

D E S C R I P T I O N

BIOMETRIC REFERENCE INFORMATION REGISTRATION SYSTEM,
APPARATUS, AND PROGRAM

5

Technical Field

Embodiments described herein relate generally to a biometric reference information registration system, apparatus, and program.

10

Background Art

When implementing communication and services through a network, it is an important technical element to authenticate a communication partner. Recently, the range of authentication targets is expanding from a user to a use
15 device terminal along with the popularization of an open network environment and the development of a federation technique for distributed services and resources.

Particularly when the authentication target is an individual, a technique of confirming the identity of the
20 individual is receiving attention now. Generally when executing authentication, it is necessary in authentication to strictly identify or match an authentication target. At this time, when the authentication target is an individual, a principal confirmation technique of strictly confirming
25 the identity of the individual is necessary.

At present, there is a biometric authentication technique as a promising technique of executing principal

confirmation. Biometric authentication is a technique for matching the unique body feature or characteristic of each individual with biometric information (to be referred to as biometric reference information hereinafter) registered in advance, and confirming the identity of the individual. As the biometric information, the fingerprint, iris, retina, face, voice, key stroke, signature, and the like are used.

Unlike an existing authentication method based on a password or the like, biometric authentication utilizes biometric information without fear of forgetting or missing, and thus can reduce the burden on the user. Biometric information is assumed to be information that is hard to copy, and is effective as a means of prevention against spoofing of a user.

Now, open networks typified by the Internet become popular, and a move to use biometric authentication as a method of authenticating a communication partner over a network in electronic commerce and the like is growing. Even in the fields of identification and the like, it is examined to perform principal confirmation of the owner of an identification certificate by using biometric authentication.

Along with this move, a technique using an authentication context for biometric authentication is known as a technique of performing biometric authentication through a network. More specifically, for example, patent literature 1 discloses a technique of summarizing process

contents regarding biometric authentication on the client side into authentication context (biometric authentication context) information for biometric authentication, and notifying a verifier over a network of the information.

5 When biometric authentication is used on a network, there is known a method using a public key infrastructure (PKI) based on asymmetric cryptography. For example, there is known a method of associating biometric reference information (biometric reference template), which is a
10 credential serving as the reference of the authenticity of biometric authentication, with a public key certificate. This biometric reference information indicates information obtained by performing feature extraction processing or the like on biometric raw information (biometric raw data), and
15 serves as reference information of matching process. Some matching algorithms use biometric raw information as biometric reference information. A known typical technique is the standard specification X.509 of RFC (Request For Comments) 3739 or the like. X.509 defines that a public
20 key certificate includes, as an option, information (hash value of biometric reference information) representing the relevance with biometric reference information. Also, ISO (International Organization for Standardization)/IEC (International Electrotechnical Commission) 24701 defines,
25 as a BRT certificate (Biometric Reference Template certificate), data obtained by adding a digital signature to the hash value of biometric reference information.

As a combination of the above-mentioned biometric authentication and PKI, there is known a technique of indirectly executing user authentication (principal confirmation) on a network by chaining biometric authentication and entity authentication using a public key certificate.

Since base information (e.g., biometric raw information) for generating biometric reference information is sensitive information such as the body feature of an individual, the privacy needs to be taken into account. Hence, it is conceivable to execute biometric authentication processing itself on the authentication target person side without saving information such as biometric reference information on the authenticator side. This method can indirectly execute lifecycle management of biometric reference information by associating a public key certificate and biometric reference information as described above.

However, the above-mentioned biometric authentication techniques have a disadvantage in which biometric reference information cannot be registered in a biometric authentication system from an arbitrary client environment through a network.

For example, biometric reference information is created regardless of which of the authentication target person side and the verifier side manages biometric reference information to be registered. In either case, it

is necessary that an authentication target person visits a store or the like designated by a verifier, and biometric raw information is sampled by a device (e.g., biometric information scanner) prepared by the verifier side. This is because the quality and security of the client environment need to be maintained at a predetermined level. That is, in order to prevent registration of low-quality biometric reference information and maintain the matching accuracy at a predetermined level, biometric information needs to be sampled in a client environment prepared by the verifier side. However, an authentication target person is disadvantageously forced to physically move, increasing the burden on the authentication target person.

To solve this disadvantage, patent literature 2 discloses a technique for registering biometric reference information from an arbitrary client environment through a network while maintaining the matching accuracy at a predetermined level.

Citation List

Patent Literatures

Patent Literature 1: Japanese Patent No. 4956096

Patent Literature 2: Jpn. Pat. Appln. KOKAI

Publication No. 2009-169517

Summary of Invention

Technical Problem

However, in the technique disclosed in patent literature 2, the study of the present inventor reveals

that secret information needs to be shared in advance
between a device (e.g., portable medium) that stores
biometric reference information, and a biometric
authentication system. It is presumed that the biometric
5 reference information is managed by a device closely
associated with the biometric authentication system.

More specifically, a specific biometric authentication
system is presumed to manage a device capable of
registering only biometric reference information (and/or
10 information that guarantees the biometric reference
information) issued by the biometric authentication system.
In this management, the user needs to hold a corresponding
device for each biometric authentication system, increasing
the burden.

15 It is an object of the present invention to provide a
biometric reference information registration system,
apparatus, and program capable of guaranteeing and storing
biometric reference information through a network without
sharing secret information in advance between a device and
20 a biometric authentication system.

A biometric reference information registration system
according to an embodiment comprises a biometric reference
information storage apparatus and biometric reference
information certificate generation apparatus configured to
25 communicate with each other through a network. The
biometric reference information registration system
registers biometric reference information of an

authentication target person in the biometric reference information storage apparatus.

The biometric reference information storage apparatus includes first private key storage means, challenge
5 information reception means, biometric reference information generation means, hash value generation means, first signature generation means, biometric authentication context generation means, biometric authentication context transmission means, certificate reception means, first
10 extraction means, hash value verification means, biometric authentication context verification means, storage means, and write means.

The first private key storage means stores a first private key of the apparatus.

15 The challenge information reception means receives challenge information from the biometric reference information certificate generation apparatus.

The biometric reference information generation means generates biometric reference information based on
20 biometric information sampled from the authentication target person.

The hash value generation means generates a hash value of the biometric reference information.

The first signature generation means generates a first
25 digital signature based on the first private key for the challenge information and the hash value of the biometric reference information.

The biometric authentication context generation means generates a biometric authentication context including the challenge information, the hash value of the biometric reference information, and the first digital signature.

5 The biometric authentication context transmission means transmits the hash value of the biometric reference information and the biometric authentication context to the biometric reference information certificate generation apparatus.

10 The certificate reception means receives, from the biometric reference information certificate generation apparatus, a biometric reference information certificate including the hash value of the biometric reference information, the biometric authentication context, and a
15 second digital signature for the hash value of the biometric reference information and the biometric authentication context.

 The first extraction means extracts the hash value of the biometric reference information and the biometric
20 authentication context from the biometric reference information certificate.

 The hash value verification means verifies the extracted hash value based on the generated hash value.

 The biometric authentication context verification
25 means verifies the extracted biometric authentication context based on the generated biometric authentication context.

The storage means is means for storing the biometric reference information and the biometric reference information certificate.

5 When respective results of the verifications by the hash value verification means and the biometric authentication context verification means represent validity, the write means writes the biometric reference information and the biometric reference information certificate in the storage means.

