

D E S C R I P T I O N

COOPERATION SERVICE PROVIDING SYSTEM AND SERVER
APPARATUS

5

Technical Field

Embodiments described herein relate generally to a cooperation service providing system and a server apparatus.

10

Background Art

As a cooperation service providing scheme in which a plurality of apparatuses mutually transmit/receive information to provide one service, there are provided a scheme of directly connecting each apparatus to another apparatus and a scheme of connecting respective apparatuses via a common bus having an ID conversion function, a log function, and the like. Among these two schemes, in the former scheme of directly connecting each apparatus to another apparatus, it is difficult to verify/audit transmitted/received contents later since there is no point where pieces of information (to be referred to as cooperation information hereinafter) mutually transmitted/received between apparatuses are integrated and managed. Consequently, the latter scheme of connecting respective apparatuses via a common bus having an ID conversion function, a log function, and the like is desired.

15

20

25

Even if IDs for identifying pieces of information held in respective apparatuses are ones for identifying the same information, the IDs themselves are generally different for the respective apparatuses. The ID conversion function is a function of certifying that IDs are ones for identifying the same information even if the IDs themselves are different for respective apparatuses. Note that examples of a scheme for implementing the ID conversion function are a table reference scheme and a function scheme.

For example, as a cooperation service providing technique to which the table reference scheme is applied, there is provided a cooperation service providing technique of implementing cooperation of IDs (that is, transmission/reception of cooperation information) between a plurality of apparatuses by storing a table in advance in a cooperation apparatus which causes the plurality of apparatuses to cooperate with each other, and referring to the table when causing the respective apparatuses to cooperate with each other.

Furthermore, as a cooperation service providing technique to which the function scheme is applied, for example, there is provided a cooperation service providing technique of implementing cooperation of IDs (that is, transmission/reception of cooperation information) between a plurality of apparatuses by decrypting, on a cooperation apparatus, information containing an ID transmitted from one of respective apparatuses to cooperate with each other

by using secret information in AES, and then re-converting the information into a code for the other apparatus to transmit it.

5 In addition, as a cooperation service providing technique to which the function scheme is applied, there is provided a cooperation service providing technique of implementing transmission/reception of cooperation information between respective apparatuses by using a public key cryptosystem for the cooperation information.

10 As for the public key cryptosystem, a technique called proxy re-encryption will now be described.

A basic model of this technique is formed from five functions (to also be referred to as algorithms hereinafter) of key generation, encryption, decryption, re-encryption key generation, and re-encryption. The key generation function, encryption function, and decryption function are the same as those of the normal public key cryptosystem.

(Key Generation) $\text{KeyGen}(1^k) \rightarrow (\text{pk}, \text{sk})$

20 Upon input of a security parameter 1^k , a key generation algorithm KeyGen outputs a set (pk, sk) of a public key pk and a private key sk .

(Encryption) $\text{Enc}(\text{pk}_A, m) \rightarrow C_A$

25 Upon input of a public key pk_A of a user A and a message m , an encryption algorithm Enc outputs ciphertext C_A destined for the user A.

(Decryption) $\text{Dec}(\text{sk}_A, C_A) \rightarrow m$

Upon input of a private key sk_A of the user A and the ciphertext C_A destined for the user A, a decryption algorithm Dec outputs the message m .

(Re-Encryption Key Generation) $ReKeyGen(pk_A, sk_A, pk_B, sk_B) \rightarrow rk_{A \rightarrow B}$

Upon input of the public key pk_A and private key sk_A of the user A and a public key pk_B and private key sk_B of a user B, a re-encryption key generation algorithm $ReKeyGen$ outputs a re-encryption key $rk_{A \rightarrow B}$.

(Re-Encryption) $ReEnc(rk_{A \rightarrow B}, C_A) \rightarrow C_B$

Upon input of the re-encryption key $rk_{A \rightarrow B}$ and the ciphertext C_A destined for the user A, a re-encryption algorithm $ReEnc$ outputs ciphertext C_B destined for the user B.

The basic model has been explained. In accordance with a scheme of implementing re-encryption, however, a model in which inputs to functions are different and a model which includes functions and keys in addition to the above-described functions and keys are also considered.

For example, as for the input of the re-encryption key generation algorithm, a model called a non-interactive model which eliminates the need for the private key sk_B of the user B, and a model in which the re-encryption key $rk_{A \rightarrow B}$ destined for the user B and a private key sk_C of a user C are input instead of the private key sk_A of the user A are considered.

In addition, there are known a model called a

unidirectional model in which re-encryption of cyphertext $C_A \rightarrow C_B$ can be performed using the re-encryption key $rk_{A \rightarrow B}$ while inverse conversion of cyphertext $C_B \rightarrow C_A$ cannot be performed, and a model called a bidirectional model in which inverse conversion can also be performed. Note that in the bidirectional mode, the re-encryption key $rk_{A \rightarrow B}$ may also be represented by $rk_{A \leftrightarrow B}$.

Furthermore, among public key cryptosystems, an ID-based encryption scheme is considered. In this case, the number of function setup operations for master key generation increases, a master key and ID are additionally input to the key generation algorithm KeyGen. In ID-based encryption, the public key pk serves as an ID.

As practical examples of the schemes, there are known schemes described in non-patent literatures 3 and 4 for the unidirectional model, a scheme described in non-patent literature 5 for the bidirectional model, and schemes described in non-patent literatures 6 and 7 and the like for ID-based encryption. Note that embodiments refer to a scheme described in non-patent literature 8.

Citation List

Patent Literatures

Patent Literature 1: Jpn. Pat. Appln. KOKAI
Publication No. 2006-195791

Non-Patent Literatures

Non-Patent Literature 1: M. Blaze, M. Strauss. Atomic
Proxy Cryptography. AT&T Labs Research TR98.5.1, 1997.

Non-Patent Literature 2: M. Blaze, G. Bleumer, M. Strauss. Divertible Protocols and Atomic Proxy Cryptography. In Eurocrypt'98, LNCS 1403, pp.127-144, 1998.

Non-Patent Literature 3: G. Ateniese, K. Fu, M. Green, S. Hohenberger. Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage. In NDSS'05, 2005.

Non-Patent Literature 4: B. Libert, D. Vergnaud. Tracing Malicious Proxies in Proxy Re-Encryption. In Pairing 2008, 2008.

Non-Patent Literature 5: R. Canetti, S. Hohenberger. Chosen-Ciphertext Secure Proxy Re-Encryption. In ACM CCS'07, 2007.

Non-Patent Literature 6: M. Green, G. Ateniese. Identity-Based Proxy Re-encryption. In ACN'07, 2007.

Non-Patent Literature 7: T. Matsuo. Proxy Re-encryption Systems for Identity-based Encryption. In Pairing 2007, 2007.

Non-Patent Literature 8: Benoit Libert, Damien Vergnaud, "Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption", Public Key Cryptography 2008, pp. 360-279.

Non-Patent Literature 9: G. Ateniese, S. Hohenberger, "Proxy re-signature: new definitions, algorithm, and applications", ACM Conference on Computer and Communications Security 2005, pp. 310-319.

Non-Patent Literature 10: A. Menezes, P. van Oorschot, S. Vanstone, "Handbook of Applied Cryptography",

CRC Press, (1996).

Summary of Invention

Technical Problem

In the above cooperation service providing techniques,
5 however, pieces of cooperation information (that is, IDs)
can be linked with each other on the cooperation apparatus,
and a process of exchanging cooperation information between
respective apparatuses cannot be audited/verified later on
the cooperation apparatus.

10 Problems to be solved by the present invention are to
prevent pieces of cooperation information from being linked
with each other on a cooperation apparatus, and provide a
cooperation service providing system which allows
auditing/verification to be performed later on the
15 cooperation apparatus, and a server apparatus.

In a cooperation service providing system according to
an embodiment, a re-encryption key issuing apparatus, a
plurality of service apparatuses for providing various
services to a user by using an ID issued for identifying
20 the user, and a cooperation apparatus for causing the
plurality of service apparatuses to cooperate with each
other are communicably connected to each other.

The cooperation apparatus comprises first storage
means, second storage means, first generation means, first
25 transmission means, and second transmission means.

The first storage means stores public keys of the
re-encryption key issuing apparatus and the service

apparatuses.

