METHOD AND APPARATUS FOR REGISTRATION OF INFORMATION WITH PLURAL INSTITUTIONS AND RECORDING MEDIUM WITH REGISTRATION PROGRAM STORED THEREON

BACKGROUND OF THE INVENTION

The present invention relates to a method and apparatus for registering a plurality of pieces of electronic information with a plurality of institutions, for example, in an electronic cash system through utilization of a telecommunication system. Further, the invention pertains to a recording medium with a registration program stored thereon.

For example, in an electronic cash system, a user registers his generated information I_A with a bank, then has the bank to sign the information I_A and issue the signed information as a license, and uses it to get another institution to issue electronic cash. In such an instance, the user needs to register different pieces of information I_A and I_B with the bank and the electronic cash issuing institution, respectively, in such a way that either of them will have no knowledge of the information registered with the other.

To register two such different pieces of information I_A and I_B, for example, with two institutions A and B without any risk of revealing to either of them what is registered with the other, it is necessary that the institution A prepare a pair of public and secret keys PK_A and SK_A, that the institution B similarly prepare a pair of public and secret keys PK_B and SK_B, and that the user enciphers the different pieces of information I_A and I_B through utilization of the public keys PK_A and PK_B, respectively, and registers the enciphered pieces of information with the institutions A and B separately of each

other. This inevitably gives rise to the problem of a heavy load of processing on the user side.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide a method and apparatus which permit registration of different pieces of user information with a plurality of institutions simply by presenting required information to each of them without providing any chance for either institution to get the information registered with the other institution.

Another object of the present invention is to provide a recording medium having stored thereon a programs for such registration of information.

The principles of the registration method according to the present invention are that the user generates the pieces of information I_A and I_B for registration with the institutions A and B, respectively, then enciphers the information I_B with a cipher key EK to obtain information $EK(I_B)$, and sends these pieces of information I_A and $EK(I_B)$ to the institution A. The institution A registers the information I_A as user information and sends the information $EK(I_B)$ to the institution B. The institution B deciphers the information $EK(I_B)$ with a cipher key EK and registers the resulting information I_B.

The registration method according to the present invention comprises the steps as follows:

When a user U registers the different pieces of information I_A and I_B with an institution A apparatus and an institution B apparatus through a user apparatus:

the user unit generates key information K to be shared with the institution B, and enciphers the pieces of information I_B and K to be registered with the institution B apparatus through the use of a public key (PK_B) of the institution B, thereby generating information $PK_B(I_B, K)$;

the user apparatus sends the pieces of information $PK_B(I_B, K)$ and I_A to the institution A apparatus;

the institution A apparatus registers the user information I_A contained in its received information and sends the remaining information $PK_B(I_B, K)$ to the institution B apparatus; and

the institution B apparatus deciphers the information $PK_B(I_B, K)$ with its own secret key SK_B to derive I_B and K, and registers I_B.

In this instance, when the institution B apparatus does not send its signature to the user apparatus to inform it of the registration of the user information, the key information K need not be generated.

Instead of generating the information $PK_B(I_B, K)$, the user apparatus may generate information $K(I_B)$ by enciphering I_B with K and information $PK_B(K)$ by enciphering K with PK_B and send these pieces of information to the institution A apparatus. The institution A apparatus sends $PK_B(K)$ and $K(I_B)$ to the institution B apparatus. The institution B apparatus deciphers the enciphered information $PK_B(K)$ with its secret key SK_B to obtain the key information K and uses it to decipher the enciphered information $K(I_B)$ to obtain the user information I_B.

Further, the institution A apparatus uses its secret key SK_A to add a signature of the institution A to information that is sent to the institution B apparatus to indicate thereto the registration of the user information with the institution A. The institution B apparatus

verifies the validity of the signature contained in the information received from the institution A apparatus through the use of its public key PK_A; the institution B apparatus proceeds to decipherment only when the signature is found valid.

The confirmation of registration may be issued to the user apparatus by mail or telephone, for instance. In the case of sending such a notice of registration, especially, the signature of the institution B to the user apparatus:

the institution B apparatus generates registration confirming information $SK_B(I_B)$ by attaching a digital signature to the user information IB through the use of the secret key SK_B, then generates information $K(SK_B(I_B))$ by enciphering the registration confirming information with the user secret key K, and sends the enciphered information to the institution A apparatus;

the institution A apparatus generates information $SK_A(I_A)$ indicative of the registration of the user information I_A by attaching thereto a digital signature through the use of the secret key SK_A, and sends the user apparatus the information $SK_A(I_A)$ and the enciphered information $K(SK_B(I_B))$ received from the institution B apparatus; and

the user apparatus obtains the registration confirming information $SK_B(I_B)$ by deciphering the information $K(SK_B(I_B))$ with the secret key K, then detects the signature $SK_A(I_A)$ of the institution A corresponding to the user information I_A and the signature $SK_B(I_B)$ of the institution B corresponding to the user information I_B, then verifies the validity of the signature $SK_A(I_A)$ by the public key PK_A of the institution A and the user information I_A and the validity of the signature $SK_B(I_B)$ by the public key PK_B and the user information I_B, and

if they are both found valid, recognizes that the user information has been duly registered with either institution.

As described above, the present invention enables the user to register different information with a different institution simply by presenting thereto the required information without incurring the possibility of the information being revealed to other institutions.

BRIEF DESCRIPTION OF THE INVENTION

Fig. 1 is a block diagram for explaining the principles of the method for registering information with a plurality of institutions according to the present invention;

Fig. 2 is a block diagram illustrating the functional configurations of a user apparatus, an institution A apparatus and an institution B apparatus according to an embodiment of the present invention;

Fig. 3 is a flowchart showing the procedure involved in the system configuration of Fig. 2;

Fig. 4 is a block diagram illustrating a modified form of the Fig. 2 embodiment;

Fig. 5 is a flowchart showing the procedure involved in the system configuration of Fig. 4;

Fig. 6 is a flowchart depicting a modification of the procedure in Fig. 3;

Fig. 7 is a flowchart depicting a modification of the procedure in Fig. 5;

Fig. 8 is a block diagram illustrating the configuration of an electronic cash system embodying the information registering method

according to the present invention;

Fig. 9 is a block diagram depicting the configurations of a user apparatus, a bank apparatus and a cash issuer apparatus for user registration processing in the electronic cash system shown in Fig. 8;

Fig. 10 is a block diagram depicting the configurations of the user apparatus, the bank apparatus and the cash issuer apparatus for electronic cash issuance processing in the electronic cash system shown in Fig. 8;

Fig. 11 is a block diagram depicting the configurations of the user apparatus and a shop apparatus for electronic cash payment processing in the electronic cash system shown in Fig. 8; and

Fig. 12 is a block diagram depicting the configurations of the bank apparatus and the cash issuer apparatus for settlement processing in the electronic cash system.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

A description will be given, with reference to Fig. 1, of the principles of the method for registering user information with a plurality of institutions according to the present invention.