10 The biometric reference information certificate generation apparatus includes account storage means, second private key storage means, challenge information transmission means, biometric authentication context reception means, second extraction means, challenge
15 information verification means, signature verification means, second signature generation means, certificate generation means, certificate write means, and certificate transmission means.

20 The account storage means stores a user ID of the authentication target person and the biometric reference information certificate in association with each other.

The second private key storage means stores a second private key of the apparatus.

25 The challenge information transmission means generates the challenge information and transmits the challenge information to the biometric reference information storage apparatus.

The biometric authentication context reception means receives the hash value of the biometric reference information and the biometric authentication context from the biometric reference information storage apparatus.

5 The second extraction means extracts challenge information from the received biometric authentication context.

 The challenge information verification means verifies the extracted challenge information based on the
10 transmitted challenge information.

 The signature verification means verifies a first digital signature in the received biometric authentication context based on a first public key corresponding to the first private key.

15 When respective results of the verifications by the challenge information verification means and the signature verification means represent validity, the second signature generation means generates the second digital signature based on the second private key for the hash value of the
20 biometric reference information and the biometric authentication context that have been received.

 The certificate generation means generates the biometric reference information certificate including the hash value of the biometric reference information, the
25 biometric authentication context, and the second digital signature.

 The certificate write means writes the generated

biometric reference information certificate in the account storage means in association with the user ID of the authentication target person.

5 The certificate transmission means transmits the generated biometric reference information certificate to the biometric reference information storage apparatus.

Brief Description of Drawings

FIG. 1 is a schematic view showing an example of the arrangement of a biometric reference information registration system according to the first embodiment.

FIG. 2 is a schematic view showing an example of the arrangement of a biometric reference information storage apparatus according to the first embodiment.

15 FIG. 3 is a schematic view showing an example of the structure of a biometric authentication context according to the first embodiment.

FIG. 4 is a schematic view for explaining a validation information temporary save unit according to the first embodiment.

20 FIG. 5 is a schematic view for explaining the validation information temporary save unit according to the first embodiment.

FIG. 6 is a schematic view showing an example of the arrangement of a biometric reference information certificate generation apparatus according to the first embodiment.

FIG. 7 is a schematic view showing an example of the

structure of a biometric reference information certificate according to the first embodiment.

FIG. 8 is a schematic view for explaining an account management unit according to the first embodiment.

5 FIG. 9 is a sequence chart for explaining an operation according to the first embodiment.

FIG. 10 is a sequence chart for explaining an operation according to the first embodiment.

10 FIG. 11 is a schematic view showing an example of the arrangement of a biometric reference information registration system according to the second embodiment.

FIG. 12 is a schematic view showing an example of the arrangement of a biometric information sampling apparatus according to the second embodiment.

15 FIG. 13 is a schematic view showing an example of the arrangement of a biometric reference information storage apparatus according to the second embodiment.

20 FIG. 14 is a schematic view showing an example of the structure of a first biometric authentication context according to the second embodiment.

FIG. 15 is a schematic view showing an example of the structure of a second biometric authentication context according to the second embodiment.

25 FIG. 16 is a schematic view showing an example of the structure of a biometric reference information certificate according to the second embodiment.

FIG. 17 is a sequence chart for explaining an

operation according to the second embodiment.

Description of Embodiments

In general, according to one embodiment, a biometric reference information registration system comprises a
5 biometric reference information storage apparatus and biometric reference information certificate generation apparatus configured to communicate with each other through a network. The biometric reference information registration system registers biometric reference
10 information of an authentication target person in the biometric reference information storage apparatus.

The biometric reference information storage apparatus includes a first private key storage module, a challenge information reception module, a biometric reference
15 information generation module, a hash value generation module, a first signature generation module, a biometric authentication context generation module, a biometric authentication context transmission module, a certificate reception module, a first extraction module, a hash value
20 verification module, a biometric authentication context verification module, a storage module, and a write module.

The first private key storage module stores a first private key of the apparatus.

The challenge information reception module receives
25 challenge information from the biometric reference information certificate generation apparatus.

The biometric reference information generation module

generates biometric reference information based on biometric information sampled from the authentication target person.

5 The hash value generation module generates a hash value of the biometric reference information.

 The first signature generation module generates a first digital signature based on the first private key for the challenge information and the hash value of the biometric reference information.

10 The biometric authentication context generation module generates a biometric authentication context including the challenge information, the hash value of the biometric reference information, and the first digital signature.

15 The biometric authentication context transmission module transmits the hash value of the biometric reference information and the biometric authentication context to the biometric reference information certificate generation apparatus.

20 The certificate reception module receives, from the biometric reference information certificate generation apparatus, a biometric reference information certificate including the hash value of the biometric reference information, the biometric authentication context, and a second digital signature for the hash value of the biometric reference information and the biometric authentication context.

25

 The first extraction module extracts the hash value of

the biometric reference information and the biometric authentication context from the biometric reference information certificate.

5 The hash value verification module verifies the extracted hash value based on the generated hash value.

 The biometric authentication context verification module verifies the extracted biometric authentication context based on the generated biometric authentication context.

10 The storage module is a module configured to store the biometric reference information and the biometric reference information certificate.

 When respective results of the verifications by the hash value verification module and the biometric authentication context verification module represent
15 validity, the write module writes the biometric reference information and the biometric reference information certificate in the storage module.

 The biometric reference information certificate
20 generation apparatus includes an account storage module, a second private key storage module, a challenge information transmission module, a biometric authentication context reception module, a second extraction module, a challenge information verification module, a signature verification
25 module, a second signature generation module, a certificate generation module, a certificate write module, and a certificate transmission module.

The account storage module stores a user ID of the authentication target person and the biometric reference information certificate in association with each other.

5 The second private key storage module stores a second private key of the apparatus.

The challenge information transmission module generates the challenge information and transmits the challenge information to the biometric reference information storage apparatus.

10 The biometric authentication context reception module receives the hash value of the biometric reference information and the biometric authentication context from the biometric reference information storage apparatus.

15 The second extraction module extracts challenge information from the received biometric authentication context.

The challenge information verification module verifies the extracted challenge information based on the transmitted challenge information.

20 The signature verification module verifies a first digital signature in the received biometric authentication context based on a first public key corresponding to the first private key.

25 When respective results of the verifications by the challenge information verification module and the signature verification module represent validity, the second signature generation module generates the second digital

signature based on the second private key for the hash value of the biometric reference information and the biometric authentication context that have been received.

5 The certificate generation module generates the biometric reference information certificate including the hash value of the biometric reference information, the biometric authentication context, and the second digital signature.

10 The certificate write module writes the generated biometric reference information certificate in the account storage module in association with the user ID of the authentication target person.

15 The certificate transmission module transmits the generated biometric reference information certificate to the biometric reference information storage apparatus.

20 An embodiment will now be described with reference to the accompanying drawings. Note that each of the following apparatuses can be implemented by either a hardware arrangement, or a combinational arrangement of a hardware resource and software. The software in the combinational arrangement includes programs that are installed in a computer from a network or non-transitory computer-readable storage media M1 to M5, executed by the processor of the computer, and cause the computer to implement the functions
25 of each apparatus, as shown in FIGS. 1 and 11.