The second storage means stores a re-encryption key for implementing re-encryption processing of enabling cyphertext data transmitted by each of the service
5 apparatuses to be decrypted using a private key of the other service apparatus without decrypting the cyphertext data into plaintext data.

Upon receiving the cyphertext data transmitted by each of the service apparatuses, the first generation means
10 generates re-encrypted data by performing re-encryption processing for the cyphertext data using the stored re-encryption key.

The first transmission means transmits the generated re-encrypted data to the other service apparatus different
15 from the service apparatus which has transmitted the cyphertext data.

The second transmission means transmits the stored public key to each of the service apparatuses.

Each of the service apparatuses comprises third
20 storage means, fourth storage means, second generation means, third transmission means, acquisition means, readout means, and fourth transmission means.

The third storage means stores the issued ID in association with user information indicating information of
25 the user unique to the service apparatus.

The fourth storage means stores a private key of the service apparatus.

In response to an operation of the user, the second generation means generates ciphertext data by performing encryption processing for the ID of the user using the public key of the encryption key issuing apparatus
5 transmitted by the cooperation apparatus.

The third transmission means transmits, to the cooperation apparatus, a request to acquire user information of a user specified by the ID indicated by the ciphertext data and stored in the other service apparatus,
10 together with the generated ciphertext data.

Upon receiving the re-encrypted data transmitted by the cooperation apparatus, the acquisition means acquires the encrypted ID by decrypting the re-encrypted data using the stored private key.

15 The readout means reads out the user information corresponding to the acquired ID from the third storage means.

The fourth transmission means transmits the readout user information to the other service apparatus via the
20 cooperation apparatus.

Brief Description of Drawings

FIG. 1 is a schematic view showing an example of the arrangement of a cooperation service providing system according to the first embodiment.

25 FIG. 2 is a sequence chart showing an example of key generation processing according to the first embodiment.

FIG. 3 is a sequence chart showing an example of ID

issuing processing according to the first embodiment.

FIG. 4 is a sequence chart showing an example of re-encryption key generation processing according to the first embodiment.

5 FIG. 5 is a sequence chart showing an example of cooperation processing according to the first embodiment.

FIG. 6 is a sequence chart showing an example of code distribution processing according to a modification of the first embodiment.

10 FIG. 7 is a sequence chart showing an example of cooperation processing according to the modification of the first embodiment.

FIG. 8 is a schematic view showing an example of the arrangement of a cooperation service providing system according to another modification of the first embodiment.

FIG. 9 is a sequence chart showing an example of cooperation processing according to the other modification of the first embodiment.

FIG. 10 is a schematic view showing an example of the arrangement of a cooperation service providing system according to the second embodiment.

FIG. 11 is a sequence chart showing an example of cooperation processing according to the second embodiment.

Description of Embodiments

25 In general, according to one embodiment, in a cooperation service providing system, a re-encryption key issuing apparatus, a plurality of service apparatuses for

providing various services to a user by using an ID issued for identifying the user, and a cooperation apparatus for causing the plurality of service apparatuses to cooperate with each other are communicably connected to each other.

5 The cooperation apparatus comprises a first storage device, a second storage device, a first generation device, a first transmission device, and a second transmission device.

10 The first storage device stores public keys of the re-encryption key issuing apparatus and the service apparatuses.

15 The second storage device stores a re-encryption key for implementing re-encryption processing of enabling cyphertext data transmitted by each of the service apparatuses to be decrypted using a private key of the other service apparatus without decrypting the cyphertext data into plaintext data.

20 Upon receiving the ciphertext data transmitted by each of the service apparatuses, the first generation device generates re-encrypted data by performing re-encryption processing for the ciphertext data using the stored re-encryption key.

25 The first transmission device transmits the generated re-encrypted data to the other service apparatus different from the service apparatus which has transmitted the ciphertext data.

 The second transmission device transmits the stored

public key to each of the service apparatuses.

Each of the service apparatuses comprises a third storage device, a fourth storage device, a second generation device, a third transmission device, an acquisition device, a readout device, and a fourth transmission device.

The third storage device stores the issued ID in association with user information indicating information of the user unique to the service apparatus.

The fourth storage device stores a private key of the service apparatus.

In response to an operation of the user, the second generation device generates ciphertext data by performing encryption processing for the ID of the user using the public key of the encryption key issuing apparatus transmitted by the cooperation apparatus.

The third transmission device transmits, to the cooperation apparatus, a request to acquire user information of a user specified by the ID indicated by the ciphertext data and stored in the other service apparatus, together with the generated ciphertext data.

Upon receiving the re-encrypted data transmitted by the cooperation apparatus, the acquisition device acquires the encrypted ID by decrypting the re-encrypted data using the stored private key.

The readout device reads out the user information corresponding to the acquired ID from the third storage

device.

The fourth transmission device transmits the readout user information to the other service apparatus via the cooperation apparatus.

5 [First Embodiment]

FIG. 1 is a schematic view showing an example of the arrangement of a cooperation service providing system according to the first embodiment. As shown in FIG. 1, a cooperation service providing system 1 includes a
10 re-encryption key issuing apparatus 10, a cooperation apparatus (to also be referred to as a server apparatus hereinafter) 20, an ID issuing apparatus 30, and a plurality of service apparatuses S_1 and S_2 .

Note that the number of service apparatuses is two in
15 this embodiment for the sake of simplicity but is not limited to this. The ID issuing apparatus 30 issues an ID for identifying a user who uses each of the service apparatuses S_1 and S_2 , and distributes the ID to the respective service apparatus. This arrangement of the ID
20 issuing apparatus 30, however, is not essential since it is only necessary to store information (to be referred to as "user information" hereinafter) of the user who uses each of the service apparatuses S_1 and S_2 in association with the ID. Any ID distribution method may be used (an
25 external apparatus which is not included in the arrangement according to this embodiment may distribute an ID).

The arrangements of the apparatuses 10 to 30, S_1 , and

S_2 will be described in detail below.

The re-encryption key issuing apparatus 10 includes a security parameter storage unit 11, a private key storage unit 12, a temporary data storage unit 13, a public parameter generation unit 14, an encryption
5 key/re-encryption key generation unit 15, a communication unit 16, and a control unit 17.

The security parameter storage unit 11 is a storage device which stores a security parameter necessary for
10 generating public parameters for key generation. The security parameter is, for example, a threshold defining a condition under which public parameters are generated.

The private key storage unit 12 is a storage device which stores a private key of a key pair (public
15 key/private key) of the re-encryption key issuing apparatus 10, which has been generated by the encryption key/re-encryption key generation unit 15 using the public parameters.

The temporary data storage unit 13 is a storage device
20 which stores the public key of the self apparatus 10 generated by the encryption key/re-encryption key generation unit 15, and temporary data such as the intermediate processing data and processing results of the public parameter generation unit 14 and encryption
25 key/re-encryption key generation unit 15.

The public parameter generation unit 14 has a function of generating public parameters for key generation by using

the security parameter read out from the security parameter storage unit 11, and a function of writing the intermediate processing data and processing result of processing of generating public parameters in the temporary data storage unit 13.

The encryption key/re-encryption key generation unit 15 has a function of generating a key pair of the self apparatus 10 by using the public parameters generated by the public parameter generation unit 14, and a function of writing the private key of the generated key pair in the private key storage unit 12 and writing the public key of the generated key pair in the temporary data storage unit 13. The encryption key/re-encryption key generation unit 15 also has a function of generating a re-encryption key using the private key of the re-encryption key issuing apparatus 10 read out from the private key storage unit 12 and the public keys of the service apparatuses S_1 and S_2 transmitted by the cooperation apparatus 20 (to be described later), and a function of writing the intermediate processing data and processing result of processing of generating a re-encryption key in the temporary data storage unit 13.

The communication unit 16 allows the self apparatus to communicate with the other apparatuses 20, 30, S_1 , and S_2 . For example, the communication unit 16 has a function of transmitting, to the cooperation apparatus 20, the public parameters generated by the public parameter generation

unit 14, and the public key of the self apparatus 10 and the re-encryption key which have been generated by the encryption key/re-encryption key generation unit 15. The communication unit 16 also has a function of transmitting various requests from the re-encryption key issuing apparatus 10 to the cooperation apparatus 20.

The control unit 17 has a function of controlling the respective units 11 to 16.

