

1. A service providing system characterized by comprising: a plurality of unit devices which independently execute authentication constituting processes constituting authentication processing that uses biometric authentication; a unit integrating device which has each of the unit devices provided therein or externally connected thereto to communicate with each of the unit devices; a user terminal which has the unit integrating device provided therein or externally connected thereto to communicate with the unit integrating device; a verifying device which verifies the execution contents of each of the authentication constituting processes in accordance with an authenticator; and a service providing device which communicates with the user terminal and the verifying device,

each of the unit devices comprising equipment certificate storage means for storing an equipment certificate issued to each of the unit devices by an equipment certificate issuer in accordance with a public key encryption method, the equipment certificate including an equipment certificate body and a digital signature generated for the equipment certificate body by a secret key to the equipment certificate issuer, the equipment certificate body including identification information for a

public key of or for secret information to generate a message authentication code of the unit device to which the authentication constituting process belongs, unit device specifying information to specify the unit device to which
5 the authentication constituting process belongs, and equipment certificate issuer information to specify the equipment certificate issuer,

evaluation report storage means for storing an evaluation report, the evaluation report including the unit
10 device specifying information of the unit device used for the execution of the authentication constituting process, biometric authentication constituting process information to specify a biometric authentication constituting process including a biometric authentication algorithm, and
15 biometric authentication accuracy indicating the accuracy of the biometric authentication by the biometric authentication algorithm,

secret information storage means for storing secret information to generate the authenticator,

20 authentication constituting process executing means for executing the authentication constituting process when each of the unit devices receives, from the unit integrating device, a random challenge value generated by the service providing device, and an authentication

constituting process execution request to request the execution of the authentication constituting process,

authenticator generating means for generating the authenticator by the use of the secret information in accordance with the equipment certificate, the evaluation report, the challenge value, and a hash value of the execution contents,

authentication context generating means for generating an authentication context, the equipment certificate, the evaluation report, the challenge value, the hash value of the execution contents, and the authenticator being described in the authentication context in a specific format,

authentication constituting process result information generating means for generating authentication constituting process result information in which the authentication context and the execution result of the authentication constituting process are described in a specific format, and

result information sending means for sending the authentication constituting process result information to the unit integrating device,

at least one of the unit devices further comprising user identification information certificate storage means for storing a user identification information

certificate issued to a user of the user terminal by a third-party organization in accordance with a public key encryption method, the user identification information certificate including a certificate body and a digital
5 signature generated for the certificate body by a secret key to the third-party organization, the certificate body including user identification information to identify the user, a hash value of biometric referential information for the user, and the third-party organization information to
10 identify the third-party organization,

the authenticator generating means of at least one of the unit devices generating the authenticator by the use of the secret information in accordance with the equipment certificate, the evaluation report, the challenge value,
15 the user identification information certificate, and the hash value of the execution contents,

the authentication context generating means of at least one of the unit devices generating an authentication context, the equipment certificate, the evaluation report,
20 the challenge value, the user identification information certificate, the hash value of the execution contents, and the authenticator being described in the authentication context in a specific format,

the unit integrating device comprising

device information storage means for storing, in association with one another, unit device specifying information for each of the unit devices, a function name indicating a function in an authentication constituting process executed by each of the unit devices, and a processing order indicating the order of processing the functions,

first ~~authentication constituting process execution request~~-sending means for sending the challenge value and the authentication constituting process execution request to the unit device specified by the unit device specifying information in accordance with the processing order and the unit device specifying information in the device information storage means in response to an authentication processing execution request to request the execution of the authentication processing and the challenge value from the user terminal,

second ~~authentication constituting process execution request~~-sending means for sending the challenge value and the authentication constituting process execution request to the unit device subsequent to the sending destination unit device in the processing order in accordance with the processing order and the unit device specifying information in the device information storage means in response to the authentication constituting process result information from

the unit device which is a sending destination of the authentication constituting process execution request,