<First Embodiment>

FIG. 1 is a schematic view showing an example of the

arrangement of a biometric reference information registration system according to the first embodiment. The biometric reference information registration system includes a biometric reference information storage apparatus 10 and biometric reference information certificate generation apparatus 20 that can communicate with each other through a network Nw. The biometric reference information storage apparatus 10 and the biometric reference information certificate generation apparatus 20 are connected in an arbitrary connection form. The biometric reference information registration system registers biometric reference information of an authentication target person in the biometric reference information storage apparatus 10. Note that the biometric reference information registration system can be rewritten into a biometric reference information storage system. Also, the term "registration" may be properly rewritten into "storage" or the like.

As shown in FIG. 2, the biometric reference information storage apparatus 10 includes an input/output unit 11, a control unit 12, a biometric information sampling unit 13, a biometric reference information generation unit 14, a biometric authentication context generation unit 15, a validation determination unit 16, a validation information temporary save unit 17, and an information storage unit 18. The biometric reference information storage apparatus 10 is desirably a device

having tamper resistance and computational ability, such as an IC (Integrated Circuit) card or a cell phone.

The input/output unit 11 is a functional unit that executes specific processing on the biometric reference information storage apparatus 10 and inputs/outputs data in accordance with an external command, like a CUI (Command User Interface) or GUI (Graphical User Interface). Data input/output (transmitted/received) to/from the input/output unit 11 include, e.g., a user ID, a password, a registration start request, challenge information, the hash value of biometric reference information, a biometric authentication context, and a biometric reference information certificate.

The control unit 12 is a functional unit for controlling the overall processing in the biometric reference information storage apparatus 10. The control unit 12 controls events and data in the biometric reference information storage apparatus 10. The control unit 12 executes a command to each functional unit of the biometric reference information storage apparatus 10, and transfers data necessary for processing. Note that this function may be omitted, and a direct call may be performed between other functional units.

The biometric information sampling unit 13 is a function for sampling biometric information of an authentication target person.

The biometric reference information generation unit 14

is a functional unit for generating biometric reference information based on biometric information sampled by the biometric information sampling unit 13.

5 The biometric authentication context generation unit 15 is a functional unit for generating a biometric authentication context for guaranteeing processing regarding biometric authentication executed by the biometric reference information storage apparatus 10. In this embodiment, the biometric reference information
10 generation unit 14 and the information storage unit 18 are guarantee targets. A preferable example of the biometric authentication context is a biometric authentication context in the ISO/IEC 24761 format. In this embodiment, the biometric authentication context is associated with
15 biometric reference information. For example, when a biometric authentication context C has the ISO/IEC 24761 format, it includes the hash value of biometric reference information, as shown in FIG. 3.

20 The biometric authentication context generation unit 15 has, for example, the following functions (f15-1) to (f15-4).

25 (f15-1) A first private key storage function of storing the first first private key of the apparatus. Note that the first private key storage function includes, e.g., a storage area for storing the first private key, and a function of writing the first private key in the storage area.

(f15-2) A hash value generation function of generating the hash value of biometric reference information. The hash value has a fixed data length depending on the hash algorithm.

5 (f15-3) A first signature generation function of generating the first digital signature based on the first private key for challenge information and the hash value of biometric reference information.

10 (f15-4) A biometric authentication context generation function of generating the biometric authentication context C including the challenge information, the hash value of biometric reference information, and the first digital signature.

15 The validation determination unit 16 is a functional unit for validating biometric reference information and a biometric reference information certificate RC. The validation determination unit 16 determines validation of biometric reference information and the biometric reference information certificate RC by verifying biometric reference
20 information and a biometric authentication context that are saved in the validation information temporary save unit 17, and a biometric reference information certificate acquired from the biometric reference information certificate generation apparatus 20. If the validation determination
25 unit 16 determines that the biometric reference information and the biometric reference information certificate RC are valid, it stores them in the information storage unit 18

and validates them.

The validation determination unit 16 has, for example, the following functions (f16-1) to (f16-4).

(f16-1) A first extraction function of extracting the
5 hash value of biometric reference information and the
biometric authentication context C from the biometric
reference information certificate RC.

(f16-2) A hash value verification function of
verifying an extracted hash value based on a generated hash
10 value.

(f16-3) A biometric authentication context
verification function of verifying an extracted biometric
authentication context based on a generated biometric
authentication context.

15 (f16-4) A write function of, when the results of
verifications by the hash value verification function
(f16-2) and the biometric authentication context
verification function (f16-3) represent validity, writing
the biometric reference information and the biometric
20 reference information certificate in the information
storage unit 18.

The validation information temporary save unit 17 is a
functional unit for temporarily saving biometric reference
information generated by the biometric reference
25 information generation unit 14 and a biometric
authentication context generated by the biometric
authentication context generation unit 15. The validation

determination unit 16 uses the saved information for validation determination of the biometric reference information and the biometric reference information certificate RC. The function implemented by the validation information temporary save unit 17 may be arranged as the function of the information storage unit 18.

For example, as shown in FIGS. 4 and 5, the validation information temporary save unit 17 can save a management number, biometric reference information, the hash value of the biometric reference information, a biometric authentication context, and a biometric reference information certificate in association with each other. Note that the management number may be omitted properly. The validation information temporary save unit 17 can be implemented as, e.g., a storage area for storing a data table that describes biometric reference information, the hash value of the biometric reference information, a biometric authentication context, and the biometric reference information certificate RC in association with each other. In the example shown in FIG. 4, valid biometric reference information certificates are saved in association with each other, as represented by lines of management numbers 1 and 2. An invalid biometric reference information certificate is not saved, as represented by a line of management number 3. Note that the management number may be omitted properly. In this example, each of biometric reference information, the hash value of the

biometric reference information, a biometric authentication context, and a biometric reference information certificate is described as binary data of a two-digit hexadecimal character string. In FIGS. 4 and 5, the biometric authentication context and the biometric reference information certificate seem to be the same data, but subsequent data, the illustration of which is omitted, are different (leading data become the same because the data format is determined).

The information storage unit 18 is a functional unit for storing biometric reference information and the biometric reference information certificate RC. The biometric reference information certificate RC is information that is generated by the biometric reference information certificate generation apparatus 20 and guarantees biometric reference information. A preferable example of the biometric reference information certificate RC is a BRT certificate defined by ISO/IEC 24761. This embodiment will explain an example using the BRT certificate as a concrete biometric reference information certificate.

As shown in FIG. 6, the biometric reference information certificate generation apparatus 20 includes an input/output unit 21, a control unit 22, a biometric authentication context verification unit 23, a certificate generation unit 24, and an account management unit 25.

The input/output unit 21 is a functional unit similar

to the input/output unit 11 of the biometric reference
information storage apparatus 10, and is a functional unit
that executes specific processing on the biometric
reference information certificate generation apparatus 20
5 and inputs/outputs data. Data input/output
(transmitted/received) to/from the input/output unit 21
include, e.g., a user ID, a password, a registration start
request, challenge information, the hash value of biometric
reference information, a biometric authentication context,
10 and a biometric reference information certificate.

The control unit 22 is a functional unit similar to
the control unit 12 of the biometric reference information
storage apparatus 10, and is a functional unit for
controlling the overall processing in the biometric
15 reference information certificate generation apparatus 20.
The control unit 22 controls events and data in the
biometric reference information certificate generation
apparatus 20.

The biometric authentication context verification unit
20 23 is a functional unit for verifying the biometric
authentication context C obtained by an interaction with
the biometric reference information storage apparatus 10.
When the biometric authentication context C has the ISO/IEC
24761 format, the biometric authentication context
25 verification unit 23 transmits, to the biometric reference
information storage apparatus 10, challenge information
(random value) for challenge & response authentication

based on the public key cryptography or MAC (Message Authentication Code), verifies the validity of the digital signature value or MAC value of the biometric authentication context C obtained from the biometric reference information storage apparatus 10, and verifies the contents of biometric processing described in the biometric authentication context C.