The cooperation apparatus 20 includes a public parameter storage unit 21, a public key storage unit 22, a re-encryption key storage unit 23, a temporary data storage unit 24, a re-encryption processing unit 25, a communication unit 26, and a control unit 27.

The public parameter storage unit 21 is a storage device which stores the public parameters transmitted by the re-encryption key issuing apparatus 10.

The public key storage unit 22 is a storage device which stores the public keys transmitted by the re-encryption key issuing apparatus 10 and the service apparatuses S_1 and S_2 .

The re-encryption key storage unit 23 is a storage device which stores the re-encryption key transmitted by the re-encryption key issuing apparatus 10.

The temporary data storage unit 24 is a storage device which stores temporary data such as the intermediate processing data and processing result of the re-encryption processing unit 25.

The re-encryption processing unit 25 has a function of re-encrypting ciphertext data transmitted by each of the service apparatuses S_1 and S_2 using the re-encryption key read out from the re-encryption key storage unit 23, and a
5 function of writing the intermediate processing data and processing result of re-encryption processing in the temporary data storage unit 24. More specifically, the re-encryption processing unit 25 has a function of re-encrypting ciphertext data transmitted from one service
10 apparatus (for example, the service apparatus S_1) into one for the other service apparatus (for example, the service apparatus S_2) (that is, generating re-encrypted data) by using the re-encryption key read out from the re-encryption key storage unit 23 without decrypting the ciphertext data
15 into plaintext data.

The communication unit 26 allows the self apparatus to communicate with the other apparatuses 10, 30, S_1 , and S_2 . The communication unit 26 has, for example, a function of writing, in the respective corresponding storage units 21
20 to 23, the public parameters transmitted by the re-encryption key issuing apparatus 10, the public keys transmitted by the re-encryption key issuing apparatus 10 and the service apparatuses S_1 and S_2 , and the re-encryption key transmitted by the re-encryption key
25 issuing apparatus 10, and a function of transmitting the re-encrypted data re-encrypted by the re-encryption processing unit 25 to the respective service apparatuses S_1

and S_2 . The communication unit 26 also has a function of transmitting the public parameters and public keys to the other apparatuses 10, 30, S_1 , and S_2 in response to requests from the apparatuses 10, 30, S_1 , and S_2 ,
5 respectively.

The control unit 27 has a function of controlling the respective units 21 to 26.

The ID issuing apparatus 30 includes an ID issuance information storage unit 31, an ID issuing unit 32, a
10 communication unit 33, and a control unit 34.

The ID issuance information storage unit 31 is a storage device which stores an ID issued by the ID issuing unit 32.

The ID issuing unit 32 has a function of issuing a
15 unique ID for identifying a user who uses each of the service apparatuses S_1 and S_2 , and a function of writing the issued ID in the ID issuance information storage unit 31.

The communication unit 33 allows the self apparatus to
20 communicate with the other apparatuses 10, 20, S_1 , and S_2 , and has, for example, a function of distributing the ID issued by the ID issuing unit 32 to the respective service apparatuses S_1 and S_2 .

The control unit 34 has a function of controlling the
25 respective units 31 to 33.

The practical arrangement of each of the service apparatuses S_1 and S_2 will be described next. The

arrangement of the service apparatus S_1 will be explained below as a representative example for the sake of simplicity.

5 The service apparatus S_1 includes a user information storage unit S_{11} , a private key storage unit S_{12} , a temporary data storage unit S_{13} , an encryption processing unit S_{14} , a decryption processing unit S_{15} , a service processing unit S_{16} , a service cooperation request unit S_{17} , a communication unit S_{18} , and a control unit S_{19} .

10 The user information storage unit S_{11} is a storage device which stores the ID distributed by the ID issuing apparatus 30 in association with the information (user information) of the user who uses the service apparatus S_1 .

15 The private key storage unit S_{12} is a storage device which stores the private key of a key pair of the self apparatus S_1 generated by the encryption processing unit S_{14} using the public parameters.

20 The temporary data storage unit S_{13} is a storage device which stores a public key of the self apparatus S_1 generated by the encryption processing unit S_{14} , and temporary data such as the intermediate processing data and processing results of the encryption processing unit S_{14} and decryption processing unit S_{15} .

25 The encryption processing unit S_{14} has a function of generating a key pair of the self apparatus S_1 using the public parameters transmitted by the cooperation apparatus 20, and a function of writing the private key of the

generated key pair in the private key storage unit S_{12} and writing the public key of the generated key pair in the temporary data storage unit S_{13} . The encryption processing unit S_{14} also has a function of generating ciphertext data by performing encryption processing for plaintext data (for example, the ID stored in the user information storage unit S_{11} or the like) using the public key of the re-encryption key issuing apparatus 10 transmitted by the cooperation apparatus 20, and a function of writing the intermediate processing data and processing result of processing of generating ciphertext data in the temporary data storage unit S_{13} .

The decryption processing unit S_{15} has a function of decrypting the re-encrypted data transmitted by the cooperation apparatus 20 by using the private key read out from the private key storage unit S_{12} , and a function of writing the intermediate processing data and processing result of decryption processing in the temporary data storage unit S_{13} .

The service processing unit S_{16} has a function of providing a service in response to a request from the user.

The service cooperation request unit S_{17} has a function of requesting the cooperation apparatus 20 via the communication unit S_{18} to acquire information held in the other service apparatus.

The communication unit S_{18} allows the self apparatus to communicate with the other apparatuses 10 to 30 and S_2 .

The communication unit S₁₈ has, for example, a function of writing the ID distributed from the ID issuing apparatus 30 in the user information storage unit S₁₁ in association with the user information, and a function of transmitting the public key and ciphertext data generated by the encryption processing unit S₁₄ to the cooperation apparatus 20. The communication unit S₁₈ also has a function of transmitting various requests from the service apparatus S₁ to the cooperation apparatus 20.

10 The control unit S₁₉ has a function of controlling the respective units S₁₁ to S₁₈.

Note that each of the service apparatuses S₁ and S₂ provides a unique service to the user, and does not share user information with the other service apparatus.

15 An example of the operation of the cooperation service providing system 1 with the above arrangement will be described with reference to sequence charts shown in FIGS. 2, 3, 4, and 5.

20 The following operation is executed in an order of (1) preprocessing and (2) cooperation processing, and (1) preprocessing is executed in an order of (1-1) key generation processing, (1-2) ID issuing processing, and (1-3) re-encryption key generation processing. Note that the preprocessing need not always be executed in the above order. For example, the ID issuing processing may be executed before the key generation processing.

The re-encryption key issuing apparatus 10 and the

respective service apparatuses S_1 and S_2 execute (1) key generation processing, as shown in FIG. 2 and indicated by steps ST1 to ST21 below.

First, the public parameter generation unit 14 of the re-encryption key issuing apparatus 10 generates public parameters $(p, \lambda, G, G_T, g, u, v, \text{and } \text{Sig})$ (step ST1). More specifically, based on a security parameter λ stored in advance in the security parameter storage unit 11, the public parameter generation unit 14 selects bilinear map groups $(G \text{ and } G_T)$ satisfying a prime number order $p > 2\lambda$, and a one-time signature $\text{Sig}(\hat{G}, \hat{S}, \hat{V})$ with strong unforgeability which satisfies generation sources $g, u, v \in G$.

In the one-time signature $\text{Sig}(\hat{G}, \hat{S}, \hat{V})$ (to be also referred to as "Sig" hereinafter), $\hat{G}$ represents a function of generating a one-time key pair (ssk, svk) , $\hat{S}$ represents a function of generating a signature σ for a message ID, and $\hat{V}$ represents a function of verifying correctness of the signature σ .

A one-time signature is described in detail in non-patent literature 10. Furthermore, G and G_T are group sets each defined by an elliptic curve, and used for a pairing function.

Pairing function: $e(g_1, g_2) = g_T$

where $g_1, g_2 \in G$ and $g_T \in G_T$.

This pairing function has characteristics given by:

$$e(g^a, g) = e(g, g^a) = e(g, g)^a$$

where $g \in G$ and $a \in \mathbb{Z}_p$

The communication unit 16 transmits the public parameters (p , λ , G , G_T , g , u , v , and Sig) generated by the public parameter generation unit 14 to the cooperation apparatus 20 (that is, the public parameters are made public to the other apparatuses 20, 30, S_1 , and S_2) (step ST2).

