

1. A service providing system ~~characterized by~~
comprising: a plurality of unit devices which independently
execute authentication constituting processes constituting
5 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
10 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
15 communicates with the user terminal and the verifying
device, characterized in that

each of the unit devices comprising
first~~equipment~~ certificate storage means for storing
an equipment certificate issued to each of the unit devices
20 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
25 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 the authentication constituting process belongs, and equipment certificate issuer information to specify the equipment certificate issuer,

second~~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, 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 authentication algorithm,

third~~secret-information~~ storage means for storing secret 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 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

5 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
10 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, and

~~authentication constituting process result information~~
15 ~~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

20 ~~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

fourth ~~user identification information certificate~~
25 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

~~fifthdevice~~ 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 sending means for sending the challenge value and ~~an~~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 ~~the~~an authentication processing execution request ~~to request the execution of the authentication processing and the~~ challenge value from the user terminal,

second 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 ~~fifthdevice~~ 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, and
~~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 fifth~~
~~storage means~~~~unit device constituting information in~~
response to the authentication constituting process result
information from the unit device which is a sending
10 destination of the 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
15 devices and the execution 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 information in the
20 authentication constituting process 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,
and

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

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

the service providing device comprising

~~sixth~~ user information storage means for storing, in association with each other, user identification

20 information in the user identification information certificate, and service user identification information which has a value different from that of the user identification information to identify the user,

~~seventh~~ service providing policy storage means for
25 storing a service providing policy indicating conditions

for 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 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 accuracy by the biometric authentication algorithm as proper,

~~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, 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 sixth user information storage 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 the verification result is proper, and

~~service information sending~~ means for sending the service information to the user terminal in accordance with

5 the read service user identification information,

the verifying device comprising

~~eighth 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,

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

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

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

20 ~~third 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

25 equipment certificate issuer,

~~fourth~~user identification information certificate

verifying means for verifying the digital signature in the user identification information certificate included in the authentication context described in the received

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

~~fifth~~evaluation report verifying means for verifying

the evaluation report included in the authentication context described in the received authentication processing

10 result information in accordance with the received service providing policy,

~~sixth~~challenge value verifying means for verifying the

challenge value in the authentication context described in the received authentication processing result information

15 in accordance with the received challenge value,

~~seventh~~execution result verifying means for verifying

that the execution result described in the received authentication processing result information is proper, and

~~user identification information sending means~~ for

20 sending, to the service providing device, the user

identification information in the user identification information certificate used for the verification by the

~~fourth~~user identification information certificate verifying means and the verification result that indicates properness

25 when all the verification results by ~~seventh~~the format

verifying means, from the first~~authenticator~~ verifying means, ~~to the equipment certificate verifying means, the user identification information certificate verifying means, the evaluation report verifying means, the challenge value verifying means, and the seventh~~execution result verifying means are proper.

2. 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, characterized in that

each of the unit devices comprising

first~~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

5 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

10 unit device to which the authentication constituting process belongs, and equipment certificate issuer information to specify the equipment certificate issuer,

secondevaluation-report storage means for storing an evaluation report, the evaluation report including the unit

15 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

20 biometric authentication accuracy ~~indicating the accuracy of the biometric authentication by~~ the biometric authentication algorithm,

thirdsecret-information storage means for storing secret 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
integrating device, a random challenge value generated by
5 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
10 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
15 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, and

~~authentication constituting process result information~~
20 ~~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

5 | ~~fourth~~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
10 | 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
15 | the user, and ~~the third-party organization information to~~
~~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
20 | certificate, the evaluation report, the challenge value,
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
25 | 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,

5 the unit integrating device comprising

~~fifth~~ 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~~,

10

first sending means for sending the challenge value and an 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 the an authentication processing execution request ~~to request the execution of the authentication processing~~ and the

15

20 challenge value from the user terminal,

second sending means for sending the challenge value and the authentication constituting process execution request to the unit device subsequent to the sending

25 destination unit device in the processing order in

accordance with the processing order and the unit device
specifying information in the fifth~~device information~~
storage means in response to the authentication
constituting process result information from the unit
5 device which is a sending destination of the authentication
constituting process execution request, and
~~authentication processing result information~~
~~generating means~~ for generating authentication processing
result information in accordance with the processing order
10 and the unit device specifying information in the fifth
storage means~~unit device constituting information~~ in
response to the authentication constituting process result
information from the unit device which is a sending
destination of the authentication constituting process
15 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 result in the authentication
20 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 information in the
authentication constituting process 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~~

5 ~~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,~~

10 ~~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,

15 and the challenge value from the service providing device,

and

~~transfer means for transferring, to the service~~

~~providing device, authentication processing result~~

~~information received from the unit integrating device,—and~~

20 ~~display means for displaying service information~~

~~received from the service providing device,~~

the service providing device comprising

ninth~~service user identification information storage~~

means for storing, in association with each other,

25 cooperated user identification information which has a

value different 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,

~~seventh 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~~

~~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

algorithm, and a reference value ~~indicating a reference for~~ regarding ~~the accuracy of the~~ biometric authentication ~~accuracy by the biometric authentication algorithm~~ as proper,

~~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, 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,

~~cooperated read~~ means for searching the ninth~~service~~
~~user identification information~~ storage means in accordance
5 with the cooperated user identification information and
reading 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
10 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

15 ~~eighth~~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
20 processing result information, and the service providing
policy,

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

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

~~third equipment certificate~~ verifying means for
5 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,

10 ~~fourth user identification information certificate~~ verifying means for verifying the digital signature in the user identification information certificate included in the authentication context described in the received authentication processing result information in accordance
15 with the public key to the third-party organization,

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

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

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

~~tenth~~~~cooperated user information~~ storage means for
5 storing, in association with each other, the user
identification information in the user identification
information certificate, and cooperated user identification
information which is the same as the former cooperated user
identification information having a value different from
10 that of the user identification information to identify the
user, and

~~cooperated user identification information sending~~
means for sending, to the service providing device, the
cooperated user identification information read from the
15 ~~tenth~~~~cooperated user information~~ storage means and the
verification result that indicates properness in accordance
with the user identification information in the user
identification information certificate used for the
verification by the ~~fourth~~~~user identification information~~
20 ~~certificate~~ verifying means when all the verification
results by seven verifying means from the first~~format~~
~~verifying means, to the authenticator verifying means, the~~
~~equipment certificate verifying means, the user~~
~~identification information certificate verifying means, the~~
25 ~~evaluation report verifying means, the challenge value~~

~~verifying means, and the seventh execution result verifying~~
means are proper.

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

5 | the second 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
10 | 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

15 | 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~~
20 | 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
25 | 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 characterized by comprising:

first~~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 the authentication constituting process belongs, and equipment certificate issuer information to specify the equipment certificate issuer;

second~~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,
biometric authentication constituting process information
to specify a biometric authentication constituting process
including a biometric authentication algorithm, and

5 | ~~biometric authentication accuracy indicating the accuracy~~
| ~~of the biometric authentication by the biometric~~
| authentication algorithm;

| ~~fourth~~user identification information certificate
storage means for storing a user identification information
10 | 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
15 | 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~~;

20 | ~~third~~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
25 | 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
5 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;

10 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
15 described in the authentication context in a specific format; and

~~authentication constituting process result information generating means for generating authentication constituting process result information in which the authentication~~
20 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~~
25 ~~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
5 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
10 integrating device via the user terminal, the authentication context and the execution result are 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
15 providing device is sent, and the verifying device verifies the execution result, the format of the authentication processing result information, the authenticator in the authentication context, the equipment certificate, the evaluation report, the user identification information
20 certificate, and the challenge value.