The biometric authentication context verification unit 23 has, for example, the following functions (f23-1) to (f23-4).

(f23-1) A challenge information transmission function of generating challenge information and transmitting the challenge information to the biometric reference information storage apparatus 10.

(f23-2) A second extraction function of extracting challenge information from the received biometric authentication context C.

(f23-3) A challenge information verification function of verifying extracted challenge information based on transmitted challenge information. The challenge information verification function compares, for example, two pieces of challenge information, and when they match each other, obtains a verification result representing validity.

(f23-4) A signature verification function of verifying, based on the first public key corresponding to the first private key, the first digital signature in a

received biometric authentication context.

As shown in FIG. 7, the certificate generation unit 24 is a functional unit for generating the biometric reference information certificate RC including the hash value of biometric reference information and the biometric authentication context C that are transmitted from the biometric reference information storage apparatus 10, as shown in FIG. 7.

The certificate generation unit 24 has, for example, the following functions (f24-1) to (f24-3).

(f24-1) A second private key storage function of storing the second private key of the apparatus. Note that the second private key storage function includes, e.g., a storage area for storing the second private key, and a function of writing the second private key in the storage area.

(f24-2) A second signature generation function of, when the respective results of verifications by the challenge information verification function (f23-3) and the signature verification function (f23-4) represent validity, generating a second digital signature based on the second private key for the hash value of biometric reference information and the biometric authentication context C that have been received.

(f24-3) A certificate generation function of generating the biometric reference information certificate RC including the hash value of biometric reference

information, the biometric authentication context, and the second digital signature.

The account management unit 25 is a functional unit for specifying the account of an authentication target person, and storing the generated biometric reference information certificate RC as the attribute value of the account of the authentication target person. The account management unit 25 can save, e.g., a management number, a user ID, a biometric reference information certificate, and a validation flag in association with each other, as shown in FIG. 8. Note that the management number and the validation flag may be omitted properly.

More specifically, the account management unit 25 has, for example, the following functions (f25-1) and (f25-2).

(f25-1) An account storage function for storing the user ID of an authentication target person and the biometric reference information certificate RC in association with each other. The account storage function can be implemented as a storage area for storing an account data table that describes a user ID and the biometric reference information certificate RC in association with each other. The account storage function may include a function of writing a user ID in advance in the account data table. Note that, for example, the control unit 22 may have the function of writing a user ID in advance in the account data table.

(f25-2) A certificate write function of writing a

generated biometric reference information certificate in the account storage function in association with the user ID of an authentication target person.

5 The account management unit 25 may be closed in the biometric reference information certificate generation apparatus 20, or may federate with an arbitrary ID management (IDentify management) system. A means for specifying the account of an authentication target person is out of the scope of each embodiment, and an arbitrary
10 means such as conventional authentication based on a user ID/password may be adopted.

Next, the operation of the biometric reference information registration apparatus having the above-described arrangement will be explained with
15 reference to the sequence charts of FIGS. 9 and 10.

As shown in FIG. 9, the biometric reference information storage apparatus 10 transmits a registration start request to the biometric reference information certificate generation apparatus 20 in response to, e.g.,
20 an operation to the input/output unit by an authentication target person (ST1). Note that, instead of the biometric reference information storage apparatus 10, the biometric reference information certificate generation apparatus 20 may transmit a registration processing start request to the
25 biometric reference information storage apparatus 10. Specifying of an authentication target person is premised to be executed before step ST1 or in response to a

registration start request in step ST1. To specify an authentication target person includes, for example, processing of writing the user ID of an authentication target person in advance in the account management unit 25, and processing of acquiring the first public key of the biometric reference information storage apparatus 10 for the authentication target person by the biometric authentication context verification unit 23. Note that the processing of acquiring the first public key is not limited to this timing, and suffices to be executed till verification processing of the first digital signature in step ST11.

First, upon receiving the registration start request in ST1, the biometric reference information certificate generation apparatus 20 generates challenge information (random value) necessary to generate the biometric authentication context C by the biometric authentication context verification unit 23 (ST2), and notifies the biometric reference information storage apparatus 10 of the challenge information (ST3). The information necessary to generate the biometric authentication context C is not limited to the challenge information, and suffices to be exchanged in steps ST1 to ST3.

Upon receiving the challenge information, the biometric reference information storage apparatus 10 controls the biometric information sampling unit 13 to sample biometric information of the authentication target

person (ST4).

The biometric reference information generation unit 14 generates biometric reference information from the biometric information sampled in step ST4 (ST5), and temporarily saves the biometric reference information in the validation information temporary save unit 17 (ST6).

The biometric authentication context generation unit 15 generates the hash value of the biometric reference information generated in step ST5 (ST7), and temporarily saves the hash value in the validation information temporary save unit 17. Note that the hash value can be generated from biometric reference information in the validation information temporary save unit 17 and thus may not be saved.

The biometric authentication context generation unit 15 generates the first digital signature based on the first private key of the apparatus 10 for the challenge information notified in step ST3 and the hash value of the biometric reference information generated in step ST7. After that, the biometric authentication context generation unit 15 generates the biometric authentication context C including the challenge information, the hash value of the biometric reference information, and the first digital signature (ST8), and temporarily saves the biometric authentication context C in the validation information temporary save unit 17 (ST9).

Then, the biometric reference information storage

apparatus 10 transmits, to the biometric reference
information certificate generation apparatus 20, the hash
value of the biometric reference information and the
biometric authentication context C that have been generated
5 in steps ST7 and ST8 (ST10).

Upon receiving the hash value of the biometric
reference information and the biometric authentication
context C, the biometric reference information certificate
generation apparatus 20 verifies the validity of the
10 biometric authentication context C based on a public key
corresponding to the private key of the biometric reference
information storage apparatus 10 and the challenge
information notified in step ST2 (ST11). More
specifically, the biometric authentication context
15 verification unit 23 verifies, based on the challenge
information transmitted in step ST2, challenge information
extracted from the biometric authentication context C. In
addition, the biometric authentication context verification
unit 23 verifies the first digital signature in the
20 received biometric authentication context based on the
first public key corresponding to the first private key of
the biometric reference information storage apparatus 10.

If the result of verification in step ST11 represents
validity, the certificate generation unit 24 generates,
25 based on the second private key of the apparatus, the
second digital signature for the hash value of the
biometric reference information and the biometric

authentication context C that have been received. The certificate generation unit 24 generates the biometric reference information certificate RC including the hash value of the biometric reference information, the biometric authentication context C, and the second digital signature (ST12). If the result of verification in step ST11 does not represent validity, the overall processing ends. At this time, the biometric reference information certificate generation apparatus 20 may notify the biometric reference information storage apparatus 10 that the processing has ended owing to a verification failure.

After step ST12, the account management unit 25 stores the generated biometric reference information certificate RC as the value of the attribute of the account of the authentication target person (ST13). Since the type of attribute to be used depends on the account structure of the authentication target person, a concrete attribute is not particularly requested in this embodiment, but is desirably an attribute capable of expressing the biometric reference information certificate RC. The processing may be modified to omit step ST13, and after confirming a success response in step ST21, store the biometric reference information certificate RC as the value of the attribute of the account of the authentication target person. In this modification, the account management unit 25 or the certificate generation unit 24 may store the biometric reference information certificate RC in an

arbitrary temporary save area.