An institution A apparatus 100, an institution B apparatus 200 and a user apparatus 300 are interconnected, for example, via communication lines, but they may be connected using a smart card or the like on which information can be recorded.

The system configuration of the present invention is based on the premise that at least institution B apparatus 100 prepares a pair of secret and public keys SK_B and PK_B and provides the public key PK_B to the user apparatus 300. A user U uses an information generating part

33 of the user apparatus 300 to generate information I_A for registration with the institution A apparatus 100 and information I_B for registration with the institution B apparatus 200. Further, the user U uses an encipher key EK to encipher the information I_B in an enciphering part 32 to obtain information $EK(I_B)$. The user U sends the information I_A and the enciphered information $EK(I_B)$ to the institution A apparatus 100, which registers the information I_A in a memory 11 in correspondence to the user U and then sends the enciphered information $EK(I_B)$ to the institution B apparatus 200. The institution B apparatus 200 deciphers the received enciphered information $PK_B(I_B)$ with a decipher key DK in a deciphering part 23 to obtain the information IB, and registers it in a memory 21 in correspondence to the user U.

In the system of Fig. 1 there are two ways of conducting encipherment of the information I_B by the enciphering part 32 of the user apparatus 300 and decipherment of the enciphered information $EK(I_B)$ by the deciphering part 23 of the institution B apparatus 200 as seen from the embodiments described later on. First, the user apparatus 300 enciphers the information I_B by using, as the encipher key EK, the public key PK_B of the institution B apparatus 200 to obtain information $PK_B(I_B)$, and sends it to the institution A apparatus 100 together with the information I_A, and the institution B apparatus 200 deciphers the enciphered information $PK_B(I_B)$ by using the secret key SK_B as the decipher key DK to obtain the information I_B. Second, the user apparatus 300 generates information $K(I_B)$ by using its generated common key K as the encipher key EK and enciphers the common key K with the public key PK_B of the institution B apparatus 200 into $PK_B(I_B)$,

and sends these pieces of information $PK_B(I_B)$ and $K(I_B)$ to the institution A apparatus 100 together with the information I_A, and the institution B apparatus 200 deciphers the enciphered information $PK_B(I_B)$ with the secret key SK_B to obtain the common key and deciphers the information $K(I_B)$ with the key K to obtain the information I_B. Accordingly, the institution A cannot get acquainted with the information I_B registered with the institution B in correspondence to the user U nor can the institution B get acquainted with the information I_A registered with the institution A in correspondence to the user U.

EMBODIMENT 1

Fig. 2 illustrates in block form an example of the system configuration for implementing the registration of user information with a plurality of institutions according to the present invention. Fig. 3 depicts procedures for registering the user information with the institutions A and B in the system configuration of Fig. 2.

This embodiment is based on the premise that the institution A apparatus 100 prepares the secret key SK_A and the public key PK_A for a public key cryptosystem and a digital signature system (see, for example, Ikeno and Koyama, "Modern Cryptology," Institute of Electronics, Information and Communication Engineers of Japan) and provides the public key PK_A to the user apparatus 300, and that the institution B apparatus 200 similarly prepares the secret key SK_B and the public key PK_B and provides the latter to the user apparatus 300.

Step S1: The user U uses an information generating part 330 of the user apparatus 300 to generate the information I_A for registration

with the institution A apparatus 100 and the information I_B for registration with the institution B apparatus 200. Further, the user U uses a common key generating part 340 to generate the common key K and an enciphering part 320 to encipher the information I_A and the common key K with the public key PK_B to generate information $PK_B(I_B, K)$, and sends the pieces of information I_A and $PK_B(I_B, K)$ to the institution A apparatus 100.

Step S2: The institution A apparatus 100 uses a registration part 120 to store the information I_A and $PK_B(I_B, K)$ in the memory 110.

Step S3: Further, the institution A apparatus 100 uses a signature generating part 130 to attach a signature $SK_A(PK_B(I_B, K))$ to the enciphered information $PK_B(I_B, K)$ through the use of the secret key SK_A, and sends the information $SK_A(PK_B(I_B, K))$ and $PK_B(I_B, K)$ to the institution B apparatus 200.

Step S4: The institution B apparatus 200 uses a signature verification part 220 to decipher the signature $SK_A(PK_B(I_B, K))$ of the institution A with the public key PK_A, and makes a check to see if the resulting information $PK_B(I_B, K))$ matches the information $PK_B(I_B, K)$ received from the institution A. If they do not match each other, the received information will be abandoned.

When they match each other, the received information $PK_B(I_B, K)$ is deciphered using the secret key SK_B in a deciphering part 230 to extract the information I_B and the common key K.

Step S5: The institution N stores the thus obtained information I_B and K in a memory 210 through a registration part 240.

Step S6: Further, the institution B generates a signature $SK_B(I_B)$ for the information I_B by a signature generating part 250 through the

use of the secret key SK_B, then enciphers the signature $SK_B(I_B)$ with the common key K by a ciphering part 260 to generate information $K(SK_B(I_B))$, then generates signature information $SK_B(K(SK_B(I_B)))$ of the institution B for the enciphered information $(SK_B(I_B))$ by the signature generating part 250, and sends the enciphered information $K(SK_B(I_B))$ and the signature information $SK_B(K(SK_B(I_B)))$ to the institution A apparatus 100.

Step S7: The institution A apparatus 100 uses a signature verification part 140 to verify the validity of the signature $SK_B(K(SK_B(I_B)))$ of the institution B with the public key PK_B. If the signature $SK_B(K(SK_B(I_B)))$ is found invalid, the received information will be abandoned or destroyed.

When the signature $SK_B(K(SK_B(I_B)))$ is found valid, the institution A generates signature information $SK_A(I_A)$ of the institution A for the user information I_A registered therewith, by a signature information generating part 150 through the use of a key K_A, and sends the signature information $SK_A(I_A)$ and the information $K(SK_B(I_B))$ to the user apparatus 300.

Step S8: The user apparatus 300 uses the common key K to decipher the enciphered information $K(SK_B(I_B))$ by a deciphering part 350 to thereby extract the signature $SK_B(I_B)$ of the institution B. The user apparatus 300 verifies the signatures $SK_A(I_A)$ and $SK_B(I_B)$ of the institutions A and B through the use of a pair of the public key PK_A of the institution A and the user information I_A and a pair of the public key PK_B of the institution B and the user information I_B, respectively. When either one of the signatures $SK_A(I_A)$ and $SK_B(I_B)$ is found invalid, the user apparatus 300 destroys both of them, and when the both

signatures are found valid, the user apparatus stores them in a memory 310.