authentication processing result information

generating means for generating authentication processing

5 result information in accordance with the processing order

and the unit device specifying information in the unit

device constituting information in response to the

authentication constituting process result information from

the unit device which is a sending destination of the

10 authentication constituting process execution request when

the sending destination unit device is the last unit device

in the processing order, the authentication context in the

authentication constituting process result information

received from each of the unit devices and the execution

15 result in the authentication constituting process result

information received from the last unit device in the

processing order being described in the authentication

processing result information in a specific format, the

execution result in the authentication constituting process

20 result information received from the last unit device in

the processing order indicating an authentication

processing result, and

authentication processing result information sending

means for sending the authentication processing result

25 information to the user terminal,

the user terminal comprising

service request sending means for sending, to the service providing device, a service request to request a service to the service providing device,

5 authentication processing execution request sending means for sending, to the unit integrating device, the challenge value and the authentication processing execution request in response to an authentication request which requests the user to perform the biometric authentication,
10 and the challenge value from the service providing device,

transfer means for transferring, to the service providing device, authentication processing result information received from the unit integrating device, and

display means for displaying service information
15 received from the service providing device,

the service providing device comprising

user information storage means for storing, in association with each other, user identification information in the user identification information
20 certificate, and service user identification information which has a value different from that of the user identification information to identify the user,

service providing policy storage means for storing a service providing policy indicating conditions for
25 providing services to the user, the service providing

policy including service identification information to identify the service, unit device specifying information used for the execution of the authentication constituting processes, biometric authentication constituting process

5 information to specify a biometric authentication constituting process including a biometric authentication algorithm, and a reference value indicating a reference for regarding the accuracy of the biometric authentication by the biometric authentication algorithm as proper,

10 authentication request sending means for generating and holding the challenge value and sending the challenge value and the authentication request to the user terminal in response to a service request from the user terminal,

sending means for sending the held challenge value,

15 the authentication processing result information, and the service providing policy to the verifying device in response to authentication processing result information from the user terminal,

read means for searching the user information storage

20 means in accordance with the user identification information and reading service user identification information associated with the user identification information in response to user identification information and a verification result from the verifying device when

25 the verification result is proper, and

service information sending means for sending the service information to the user terminal in accordance with the read service user identification information,

the verifying device comprising

5 public key storage means for storing a public key to the equipment certificate issuer of each of the unit devices and a public key to the third-party organization,

receiving means for receiving, from the service providing device, the challenge value, the authentication
10 processing result information, and the service providing policy,

format verifying means for verifying that the received authentication processing result information fits the specific format,

15 authenticator verifying means for verifying an authenticator in the authentication context described in the received authentication processing result information,

equipment certificate verifying means for verifying the digital signature in the equipment certificate included
20 in the authentication context described in the received authentication processing result information in accordance with the public key to the equipment certificate issuer,

user identification information certificate verifying means for verifying the digital signature in the user
25 identification information certificate included in the

authentication context described in the received authentication processing result information in accordance with the public key to the third-party organization,

evaluation report verifying means for verifying the
5 evaluation report included in the authentication context described in the received authentication processing result information in accordance with the received service providing policy,

challenge value verifying means for verifying the
10 challenge value in the authentication context described in the received authentication processing result information in accordance with the received challenge value,

execution result verifying means for verifying that the execution result described in the received
15 authentication processing result information is proper, and

user identification information sending means for sending, to the service providing device, the user identification information in the user identification information certificate used for the verification by the
20 user identification information certificate verifying means and the verification result that indicates properness when all the verification results by the format verifying means, the authenticator verifying means, the equipment certificate verifying means, the user identification
25 information certificate verifying means, the evaluation

report verifying means, the challenge value verifying means, and the execution result verifying means are proper.

