

WHAT IS CLAIMED IS:

1. An authentication method for providing non-repudiation service, comprising:

5 an authentication request reception procedure in which an authentication service device receives a request to authenticate a user and information about the user from an online service server;

 a signed information reception procedure in which the
10 authentication service device receives signed information, obtained by signing unique identification information of a mobile terminal of the user, which is extracted from the mobile terminal of the user, with an authentication key, from the mobile terminal of the user, the unique identification
15 information of the mobile terminal being obtained depending on a result of biometric authentication of the user;

 a signed information verification procedure in which the authentication service device performs primary verification in accordance with the biometric authentication of the user by
20 verifying the signed information using a previously retained authentication key corresponding to the user;

 a mobile terminal verification request procedure in which, depending on a result of the primary verification, the authentication service device requests a communications company
25 server to verify mobile terminal information, which includes both the unique identification information of the mobile terminal of the user included in the signed information and the information about the user provided from the online service server; and

30

an authentication result creation procedure in which the authentication service device receives verification of whether the user of the mobile terminal is authentic and whether the user is in possession of the mobile terminal from the communications company server, performs secondary verification in accordance with the verification of whether the user of the mobile terminal is authentic and whether the user is in possession of the mobile terminal and creates an authentication result based on the verification, the verification being performed based on the mobile terminal information.

2. The authentication method of claim 1, wherein:

the authentication request reception procedure is configured such that, in response to the request to authenticate the user, a challenge value is created and sent to the mobile terminal of the user;

the signed information reception procedure is configured such that the signed information, obtained by signing combined information, which includes the unique identification information of the mobile terminal of the user and the challenge value, with the authentication key, is received from the mobile terminal of the user; and

the signed information verification procedure is configured such that the challenge value, included in the signed information, is verified using the previously retained authentication key corresponding to the user.

3. The authentication method of claim 2, wherein:

the signed information reception procedure is configured to receive the signed information and the unique identification

information of the mobile terminal of the user from the mobile terminal; and

the signed information verification procedure comprises:

creating verification information, which includes the
5 challenge value and the unique identification information of the mobile terminal of the user, and applying a hash function to the verification information so as to obtain hashed verification information; and

extracting combined information to which the hash function
10 has been applied from the signed information using the previously retained authentication key corresponding to the user, and performing verification by comparing the hashed verification information with the extracted combined information to which the hash function has been applied.

15

4. The authentication method of claim 1, wherein the authentication request reception procedure comprises

sending a push message for executing an authentication application to the mobile terminal corresponding to the user in
20 response to the request to authenticate the user from the online service server.

5. An authentication method for providing non-repudiation service, comprising:

25 a biometric authentication procedure in which, when authenticating a user in order to enable use of an online service, a mobile terminal of the user performs biometric authentication of the user;

a signed information sending procedure in which, depending
30 on a result of the biometric authentication, the mobile

terminal of the user creates signed information by signing unique identification information of the mobile terminal of the user, which is extracted from the mobile terminal of the user, with an authentication key and sends the signed information to
5 an authentication service device; and

an authentication result reception procedure in which the authentication service device performs primary verification in accordance with the biometric authentication of the user based on the signed information and performs secondary verification
10 based on verification of whether the user of the mobile terminal is authentic and whether the user is in possession of the mobile terminal through a communications company server based on the unique identification information of the mobile terminal of the user included in the signed information and the
15 information about the user provided from the online service server, and then the mobile terminal receives a result of the verification created by performing the primary verification and the secondary verification from the authentication service server.

20

6. The authentication method of claim 5, wherein:

in the biometric authentication procedure, a challenge value for authenticating the user is received from the authentication service device; and

25 in the signed information sending procedure, depending on the result of the biometric authentication, signed information is created by signing combined information, which includes the challenge value and the unique identification information of the mobile terminal of the user.

30

7. The authentication method of claim 5, wherein the biometric authentication procedure is configured such that an authentication application installed in the mobile terminal of the user requests an authentication apparatus installed in the mobile terminal of the user to perform biometric authentication of the user and receives a result of biometric authentication, obtained by performing biometric authentication of the user, from the authentication apparatus.

10 8. The authentication method of claim 6, wherein:
the signed information sending procedure comprises:
creating, by an authentication application installed in the mobile terminal of the user, combined information, which includes the challenge value and the unique identification information of the mobile terminal of the user, depending on
15 the result of the biometric authentication;
requesting, by the authentication application, an authentication apparatus installed in the user mobile terminal to sign the combined information;
20 receiving, by the authentication application, the signed information, which is created by applying a hash function to the combined information so as to obtain hashed information and by signing the hashed information with the authentication key, from the authentication apparatus; and
25 sending, by the authentication application, the signed information to the authentication service device, and
the authentication result reception procedure is configured such that the authentication application receives the result of the verification from the authentication service
30 device.