In the embodiment of Fig. 2, the purpose of attaching the signature of the institution A to the information $PK_B(I_B, K)$ to be sent to the institution B through the use of the secret key SK_A is to enable the institution B to make sure that its received information $SK_A(PK_B(I_B, K))$ has been sent via a normal route, i.e. from the institution A. The institution B verifies the validity of the signed information $PK_B(I_B, K)$ from the institution A by the use of the public key PKA, thereby making sure that the information $PK_B(I_B, K)$ has been duly received from the institution A. If such a verification is unnecessary, however, the institution A may send to the institution B only the received information $PK_B(I_B, K)$ intact with no signature attached thereto. Similarly, when there is no need for the institution A to make sure that its received information $K(SK_B(I_B))$ has been received from the institution B, the institution B needs only to send to the institution A the information $K(SK_B(I_B, K))$ without attaching thereto its signature. The institution A sends the received information $K(SK_B(I_B, K))$ intact to the user U.

The embodiment of Fig. 2 described above may be modified as depicted in Fig. 4. A modified registration procedure is shown in Fig. 5 in correspondence to Fig. 3. In Fig. 4 the parts corresponding to those in Fig. 2 are identified by the same reference numerals. Instead of generating the enciphered information $PK_B(I_B, K)$, the user apparatus 300 generates, in step S1, information $K(I_B)$ by enciphering the information I_B with the key information K in an enciphering part 321 and information $PK_B(K)$ by enciphering the key information K with the

public key PK_B in an enciphering part 322, and sends these pieces of information $K(I_B)$ and $PK_B(K)$ to the institution A apparatus 100.

The institution A apparatus 100 stores, in step S2, the user information I_A in the memory 110 and stores therein the information $K(I_B)$ in place of the information $PK_B(I_B, K)$, and in step S3 attaches its signature to the information $K(I_B)$ with the secret key SK_A in the signing part 130, thereafter sending the signature $SK_A(K(I_B))$ and the pieces of information $PK_B(K)$ and $K(I_B)$ to the institution B apparatus 200.

The institution B apparatus 200 verifies, in step S4, the signature $SK_A(K(I_B))$ with the key PK_A in the verification part 220. If the signature is found valid, the institution B apparatus 200 deciphers the information $PK_B(K)$ with the secret key SK_B in a deciphering part 231 to obtain the key information K, and uses the key information K to decipher the information $K(I_B)$ in a deciphering part 232 to obtain the information I_B. In step S5 the user information I_B and the key information K thus deciphered are stored in the memory 210.

In Fig. 4 there is omitted the procedure for sending the signatures $SK_A(I_A)$ and $SK_B(I_B)$ to the user U for indicating thereto the registration of the user information because the procedure is identical with that described above with reference to Figs. 2 and 3.

In the embodiments of Figs. 2 and 4 the institution A apparatus 100 has been described to send the enciphered information signed with the secret key SK_A, as information indicative of registration of the information I_A, to the institution B apparatus 200. If, however, the information I_A and the information I_B are merely registered with the institution A apparatus 100 and the institution B apparatus 200, respectively, without any possibility of the information registered

with either of the institution apparatuses being revealed to the other, the signature by the secret key SK_A need not be sent to the institution B apparatus 200. That is, the signing in the signing part 130 in step S3 can be omitted; in the case of Fig. 3, only the information $PK_B(I_B,K)$ may sent to the institution B as depicted in Fig. 6, and in the case of Fig. 5, the information $K(I_B)$ and $PK_B(K)$ may be sent to the institution B as depicted in Fig. 7. Accordingly, in the cases of Figs. 6 and 7, the institution B does not verify the signature of the institution A in step S4, but instead it only obtains the information I_B and the key K by decipherment using the secret key SK_B.

Moreover, the pieces of user information I_A and I_B need only to be registered with the institution A apparatus 100 and the institution B apparatus B 200, respectively, and notice of registration may be served to the user U, for example, by mail or telephone, not electronically. In such an instance and when the user apparatus 200 does not require the signatures $SK_A(I_A)$ and $SK_B(I_B)$ of the institution A apparatus 100 and the institution B apparatus 200 that are attached to the information I_A and the information I_B, respectively, the signature verification parts 140 and 360, the signing parts 150 and 250, the enciphering part 260 and the deciphering part 350 in Fig. 2 and the associated processing can be omitted, and in the Fig. 2 embodiment the key information can be dispensed with. For example, in an electronic cash system the institution A apparatus 100 is a bank and the institution B apparatus 200 an electronic cash issuing institution; except in the case where the institution A apparatus 100 calls for information containing I_B so as to deal with an abuse of electronic cash, there is no need for registering the pieces of information $PK_B(I_B, K)$ and

$K(I_B)$ with the institution A apparatus 100 in the examples of Figs. 2 and 4.

The institution A apparatus 100, the institution B apparatus 200 and the user apparatus 300 have the functional configurations shown in Figs. 2 and 3; their processing is computerized and a recording medium is used which has the program therefor recorded thereon.

EMBODIMENT 2

Next, the present invention will be described as being applied to a hierarchical electronic cash system and an apparatus therefor.

Fig. 8 illustrates an example of the system configuration to which this embodiment is applied. An apparatus of an electronic cash issuing institution (hereinafter referred to as an issuer I) 200, apparatuses of a plurality of institutions that manage user information (account information) and effect settlement of electronic cash with shops (hereinafter referred to simply as banks) 100, an apparatus of a person who has electronic cash issued (hereinafter referred to simply as a user) 300, and an apparatus of an institution that receives electronic cash from the user (hereinafter referred to simply as a shop) 400 are interconnected via communication lines or the like. These apparatuses may also be connected using a smart card.

The bank 100 makes public in advance a public key PS_B for digital signature that is set by a signature verification function V_B and the function V_B, and pregenerates a secret key SS_B that is set by a function S_B. The issuer 200 makes public beforehand a public encipher key PE_I that is set by a function E_I and a public key PS_I for

digital signature that is set by a function V_I, and pregenerates a secret cipher key SE_I that is set by a function D_I and a secret signature key SS_I that is set by a function S_I. To make the cipher key PE_I public is based on the premise of making public the cipher function E_I that uses the public cipher key PE_I. Likewise, to make the key PS_I for digital signature public is based on the premise of making public the signature verification function $V_I=V_{PSI}$ that uses the public key PS_I.

In this embodiment, when the user 300 requests the bank 100 to do a procedure for the issue of electronic cash of a face value X, the bank 100 withdraws the amount of money X from the account of the user 300 and sends the user's request to the issuer 200 after attaching a digital signature to the request to certify its validity. The issuer 200 verifies the validity of the request and issues electronic cash of the face value X to the user 300.