Upon receiving the public parameters (p , λ , G , G_T , g , u , v , and Sig) transmitted by the re-encryption key issuing apparatus 10, the communication unit 26 of the cooperation apparatus 20 writes (registers) the public parameters in the public parameter storage unit 21 (step ST3).

The communication unit 16 of the re-encryption key issuing apparatus 10 requests the cooperation apparatus 20 to distribute the public parameters (step ST4).

Upon receiving the request from the re-encryption key issuing apparatus 10 in step ST4, the communication unit 26 of the cooperation apparatus 20 transmits the public parameters (p , λ , G , G_T , g , u , v , and Sig) stored in the public parameter storage unit 21 to the re-encryption key issuing apparatus 10 (step ST5).

Subsequently, upon receiving, via the communication unit 16, the public parameters (p , λ , G , G_T , g , u , v , and Sig) transmitted by the cooperation apparatus 20, the encryption key/re-encryption key generation unit 15 of the re-encryption key issuing apparatus 10 generates a key pair of the re-encryption key issuing apparatus 10 using the

public parameters (step ST6). More specifically, when identification information of the re-encryption key issuing apparatus 10 is indicated by i , the encryption key/re-encryption key generation unit 15 generates a private key $x_i \in \mathbb{Z}_p^*$ of the re-encryption key issuing apparatus 10, and generates a public key $X_i = g^{x_i}$ of the re-encryption key issuing apparatus 10 using the private key x_i .

The encryption key/re-encryption key generation unit 15 writes the private key x_i of the key pair of the self apparatus 10 generated in step ST6 in the private key storage unit 12, and writes the public key X_i of the generated key pair of the self apparatus 10 in the temporary data storage unit 13 (step ST7).

The communication unit 16 transmits the public key X_i stored in the temporary data storage unit 13 to the cooperation apparatus 20 (that is, the public key X_i is made public to the other apparatuses 20, 30, S_1 , and S_2) (step ST8).

After that, upon receiving the public key X_i of the re-encryption key issuing apparatus 10 transmitted by the re-encryption key issuing apparatus 10, the communication unit 26 of the cooperation apparatus 20 writes (registers) the public key in the public key storage unit 22 (step ST9).

Similarly, the service apparatus S_1 executes processes similar to those in steps ST4 to ST9 for the key pair of

the service apparatus S_1 , writes a private key x_j in the private key storage unit S_{12} of the service apparatus S_1 , and transmits a public key X_j to the cooperation apparatus 20, thereby registering the public key X_j of the service apparatus S_1 in the public key storage unit 22 of the cooperation apparatus 20 (steps ST10 to ST15).

Furthermore, the service apparatus S_2 executes processes similar to those in steps ST4 to ST9 for the key pair of the service apparatus S_2 , writes a private key x_k in a private key storage unit S_{22} of the service apparatus S_2 , and transmits a public key X_k to the cooperation apparatus 20, thereby registering the public key X_k of the service apparatus S_2 in the public key storage unit 22 of the cooperation apparatus 20 (steps ST16 to ST21).

Then, the key generation processing is completed. After that, the respective apparatuses 10 to 30, S_1 , and S_2 can acquire and use the public parameters and public keys made public to the public parameter storage unit 21 and public key storage unit 22 of the cooperation apparatus 20, as needed.

The ID issuing apparatus 30 executes (1-2) ID issuing processing, as shown in FIG. 3 and indicated by steps ST31 to ST35 below.

First, the ID issuing unit 32 of the ID issuing apparatus 30 issues an ID for identifying a user who uses each of the service apparatuses S_1 and S_2 , and writes the issued ID in the ID issuance information storage unit 31

(step ST31).

The communication unit 33 distributes the ID stored in the ID issuance information storage unit 31 to the service apparatus S_1 (step ST32).

5 After that, upon receiving the ID distributed by the ID issuing apparatus 30, the communication unit S_{18} of the service apparatus S_1 writes the ID in the user information storage unit S_{11} in association with user information (step ST33).

10 Similarly, the communication unit 33 of the ID issuing apparatus 30 executes processing similar to that in step ST32 for the service apparatus S_2 (step ST34), and a communication unit S_{28} of the service apparatus S_2 executes processing similar to that in step ST33 to write the ID in
15 a user information storage unit S_{21} in association with user information (step ST35).

Then, the ID issuing processing is completed.

The re-encryption key issuing apparatus 10 executes (1-3) re-encryption key generation processing, as shown in
20 FIG. 4 and indicated by steps ST41 to ST45 below. Note that processing of generating a re-encryption key for converting ciphertext data for the re-encryption key issuing apparatus 10 into one for the service apparatus S_2 will be described.

25 First, the communication unit 16 of the re-encryption key issuing apparatus 10 requests the cooperation apparatus 20 to distribute the public parameters and the public key

of the service apparatus S_2 (step ST41).

Upon receiving the request from the re-encryption key issuing apparatus 10 in step ST41, the communication unit 26 of the cooperation apparatus 20 transmits, to the
5 re-encryption key issuing apparatus 10, the public parameters $(p, \lambda, G, G_T, g, u, v, \text{and Sig})$ stored in the public parameter storage unit 21 and the public key X_k of the service apparatus S_2 stored in the public key storage unit 22 (step ST42).

10 Upon receiving, via the communication unit 16, the public parameters $(p, \lambda, G, G_T, g, u, v, \text{and Sig})$ and the public key X_k of the service apparatus S_2 , the encryption key/re-encryption key generation unit 15 of the re-encryption key issuing apparatus 10 generates a
15 re-encryption key $R_{ik} = X_k^{1/x_i} = g^{x_k/x_i}$ for converting ciphertext data for the re-encryption key issuing apparatus 10 into one for the service apparatus S_2 by using the acquired information and the private key x_i of the self apparatus 10 read out from the private key storage unit 12
20 (step ST43).

The communication unit 16 transmits the generated re-encryption key R_{ik} to the cooperation apparatus 20 (step ST44).

After that, upon receiving the re-encryption key R_{ik}
25 transmitted by the re-encryption key issuing apparatus 10, the communication unit 26 of the cooperation apparatus 20 writes (registers) the re-encryption key in the

re-encryption key storage unit 23 (step ST45).

Then, the re-encryption key generation processing is completed. Note that a re-encryption key for converting ciphertext data for the re-encryption key issuing apparatus 10 into one for the service apparatus S_2 is generated in this example. The present invention, however, is not limited to this, and a re-encryption key for converting ciphertext data for the re-encryption key issuing apparatus 10 into one for the service apparatus S_1 may be generated.

The cooperation apparatus 20 and the respective service apparatuses S_1 and S_2 execute (2) cooperation processing, as shown in FIG. 5 and indicated by steps ST51 to ST62 below.

First, in response to a request from the user, the communication unit S_{18} of the service apparatus S_1 requests the cooperation apparatus 20 to distribute the public parameters and the public key of the re-encryption key issuing apparatus 10 (step ST51).

In response to the request from the service apparatus S_1 in step ST51, the communication unit 26 of the cooperation apparatus 20 transmits, to the service apparatus S_1 , the public parameters (p , λ , G , G_T , g , u , v , and Sig) stored in the public parameter storage unit 21 and the public key X_i of the re-encryption key issuing apparatus 10 stored in the public key storage unit 22 (step ST52).

Upon receiving the public parameters (p , λ , G , G_T , g ,

u, v, and Sig) and the public key X_i via the communication unit S_{18} , the encryption processing unit S_{14} of the service apparatus S_1 reads out the ID corresponding to the user in step ST51 from the user information storage unit S_{11} (step
5 ST53).

The encryption processing unit S_{14} performs encryption processing for the ID read out from the user information storage unit S_{11} using the public key X_i of the re-encryption key issuing apparatus 10, thereby generating
10 ciphertext data (step ST54).

As indicated by steps ST54-1 to ST54-4 below, the encryption processing performed by the encryption processing unit S_{14} will be described in detail.

First, the encryption processing unit S_{14} generates a
15 key pair $(ssk, svk) \leftarrow \hat{G}(\lambda)$ of a signature key ssk and a verification key svk in a one-time signature based on the security parameter λ of the public parameters and the key pair generation function $\hat{G}$ (step ST54-1), and sets the verification key svk in first encrypted data C_1 ($C_1 = svk$).