In any case, the input/output unit 21 of the biometric reference information certificate generation apparatus 20 transmits the biometric reference information certificate
5 RC generated in step ST12 to the biometric reference information storage apparatus 10 (ST14).

As shown in FIG. 10, the biometric reference information storage apparatus 10 receives the biometric reference information certificate RC (ST15), and the
10 validation determination unit 16 extracts the hash value of the biometric reference information and the biometric authentication context C from the biometric reference information certificate RC (ST16).

The validation determination unit 16 compares and
15 verifies the hash value of the extracted biometric reference information and the hash value of biometric reference information in the validation information temporary save unit 17 (ST17). If these hash values do not match each other as a result of the comparison and
20 verification in step ST17, the overall processing ends. At this time, the biometric reference information storage apparatus 10 may notify the biometric reference information certificate generation apparatus 20 that the processing has ended owing to a verification failure. When only biometric
25 reference information is temporarily saved in the validation information temporary save unit 17, the validation determination unit 16 suffices to generate the

hash value of the biometric reference information in this step.

If these hash values match each other as a result of the comparison and verification in step ST17, the validation determination unit 16 compares and verifies the biometric authentication context C extracted in step ST16 and the biometric authentication context C in the validation information temporary save unit 17 (ST18). If the biometric authentication contexts C do not match each other as a result of the comparison and verification in step ST18, the overall processing ends. At this time, the biometric reference information storage apparatus 10 may notify the biometric reference information certificate generation apparatus 20 that the processing has ended owing to a verification failure. Steps ST17 and ST18 may be executed in a reverse order.

If the biometric authentication contexts C match each other as a result of the comparison and verification in step ST18, the validation determination unit 16 stores, in the information storage unit 18, the biometric reference information in the validation information temporary save unit 17 and the biometric reference information certificate RC received in step ST15 (ST19). The validation determination unit 16 validates the biometric reference information certificate RC by saving the biometric reference information certificate RC in the validation information temporary save unit 17 (ST20).

Thereafter, the biometric reference information storage apparatus 10 notifies the biometric reference information certificate generation apparatus 20 of a success response representing the success of all processes (ST21). Note that the success response may include, e.g., at least one of pieces of information (e.g., user ID and biometric reference information certificate RC) associated with the validation flag in the account management unit 25.

Upon receiving the success response, the biometric reference information certificate generation apparatus 20 controls the account management unit 25 to update, e.g., the validation flag associated with information in the success response to be true.

As described above, according to the first embodiment, the biometric reference information certificate generation apparatus 20 transmits challenge information to the biometric reference information storage apparatus 10. The biometric reference information storage apparatus 10 transmits, to the biometric reference information certificate generation apparatus 20, the hash value of biometric reference information, and the biometric authentication context C including the challenge information, the hash value of the biometric reference information, and the first digital signature. The biometric reference information certificate generation apparatus 20 verifies the challenge information, then verifies the first digital signature by using the first

public key, and transmits, to the biometric reference
information storage apparatus 10, the biometric reference
information certificate RC including the biometric
authentication context, the hash value of the biometric
5 reference information, and the second digital signature.
The biometric reference information storage apparatus 10
verifies the hash value of the biometric reference
information and the biometric authentication context C, and
stores the biometric reference information and the
10 biometric reference information certificate RC.

In this manner, challenge & response authentication,
authentication based on a public key, authentication based
on a hash value, and the like are used without using shared
secret information. With this arrangement, biometric
15 reference information can be guaranteed and stored through
the network Nw without sharing secret information in
advance between the device (biometric reference information
storage apparatus 10) and the biometric authentication
system.

20 For example, biometric reference information can be
guaranteed online for a biometric authentication system
selected by an authentication target person using a device
selected by the authentication target person, and the
biometric reference information can be stored in the
25 device. Therefore, improvement of the user friendliness
when registering or updating biometric reference
information in the biometric authentication system can be

expected.

Since secret information need not be shared in advance between the device and the biometric authentication system, the user need not possess a corresponding device for each
5 biometric authentication system, and the burden of possessing a device can be reduced.

<Second Embodiment>

FIG. 11 is a schematic view showing an example of the arrangement of a biometric reference information
10 registration system according to the second embodiment. FIGS. 12 and 13 are schematic views showing an example of the arrangements of respective apparatuses in the system. The same reference numerals as those in the above-described drawings denote the same parts, a detailed description
15 thereof will not be repeated, and a difference will be mainly described here.

The the first embodiment has explained an arrangement in which the single biometric reference information storage apparatus 10 generates biometric reference information.
20 However, the present invention is not limited to this, and the biometric reference information storage apparatus 10 may be divided into an apparatus including either the biometric information sampling unit 13 or the biometric reference information generation unit 14, or an apparatus
25 including both the biometric information sampling unit 13 and the biometric reference information generation unit 14. FIGS. 11, 12, and 13 show an example of an arrangement in

which a biometric information sampling apparatus 10a
including a biometric information sampling unit 13, and a
biometric reference information storage apparatus 10
including a biometric reference information generation unit
5 14 are separated.

In this case, biometric authentication context
generation units 15a and 15 are arranged in the respective
separated apparatuses 10a and 10, and generate biometric
authentication contexts C1 and C2, respectively, similarly
10 to the operation described in the first embodiment. It is
only necessary to manage the generated biometric
authentication contexts C1 and C2 altogether in a
validation information temporary save unit 17 of the
biometric reference information storage apparatus 10.

Note that the first biometric authentication context
C1 is generated by the biometric information sampling
apparatus 10a, and includes challenge information, the hash
value of biometric information, and the 0th digital
signature, as shown in FIG. 14. The 0th digital signature
15 is generated by signature processing on challenge
information and the hash value of biometric information
based on the 0th private key of the biometric information
sampling apparatus 10a.

The second biometric authentication context C2 is
25 generated by the biometric reference information storage
apparatus 10, and includes challenge information, the hash
value of biometric information, the hash value of biometric

reference information, and the first digital signature, as shown in FIG. 15. The hash value of biometric information is the hash value of biometric information given as an input to the biometric reference information storage apparatus 10. The first digital signature is generated by signature processing on challenge information and the hash value of biometric reference information based on the first private key of the biometric reference information storage apparatus 10.

A biometric reference information certificate RC is generated by a biometric reference information certificate generation apparatus 20, and includes the first biometric authentication context C1, the second biometric authentication context C2, the hash value of biometric reference information, and the second digital signature, as shown in FIG. 16. The second digital signature is generated by signature processing on the first biometric authentication context C1, the second biometric authentication context C2, and the hash value of biometric reference information based on the second private key of the biometric reference information certificate generation apparatus 20.

The two biometric authentication contexts C1 and C2 are stored in even the biometric authentication context storage area in the validation information temporary save unit 17 shown in FIGS. 4 and 5.

Next, the operation of the biometric reference

information registration system having the above-described arrangement will be explained with reference to the sequence chart of FIG. 17.

5 Assume that steps ST1 to ST3 are executed in the above-described way.

If the biometric reference information storage apparatus 10 receives challenge information from the biometric reference information certificate generation apparatus 20, it transmits the challenge information and a
10 biometric information sampling request to the biometric information sampling apparatus 10a (ST4-1).