In this instance, the user 300 generates, as electronic cash issuance request information, information that contains a signature verification key N_U necessary for the verification of a signature of the user in the procedure for his payment of electronic cash to a shop. And the user 300 follows the procedure in Embodiment 1 to register his real name with the bank 100 in correspondence to his account and the signature verification key N_U with the electronic cash issuing institution 200.

(A) User Registration Procedure

Step 1: A description will be given first, with reference to Fig. 9 depicting functional blocks of the user 300, the bank 100 and the issuer 200, of a procedure for the user 300 to register his information with the bank 100 and the issuer 200. The user 300 uses a digital

signature key generating part 330 to generate a signature generating key SS_U, that is, a signature generating function S_U and a signature verification key N_U. Further, the user 300 generates a cipher key K, using a cipher key generating part 340 for a common cipher key (see, for example, Ikeno and Koyama, "Modern Cryptology," Institute of Electronics, Information and Communication Engineers of Japan). The signature generating key SS_U, the signature verification key N_U and the cipher key K thus generated are held in a memory 30M (Fig. 10). Next, the user 300 calculates $E_I(K, N_U)$ by means of an encipherment part 320 for calculating the cipher function E_I, and sends the calculated information to the bank 100 together with the user's name U.

Step S2: The bank 100 first makes sure that the user's name U corresponds to an authorized user having an account, and then records the user's name U and the information $E_I(K, N_U)$ in a pair in a user data base 110.

Next, the bank 100 uses the signature function S_B in a signature generating part 130 to calculate its signature $s_B=S_B(E_I, K, N_U))$ for the information $E_I(K, N_U)$, and sends information $\{E_I(K, N_U), s_B\}$ to the issuer 200.

Step S3: The issuer 200 verifies the validity of the signature s_B sent from the bank 100, using the signature verification function V_B in a signature verification part 220. If the signature is found valid, the issuer 200 deciphers the information $E_I(K, N_U)$ with the secret cipher key SE_I in a decipherment part 230, thereby obtaining the keys K and N_U. Next, the issuer 200 a signature $S_I(N_U)$ for the key information N_U in a signature generating part 250, and stores the pieces of information N_U and $E_I(K, N_U)$ in a pair in an inspection data base 210. Further, the

issuer 200 uses the key K as an encipher key in an encipherment part 260 to encipher the signature $S_I(N_U)$ into $E_K(S_I(N_U))$, and sends it to the bank 100.

Step S4: The bank 100 sends the information $E_K(S_I(N_U))$ to the user 300.

Step S5: The user 300 deciphers its received information $E_K(S_I(N_U))$ with the key K in a decipherment part 350, thereby extracting the signature $S_I(N_U)$ of the issuer 200. Here, let $L=\{N_U, S_I(N_U)\}$ represent a license of the user U.

This registration procedure corresponds to that in the Fig. 3 embodiment. That is, the signature verification key N_U of the user U corresponds to the information I_B in Fig. 3 and the user's real name U to the information I_A. The bank 100 has knowledge of the correspondence between the enciphered information $E_I(K, N_U)$ and the user U but cannot decipher the information $E_I(K, N_U)$, and hence it will be unable to get acquainted with the keys K and N_U (that is, it will not be able to know the information I_B). On the other hand, the electronic cash issuing institution 200 knows that the bank 100 has the enciphered information $E_I(K, N_U)$ but cannot get acquainted with its correspondence to the user U, and hence it will not be able to know the user's real name, that is, the information I_A.

(B) Electronic Cash Issuing Procedure

Next, a description will be given, with reference to Fig. 10, of the procedure for the user to have electronic cash issued.

Incidentally, the issuer 200 holds secretly the secret key SE_I corresponding to the public cipher key PE_I and the decipher function $D_I=D_{SEI}$ using the key SE_I in a memory 10M (Fig. 10) in correspondence

to the cipher function E_I using the public key PE_I; that is, the issuer 200 holds the key SE_I in secret. Further, the issuer 200 holds secretly the signature generating function $S_I=S_{SSI}$ using the secret key SS_I corresponding to the public cipher key PS_I in a memory 20M (Fig. 10) in correspondence to the signature verification function V_I using the public key PS_I; that is, the issuer 200 holds the key SS_I in secret. Similarly, the bank 100 holds secretly the signature generating function $S_B=S_{SSB}$ using the secret key SS_B corresponding to the public key PS_B in the memory 10M in correspondence to the signature verification function V_B using the public key PS_B; that is, the bank 100 holds the key SS_B in secret.

The user 300 goes through the following procedure to ask the bank 100 to withdraw the amount of money X from his account so as to request the issue of electronic cash of the face value X.

Step S1: The user 300 reads out from the memory 30M the cipher key K, the signature generating key SS_U, the signature generating function S_U and the signature verification key N_U pregenerated by the user 300. Next, the user 300 generates, as a request for the issue of electronic cash, information $E_I(X, K, N_U)$ obtained by enciphering (X, K, N_U) with the public encipher function E_I and the encipher key PE_I in the encipherment part 320, and sends the bank 100 a message for requesting it to withdraw the amount of money X from the account of the user U and the enciphered information $E_I(X, K, N_U)$. The cipher key K is one that the issuer 200 uses to encipher return information $S_I(X, N_U)$ addressed to the user 300 as described later on. Incidentally, it is desirable that this message be authenticated, for example, by the digital signature of the user U.

Step S2: The bank 100 checks the balance of the user U and reduces the balance by the amount of money X. Alternatively, the user's request for withdrawal may be recorded. The user's signature, if attached to his request, will be of particularly high probative value. The withdrawal from the user's account may be made at any time after checking the balance.

Next, the bank 100 calculates, in the signature generating part 130, its signature $s_B=S_B(X, E_I(X, K, N_U))$ for the amount of money X and the information $E_I(X, K, N_U)$ received as the electronic cash issuance request from the user 300, and sends information $\{S, E_I(X, K, N_U), s_B\}$ to the issuer 200.

Step S3: The issuer 200 verifies the validity of the signature s_B received from the bank 100, using the signature verification function V_B in the signature verification part 220. If the signature is found valid, the issuer 200 deciphers the information $E_I(X, K, N_U)$ with the secret cipher key SE_I in the decipherment part 230, obtaining the individual pieces of information X, K, and N_U. Next, the issuer 200 makes a check in a comparison part 240 to determine if the amount X received from the bank 100 and the amount X deciphered as mentioned above. If the information X is found valid, the issuer 200 generates, in the signature generating part 250, its signature $S_I(X, N_U)$ for information (X, N_U) containing the key N_U for verifying the signature of the user 300.

Further, the issuer 200 records a set of pieces of information N_U, $E_I(X, K, N_U)$ and K and information B of the bank 100 (its name or identification number) in the inspection data base 210 in correspondence to an initial value Y=0 of the total amount of money

used Y.