20 After generating a first random number $r \in \mathbb{Z}_p^*$, the encryption processing unit S_{14} generates second, third, and fourth encrypted data C_2 , C_3 , and C_4 for $ID \in G_T$ as plaintext data based on the first random number r (step ST54-2), given by:

$$C_2 = X_i^r$$

$$C_3 = e(g, g)^r \cdot \text{ID}$$

$$C_4 = \left(u^{\text{svk} \cdot v} \right)^r$$

More specifically, the encryption processing unit S_{14} generates the second encrypted data C_2 based on the public key X_i of the re-encryption key issuing apparatus 10 and the first random number r . The encryption processing unit S_{14} generates the third encrypted data C_3 using the pairing function based on the generation source g of the public parameters, the first random number r , and the ID. Also, the encryption processing unit S_{14} generates the fourth encrypted data C_4 based on the generation sources u and v of the public parameters, the generated verification key svk , and the first random number r .

After the end of step ST54-2, the encryption processing unit S_{14} generates the one-time signature σ by the signature generation function $\hat{S}$ of the public parameters and the generated signature key ssk for the third and fourth encrypted data C_3 and C_4 (step ST54-3), given by:

$$\sigma = \hat{S}(\text{ssk}, (C_3, C_4))$$

After that, the encryption processing unit S_{14} generates ciphertext data $C_1 = (C_1, C_2, C_3, C_4, \sigma)$ including the first to fourth encrypted data C_1 to C_4 and the one-time signature σ , and writes the obtained ciphertext

data in the temporary data storage unit S_{13} (step ST54-4).

As described above, when the processes in steps ST54-1 to ST54-4 are complete, ciphertext data is generated.

After step ST54, the service cooperation request unit
5 S_{17} requests, via the communication unit S_{18} , the cooperation apparatus 20 to acquire information held in the service apparatus S_2 by using the ciphertext data generated by the encryption processing unit S_{14} (step ST55).

Upon receiving the request and ciphertext data from
10 the service apparatus S_1 via the communication unit 26 in step ST55, the re-encryption processing unit 25 of the cooperation apparatus 20 re-encrypts the ciphertext data using the re-encryption key R_{ik} stored in advance in the re-encryption key storage unit 23 (step ST56).

15 As indicated by steps ST56-1 to ST56-3 below, the re-encryption processing performed by the re-encryption processing unit 25 will be described.

First, the re-encryption processing unit 25 verifies ciphertext data C_{ki} using the public parameters and the
20 following verification equations (step ST56-1):

$$e\left(C_2, u^{C_1 \cdot v}\right) \stackrel{?}{=} e\left(X_i, C_4\right)$$

$$\hat{V}\left(C_{1,\sigma}, (C_3, C_4)\right) \stackrel{?}{=} 1$$

If the two verification equations hold, verification succeeds. On the other hand, if at least one of the verification equations does not hold, verification fails.

If verification succeeds, the re-encryption processing unit 25 generates a second random number $t \in Z_p^*$, and generates first, second, and third re-encrypted data C_2' , C_2'' , C_2''' (step ST56-2), given by:

$$C_2' = X_i^t$$

$$C_2'' = R_{ik}^{1/t} = g^{(x_k/x_i)^{t-1}}$$

5

$$C_2''' = C_2^t = X_i^{rt}$$

More specifically, in step ST56-2, the re-encryption processing unit 25 generates the first re-encrypted data C_2' based on the public key X_i of the re-encryption key issuing apparatus 10 and the second random number t . The re-encryption processing unit 25 generates the second re-encrypted data C_2'' based on the re-encryption key R_{ik} and the second random number t . Furthermore, the re-encryption processing unit 25 generates the third re-encrypted data C_2''' based on the second encrypted data C_2 and the second random number t .

After the end of step ST56-2, the re-encryption processing unit 25 generates re-encrypted data $C_k = (C_1, C_2', C_2'', C_2''', C_3, C_4, \sigma)$ by replacing the second encrypted data C_2 of the ciphertext data C_1 with the first to third re-encrypted data C_2' to C_2''' , and writes the obtained re-encrypted data in the temporary data storage unit 24 (step ST56-3).

As described above, when the processes in steps ST56-1

to ST56-3 are complete, re-encrypted data is generated.

After step ST56, the communication unit 26 transmits the generated re-encrypted data C_k to the service apparatus S_2 (step ST57), and requests to acquire information held in the service apparatus S_2 by using the re-encrypted data.

Upon receiving, via the communication unit S_{28} , the re-encrypted data C_k transmitted by the cooperation apparatus 20, a decryption processing unit S_{25} of the service apparatus S_2 decrypts the re-encrypted data using the private key x_k stored in advance in the private key storage unit S_{22} , thereby acquiring the ID (step ST58).

As indicated by steps ST58-1 and ST58-2 below, the decryption processing performed by the decryption processing unit S_{25} will be described in detail.

First, the decryption processing unit S_{25} verifies the re-encrypted data C_k using the public parameters, the public key X_k of the self apparatus S_2 , and the following verification equations (step ST58-1):

$$\begin{aligned} e(C'_2, C''_2) &\stackrel{?}{=} e(X_k, g) \\ e\left(C'''_2, u^{C_1} \cdot v\right) &\stackrel{?}{=} e(C'_2, C_4) \\ \hat{V}\left(C_{1,\sigma}, (C_3, C_4)\right) &\stackrel{?}{=} 1 \end{aligned}$$

If the three verification equations hold, verification succeeds. On the other hand, if at least one of the three verification equations does not hold, verification fails.

If verification succeeds, the decryption processing unit S₂₅ decrypts the ID from the re-encrypted data C_k based on the private key x_k of the self apparatus S₂ (step ST58-2), given by:

5

$$ID = C_3 / \left(e(C_2'', C_2''')^{1/x_k} \right)$$

As described above, when the processes in steps ST58-1 and ST58-2 are complete, the ID is acquired.

After step ST58, a service processing unit S₂₆ of the service apparatus S₂ reads out user information
10 corresponding to the ID decrypted by the decryption processing unit S₂₅ from the user information storage unit S₂₁ (step ST59).

The communication unit S₂₈ transmits, as cooperation information, the user information read out by the service
15 processing unit S₂₆ to the cooperation apparatus 20 (step ST60).

Upon receiving the cooperation information transmitted by the service apparatus S₂, the communication unit 26 of the cooperation apparatus 20 transmits the cooperation
20 information to the service apparatus S₁ (step ST61).

After that, the communication unit S₁₈ of the service apparatus S₁ receives the cooperation information transmitted by the cooperation apparatus 20. Thus, the service apparatus S₁ acquires the cooperation information
25 (step ST62).

According to the above-described first embodiment, the

arrangement which includes the cooperation apparatus 20 including the re-encryption processing unit 25, the service apparatus S_1 including the encryption processing unit S_{14} , the decryption processing unit S_{15} , and the service cooperation request unit S_{17} , and the service apparatus S_2 including an encryption processing unit S_{24} , the decryption processing unit S_{25} , and a service cooperation request unit S_{27} prevent the cooperation apparatus 20 from linking IDs with each other in a process of exchanging cooperation information between the service apparatuses S_1 and S_2 , thereby improving the security for the cooperation information.

Also, it is possible to audit/verify later a process of exchanging cooperation information between the service apparatuses S_1 and S_2 by using the pieces of information held in the re-encryption key issuing apparatus 10 and cooperation apparatus 20 (that is, without requiring the pieces of secret information of the service apparatuses S_1 and S_2).

Note that in this embodiment, the ID stored in each of the user information storage units S_{11} and S_{21} of the service apparatuses S_1 and S_2 is encrypted using the re-encryption scheme. The present invention, however, is not limited to this. For example, hybrid encryption in which an ID is encrypted using a common encryption scheme and then the common key is encrypted using a re-encryption scheme may be applied.

[Modification]

A modification of the first embodiment will be explained with reference to sequence charts shown in FIGS. 6 and 7. In this modification, a code (a code before
5 distribution corresponds to a first code in claim 2) generated from a user ID issued by the ID issuing apparatus 30 is distributed to each of the service apparatuses S_1 and S_2 , and used to execute cooperation processing. Note that (1-1) key generation processing and (1-3) re-encryption key
10 generation processing are the same as those in the aforementioned first embodiment and a detailed description thereof will be omitted.

A description of (1-2') code distribution processing and (2') cooperation processing different from the
15 aforementioned first embodiment will be provided below.

