

METHOD, DEVICE AND APPLICATION FOR PROVIDING AUTHENTICATION  
SERVICE OF NON-REPUDIATION

BACKGROUND OF THE INVENTION

5

Field of the Invention

The present invention relates generally to an authentication method, device and application for providing non-repudiation service. More particularly, the present  
10 invention relates to an authentication method in which, when a user who wishes to use an online service is authenticated, the result of biometric authentication, performed through the mobile terminal of the user, is signed and combined with the identification information of the mobile terminal, the combined  
15 information is sent to an authentication service server, and based on the received information, the authentication service server verifies not only the signed result of the biometric authentication but also whether the user of the mobile terminal is authentic and whether the user is in possession of the  
20 mobile terminal by interworking with the server of a communications company, thus taking advantage of the convenience of biometric authentication and providing non-repudiation service.

25 Description of the Related Art

With the development of Information and Communications Technology (ICT), the use of the Internet has increased in various fields from business to daily life. Accordingly, unless online services using the Internet are provided, there  
30 may be many difficulties in business and in daily life.

As online services have come to be available in a wide

range of fields, the identification or authentication of users is becoming more important. Particularly, when online financial services are used, the authentication of a user is necessarily performed in order to prevent damage attributable  
5 to financial fraud.

Accordingly, authentication techniques for performing user authentication are being strengthened, and in order to easily perform authentication and improve security, various authentication techniques using mobile terminals are being  
10 proposed.

Recently, in online financial services, when a digitally signed public certificate is used, a One-Time Password (OTP) or a security code card is used along with the public certificate, whereby security is improved. Furthermore, an authentication  
15 service using an Automatic Response System (ARS) or a Short Messaging Service (SMS), in which a user is asked to approve an authentication request made through a mobile terminal and authentication is performed based on the user's approval, is additionally applied.

20 However, these conventional authentication techniques are inconvenient in that the authentication procedure can be performed only when a public certificate is carried by a user. Also, the authentication techniques using an ARS or SMS authenticate a user merely by checking whether the user is in  
25 possession of the corresponding mobile terminal. Accordingly, when the public certificate and the mobile terminal of a user are stolen or illegally copied by a third party or when a third party interrupts an authentication procedure using malicious code, user authentication may be performed by the malevolent  
30 third party.

In order to solve the security problems and inconvenience of the authentication techniques, an authentication method using biometrics is widely used, and the Fast IDentity Online (FIDO) Alliance is working on open standards for an authentication method using biometrics in the online environment.

FIDO provides standard specifications for new authentication systems in which authentication may be performed through a simple procedure that no one can perform in place of a user by using fingerprint recognition, iris recognition, face recognition, and the like, rather than using an ID and password. FIG. 1 shows the concept of the authentication method based on a Universal Authentication Framework (UAF) according to the FIDO specifications.

The UAF authentication method proposes a "Passwordless Experience", in which authentication is performed without the input of a password, and because an authenticator is included in a terminal device, when the terminal device recognizes the unique biometric information of a user, such as fingerprints or the like, the user is authenticated using the authentication information included in the terminal device.

This authentication method based on biometrics is advantageous in that authentication may be easily performed by eliminating the need for a digital signature using a public certificate or the input of a password. However, because the terminal itself performs authentication as an authenticator, if a user denies having performed the authentication process, there is no method for verifying whether the user has performed the authentication process and preventing such repudiation of the user. Particularly, if a third party registers his or her



authentication method for providing non-repudiation service according to the present invention may include an authentication request reception procedure in which an authentication service device receives a request to  
5 authenticate a user and information about the user from an online service server; a signed information reception procedure in which the authentication service device receives signed information, obtained by signing identification information of a mobile terminal of the user with an authentication key, from  
10 the mobile terminal of the user, the identification 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 verifies the signed information using a previously  
15 retained authentication key corresponding to the user; a mobile terminal verification request procedure in which, depending on a result of verifying the signed information, the authentication service device requests a communications company server to verify mobile terminal information, which includes  
20 both the identification information of the mobile terminal and the information about the user; and 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  
25 the mobile terminal from the communications company server and creates an authentication result based on the verification, the verification being performed based on the mobile terminal information.

Desirably, the authentication request reception procedure  
30 may be 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 may be configured such that the signed information, obtained by signing combined information, which  
5 includes the 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 may be configured such that the challenge value, included in the signed  
10 information, is verified using the previously retained authentication key corresponding to the user.

Desirably, the signed information reception procedure may be configured to receive the signed information and the identification information of the mobile terminal of the user  
15 from the mobile terminal, and the signed information verification procedure may include creating verification information, which includes the challenge value and the identification information of the mobile terminal of the user, and applying a hash function to the verification information so  
20 as to obtain hashed verification information; and extracting combined information to which the hash function 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  
25 information with the extracted combined information to which the hash function has been applied.

Desirably, the authentication request reception procedure may include sending a push message for executing an authentication application to the mobile terminal corresponding  
30 to the user in response to the request to authenticate the user

from the online service server.

Also, another embodiment of an authentication method for providing non-repudiation service according to the present invention may include 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 on a result of the biometric authentication, the mobile terminal of the user creates signed information by signing identification information of the mobile terminal with an authentication key and sends the signed information to an authentication service device; and an authentication result reception procedure in which the authentication service device verifies 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, and then the mobile terminal receives a result of the verification from the authentication service server.

Desirably, in the biometric authentication procedure, a challenge value for authenticating the user may be received from the authentication service device; and in the signed information sending procedure, depending on the result of the biometric authentication, signed information may be created by signing combined information, which includes the challenge value and the identification information of the mobile terminal of the user.

Desirably, the biometric authentication procedure may be 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  
5 apparatus.

