

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 authentication context in the validation information save means;
15

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

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 biometric reference information and the biometric authentication context;
25

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 generated-hash value in
the validation information save means;

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

storage means (18) for storing the biometric reference
information and the biometric reference information
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
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
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
user ID of the authentication target person, or the
biometric reference information certificate,

the biometric reference information certificate
generation apparatus including:

account storage means (25) for storing a user ID of
the authentication target person,—and 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 storage means in association with the user ID of the authentication target person;—and

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.

2. A biometric reference information storage apparatus (10) configured to communicate with a biometric 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 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;

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 authentication context in the validation information save
25 means;

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

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

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

storage means (18) for storing the biometric reference information and the biometric reference information 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 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 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 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, 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 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 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 biometric reference information certificate including the hash value of the biometric reference information, the biometric authentication context, and the second digital signature, ~~and~~ transmits the biometric reference information certificate to the biometric reference information storage 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.

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

10 account storage means (25) for storing a user ID of an authentication target person, ~~—and~~ a 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;

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

 biometric authentication context reception means (21)
20 for, when the biometric reference 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
25 information certificate being valid in 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
30 biometric reference information in the 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 and the hash value of the biometric reference information, generates a biometric authentication context including the challenge
5 information, the hash value of the biometric reference information, and the first digital signature, writes the generated biometric authentication context in the validation information save means, and transmits the hash value of the biometric reference information and the
10 biometric authentication context to the biometric reference 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;

15 second extraction 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
20 transmitted challenge information;

 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;

25 second signature generation means (24) for, when respective results of the verifications by the challenge information verification means and the signature
verification means represent validity, generating athe
second digital signature based on the second private key
30 for the hash value of the biometric reference information and the 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
5 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;—and

10 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
15 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,

20 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
25 authentication context from the biometric reference information certificate, verifies the extracted hash value based on the generated—hash value in the validation
information save means, verifies the extracted biometric authentication context based on the generated—biometric
30 authentication context in the validation information save
means, and—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
5 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.

10 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)
15 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
20 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:

25 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;

30 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;

5 | 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;

10 | 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;

15 | means (15) 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 authentication context in the validation information save means;

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

25 | 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 biometric reference information and the biometric authentication context;

30 | 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 generated 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 generated biometric authentication context;—and

means (16) for, when respective results of the verifications represent validity, writing the biometric
10 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
15 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
20 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,

25 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
30 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 information from the biometric authentication context, verifies the extracted challenge information based on the transmitted challenge information, verifies a first digital
5 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
10 biometric reference information certificate including the hash value of the biometric reference information, the biometric authentication context, and the second digital signature, and—transmits the biometric reference information certificate to the biometric reference
15 information storage 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
20 reference information certificate in the success response.

5. A program used for a biometric reference information certificate generation apparatus (20)
25 configured to communicate with a biometric reference 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
30 stores a user ID of the authentication target person, a 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:

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

5 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;

10 means (21) for, when the biometric reference 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
15 biometric reference information certificate being valid in 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,
20 writes the generated biometric reference information in the 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
25 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,
30 writes the 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

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;

5 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;

10 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;

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

 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;

25 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;~~and~~

 means (21) for transmitting the generated biometric
30 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,

5 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 generated—hash value in the validation information save means, verifies the extracted biometric authentication context based on the generated—biometric authentication context in the validation information save means, and—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.

10

15

20

25