In the biometric information sampling apparatus 10a, an input/output unit 11a receives the challenge information and the biometric information sampling request. Then, a
15 control unit 12a sends the challenge information to the biometric authentication context generation unit 15a, and activates the biometric information sampling unit 13. The biometric information sampling unit 13 samples biometric information of an authentication target person (ST4-2).
20 The biometric information is sent to the biometric authentication context generation unit 15a via the control unit 12a. Note that the control unit 12a may be omitted, and the respective units 11a, 13, and 15a may directly transfer information.

25 The biometric authentication context generation unit 15a of the biometric information sampling apparatus 10a generates the hash value of the biometric reference

information generated in step ST4-2.

The biometric authentication context generation unit 15a generates the 0th digital signature based on the 0th private key of the apparatus 10a for the challenge information received in step ST4-1 and the generated hash value of the biometric reference information. Also, the biometric authentication context generation unit 15a generates the first biometric authentication context C1 including the challenge information, the hash value of the biometric reference information, and the 0th digital signature (ST4-1).

After that, the biometric authentication context generation unit 15a transmits the first biometric authentication context C1 and the biometric information sampled in step ST4-2 to the biometric reference information storage apparatus 10 (ST4-4).

The biometric reference information generation unit 14 generates biometric reference information from the biometric information sampled in step ST4-4 (ST5), and temporarily saves the biometric reference information in the validation information temporary save unit 17 (ST6). Also, the biometric reference information generation unit 14 temporarily saves the first biometric authentication context C1 sampled in step ST4-4 in the validation information temporary save unit 17.

Then, the apparatuses 10 and 20 execute the same processes as those in step ST7 and subsequent steps, except

that the two biometric authentication contexts C1 and C2 are used.

For example, in steps ST8 and ST9, the biometric authentication context generation unit 15 generates the second biometric authentication context C2 including challenge information, the hash value of biometric reference information, and the first digital signature, and temporarily saves the second biometric authentication context C2 in the validation information temporary save unit 17.

In steps ST8 and ST9, the biometric reference information storage apparatus 10 transmits the hash value of the biometric reference information and the first and second biometric authentication contexts C1 and C2 to the biometric reference information certificate generation apparatus 20.

In step ST11, a biometric authentication context verification unit 23 verifies the validity of the respective biometric authentication contexts C1 and C2 based on the 0th public key corresponding to the 0th private key of the biometric information sampling apparatus 10a, the first public key corresponding to the first private key of the biometric reference information storage apparatus 10, and the challenge information notified in step ST2.

More specifically, the biometric authentication context verification unit 23 verifies pieces of challenge

information extracted from the respective biometric authentication contexts C1 and C2 based on the challenge information transmitted in step ST2. The biometric authentication context verification unit 23 verifies the
5 0th digital signature in the received first biometric authentication context C1 based on the 0th public key corresponding to the 0th private key of the biometric information sampling apparatus 10a. Similarly, the biometric authentication context verification unit 23
10 verifies the first digital signature in the received second biometric authentication context C2 based on the first public key corresponding to the first private key of the biometric reference information storage apparatus 10.

In step ST12, when the verification result in step
15 ST11 represents validity, the certificate generation unit 24 generates the second digital signature based on the second private key of the apparatus for the hash value of the biometric reference information and the respective biometric authentication contexts C1 and C2 that have been
20 received. The certificate generation unit 24 generates the biometric reference information certificate RC including the hash value of the biometric reference information, the respective biometric authentication contexts C1 and C2, and the second digital signature.

25 In step ST16, the validation determination unit 16 extracts the hash value of the biometric reference information and the respective biometric authentication

contexts C1 and C2 from the biometric reference information certificate RC.

In step ST18, the validation determination unit 16 compares and verifies the first biometric authentication context C1 extracted in step ST16, and the first biometric authentication context C1 in the validation information temporary save unit 17. Similarly, the validation determination unit 16 compares and verifies the second biometric authentication context C2 extracted in step ST16, and the second biometric authentication context C2 in the validation information temporary save unit 17.

Thereafter, processes in step ST19 and subsequent steps are executed in the above-described way.

As described above, according to the second embodiment, even when the biometric information sampling unit 13 is separated from the biometric reference information storage apparatus 10 in the first embodiment, the same effects as those in the first embodiment can be obtained.

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 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.

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
5 software, and MW (middleware) such as network software may execute a part of the processes to realize the embodiment.

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
10 transmitted through a LAN, the Internet, or the like is downloaded and stored or temporarily stored.

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
15 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
20 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
25 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 embodiments have been presented by way of example only, and are not intended to limit the scope of the inventions.

5 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 embodiments described herein may be made without departing from the spirit of the inventions. The accompanying claims
10 and their equivalents are intended to cover such forms or modifications as would fall within the scope and spirit of the inventions.

C L A I M S

1. A biometric reference information registration
5 system characterized by comprising a biometric reference
information storage apparatus (10) and biometric reference
information certificate generation apparatus (20)
configured to communicate with each other through a
network, the biometric reference information registration
10 system registering biometric reference information of an
authentication target person in the biometric reference
information storage apparatus,

the biometric reference information storage apparatus
including:

15 first private key storage means (15) for storing a
first private key of the apparatus;

validation information save means (17) which saves
biometric reference information saved temporarily, a hash
value of the biometric reference information, a biometric
20 authentication context, and a biometric reference
information certificate being valid in association with
each other, an invalid biometric reference information
certificate not being saved;

challenge information reception means (11) for
25 receiving challenge information from the biometric
reference information certificate generation apparatus;

biometric reference information generation means (14)
for generating biometric reference information based on
biometric information sampled from the authentication
30 target person;

means (14) for writing the generated biometric
reference information in the validation information save
means;

hash value generation means (15) for generating a hash value of the biometric reference information;

means (15) for writing the generated hash value in the validation information save means;

5 first signature generation means (15) for generating a first digital signature based on the first private key for the challenge information and the hash value of the biometric reference information;

biometric authentication context generation means (15)
10 for generating a biometric authentication context (C) including the challenge information, the hash value of the biometric reference information, and the first digital signature;

means (15) for writing the generated biometric
15 authentication context in the validation information save means;

biometric authentication context transmission means
(11) for transmitting the hash value of the biometric
reference information and the biometric authentication
20 context to the biometric reference information certificate generation apparatus;

certificate reception means (11) for receiving, from the biometric reference information certificate generation apparatus, a biometric reference information certificate
25 including the hash value of the biometric reference information, the biometric authentication context, and a second digital signature for the hash value of the biometric reference information and the biometric authentication context;

30 first extraction means (16) for extracting the hash value of the biometric reference information and the biometric authentication context from the biometric reference information certificate;

hash value verification means (16) for verifying the extracted hash value based on the hash value in the validation information save means;

biometric authentication context verification means
5 (16) for verifying the extracted biometric authentication context based on the biometric authentication context in the validation information save means;

storage means (18) for storing the biometric reference information and the biometric reference information
10 certificate; and

write means (16) for, when respective results of the verifications by the hash value verification means and the biometric authentication context verification means represent validity, writing the biometric reference
15 information and the biometric reference information certificate in the storage means,

means (16) for, when respective results of the verifications by the hash value verification means and the biometric authentication context verification means
20 represent validity, validating the biometric reference information certificate by writing the biometric reference information certificate in the validation information save means; and

means for transmitting a success response to the
25 biometric reference information certificate generation apparatus after the validating the biometric reference information certificate, the success response including a user ID of the authentication target person, or the biometric reference information certificate,