The cooperation apparatus 20, the ID issuing apparatus 30, and the respective service apparatuses S_1 and S_2 execute (1-2') code distribution processing, as shown in FIG. 6 and indicated by steps ST71 to ST79 below.

20 First, the ID issuing unit 32 of the ID issuing apparatus 30 issues an ID for identifying a user who uses each of the service apparatuses S_1 and S_2 , and writes the issued ID in the ID issuance information storage unit 31 (step ST71).

25 The communication unit 33 requests the cooperation apparatus 20 to distribute the public key of the re-encryption key issuing apparatus 10 (step ST72).

Upon receiving the request from the ID issuing apparatus 30 in step ST72, the communication unit 26 of the cooperation apparatus 20 transmits the public key X_i of the re-encryption key issuing apparatus 10 stored in the public key storage unit 22 to the ID issuing apparatus 30 (step ST73).

Upon receiving, via the communication unit 33, the public key X_i of the re-encryption key issuing apparatus 10 transmitted by the cooperation apparatus 20, the ID issuing unit 32 of the ID issuing apparatus 30 performs encryption processing for the ID stored in the ID issuance information storage unit 31 using the public key to generate the first code (the first code in claim 2) for the service apparatus S_1 , and then writes the generated first code and various parameters (to be referred to as the first parameters hereinafter) used to generate the first code in the ID issuance information storage unit 31 (step ST74). Note that the processing in step ST74 is executed for all IDs stored in the ID issuance information storage unit 31.

The communication unit 33 transmits the plurality of first codes and the first parameters stored in the ID issuance information storage unit 31 to the service apparatus S_1 (step ST75).

After that, upon receiving the first codes and first parameters transmitted by the ID issuing apparatus 30, the communication unit S_{18} of the service apparatus S_1 writes them in the user information storage unit S_{11} in

association with pieces of user information, respectively (step ST76).

Similarly, the ID issuing unit 32 of the ID issuing apparatus 30 executes processes similar to those in steps
5 ST74 to ST76 for the second code (the first code in claim 2) for the service apparatus S_2 . After generating the second codes, the second codes and various parameters (to be referred to as the second parameters hereinafter) used to generate the second codes are transmitted to the
10 service apparatus S_2 . After that, upon receiving the second codes and second parameters transmitted by the ID issuing apparatus 30, the communication unit S_{28} of the service apparatus S_2 writes them in the user information storage unit S_{21} in association with pieces of user
15 information, respectively (steps ST77 to ST79).

Then, the code distribution processing is completed.

The cooperation apparatus 20 and the respective service apparatuses S_1 and S_2 execute (2') cooperation processing, as shown in FIG. 7 and indicated by steps ST81
20 to ST93 below.

First, in response to a request from a user, the encryption processing unit S_{14} of the service apparatus S_1 reads out the first code associated with the user information of the user from the user information storage
25 unit S_{11} (step ST81).

The service cooperation request unit S_{17} requests, via the communication unit S_{18} , the cooperation apparatus 20 to

acquire information held in the service apparatus S_2 by using the first code read out by the encryption processing unit S_{14} (step ST82).

5 Upon receiving, via the communication unit 26, the request and first code from the service apparatus S_1 in step ST82, the re-encryption processing unit 25 of the cooperation apparatus 20 re-encrypts the first code using the re-encryption key R_{ik} stored in advance in the re-encryption key storage unit 23 (that is, re-encrypted
10 data is generated) (step ST83).

 The communication unit 26 transmits the generated re-encrypted data to the service apparatus S_2 (step ST84), and requests to acquire information held in the service apparatus S_2 by using the re-encrypted data.

15 Upon receiving, via the communication unit S_{28} , the re-encrypted data transmitted by the cooperation apparatus 20, the decryption processing unit S_{25} of the service apparatus S_2 decrypts the re-encrypted data using the private key x_k stored in advance in the private key storage
20 unit S_{22} , thereby acquiring an ID (step ST85).

 The communication unit S_{28} requests the cooperation apparatus 20 to distribute the public key of the re-encryption key issuing apparatus 10 (step ST86).

25 Upon receiving the request from the service apparatus S_2 in step ST86, the communication unit 26 of the cooperation apparatus 20 transmits the public key X_1 of the re-encryption key issuing apparatus 10 stored in the public

key storage unit 22 to the service apparatus S_2 (step ST87).

Upon receiving, via the communication unit S_{28} , the public key X_i of the re-encryption key issuing apparatus 10 transmitted by the cooperation apparatus 20, the encryption processing unit S_{24} of the service apparatus S_2 performs encryption processing for the ID decrypted in step ST85 by using the public key and the second parameters stored in advance in the user information storage unit S_{21} , thereby generating a second prime code (the second code in claim 2) for the service apparatus S_2 (step ST88).

The service processing unit S_{26} compares the generated second prime code with the second code stored in advance in the user information storage unit S_{21} and read out from it, thereby specifying the user based on the matching codes (step ST89).

The service processing unit S_{26} writes, in the user information storage unit S_{21} , the user information of the specified user and the second prime code generated by the encryption processing unit S_{24} in association with each other (step ST90).

The communication unit S_{28} transmits, as cooperation information, the user information stored in the user information storage unit S_{21} by the service processing unit S_{26} to the cooperation apparatus 20 (step ST91).

Upon receiving the cooperation information transmitted by the service apparatus S_2 , the communication unit 26 of

the cooperation apparatus 20 transmits the cooperation information to the service apparatus S_1 (step ST92).

After that, the communication unit S_{18} of the service apparatus S_1 receives the cooperation information
5 transmitted by the cooperation apparatus 20. Thus, the service apparatus S_1 acquires the cooperation information (step ST93).

According to the above-described modification of the first embodiment, similarly to the aforementioned first
10 embodiment, the arrangement which includes the cooperation apparatus 20 including the re-encryption processing unit 25, and the plurality of service apparatuses S_1 and S_2 respectively including the encryption processing units S_{14} and S_{24} , decryption processing units S_{15} and S_{25} , and
15 service cooperation request units S_{17} and S_{27} prevents the cooperation apparatus 20 from linking IDs with each other in a process of exchanging cooperation information between the service apparatuses S_1 and S_2 , thereby improving the security for the cooperation information.

20 It is also possible to audit/verify later a process of exchanging cooperation information between the service apparatuses S_1 and S_2 by using the pieces of information held in the re-encryption key issuing apparatus 10 and cooperation apparatus 20 (that is, without requiring the
25 pieces of secret information of the service apparatuses S_1 and S_2).

Note that as another modification of the first

embodiment, a cooperation service providing system having an arrangement shown in FIG. 8 is applicable. This arrangement is obtained by simplifying the arrangement shown in FIG. 1 described above, and can operate, as shown in FIG. 9.

Simplifying the arrangement imposes an inconvenience to some extent when performing auditing on the cooperation apparatus 20 but can reduce the system cost required for implementing a cooperation service providing system.

[Second Embodiment]

FIG. 10 is a schematic view showing an example of the arrangement of a cooperation service providing system according to the second embodiment. Unlike the aforementioned first embodiment, a cooperation service providing system 1' has an arrangement obtained by excluding the ID issuing apparatus 30 from the cooperation service providing system 1. This embodiment is a modification of the aforementioned first embodiment. Assuming that a cooperation mechanism already exists between service apparatuses S_1 and S_2 , data exchanged between the service apparatuses S_1 and S_2 are protected in cooperation processing. Unlike the user information storage units S_{11} and S_{21} in the aforementioned first embodiment, cooperation information storage units S_{11}' and S_{21}' of the service apparatuses S_1 and S_2 need only store cooperation information (corresponding to the user information in the first embodiment) in association with a

user, and need not always store an ID for identifying the user.

5 A description of (2") cooperation processing different from the aforementioned first embodiment will be provided below.

A cooperation apparatus 20 and the service apparatuses S_1 and S_2 execute (2") cooperation processing, as shown in FIG. 11 and indicated by steps ST101 to ST113.

10 First, in response to a request from a user, a service cooperation request unit S_{17} of the service apparatus S_1 requests, via a communication unit S_{18} , the cooperation apparatus 20 to acquire information held in the service apparatus S_2 (step ST101).

