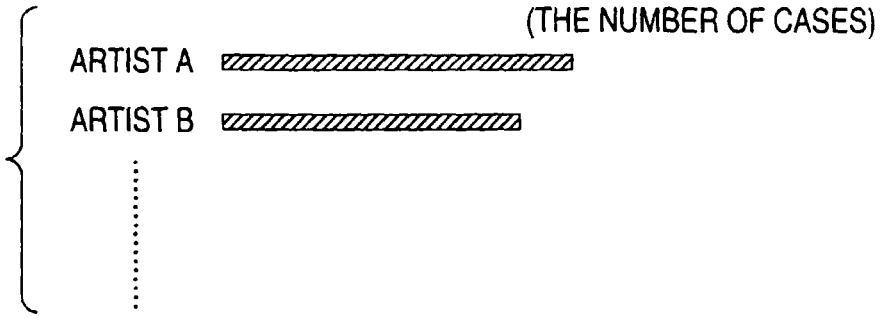


FIG. 61

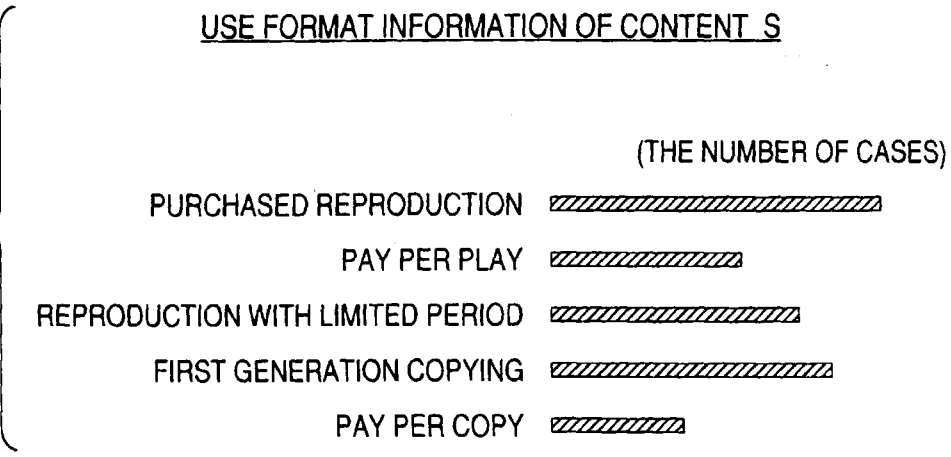

USE FORMAT INFORMATION OF CONTENT S
(THE NUMBER OF CASES)
PURCHASED REPRODUCTION
PAY PER PLAY
REPRODUCTION WITH LIMITED PERIOD
FIRST GENERATION COPYING
PAY PER COPY

FIG. 62

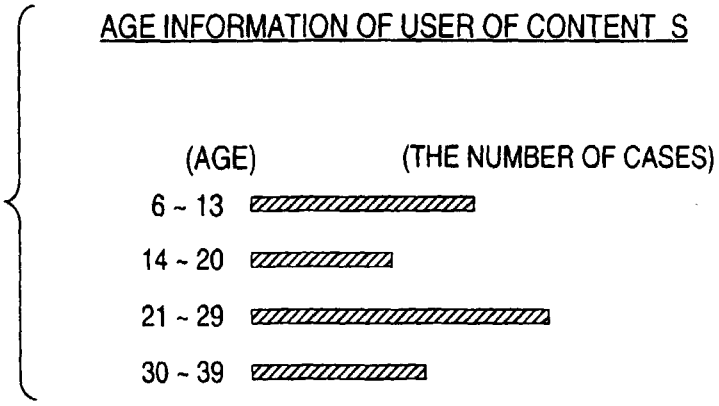

AGE INFORMATION OF USER OF CONTENT S
(AGE)
(THE NUMBER OF CASES)
6 ~ 13
14 ~ 20
21 ~ 29
30 ~ 39

FIG. 63

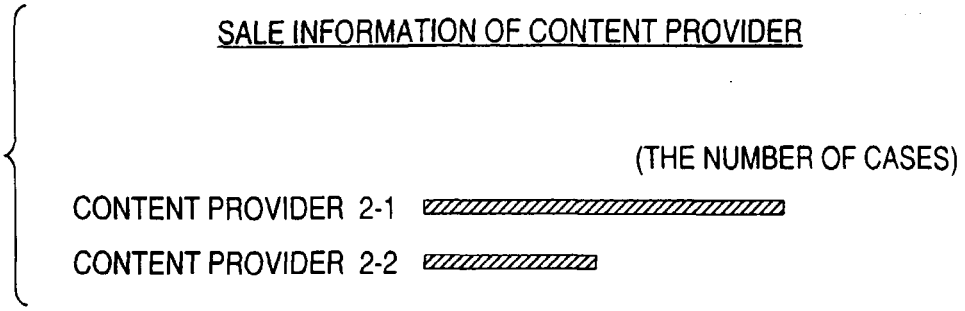
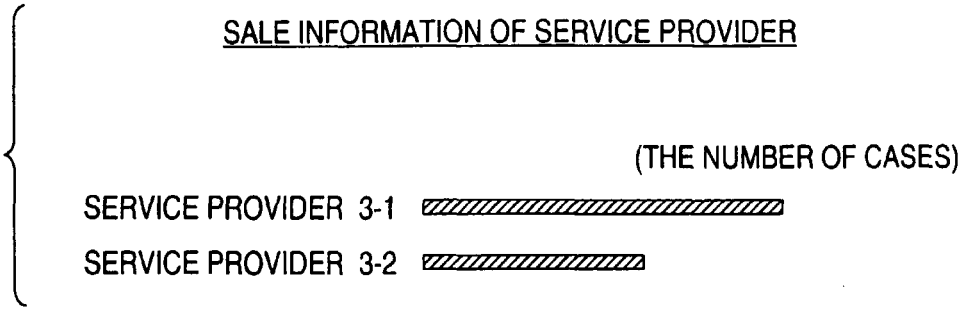

SALE INFORMATION OF CONTENT PROVIDER
(THE NUMBER OF CASES)
CONTENT PROVIDER 2-1
CONTENT PROVIDER 2-2

FIG. 64


SALE INFORMATION OF SERVICE PROVIDER
(THE NUMBER OF CASES)
SERVICE PROVIDER 3-1
SERVICE PROVIDER 3-2