2. A service providing system characterized by comprising: a plurality of unit devices which independently
5 execute authentication constituting processes constituting authentication processing that uses biometric authentication; a unit integrating device which has each of the unit devices provided therein or externally connected thereto to communicate with each of the unit devices; a
10 user terminal which has the unit integrating device provided therein or externally connected thereto to communicate with the unit integrating device; a verifying device which verifies the execution contents of each of the authentication constituting processes in accordance with an
15 authenticator; and a service providing device which communicates with the user terminal and the verifying device,

each of the unit devices comprising

equipment certificate storage means for storing an
20 equipment certificate issued to each of the unit devices by an equipment certificate issuer in accordance with a public key encryption method, the equipment certificate including an equipment certificate body and a digital signature generated for the equipment certificate body by a secret
25 key to the equipment certificate issuer, the equipment

certificate body including identification information for a public key of or for secret information to generate a message authentication code of the unit device to which the authentication constituting process belongs, unit device
5 specifying information to specify the unit device to which the authentication constituting process belongs, and equipment certificate issuer information to specify the equipment certificate issuer,

evaluation report storage means for storing an
10 evaluation report, the evaluation report including the unit device specifying information of the unit device used for the execution of the authentication constituting process, biometric authentication constituting process information to specify a biometric authentication constituting process
15 including a biometric authentication algorithm, and biometric authentication accuracy indicating the accuracy of the biometric authentication by the biometric authentication algorithm,

secret information storage means for storing secret
20 information to generate the authenticator,

authentication constituting process executing means for executing the authentication constituting process when each of the unit devices receives, from the unit
25 | integrating device, a random challenge value generated by the service providing device, and an authentication

constituting process execution request to request the execution of the authentication constituting process,

authenticator generating means for generating the authenticator by the use of the secret information in accordance with the equipment certificate, the evaluation report, the challenge value, and a hash value of the execution contents,

authentication context generating means for generating an authentication context, the equipment certificate, the evaluation report, the challenge value, the hash value of the execution contents, and the authenticator being described in the authentication context in a specific format,

authentication constituting process result information generating means for generating authentication constituting process result information in which the authentication context and the execution result of the authentication constituting process are described in a specific format, and

result information sending means for sending the authentication constituting process result information to the unit integrating device,

at least one of the unit devices further comprising user identification information certificate storage means for storing a user identification information

certificate issued to a user of the user terminal by a
third-party organization in accordance with a public key
encryption method, the user identification information
certificate including a certificate body and a digital
5 signature generated for the certificate body by a secret
key to the third-party organization, the certificate body
including user identification information to identify the
user, a hash value of biometric referential information for
the user, and the third-party organization information to
10 identify the third-party organization,

the authenticator generating means of at least one of
the unit devices generating the authenticator by the use of
the secret information in accordance with the equipment
certificate, the evaluation report, the challenge value,
15 the user identification information certificate, and the
hash value of the execution contents,

the authentication context generating means of at
least one of the unit devices generating an authentication
context, the equipment certificate, the evaluation report,
20 the challenge value, the user identification information
certificate, the hash value of the execution contents, and
the authenticator being described in the authentication
context in a specific format,

the unit integrating device comprising

device information storage means for storing, in association with one another, unit device specifying information for each of the unit devices, a function name indicating a function in an authentication constituting process executed by each of the unit devices, and a processing order indicating the order of processing the functions,

first ~~authentication constituting process execution request~~-sending means for sending the challenge value and the authentication constituting process execution request to the unit device specified by the unit device specifying information in accordance with the processing order and the unit device specifying information in the device information storage means in response to an authentication processing execution request to request the execution of the authentication processing and the challenge value from the user terminal,

second ~~authentication constituting process execution request~~-sending means for sending the challenge value and the authentication constituting process execution request to the unit device subsequent to the sending destination unit device in the processing order in accordance with the processing order and the unit device specifying information in the device information storage means in response to the authentication constituting process result information from

the unit device which is a sending destination of the authentication constituting process execution request,