9. The authentication method of claim 5, further comprising:

receiving, by the mobile terminal of the user, a message
5 for executing an authentication application from the authentication service device when authenticating the user in order to use the online service, and thereby executing the authentication application installed in the mobile terminal of the user.

10

10. The authentication method of claim 5, further comprising:

executing an authentication application installed in the mobile terminal of the user in response to a request to
15 authenticate the user from an online service application in order to enable the use of the online service, the online service application being installed in the mobile terminal of the user in order to use the online service therein.

20 11. The authentication method of any one of claims 1 to 10, wherein the unique identification information of the mobile terminal of the user includes one or more of an identification number of a USIM, a phone number of the mobile terminal, and a serial number of the mobile terminal.

25

12. The authentication method of any one of claims 1 to 10, wherein the authentication key is a pair of keys, including a private key and a public key,

wherein the mobile terminal retains the private key and
30 the authentication service device retains the public key.

13. An authentication service device, which is configured to:

receive a request to authenticate a user and information
5 about the user from an online service server;

receive signed information, which is obtained by signing
unique identification information of a mobile terminal of the
user with an authentication key depending on a result of
biometric authentication of the user, from the mobile terminal
10 of the user;

perform primary verification in accordance with the
biometric authentication of the user by verifying the signed
information using a previously retained authentication key;

perform secondary verification based on verification of
15 whether the user of the mobile terminal is authentic and
whether the user is in possession of the mobile terminal
through a server of a communications company based on the
unique identification information of the mobile terminal of the
user included in the signed information and the information
20 about the user provided from the online service server;

create an authentication result based on the primary
verification and the secondary verification; and

provide the authentication result.

25 14. The authentication service device of claim 13, wherein
the authentication service device comprises:

an authentication service processing unit for receiving
the request to authenticate the user and information about the
user from the online service server, receiving signed
30 information, obtained by signing the unique identification

information of the mobile terminal of the user with the authentication key depending on a result of the biometric authentication of the user, from the mobile terminal of the user, performing primary verification by verifying the signed
5 information with the previously retained authentication key, performing secondary verification based on verification of whether the user of the mobile terminal is authentic and whether the user is in possession of the mobile terminal through the server of the communications company based on
10 mobile terminal information, which includes the unique identification information of the mobile terminal and the information about the user, creating an authentication result based on the primary verification and the secondary verification, and providing the authentication result; and
15 a communications company server connection unit for requesting the server of the communications company to verify the mobile terminal information by interworking with the server of the communications company to which the mobile terminal of the user is subscribed, and receiving a result of the
20 verification of whether the user of the mobile terminal is authentic and whether the user is in possession of the mobile terminal from the server of the communications company.

15. The authentication service device of claim 14, wherein
25 the authentication service processing unit is configured to:

create a challenge value and send the challenge value to the mobile terminal of the user in response to the request to authenticate the user from the online service server; and

receive signed information, obtained by signing combined
30 information, which includes the unique identification

information of the mobile terminal of the user and the challenge value, with the authentication key, from the mobile terminal of the user, and verify the signed information.

5 16. The authentication service device of claim 14, wherein the authentication service processing unit sends a push message for executing an authentication application to the mobile terminal of the user in response to the request to authenticate the user from the online service server.

10

 17. The authentication service device of claim 14, further comprising

 an authentication service registration unit for registering use of an authentication service for the user in
15 response to a request to register the use of the authentication service from the mobile terminal of the user, receiving the authentication key, which is created for biometric authentication of the user, from the mobile terminal of the user, and storing the authentication key therein.

20

 18. A mobile terminal of a user, the mobile terminal being installed with an authentication application for extracting unique identification information of the mobile terminal of the user and sending signed information, which is obtained by
25 signing the unique identification information of the mobile terminal of the user with an authentication key depending on a result of biometric authentication of the user, to an authentication service device when authenticating the user in order to enable use of an online service, and for receiving,
30 from the authentication service device, an authentication

result created by performing primary verification in accordance with the biometric authentication of the user based on the signed information and performing secondary verification based on verification of whether the user of the mobile terminal is authentic and whether the user is in possession of the mobile terminal based on the unique identification information of the mobile terminal of the user included in the signed information and the information about the user provided from the online service server.

10

19. The mobile terminal of claim 18, wherein the authentication application is configured to:

receive a challenge value according to authentication of the user from the authentication service device;

15 request an authentication apparatus installed in the mobile terminal of the user to perform biometric authentication of the user;

create combined information, which includes the challenge value and the unique identification information of the mobile terminal, depending on the result of biometric authentication;

20 request the authentication apparatus to sign the combined information;

receive the signed information, obtained by signing the combined information, from the authentication apparatus; and

25 send the signed information to the authentication service device.

20. The mobile terminal of claim 18, wherein the authentication application is automatically executed in response to a request to authenticate the user in order to use the online service from an online service application or upon
5 receiving a push message sent from the authentication service device, the online service application being installed in the mobile terminal of the user in order to use the online service therein.