15 Upon receiving the request from the service apparatus S_1 in step ST101, a communication unit 26 of the cooperation apparatus 20 executes cooperation processing of causing the service apparatuses S_1 and S_2 to cooperate with each other by using, for example, a conventional method (step ST102).

20 The communication unit 26 transmits the request from the service apparatus S_1 in step ST102 to the service apparatus S_2 (step ST103).

25 Upon receiving the request of the service apparatus S_1 transmitted by the cooperation apparatus 20, a communication unit S_{28} of the service apparatus S_2 reads out cooperation information corresponding to the user in step ST101 from the cooperation information storage unit

S_{21}' (step ST104).

The communication unit S_{28} requests the cooperation apparatus 20 to distribute a public key of a re-encryption key issuing apparatus 10 (step ST105).

5 Upon receiving the request transmitted by the service apparatus S_2 in step ST105, the communication unit 26 of the cooperation apparatus 20 transmits a public key X_i of the re-encryption key issuing apparatus 10 stored in a public key storage unit 22 to the service apparatus S_2
10 (step ST106).

 Upon receiving, via the communication unit S_{28} , the public key X_i of the re-encryption key issuing apparatus 10 transmitted by the cooperation apparatus 20, an encryption processing unit S_{24} of the service apparatus S_2 performs
15 encryption processing for the cooperation information read out in step ST104 by using the public key, thereby generating ciphertext data (step ST107).

 The communication unit S_{28} transmits the generated ciphertext data to the cooperation apparatus 20 (step
20 ST108).

 Upon receiving the ciphertext data transmitted by the service apparatus S_2 , the communication unit 26 of the cooperation apparatus 20 executes cooperation processing of causing the service apparatuses S_1 and S_2 to cooperate with
25 each other, similarly to the processing in step ST102 (step ST109).

 A re-encryption processing unit 25 performs

re-encryption processing for the ciphertext data received by the communication unit 26 by using a re-encryption key R_{ij} stored in advance in a re-encryption key storage unit 23, thereby generating re-encrypted data (step ST110).

5 The communication unit 26 transmits the re-encrypted data generated by the re-encryption processing unit 25 to the service apparatus S_1 (step ST111).

 Upon receiving, via the communication unit S_{18} , the re-encrypted data transmitted by the cooperation apparatus
10 20, the decryption processing unit S_{15} of the service apparatus S_1 decrypts the re-encrypted data using a private key x_j stored in advance in a private key storage unit S_{12} (step ST112).

 After that, the service apparatus S_1 acquires the
15 cooperation information (step ST113).

 According to the above-described second embodiment, the arrangement which includes the cooperation apparatus 20 including the re-encryption processing unit 25, the service apparatus S_1 including the cooperation information storage unit S_{11}' , an encryption processing unit S_{14} , a decryption
20 processing unit S_{15} , and a service cooperation request unit S_{17} , and the service apparatus S_2 including the cooperation information storage unit S_{21}' , the encryption processing unit S_{24} , a decryption processing unit S_{25} , and a service
25 cooperation request unit S_{27} prevents the cooperation apparatus 20 from linking the pieces of cooperation information with each other in a process of exchanging

cooperation information between the service apparatuses S_1 and S_2 , and encrypts the pieces of cooperation information in the service apparatuses S_1 and S_2 , thereby improving the security for the cooperation information.

5 It is also possible to audit later a process of exchanging cooperation information between the service apparatuses S_1 and S_2 by using the pieces of information held in the re-encryption key issuing apparatus 10 and cooperation apparatus 20 (that is, without requiring the
10 pieces of secret information of the service apparatuses S_1 and S_2).

 Note that in this embodiment, the pieces of cooperation information respectively stored in the cooperation information storage units $S_{11'}$ and $S_{21'}$ of the
15 service apparatuses S_1 and S_2 are encrypted using the re-encryption scheme. The present invention, however, is not limited to this. For example, hybrid encryption in which cooperation information is encrypted using a common encryption scheme and then the common key is encrypted
20 using a re-encryption scheme may be applied.

 According to at least one of the above-described embodiments, the arrangement which includes the cooperation apparatus 20 including the re-encryption processing unit
25 25, and the plurality of service apparatuses S_1 and S_2 respectively including the encryption processing units S_{14} and S_{24} , decryption processing units S_{15} and S_{25} , and service cooperation request units S_{17} and S_{27} prevents the

cooperation apparatus from linking pieces of cooperation information with each other, and allows auditing/ verification to be performed alter on the cooperation apparatus.

5 The method described in the embodiment can also be stored in a storage medium such as a magnetic disk (floppyTM disk, hard disk, or the like), an optical disk (CD-ROM, DVD, or the like), a magneto-optical disk (MO), or a semiconductor memory as a program which can be executed
10 by a computer and distributed.

As the storage medium, any configuration which is a computer-readable storage medium in which a program can be stored may be used regardless of a storage format.

15 An OS (operating system) which operates on a computer on the basis of an instruction of a program installed from the storage medium in the computer, database management software, and MW (middleware) such as network software may execute a part of the processes to realize the embodiment.

20 Furthermore, the storage medium according to the present invention includes not only a medium independent of a computer but also a storage medium in which a program transmitted through a LAN, the Internet, or the like is downloaded and stored or temporarily stored.

25 The number of storage media is not limited to one. A case in which the process in the embodiment is executed from a plurality of media is included in the storage medium according to the present invention. Any medium

configuration may be used.

A computer according to the present invention is to execute the processes in the embodiments on the basis of the program stored in a storage medium. The computer may
5 have any configuration such as one apparatus constituted by a personal computer or a system in which a plurality of apparatuses are connected by a network.

A computer in each embodiment includes not only a personal computer but also an arithmetic processing
10 apparatus, a microcomputer, or the like included in an information processing apparatus. The computer is a generic name of an apparatus and a device which can realize the functions of the present invention by a program.

While certain embodiments have been described, these
15 embodiments have been presented by way of example only, and are not intended to limit the scope of the inventions. Indeed, the novel embodiments described herein may be embodied in a variety of other forms; furthermore, various omissions, substitutions and changes in the form of the
20 embodiments described herein may be made without departing from the spirit of the inventions. The accompanying claims and their equivalents are intended to cover such forms or modifications as would fall within the scope and spirit of the inventions.

25

C L A I M S

1. A cooperation service providing system (1) in which a re-encryption key issuing apparatus (10), a plurality of service apparatuses (S_1 , S_2) for providing various services to a user by using an ID issued for identifying the user, and a cooperation apparatus (20) for causing the plurality of service apparatuses to cooperate with each other are communicably connected to each other, characterized in that

the cooperation apparatus comprises

first storage means (22) for storing public keys of the re-encryption key issuing apparatus and the service apparatuses,

second storage means (23) for storing a re-encryption key for implementing re-encryption processing of enabling ciphertext data transmitted by each of the service apparatuses to be decrypted using a private key of the other service apparatus without decrypting the ciphertext data into plaintext data,

first generation means (25) for generating, upon receiving the ciphertext data transmitted by each of the service apparatuses, re-encrypted data by performing re-encryption processing for the ciphertext data using the stored re-encryption key,

first transmission means (26) for transmitting the generated re-encrypted data to the other service apparatus different from the service apparatus which has transmitted

the ciphertext data, and

second transmission means (26) for transmitting the stored public key to each of the service apparatuses, and each of the service apparatuses comprises

5 third storage means (S_{11} , S_{21}) for storing the issued ID in association with user information indicating information of the user unique to the service apparatus,

fourth storage means (S_{12} , S_{22}) for storing a private key of the service apparatus,

10 third transmission means (S_{17} , S_{27}) for transmitting, to the cooperation apparatus, ciphertext data in which the ID of the user generated by using the public key of the re-encryption key issuing apparatus stored in the first storage means of the cooperation apparatus is encrypted, and a request to acquire user information of a user
15 specified by the ID indicated by the ciphertext data and stored in the other service apparatus, in response to an operation of the user,

acquisition means (S_{15} , S_{25}) for acquiring, upon
20 receiving the re-encrypted data transmitted by the cooperation apparatus, the encrypted ID by decrypting the re-encrypted data using the stored private key,

readout means (S_{14} , S_{24}) for reading out the user information corresponding to the acquired ID from the third
25 storage means, and

fourth transmission means (S_{18} , S_{28}) for transmitting the readout user information to the other service apparatus

via the cooperation apparatus.