authentication processing result information

generating means for generating authentication processing

5 result information in accordance with the processing order

and the unit device specifying information in the unit

device constituting information in response to the

authentication constituting process result information from

the unit device which is a sending destination of the

10 authentication constituting process execution request when

the sending destination unit device is the last unit device

in the processing order, the authentication context in the

authentication constituting process result information

received from each of the unit devices and the execution

15 result in the authentication constituting process result

information received from the last unit device in the

processing order being described in the authentication

processing result information in a specific format, the

execution result in the authentication constituting process

20 result information received from the last unit device in

the processing order indicating an authentication

processing result, and

authentication processing result information sending

means for sending the authentication processing result

25 information to the user terminal,

the user terminal comprising

service request sending means for sending, to the service providing device, a service request to request a service to the service providing device,

5 authentication processing execution request sending means for sending, to the unit integrating device, the challenge value and the authentication processing execution request in response to an authentication request which requests the user to perform the biometric authentication,
10 and the challenge value from the service providing device,

transfer means for transferring, to the service providing device, authentication processing result information received from the unit integrating device, and

display means for displaying service information
15 received from the service providing device,

the service providing device comprising

service user identification information storage means for storing, in association with each other, cooperated user identification information which has a value different
20 from that of the user identification information to identify the user, and service user identification information which has a value different from those of the cooperated user identification information and the user identification information to identify the user,

service providing policy storage means for storing a service providing policy indicating conditions for providing services to the user, the service providing policy including service identification information to
5 identify the service, unit device specifying information used for the execution of the authentication constituting processes, biometric authentication constituting process information to specify a biometric authentication constituting process including a biometric authentication
10 algorithm, and a reference value indicating a reference for regarding the accuracy of the biometric authentication by the biometric authentication algorithm as proper,

authentication request sending means for generating and holding the challenge value and sending the challenge
15 value and the authentication request to the user terminal in response to a service request from the user terminal,

sending means for sending the held challenge value, the authentication processing result information, and the service providing policy to the verifying device in
20 response to authentication processing result information from the user terminal,

cooperated read means for searching the service user identification information storage means in accordance with the cooperated user identification information and reading
25 service user identification information associated with the

cooperated user identification information in response to the cooperated user identification information and the verification result from the verifying device when the verification result is proper, and

5 service information sending means for sending the service information to the user terminal in accordance with the read service user identification information,

the verifying device comprising

public key storage means for storing a public key to
10 the equipment certificate issuer of each of the unit devices and a public key to the third-party organization,

receiving means for receiving, from the service providing device, the challenge value, the authentication processing result information, and the service providing
15 policy,

format verifying means for verifying that the received authentication processing result information fits the specific format,

authenticator verifying means for verifying an
20 authenticator in the authentication context described in the received authentication processing result information,

equipment certificate verifying means for verifying the digital signature in the equipment certificate included in the authentication context described in the received

authentication processing result information in accordance with the public key to the equipment certificate issuer,

user identification information certificate verifying means for verifying the digital signature in the user

5 identification information certificate included in the

authentication context described in the received

authentication processing result information in accordance with the public key to the third-party organization,

evaluation report verifying means for verifying the
10 evaluation report included in the authentication context described in the received authentication processing result information in accordance with the received service providing policy,

challenge value verifying means for verifying the
15 challenge value in the authentication context described in the received authentication processing result information in accordance with the received challenge value,

execution result verifying means for verifying that the execution result described in the received
20 authentication processing result information is proper,

cooperated user information storage means for storing, in association with each other, the user identification information in the user identification information certificate, and cooperated user identification information
25 which is the same as the former cooperated user

identification information having a value different from that of the user identification information to identify the user, and

cooperated user identification information sending
5 means for sending, to the service providing device, the cooperated user identification information read from the cooperated user information storage means and the verification result that indicates properness in accordance with the user identification information in the user
10 identification information certificate used for the verification by the user identification information certificate verifying means when all the verification results by the format verifying means, the authenticator verifying means, the equipment certificate verifying means,
15 the user identification information certificate verifying means, the evaluation report verifying means, the challenge value verifying means, and the execution result verifying means are proper.