Then, the issuer 200 enciphers its signature $S_I(X, N_U)$ into information $E_K(S_I(X, N_U))$, using the cipher key K in the encipherment part 260, and sends the enciphered information $E_K(S_I(X, N_U))$ to the bank 100.

Step S4: The bank 100 sends the user 300 the enciphered information $E_K(S_I(X, N_U))$ received from the issuer 200.

Step S5: The user 300 uses the key K in the decipherment part 350 to decipher the received information $E_K(S_I(X, N_U))$, obtaining the signature $S_I(X, N_U)$ of the issuer 200.

In this instance, letting the initial value of the balance x of electronic cash be represented by x=X, information $C=\{x, X, N_U, S_I(N_U), S_I(X, N_U)\}$ is stored as electronic cash of the amount X in the memory 30M, together with the key information SSU. The electronic cash C will hereinafter be called electronic cash issued from the issuer 200.

While in this embodiment the user 300 has been described to generate the signature verification key N_U, it may also be generated by a different institution, for example, by the issuer 200. In such an instance, the user 300 sends information EI(X, K) to the bank 100. The bank 100 processes the information in the same manner as is the case with the information $E_I(X, K, N_U)$ and the issuer 200 also performs processing in the same manner as in the above, thereby verifying the validity of the signature attached to the information $(X, E_I(X, K))$ and deciphers it to obtain X and K. After this, the issuer 200 generates the signature verification key N_U and processes X and N_U in the same manner as in the above, and sends $E_K(N_U)$ to the user 300 via the bank 100.

(C) Payment of Electronic Cash

Next, A description will be given, with reference to Fig. 11, of the procedure for the user 300 to pay an amount of money y (where $y \leq x$) to the shop 400 with the electronic cash C of the face value X and the balance x.

Step S1: The user 300 sends the shop 400 the electronic cash $C=\{x, X, N_U, S_I(X, N_U), S_I(N_U)\}$ read out of the memory 30M.

Step S2: The shop 400 verifies the validity of the issuer's signatures $S_I(N_U)$ and $S_I(X, N_U)$ in a signature verification part 410 using the public key PS_I for verification of the signature of the issuer 200. If they are found valid, the shop 400 generates random numbers R_1 and R_2 in a random generating part 450, then generates in a randomizing part 460 a value G_1 obtained by randomizing information W corresponding to the shop 400 with the random number R_1 and a value G_2 obtained by randomizing a signature verification key N_W with the random number R_2, and sends these values G_1 and G_2 to the user 300 along with a transaction identifier T_S generated in a transaction identifier generating part 430. The transaction identifier T_S is, for example, information containing the date and time of transaction.

Step S3: The user 300 receives the transaction identifier T_S and the values G1 and G1 in a one-way function calculating part 380 to obtain a function $e=f(T_S, G_1, G_2)$, then generates a user signature $S_U(e, y)$ for the function e and the amount of money y to be paid in a signature generating part 370, and sends the user signature and the amount of money y to the shop 400.

Step S4: As is the case with the user 300, the shop 400 calculates the function e from the transaction identifier T_S and the

values G_1 and G_2 in a one-way function calculating part 420, then verifies the validity of the user signature $S_U(e, y)$ in a signature verification part 440 through the use of the signature verification key N_U received from the user 300, and makes a check in a comparison part 470 to see if $y \leq x$. If both of them are found valid, the shop 400 admits or acknowledges payment with the electronic cash in the amount y concerned, and stores all communication data $H=\{x, X, N_U, S_I(N_U), S_I(X, N_U), T_S, G_1, G_2, R_1, R_2, y, S_U(e, y)\}$ in a memory 480.

(D) Settlement

A description will be given finally, with reference to Fig. 12, of a method for the settlement of accounts between the shop 400 and the bank 100.

Step S1: The shop 400 sends the issuer 200 all the communication data $H=\{x, X, N_U, S_I(N_U), S_I(X, N_U), T_S, G_1, G_2, R_1, R_2, y, S_U(e, y)\}$ between the user 300 and the shop 400.

Step S2: A decision/control part 295 of the issuer apparatus 200 makes a check to see if the signature verification key N_U for the user 300 contained in the communication data H is stored in the inspection data base 210. When (X, N_U) is not stored in the inspection data base 210, the issuer 200 considers that the user 300 has made an invalid payment, and begins a malicious adversary specifying procedure. When (X, N_U) is stored, the issuer 200 calculates in an adding part 270 a total amount of money used, Y+y, corresponding to (X, N_U), then compares the total value Y+y with the face value X in a comparison part 290, and performs the following processing based on the result of comparison.

(a) If the total value Y+y is smaller than the face value X, the shop 400 will request the bank 100 to pay the money y into its bank account. In this case, the bank that has the account of the shop 400 need not always be the bank 100 with which the user 300 has his account. The issuer 200 updates the total value Y in the inspection data base 210 with Y+y, and stores the communication data H in a history data base 280.

(b) If Y+y=X, the shop 400 will request the bank 100 to pay the money y into its bank account. And since the electronic cash has been spent in full, the issuer 200 deletes the information (X, N_U) and the corresponding total amount Y from the inspection data base 210.

(c) If Y+y>X, the issuer 200 deletes the information (X, N_U) and the corresponding total amount Y from the inspection data base 210; in this case, too, the issuer 200 considers that an invalid payment by the user 300 has been made, and performs the malicious adversary specifying procedure.

Step S3: In the malicious adversary specifying procedure, the issuer 200 sends, prior to the deletion of the information (X, N_U), the bank 100 information as evidence of the malicious play (all communication data H concerning the invalid payment) read out of the history data base 280 and the pieces of information (K, N_U) and $E_I(K, N_U)$ read out of the inspection data base 210. The bank 100 verifies the validity of the evidence of the malicious play (all the communication data H concerning the invalid payment) with the signature verification key N_U in the signature verification part 140. If the evidence is valid, the bank 100 will specifies the malicious user U from the user data base 110, using the enciphered information $E_I(K, N_U)$ as a key.

In Embodiment 2 described above, it is possible, in general, to convert a given function g to $g(X, N_U)=n$ or $\{g(X), g(N_U)\}=n$ and use the n as a value corresponding to (X, N_U). That is, the above-described embodiment employs an identity function as the function g. Further, the information $E_I(X, K, N_U)$ may be considered as a combination of the pieces of information $E_I(X, K)$ and $E_I(N_U)$.

EFFECT OF THE INVENTION

As described above, according to the present invention, when the user sends pieces of information $PK_B(I_B)$ and I_A or $PK_B(K)$, $K(I_B)$ and I_A to the institution A apparatus (a bank, for instance) from the user apparatus, the user information I_A is registered with the institution A apparatus, then the information containing I_B is sent therefrom to the institution B apparatus without any risk of the user information I_B being revealed to the institution A apparatus and is registered with the institution B apparatus. Accordingly, the user needs not to perform processing for individual registration of user information with the institution A apparatus and the institution B apparatus; hence, the registration processing is simple.