2. A cooperation service providing system (1) in which a re-encryption key issuing apparatus (10), a plurality of service apparatuses (S_1 , S_2) for providing various services to a user by using an ID issued for identifying the user, and a cooperation apparatus (20) for causing the plurality of service apparatuses to cooperate with each other are communicably connected to each other, characterized in that

10 the cooperation apparatus comprises

first storage means (22) for storing public keys of the re-encryption key issuing apparatus and the service apparatuses,

15 second storage means (23) for storing a re-encryption key for implementing re-encryption processing of enabling ciphertext data transmitted by each of the service apparatuses to be decrypted using a private key of the other service apparatus without decrypting the ciphertext data into plaintext data,

20 first generation means (25) for generating, upon receiving the ciphertext data transmitted by each of the service apparatuses, re-encrypted data by performing re-encryption processing for the ciphertext data using the stored re-encryption key,

25 first transmission means (26) for transmitting the generated re-encrypted data to the other service apparatus different from the service apparatus which has transmitted

the ciphertext data, and

second transmission means (26) for transmitting the stored public key to each of the service apparatuses, and each of the service apparatuses comprises

5 third storage means (S_{11} , S_{21}) for storing the issued ID linked with a first code unique to the service apparatus in association with user information indicating information of the user unique to the service apparatus,

fourth storage means (S_{12} , S_{22}) for storing a private
10 key of the service apparatus,

third transmission means (S_{17} , S_{27}) for transmitting, to the cooperation apparatus, ciphertext data in which the ID of the user generated by using the public key of the re-encryption key issuing apparatus stored in the first
15 storage means of the cooperation apparatus and the first code linked with the ID are encrypted, and a request to acquire user information of a user specified by the ID indicated by the ciphertext data and stored in the other service apparatus, in response to an operation of the user,

20 acquisition means (S_{15} , S_{25}) for acquiring, upon receiving the re-encrypted data transmitted by the cooperation apparatus, the encrypted ID by decrypting the re-encrypted data using the stored private key,

encryption/generation means (S_{14} , S_{24}) for encrypting
25 the decrypted ID to generate a second code,

readout means (S_{16} , S_{26}) for reading out the user information corresponding to the first code from the third

storage means,

specifying means (S_{16} , S_{26}) for specifying the user information by comparing the first code with the second code, and

5 fourth transmission means (S_{18} , S_{28}) for transmitting the readout user information to the other service apparatus via the cooperation apparatus.

3. A server apparatus of a cooperation service providing system in which a re-encryption key issuing
10 apparatus (10), a plurality of service apparatuses (S_1 , S_2) for providing various services to a user by using an ID issued for identifying the user, and a cooperation apparatus (20) for causing the plurality of service apparatuses to cooperate with each other are communicably
15 connected to each other, each of the service apparatuses includes first storage means (S_{11} , S_{21}) for storing the issued ID in association with user information indicating information of the user unique to the service apparatus, second storage means (S_{12} , S_{22}) for storing a private key
20 of the service apparatus, first generation means (S_{14} , S_{24}) for generating, in response to an operation of the user, ciphertext data by performing encryption processing for the ID of the user using a public key of the re-encryption key issuing apparatus transmitted by the cooperation apparatus,
25 first transmission means (S_{17} , S_{27}) for transmitting, to the cooperation apparatus, the generated ciphertext data and a request to acquire user information of a user

specified by the ID indicated by the ciphertext data and stored in the other service apparatus, acquisition means (S₁₅, S₂₅) for acquiring, upon receiving re-encrypted data transmitted by the cooperation apparatus, the encrypted ID
5 by decrypting the re-encrypted data using the stored private key, readout means (S₁₄, S₂₄) for reading out the user information corresponding to the acquired ID from the first storage means, and second transmission means (S₁₈, S₂₈) for transmitting the readout user information to the
10 other service apparatus via the cooperation apparatus, the server apparatus characterized by comprising:

third storage means (22) for storing public keys of the re-encryption key issuing apparatus and the service apparatuses;

15 fourth storage means (23) for storing a re-encryption key for implementing re-encryption processing of enabling ciphertext data transmitted by each of the service apparatuses to be decrypted using a private key of the other service apparatus without decrypting the ciphertext
20 data into plaintext data;

second generation means (25) for generating, upon receiving the ciphertext data transmitted by each of the service apparatuses, re-encrypted data by performing re-encryption processing for the ciphertext data using the
25 stored re-encryption key;

third transmission means (26) for transmitting the generated re-encrypted data to the other service apparatus

different from the service apparatus which has transmitted the ciphertext data; and

fourth transmission means (26) for transmitting the stored public key to each of the service apparatuses.

5 4. A cooperation service providing system (1) in which a re-encryption key issuing apparatus (10), a plurality of service apparatuses (S_1 , S_2) for providing various services to a user, and a cooperation apparatus (20) for causing the plurality of service apparatuses to
10 cooperate with each other are communicably connected to each other, characterized in that

the cooperation apparatus comprises

first storage means (22) for storing public keys of the re-encryption key issuing apparatus and the service
15 apparatuses,

second storage means (23) for storing a re-encryption key for implementing re-encryption processing of enabling ciphertext data transmitted by each of the service apparatuses to be decrypted using a private key of the
20 other service apparatus without decrypting the ciphertext data into plaintext data,

first generation means (25) for generating, upon receiving the ciphertext data transmitted by each of the service apparatuses, re-encrypted data by performing
25 re-encryption processing for the ciphertext data using the stored re-encryption key,

first transmission means (26) for transmitting the

generated re-encrypted data to the other service apparatus different from the service apparatus which has transmitted the ciphertext data, and

second transmission means (26) for transmitting the
5 stored public key to each of the service apparatuses, and
each of the service apparatuses comprises

third storage means (S_{11} , S_{21}) for storing cooperation information for cooperation between the service apparatuses in association with the user,

10 fourth storage means (S_{12} , S_{22}) for storing a private key of the service apparatus,

second generation means (S_{14} , S_{24}) for generating, in response to an operation of the user, ciphertext data by performing encryption processing for the cooperation
15 information associated with the user by using the public key of the re-encryption key issuing apparatus transmitted by the cooperation apparatus,

third transmission means (S_{18} , S_{28}) for transmitting the generated ciphertext data to the cooperation apparatus,
20 and

acquisition means (S_{15} , S_{25}) for acquiring, upon receiving the re-encrypted data transmitted by the cooperation apparatus, the encrypted cooperation information by decrypting the re-encrypted data using the
25 stored private key.

5. A server apparatus of a cooperation service providing system in which a re-encryption key issuing

apparatus (10), a plurality of service apparatuses (S_1 , S_2)
for providing various services to a user, and a cooperation
apparatus (20) for causing the plurality of service
apparatuses to cooperate with each other are communicably
5 connected to each other, each of the service apparatuses
includes first storage means (S_{11} , S_{21}) for storing
cooperation information for cooperation between the service
apparatuses in association with the user, second storage
means (S_{12} , S_{22}) for storing a private key of the service
10 apparatus, first generation means (S_{14} , S_{24}) for
generating, in response to an operation of the user,
ciphertext data by performing encryption processing for the
cooperation information associated with the user by using a
public key of the re-encryption key issuing apparatus
15 transmitted by the cooperation apparatus, first
transmission means (S_{18} , S_{28}) for transmitting the
generated ciphertext data to the cooperation apparatus, and
acquisition means (S_{15} , S_{25}) for acquiring, upon receiving
re-encrypted data transmitted by the cooperation apparatus,
20 the encrypted cooperation information by decrypting the
re-encrypted data using the stored private key, the server
apparatus characterized by comprising:

third storage means (22) for storing public keys of
the re-encryption key issuing apparatus and the service
25 apparatuses;

fourth storage means (23) for storing a re-encryption
key for implementing re-encryption processing of enabling

ciphertext data transmitted by each of the service apparatuses to be decrypted using a private key of the other service apparatus without decrypting the ciphertext data into plaintext data;

5 second generation means (25) for generating, upon receiving the ciphertext data transmitted by each of the service apparatuses, re-encrypted data by performing re-encryption processing for the ciphertext data using the stored re-encryption key;

10 third transmission means (26) for transmitting the generated re-encrypted data to the other service apparatus different from the service apparatus which has transmitted the ciphertext data; and

 fourth transmission means (26) for transmitting the
15 stored public key to each of the service apparatuses.