3. The service providing system according to claim 1
20 or claim 2, characterized in that

the authenticator verifying means verifies the authenticator generated by each of the unit devices in accordance with information identical or corresponding to the secret information in each of the unit devices.

4. The service providing system according to claim 1 or claim 2, characterized in that

the secret information in the secret information storage means is a secret key in a public key encryption method, and

the authenticator generated by the authenticator generating means is a digital signature generated on the basis of the secret key.

5. At least one of a plurality of unit devices used in a service providing system, the service providing system characterized by comprising the unit devices which independently execute authentication constituting processes constituting authentication processing that uses biometric authentication, a unit integrating device which has each of the unit devices provided therein or externally connected thereto to communicate with each of the unit devices, a user terminal which has the unit integrating device provided therein or externally connected thereto to communicate with the unit integrating device, a verifying device which verifies the execution contents of each of the authentication constituting processes in accordance with an authenticator, and a service providing device which communicates with the user terminal and the verifying device, the unit device comprising:

equipment certificate storage means for storing an equipment certificate issued to each of the unit devices by an equipment certificate issuer in accordance with a public key encryption method, the equipment certificate including
5 an equipment certificate body and a digital signature generated for the equipment certificate body by a secret key to the equipment certificate issuer, the equipment certificate body including identification information for a public key of or for secret information to generate a
10 message authentication code of the unit device to which the authentication constituting process belongs, unit device specifying information to specify the unit device to which the authentication constituting process belongs, and equipment certificate issuer information to specify the
15 equipment certificate issuer;

evaluation report storage means for storing an evaluation report, the evaluation report including the unit device specifying information of the unit device used for the execution of the authentication constituting process,
20 biometric authentication constituting process information to specify a biometric authentication constituting process including a biometric authentication algorithm, and biometric authentication accuracy indicating the accuracy of the biometric authentication by the biometric
25 authentication algorithm;

user identification information certificate storage means for storing a user identification information certificate issued to a user of the user terminal by a third-party organization in accordance with a public key encryption method, the user identification information certificate including a certificate body and a digital signature generated for the certificate body by a secret key to the third-party organization, the certificate body including user identification information to identify the user, a hash value of biometric referential information for the user, and the third-party organization information to identify the third-party organization;

secret information storage means for storing secret information to generate the authenticator;

authentication constituting process executing means for executing the authentication constituting process when receiving, from the unit integrating device, a random challenge value generated by the service providing device, and an authentication constituting process execution request to request the execution of the authentication constituting process;

authenticator generating means for generating the authenticator by the use of the secret information in accordance with the equipment certificate, the evaluation report, the challenge value, the user identification

information certificate, and a hash value of the execution contents;

authentication context generating means for generating an authentication context, the equipment certificate, the evaluation report, the challenge value, the user identification information certificate, the hash value of the execution contents, and the authenticator being described in the authentication context in a specific format;

authentication constituting process result information generating means for generating authentication constituting process result information in which the authentication context and the execution result of the authentication constituting process are described in a specific format;

and

result information sending means for sending the authentication constituting process result information to the unit integrating device,

wherein the authentication context and the execution result are extracted as the authentication constituting process result information by the unit integrating device,

the extracted authentication context and execution result are described in authentication processing result information in a specific format by the unit integrating device, and

the authentication processing result information is sent to the service providing device from the unit integrating device via the user terminal, the authentication context and the execution result are

5 extracted by the verifying device after the authentication processing result information to which the challenge value and a service providing policy are added by the service providing device is sent, and the verifying device verifies the execution result, the format of the authentication

10 processing result information, the authenticator in the authentication context, the equipment certificate, the evaluation report, the user identification information certificate, and the challenge value.