Further, the institution A apparatus attaches its signature to the information received from the user apparatus and sends the signed information to the institution B apparatus. The institution B apparatus verifies the validity of the signature attached to the information received from the institution A apparatus. When the signature is found valid, it can be recognized that the institution A apparatus has already registered the information I_A received from the user apparatus.

With the present invention applied to the electronic cash issuing procedure, the user needs only to perform a single procedure through a bank to register his real name U with the bank without any risk of the name being revealed to the issuer and the user signature verification key NU with the issuer without any risk of the key being revealed to the bank.

It will be apparent that many modifications and variations may be effected without departing from the scope of the novel concepts of the present invention.

WHAT IS CLAIMED IS:

1. A method by which a user registers different pieces of information with institutions A and B, respectively, said method comprising the steps wherein:

(a) said user generates pieces of information I_A and I_B to be registered with said institutions A and B, respectively;

(b) said user enciphers said information I_B with an encipher key EK to obtain enciphered information $EK(I_B)$, and sends said information I_A and said enciphered information $EK(I_B)$ to said institution A;

(c) said institution A registers said information I_A as information corresponding to the real name of said user, and sends said information $EK(I_B)$ to said institution B; and

(d) said institution B deciphers said information $EK(I_B)$ with a decipher key DK to obtain said information I_B, and registers it.

2. The method of claim 1, which further comprises a step wherein said institution B pregenerates a public key PK_B and a secret key SK_B as said encipher key EK and said decipher key, respectively, and provides said public key PK_B to said user, and in which:

said step (b) is a step of enciphering said information IB with said public key PK_B used as said encipher key EK to obtain information $PKB(I_B)$ as said information $EK(I_B)$ and sending it as said information $EK(I_B)$ to said institution A, together with said information I_A;

said step (c) includes a step of sending said information $PK_B(I_B)$ as said information $EK(I_B)$ to said institution B; and

said step (d) includes a step of deciphering said information $PK_B(I_B)$ with said secret key SK_B used as said decipher key DK to obtain

said information I_B.

3. The method of claim 1, which further comprises a step wherein said institution B pregenerates a public key PK_B and a secret key SK_B and provides said public key PK_B to said user, and in which:

said step (b) includes a step of generating a common cipher key K as said encipher key EK, enciphering said information I_B with said common cipher key K to obtain information $K(I_B)$ as said information $EK(I_B)$, enciphering said common cipher key K with said public key PK_B to obtain information $PK_B(K)$, and sending said pieces of information $K(I_B)$ and $PK_B(K)$ as said information $EK(I_B)$ to said institution A, together with said information I_A;

said step (c) includes a step of sending said pieces of information $K(I_B)$ and $PK_B(K)$ as said information $EK(I_B)$ to said institution B; and

said step (d) includes, as a process for deciphering said information $DK(I_B)$ with said decipher key DK, a step of deciphering said information $PK_B(K)$ with said secret key SK_B to obtain said common cipher key K and deciphering said information $K(I_B)$ with said common cipher key K to obtain said information I_B.

4. The method of claim 3, which further comprises a step wherein said institution A pregenerates a public key PK_A and a secret key SK_A and making said public key PK_A public; and in which:

said step (c) includes a step of generating a signature $SK_A(K(I_B))$ of said institution A for said information $K(I_B)$ contained in information received from said user apparatus, and sending said signature $SK_A(K(I_B))$ to said institution B, together with said pieces of information $PK_B(K)$ and $K(I_B)$; and

said step (d) includes a step of verifying, with said public key PK_A, the validity of said signature $SK_A(K(I_B))$ in information received from said institution A and, if said signature is found valid, deciphering said information $PK_B(K)$.

5. The method of claim 1, which further comprises a step wherein said institution B pregenerates a public key PK_B and a secret key SK_B as said encipher key EK and said decipher key DK, and provides said public key PK_B to said user, and in which:

said step (b) includes a step of generating a common cipher key K, enciphering said information I_B and said common cipher key K with said public key PK_B used as said encipher key EK to obtain information $PK_B(I_B, K)$ as said information $EK(I_B)$, and sending said information $PK_B(I_B, K)$ to said institution A, together with said information I_A;

said step (c) includes a step of registering said pieces of information I_A and $PK_B(I_B,K)$ received from said user, as information corresponding to the real name of said user, and sending said information $PK_B(I_B, K)$ as said information $EK(I_B)$ to said institution B; and

said step (d) includes a step of deciphering, with said secret key SK_B, said information $PK_B(I_B, K)$ in information received from said institution A to obtain said information I_B and said common cipher key K and registering at least said information I_B.

6. The method of claim 2 or 5, which further comprises a step wherein:

said institution A pregenerates a public key PK_A and a secret key SK_A;

said institution A generates, with said secret key SK_A, its signature for information enciphered with said public key PK_B, contained in information received from said user, and also sends said signature to said institution B; and

said institution B verifies, with said public key PK_A, said signature in information received from said institution A and, if said signature is found valid, deciphers, with said secret key SK_B, said information enciphered with said public key PK_B.

7. The method of claim 3, 4, or 5, which further comprises the steps wherein:

said institution B:

(1) registers said deciphered said common cipher key K together with said information I_B;

(2) generates a digital signature $SK_B(I_B)$ for said information I_B through the use of said secret key SK_B;

(3) generating information $K(SK_B(I_B))$ by enciphering said digital signature $SK_B(I_B)$ with said common cipher key K;

(4) generating a signature $SK_B(K(SK_B(I_B)))$ of said institution B for said information $K(SK_B(I_B))$; and

(5) sends said information $K(SK_B(I_B))$ and said signature $SK_B(K(SK_B(I_B)))$ therefor to said institution A;

said institution A:

(6) verifies the validity of said signature $SK_B(K(SK_B(I_B)))$ in information received from said institution B, through the use of said public key PK_B;

(7) if said signature $SK_B(K(SK_B(I_B)))$ is found valid, generates a digital signature $SK_A(I_A)$ for said information I_A; and

(8) sends said digital signature $SK_A(I_A)$ and said information $K(SK_B(I_B))$ received from said institution B to said user; and

said user:

(9) deciphers said information $K(SK_B(I_B))$ in information received from said institution A through the use of said common cipher key, thereby obtaining said digital signature $SK_B(I_B)$; and

(10) verifies the validity of said signatures $SK_A(I_A)$ and $SK_B(I_B)$ and, if they are both found valid, recognizes that said pieces of information I_A and I_B have been registered with said institution A and said institution B, respectively.

8. The method of 3, 4, or 5, wherein said institution A also registers information containing said information I_B in said information received from said user.