30 the biometric reference information certificate generation apparatus including:

account storage means (25) for storing a user ID of the authentication target person, the biometric reference

information certificate, and a validation flag in association with each other;

second private key storage means (24) for storing a second private key of the apparatus;

5 challenge information transmission means (23) for generating the challenge information and transmitting the challenge information to the biometric reference information storage apparatus;

biometric authentication context reception means (21)
10 for receiving the hash value of the biometric reference information and the biometric authentication context from the biometric reference information storage apparatus;

second extraction means (23) for extracting challenge information from the received biometric authentication
15 context;

challenge information verification means (23) for verifying the extracted challenge information based on the transmitted challenge information;

signature verification means (23) for verifying a
20 first digital signature in the received biometric authentication context based on a first public key corresponding to the first private key;

second signature generation means (24) for, when
25 respective results of the verifications by the challenge information verification means and the signature verification means represent validity, generating the second digital signature based on the second private key for the hash value of the biometric reference information and the biometric authentication context that have been
30 received;

certificate generation means (24) for generating the biometric reference information certificate including the hash value of the biometric reference information, the

biometric authentication context, and the second digital signature;

certificate write means (25) for writing the generated biometric reference information certificate in the account
5 storage means in association with the user ID of the authentication target person;

certificate transmission means (21) for transmitting the generated biometric reference information certificate to the biometric reference information storage apparatus;
10 and

means for, upon receiving the success response from the biometric reference information storage apparatus, updating the validation flag in the account storage means to a true value of the true value or a false value based on
15 the user ID or the biometric reference information certificate in the success response.

2. A biometric reference information storage apparatus (10) configured to communicate with a biometric
20 reference information certificate generation apparatus (20) through a network, characterized by comprising:

first private key storage means (15) for storing a first private key of the apparatus;

validation information save means (17) which saves
25 biometric reference information saved temporarily, a hash value of the biometric reference information, a biometric authentication context, and a biometric reference information certificate being valid in association with each other, an invalid biometric reference information
30 certificate not being saved;

challenge information reception means (11) for receiving challenge information from the biometric reference information certificate generation apparatus;

biometric reference information generation means (14)
5 for generating biometric reference information based on biometric information sampled from the authentication target person;

means (14) for writing the generated biometric reference information in the validation information save
10 means;

hash value generation means (15) for generating a hash value of the biometric reference information;

means (15) for writing the generated hash value in the validation information save means;

15 first signature generation means (15) for generating a first digital signature based on the first private key for the challenge information and the hash value of the biometric reference information;

biometric authentication context generation means (15)
20 for generating a biometric authentication context (C) including the challenge information, the hash value of the biometric reference information, and the first digital signature;

means (15) for writing the generated biometric
25 authentication context in the validation information save means;

biometric authentication context transmission means
(11) for transmitting the hash value of the biometric reference information and the biometric authentication
30 context to the biometric reference information certificate generation apparatus;

certificate reception means (11) for receiving, from the biometric reference information certificate generation

apparatus, a biometric reference information certificate including the hash value of the biometric reference information, the biometric authentication context, and a second digital signature for the hash value of the
5 biometric reference information and the biometric authentication context;

first extraction means (16) for extracting the hash value of the biometric reference information and the biometric authentication context from the biometric
10 reference information certificate;

hash value verification means (16) for verifying the extracted hash value based on the hash value in the validation information save means;

biometric authentication context verification means
15 (16) for verifying the extracted biometric authentication context based on the biometric authentication context in the validation information save means;

storage means (18) for storing the biometric reference information and the biometric reference information
20 certificate;

write means (16) for, when respective results of the verifications by the hash value verification means and the biometric authentication context verification means represent validity, writing the biometric reference
25 information and the biometric reference information certificate in the storage means,

means (16) for, when respective results of the verifications by the hash value verification means and the biometric authentication context verification means
30 represent validity, validating the biometric reference information certificate by writing the biometric reference information certificate in the validation information save means; and

means for transmitting a success response to the biometric reference information certificate generation apparatus after the validating the biometric reference information certificate, the success response including a
5 user ID of the authentication target person, or the biometric reference information certificate,

wherein the biometric reference information certificate generation apparatus has account storage means for storing a user ID of the authentication target person,
10 the biometric reference information certificate, and a validation flag in association with each other, transmits the challenge information to the biometric reference information storage apparatus, receives the hash value of the biometric reference information and the biometric
15 authentication context from the biometric reference information storage apparatus, extracts challenge information from the biometric authentication context, verifies the extracted challenge information based on the transmitted challenge information, verifies a first digital
20 signature in the biometric authentication context based on a first public key corresponding to the first private key, when respective results of the verifications represent validity, generates the second digital signature based on a second private key of the apparatus, generates the
25 biometric reference information certificate including the hash value of the biometric reference information, the biometric authentication context, and the second digital signature, transmits the biometric reference information certificate to the biometric reference information storage
30 apparatus, upon receiving the success response from the biometric reference information storage apparatus, updates the validation flag in the account storage means to a true value of the true value or a false value based

on the user ID or the biometric reference information certificate in the success response.

3. A biometric reference information certificate
5 generation apparatus (20) configured to communicate with a
biometric reference information storage apparatus (10)
through a network, characterized by comprising:

account storage means (25) for storing a user ID of an
authentication target person, a biometric reference
10 information certificate, and a validation flag in
association with each other;

second private key storage means (24) for storing a
second private key of the apparatus;

challenge information transmission means (23) for
15 generating challenge information and transmitting the
challenge information to the biometric reference
information storage apparatus;

biometric authentication context reception means (21)
for, when the biometric reference information storage
20 apparatus has validation information save means (17) which
saves biometric reference information saved temporarily, a
hash value of the biometric reference information, a
biometric authentication context, and a biometric reference
information certificate being valid in association with
25 each other, an invalid biometric reference information
certificate not being saved, generates biometric reference
information based on biometric information sampled from the
authentication target person, writes the generated
biometric reference information in the validation
30 information save means, generates a hash value of the
biometric reference information, writes the generated hash
value in the validation information save means, generates a
first digital signature based on a first private key of the

apparatus for the challenge information and the hash value of the biometric reference information, generates a biometric authentication context including the challenge information, the hash value of the biometric reference information, and the first digital signature, writes the
5 generated biometric authentication context in the validation information save means, and transmits the hash value of the biometric reference information and the biometric authentication context to the biometric reference
10 information certificate generation apparatus, receiving the hash value of the biometric reference information and the biometric authentication context from the biometric reference information storage apparatus;

second extraction means (23) for extracting challenge
15 information from the received biometric authentication context;

challenge information verification means (23) for verifying the extracted challenge information based on the transmitted challenge information;

20 signature verification means (23) for verifying a first digital signature in the received biometric authentication context based on a first public key corresponding to the first private key;

second signature generation means (24) for, when
25 respective results of the verifications by the challenge information verification means and the signature verification means represent validity, generating a second digital signature based on the second private key for the hash value of the biometric reference information and the
30 biometric authentication context that have been received;

certificate generation means (24) for generating the biometric reference information certificate including the hash value of the biometric reference information, the

biometric authentication context, and the second digital signature;

certificate write means (25) for writing the generated biometric reference information certificate in the account storage means in association with the user ID of the authentication target person;

certificate transmission means (21) for transmitting the generated biometric reference information certificate to the biometric reference information storage apparatus, and

means for, upon receiving the success response from the biometric reference information storage apparatus, updating the validation flag in the account storage means to a true value of the true value or a false value based on the user ID or the biometric reference information certificate in the success response,

wherein the biometric reference information storage apparatus receives the biometric reference information certificate from the biometric reference information certificate generation apparatus, extracts a hash value of the biometric reference information and the biometric authentication context from the biometric reference information certificate, verifies the extracted hash value based on the hash value in the validation information save means, verifies the extracted biometric authentication context based on the biometric authentication context in the validation information save means, when respective results of the verifications represent validity, writes the biometric reference information and the biometric reference information certificate in storage means, validates the biometric reference information certificate by writing the biometric reference information certificate in the validation information save means, and transmits a success

response to the biometric reference information certificate generation apparatus, the success response including a user ID of the authentication target person, or the biometric reference information certificate.