9. The method of claim 3, 4, or 5, which further comprises the steps wherein:

said institution B:

(1) registers said deciphered common cipher key K together with said information I_B;

(2) generates a digital signature $SK_B(I_B)$ for said information I_B through the use of said secret key SK_B;

(3) enciphers said digital signature $SK_B(I_B)$ with said common cipher key K, thereby obtaining information $K(SK_B(I_B))$; and

(4) sends said information $K(SK_B(I_B))$ to said institution A;

said institution A:

(5) sends said information $K(SK_B(I_B))$ received from said institution B to said user; and

said user:

(7) deciphers said information $K(SK_B(I_B))$ from said institution A with said common cipher key K, thereby obtaining said digital signature $SK_B(I_B)$ of said institution B for said information I_B; and

(8) verifies the validity of said digital signature $SK_B(I_B)$ with said public key PK_B and, if said digital signature $SK_B(I_B)$ is found valid, recognizes that said information I_B has been registered with said institution B.

10. A user apparatus in a system in which a user registers different pieces of information I_A and I_B with institutions A and B, respectively, said user apparatus comprising:

a memory for storing a public key PK_B of said institution B;

common key generating means for generating a common cipher key K and for storing it in said memory;

information generating means for generating said information I_A for registration with said institution A and said information I_B for registration with said institution B and for storing said pieces of information I_A and I_B in said memory;

encipher means for enciphering said information I_B and said common cipher key K with said public key PK_B to generate information $PK_B(I_B, K)$;

means for sending said information $PK_B(I_B, K)$ and said information I_A to said institution A;

decipher means for deciphering information $K(SK_B(I_B))$ received from said institution A to obtain a signature $SK_B(I_B)$; and

signature verification means for verifying the validity of said signature $SK_B(I_B)$ with said public key PK_B and said information I_B.

* C L M S *

11. A user apparatus in a system in which a user registers different pieces of information I_A and I_B with institutions A and B, respectively, said user apparatus comprising:

a memory for storing a public key PK_B of said institution B;

common key generating means for generating a common cipher key K and for storing it in said memory;

information generating means for generating said information I_A for registration with said institution A and said information I_B for registration with said institution B and for storing said pieces of information I_A and I_B in said memory;

first encipher means for enciphering said common cipher key K with said public key PK_B to generate information $PK_B(K)$;

second encipher means for enciphering said information I_B with said common cipher key K to generate information $K(I_B)$;

means for sending said pieces of information $PK_B(K)$, $K(I_B)$ and I_A to said institution A;

decipher means for deciphering information $K(SK_B(I_B))$ received from said institution A to obtain a signature $SK_B(I_B)$; and

signature verification means for verifying the validity of said signature $SK_B(I_B)$ with said public key PK_B and said information I_B.

12. The user apparatus of claim 10 or 11, wherein said memory has held therein a public key PK_A of said institution A and said signature verification means includes means for verifying the validity of a signature $SK_A(I_A)$ received from said institution A through the use of said public key PK_A and said information I_A.

13. An institution A apparatus in a system in which a user registers different pieces of information I_A and I_B with institutions A

and B, respectively, said institution A apparatus comprising:

a memory for storing a public key PK_B of said institution B;

means for storing in said memory said information I_A and information $PK_B(I_B)$ received from said user;

means for sending said information $PK_B(I_B, K)$ to said institution B; and

means for sending information $K(SK_B(I_B))$ received from said institution B to said user.

14. An institution A apparatus in a system in which a user registers different pieces of information with institutions A and B, respectively, said institution A apparatus comprising:

a memory for storing a public key PK_B of said institution B;

means for storing in said memory said information I_A and pieces of information $K(I_B)$ and $PK_B(K)$ received from said user;

means for sending said pieces of information $PK_B(K)$ and $K(I_B)$ received from said user to said institution B; and

means for sending information $K(SK_B(I_B))$ received from said institution B to said user.

15. The institution A apparatus of claim 13, wherein said memory has held therein a secret key SK_A and a public key PK_A of said institution A, which further comprises signing means for signing said information $PK_B(I_B, K)$ received from said user through the use of said secret key SK_A to thereby obtain signature information $SK_A(PK_B(I_B, K))$, and wherein said sending means sends said signature information $SK_A(PK_B(I_B, K))$ to said institution B together with said information $PK_B(I_B, K)$.

16. The institution A apparatus of claim 14, wherein said memory has held therein a secret key SK_A and a public key PK_A of said institution A, which further comprises signing means for signing said information $K(I_B)$ received from said user through the use of said secret key SK_A to thereby obtain signature information $SK_A(K(I_B))$, and wherein said sending means sends said signature information $SK_A(K(I_B))$ to said institution B together with said pieces of information $K(I_B)$ and $PK_B(K)$.

17. The institution A apparatus of claim 13, 14, 15 or 16, which further comprises signature verification means for verifying, through the use of said public key PK_B, the validity of each of said information $K(SK_B(I_B))$ and its signature $SK_B(K(SK_B(I_B)))$ received from said institution B.

18. The institution A apparatus of claim 13, 14, 15 or 16, which further comprises signing means for signing said information I_A in said memory with said secret key SK_B to thereby generate a signature $SK_A(I_A)$, said signature $SK_A(I_A)$ being sent to said user together with said information $K(SK_B(I_B))$ received from said institution B.

19. An institution B apparatus in a system in which a user registers different pieces of information I_A and I_B with institutions A and B, respectively, said institution B apparatus comprising:

a memory for storing secret and public keys SK_B and PK_B of said institution B;

decipher means for deciphering information $PK_B(I_B, K)$ from said institution A with said secret key SK_B and for storing the deciphered information I_B and common cipher key K in said memory;

signing means for signing information I_B in said memory with said secret key SK_B to obtain a signature $SK_B(I_B)$;

encipher means for enciphering said signature $SK_B(I_B)$ with said common cipher key K to generate information $K(SK_B(I_B))$; and

means for sending said information $K(SK_B(I_B))$ to said institution A.

20. An institution B apparatus in a system in which a user registers different pieces of information I_A and I_B with institutions A and B, respectively, said institution B apparatus comprising:

a memory for storing secret and public keys SK_B and PK_B of said institution B;

first decipher means for deciphering information $PK_B(K)$ from said institution A with said secret key SK_B to obtain a common cipher key K;

second decipher means for deciphering information $K(I_B)$ from said institution A with said common cipher key K;

means for storing said deciphered information I_B and said common cipher key K in said memory;

signing means for signing said information I_B in said memory with said secret key SK_B to obtain a signature $SK_B(I_B)$;

encipher means for enciphering said signature $SK_B(I_B)$ with said common cipher key K to generate information $K(SK_B(I_B))$; and

means for sending said information $K(SK_B(I_B))$ to said institution A.

21. The institution B apparatus of claim 19 or 20, which further comprises signing means for signing said information $K(SK_B(I_B))$ with said secret key SK_B to generate signature information $SK_B(K(SK_B(I_B)))$,

said signature information $SK_B(K(SK_B(I_B)))$ being sent to said institution A together with said information $K(SK_B(I_B))$.

22. A recording medium having recorded thereon a program for execution by a computer of a user apparatus in a system in which a user registers different pieces of information I_A and I_B with institutions A and B, respectively, said program comprising the steps of:

generating a common cipher key K;

generating said information I_A for registration with said institution A and said information I_B for registration with said institution B;

storing said common cipher key K and said pieces of information I_A and I_B in a memory;

enciphering said information I_B and said common cipher key K with a public key PK_B of said institution B to obtain information $PK_B(I_B, K)$;

sending said pieces of information I_A and $PK_B(I_B, K)$ to said institution A;

deciphering information $K(SK_B(I_B))$ from said institution A with said common cipher key K to obtain a signature $SK_B(I_B)$; and

verifying the validity of said deciphered signature $SK_B(I_B)$ with said public key PK_B and said information I_B.

23. A recording medium having recorded thereon a program for execution by a computer of a user apparatus in a system in which a user registers different pieces of information I_A and I_B with institutions A and B, respectively, said program comprising the steps of:

generating a common cipher key K;

generating said information I_A for registration with said institution A and said information I_B for registration with said institution B;

storing said common cipher key K and said pieces of information I_A and I_B in a memory;

enciphering said common cipher key K with a public key PK_B of said institution B to generate information $PK_B(K)$;

enciphering said information I_B with said common cipher key K to obtain information $K(I_B)$;

sending said pieces of information I_A, $PK_B(K)$ and $K(I_B)$ to said institution A;

deciphering information $K(SK_B(I_B))$ from said institution A with said common cipher key K to obtain a signature $SK_B(I_B)$; and

verifying the validity of said deciphered signature $SK_B(I_B)$ with said public key PK_B and said information I_B.

24. The recording medium according to claim 22 or 23, wherein said program further comprises a step of verifying the validity of a signature $SK_A(I_A)$ from said institution A with its public key PK_A and said information I_A.

25. A recording medium having recorded thereon a program for execution by a computer of an institution A apparatus in a system in which a user registers different pieces of information I_A and I_B with institutions A and B, respectively, said program comprising the steps of:

storing said information I_A and information $PK_B(I_B, K)$ from said user in a memory;

sending said information $PK_B(I_B, K)$ to said institution B; and

sending information $K(SK_B(I_B))$ from said institution B to said user.

26. A recording medium having recorded thereon a program for execution by a computer of an institution A apparatus in a system in which a user registers different pieces of information I_A and I_B with institutions A and B, respectively, said program comprising the steps of:

storing said information I_A and pieces of information $K(I_B)$ and $PK_B(K)$ from said user in a memory;

sending said pieces of information $PK_B(K)$ and $K(I_B)$ to said institution B; and

sending information $K(SK_B(I_B))$ from said institution B to said user.

27. The recording medium of claim 25, wherein said memory has stored therein secret and public keys SK_A and PK_A of said institution A and said program further comprises a step of signing said information $PK_B(I_B, K)$ with said secret key SK_A to obtain signature information $SK_A(PK_B(I_B, K))$, said signature information $SK_A(PK_B(I_B, K))$ being sent to said institution B together with said information $PK_B(I_B, K)$.

28. The recording medium of claim 26, wherein said memory has stored therein secret and public keys SK_A and PK_A of said institution A and said program further comprises a step of signing said information $K(I_B)$ with said secret key SK_A to obtain signature information $SK_A(K(I_B))$, said signature information $SK_A(K(I_B))$ being sent to said institution B together with said pieces of information $K(I_B)$ and

$PK_B(K)$.

29. The recording medium of claim 25 , 26, 27 or 28 wherein said program further comprises a step of verifying, with a public key PK_B, the validity of each of said information $K(SK_B(I_B))$ and its signature $SK_B(K(SK_B(I_B)))$ received from said institution B.

30. The recording medium of claim 25 , 26, 27 or 28 wherein said program further comprises a step of signing said information I_A in said memory with a secret key SK_A of said institution A to generate a signature $SK_A(I_A)$, said signature $SK_A(I_A)$ being sent to said user together with said information $SK_B(I_B)$ received from said institution B.

31. A recording medium having recorded thereon a program for execution by a computer of an institution B apparatus in a system in which a user registers different pieces of information I_A and I_B with institutions A and B, respectively, said program comprising the steps of:

deciphering information $PK_B(I_B, K)$ from said institution A with a secret key SK_B to obtain said information I_B and a common cipher key K;

storing said information I_B and said common cipher key K in a memory;

signing said information I_B with said secret key SK_B to generate a signature $SK_B(I_B)$;

enciphering said signature $SK_B(I_B)$ with said common cipher key K to generate information $K(SK_B(I_B))$; and

sending said information $K(SK_B(I_B))$ to said institution A.

32. A recording medium having recorded thereon a program for execution by a computer of an institution B apparatus in a system

in which a user registers different pieces of information I_A and I_B with institutions A and B, respectively, said program comprising the steps of:

deciphering information $PK_B(K)$ from said institution A with a secret key SK_B to obtain a common cipher key K;

deciphering information $K(I_B)$ from said institution A with said common cipher key K to obtain said information I_B;

storing said deciphered information I_B and said common cipher key K in a memory;

signing said information I_B with said secret key SK_B to generate a signature $SK_B(I_B)$;

enciphering said signature $SK_B(I_B)$ with said common cipher key K to generate information $K(SK_B(I_B))$; and

sending said information $K(SK_B(I_B))$ to said institution A.

33. The recording medium of claim 31, wherein said program further comprises a step of verifying the validity of each of said information $PK_B(I_B, K)$ from said institution A and its signature $SK_A(PK_B(I_B, K))$ with a public key PK_A and, if they are both found valid, deciphering said information $PK_B(I_B, K)$ with said secret key SK_B to obtain said information I_B and said common cipher key K.

34. The recording medium of claim 32, wherein said program further comprises a step of verifying the validity of each of information $PK_B(K)$ from said institution A and its signature $SK_A(K(I_B))$ with a public key PK_A and, if they are both found valid, deciphering said information $PK_B(K)$ with said secret key SK_B to obtain said common cipher key K.

35. The recording medium of claim 31, 32, 33 or 34, wherein

* C L M S *

said program further comprises a step of signing said information $K(SK_B(I_B)$ with said secret key SKB to generate signature information $SK_B(K(SK_B(I_B)))$, said signature information $SK_B(K(SK_B(I_B)))$ being sent to said institution A together with said information $K(SK_B(I_B))$.