5

4. A program used for a biometric reference information storage apparatus (10) configured to communicate with a biometric reference information certificate generation apparatus (20) through a network, the biometric reference information storage apparatus (10) including first private key storage means and storage means, the validation information save means which saves biometric reference information saved temporarily, a hash value of the biometric reference information, a biometric authentication context, and a biometric reference information certificate being valid in association with each other, an invalid biometric reference information certificate not being saved, the program characterized by causing the biometric reference information storage apparatus (10) to function as:

means for writing a first private key of the apparatus in the first private key storage means (15);

means (11) for receiving challenge information from the biometric reference information certificate generation apparatus;

means (14) for generating biometric reference information based on biometric information sampled from an authentication target person;

means (14) for writing the generated biometric reference information in the validation information save means;

means (15) for generating a hash value of the biometric reference information;

means (15) for writing the generated hash value in the validation information save means;

means (15) for generating a first digital signature based on the first private key for the challenge
5 information and the hash value of the biometric reference information;

means (15) for generating a biometric authentication context (C) including the challenge information, the hash value of the biometric reference information, and the first
10 digital signature;

means (15) for writing the generated biometric authentication context in the validation information save means;

means (11) for transmitting the hash value of the
15 biometric reference information and the biometric authentication context to the biometric reference information certificate generation apparatus;

means (11) for receiving, from the biometric reference information certificate generation apparatus, a biometric
20 reference information certificate including the hash value of the biometric reference information, the biometric authentication context, and a second digital signature for the hash value of the biometric reference information and the biometric authentication context;

25 means (16) for extracting the hash value of the biometric reference information and the biometric authentication context from the biometric reference information certificate;

hash value verification means (16) for verifying the
30 extracted hash value based on the hash value in the validation information save means;

biometric authentication context verification means (16) for verifying the extracted biometric authentication

- 61 -

context based on the generated biometric authentication context;

means (16) for, when respective results of the verifications represent validity, writing the biometric
5 reference information and the biometric reference information certificate in the storage means (18),

means (16) for, when respective results of the verifications by the hash value verification means and the biometric authentication context verification means
10 represent validity, validating the biometric reference information certificate by writing the biometric reference information certificate in the validation information save means; and

means for transmitting a success response to the
15 biometric reference information certificate generation apparatus after the validating the biometric reference information certificate, the success response including a user ID of the authentication target person, or the biometric reference information certificate,

20 wherein the biometric reference information certificate generation apparatus has account storage means for storing a user ID of the authentication target person, the biometric reference information certificate, and a validation flag in association with each other, transmits
25 the challenge information to the biometric reference information storage apparatus, receives the hash value of the biometric reference information and the biometric authentication context from the biometric reference information storage apparatus, extracts challenge
30 information from the biometric authentication context, verifies the extracted challenge information based on the transmitted challenge information, verifies a first digital signature in the biometric authentication context based on

a first public key corresponding to the first private key, when the respective results of the verifications represent validity, generates the second digital signature based on a second private key of the apparatus, generates the
5 biometric reference information certificate including the hash value of the biometric reference information, the biometric authentication context, and the second digital signature, transmits the biometric reference information certificate to the biometric reference information storage
10 apparatus, and upon receiving the success response from the biometric reference information storage apparatus, updates the validation flag in the account storage means to a true value of the true value or a false value based on the user ID or the biometric reference information
15 certificate in the success response.

5. A program used for a biometric reference information certificate generation apparatus (20) configured to communicate with a biometric reference
20 information storage apparatus (10) through a network, the biometric reference information certificate generation apparatus (20) including account storage means and second private key storage means, the account storage means which stores a user ID of the authentication target person, a
25 biometric reference information certificate, and a validation flag in association with each other, the program characterized by causing the biometric reference information certificate generation apparatus to function as:

30 means for writing a user ID of an authentication target person in the account storage means (25);

means for writing a second private key of the apparatus in the second private key storage means (24);

means (23) for generating challenge information and transmitting the challenge information to the biometric reference information storage apparatus;

means (21) for, when the biometric reference
5 information storage apparatus has validation information save means (17) which saves biometric reference information saved temporarily, a hash value of the biometric reference information, a biometric authentication context, and a biometric reference information certificate being valid in
10 association with each other, an invalid biometric reference information certificate not being saved, generates biometric reference information based on biometric information sampled from the authentication target person, writes the generated biometric reference information in the
15 validation information save means, generates a hash value of the biometric reference information, writes the generated hash value in the validation information save means, generates a first digital signature based on a first private key of the apparatus for the challenge information
20 and the hash value of the biometric reference information, generates a biometric authentication context including the challenge information, the hash value of the biometric reference information, and the first digital signature, writes the generated biometric authentication context in
25 the validation information save means, and transmits the hash value of the biometric reference information and the biometric authentication context to the biometric reference information certificate generation apparatus, receiving the hash value of the biometric reference information and the
30 biometric authentication context from the biometric reference information storage apparatus;

means (23) for extracting challenge information from the received biometric authentication context;

challenge information verification means (23) for verifying the extracted challenge information based on the transmitted challenge information;

signature verification means (23) for verifying a
5 first digital signature in the received biometric authentication context based on a first public key corresponding to the first private key;

means (24) for, when respective results of the verifications by the challenge information verification
10 means and the signature verification means represent validity, generating a second digital signature based on the second private key for the hash value of the biometric reference information and the biometric authentication context that have been received;

15 means (24) for generating the biometric reference information certificate including the hash value of the biometric reference information, the biometric authentication context, and the second digital signature;

means (25) for writing the generated biometric
20 reference information certificate in the account storage means in association with the user ID of the authentication target person;

means (21) for transmitting the generated biometric reference information certificate to the biometric
25 reference information storage apparatus, and

means for, upon receiving the success response from the biometric reference information storage apparatus, updating the validation flag in the account storage means to a true value of the true value or a false value based on
30 the user ID or the biometric reference information certificate in the success response,

wherein the biometric reference information storage apparatus receives the biometric reference information

certificate from the biometric reference information
certificate generation apparatus, extracts a hash value of
the biometric reference information and the biometric
authentication context from the biometric reference
5 information certificate, verifies the extracted hash value
based on the hash value in the validation information save
means, verifies the extracted biometric authentication
context based on the biometric authentication context in
the validation information save means, when respective
10 results of the verifications represent validity, writes the
biometric reference information and the biometric reference
information certificate in storage means, validates the
biometric reference information certificate by writing the
biometric reference information certificate in the
15 validation information save means, and transmits a success
response to the biometric reference information certificate
generation apparatus, the success response including a user
ID of the authentication target person, or the biometric
reference information certificate.