Desirably, the signed information sending procedure may include creating, by an authentication application installed in the mobile terminal of the user, combined information, which includes the challenge value and the identification information  
10 of the mobile terminal of the user, depending on 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; receiving, by the authentication application, the signed information, which  
15 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 sending, by the authentication application, the signed information to the authentication  
20 service device, and the authentication result reception procedure may be configured such that the authentication application receives the result of the verification of whether the user of the mobile terminal is authentic and whether the user is in possession of the mobile terminal from the  
25 authentication service device.

Desirably, the authentication method may further include receiving, by the mobile terminal of the user, a message for executing an authentication application from the authentication service device when authenticating the user in order to use the  
30 online service, and thereby executing the authentication

application installed in the mobile terminal of the user.

Desirably, the authentication method may further include executing an authentication application installed in the mobile terminal of the user in response to a request to 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.

Here, the identification information of the mobile terminal of the user may include 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.

Here, the authentication key is a pair of keys, including a private key and a public key, wherein the mobile terminal may retain the private key and the authentication service device may retain the public key.

Also, an authentication service device according to the present invention may be configured to receive signed information, which is obtained by signing identification information of a mobile terminal of a user with an authentication key depending on a result of biometric authentication of the user, from the mobile terminal, to verify the signed information using a previously retained authentication key, to create an authentication result 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 server of a communications company, and to provide the authentication result.

Desirably, the authentication service device may include an authentication service processing unit for receiving a

request to authenticate a user and information about the user from an online service server, receiving signed information, obtained by signing identification information of a mobile terminal of the user with the authentication key depending on a  
5 result of the biometric authentication of the user, from the mobile terminal of the user, verifying the signed information with the previously retained authentication key, creating an authentication result based on verification of whether the user of the mobile terminal is authentic and whether the user is in  
10 possession of the mobile terminal through the server of the communications company based on mobile terminal information, which includes the identification information of the mobile terminal and the information about the user, and providing the authentication result; and a communications company server  
15 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 verification of whether the user of  
20 the mobile terminal is authentic and whether the user is in possession of the mobile terminal from the server of the communications company.

Desirably, the authentication service processing unit may be configured to create a challenge value and send the  
25 challenge value to the mobile terminal of the user in response to the request to authenticate the user from the online service server, to receive signed information, obtained by signing combined information, which includes the identification information of the mobile terminal of the user and the  
30 challenge value, with the authentication key, from the mobile

terminal of the user, and to verify the signed information.

Desirably, the authentication service processing unit may send a push message for executing an authentication application to the mobile terminal of the user in response to the request  
5 to authenticate the user from the online service server.

Desirably, the authentication service device may further include an authentication service registration unit for registering use of an authentication service for the user in response to a request to register the use of the authentication  
10 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.

Also, an authentication application installed in a mobile  
15 terminal of a user according to the present invention may be configured to send signed information, which is obtained by signing 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  
20 service device when authenticating the user in order to enable use of an online service, and to receive an authentication result based on verification of whether the user of the mobile terminal is authentic and whether the user is in possession of the mobile terminal from the authentication service device.

Desirably, the authentication application may be configured to receive a challenge value according to authentication of the user from the authentication service device, to request an authentication apparatus installed in the mobile terminal of the user to perform biometric authentication  
25 of the user, to create combined information, which includes the  
30

challenge value and the identification information of the mobile terminal, depending on the result of biometric authentication, to request the authentication apparatus to sign the combined information, to receive the signed information, 5 obtained by signing the combined information, from the authentication apparatus, and to send the signed information to the authentication service device.

Desirably, the authentication application may be automatically executed in response to a request to authenticate 10 the user in order to use the online service from an online service application or upon 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.

15 As described above, according to the present invention, a result of biometric authentication is signed and combined with the identification information of the mobile terminal of a user, and the combined information is sent from the mobile terminal to an authentication service server, whereby the 20 authentication service server verifies not only the signed result of biometric authentication but also whether the user of the mobile terminal is authentic and whether the user is in possession of the mobile terminal by interworking with the server of a communications company. Therefore, it is possible 25 to take advantage of the convenience of biometric authentication and to provide non-repudiation service.

Furthermore, even when a third party registers his or her biometric information as the biometric information of a user in order to impersonate the user, the biometric information of the 30 user is first verified, and whether the user is authentic and

whether the user is in possession of the mobile terminal are additionally verified using the information about the user and the identification information of the mobile terminal, whereby the malevolent third party may be prevented from being approved  
5 through biometric authentication.

#### BRIEF DESCRIPTION OF THE DRAWINGS

The above and other objects, features and other advantages  
10 of the present invention will be more clearly understood from the following detailed description when taken in conjunction with the accompanying drawings, in which:

FIG. 1 shows an authentication method based on a Universal Authentication Framework (UAF) according to FIDO standards;

15 FIG. 2 illustrates a block diagram of an embodiment of an authentication system for providing non-repudiation service according to the present invention;

FIG. 3 illustrates a block diagram of an embodiment of an authentication service device in an authentication system for  
20 providing non-repudiation service according to the present invention;

FIG. 4 illustrates a block diagram of an embodiment of a user's mobile terminal in an authentication system for providing non-repudiation service according the present  
25 invention;

FIG. 5 illustrates a flowchart of an embodiment of a method for providing non-repudiation service according to the present invention;

FIG. 6 illustrates a flowchart of another embodiment of a  
30 method for providing non-repudiation service according to the

present invention; and

FIG. 7 illustrates a flowchart of an embodiment of the process in which a result of biometric authentication is combined with the identification information of a user's mobile terminal and the combined information is signed in a method for providing non-repudiation service according to the present invention.

#### DETAILED DESCRIPTION OF THE INVENTION

10

The advantages and features of the present invention and methods of achieving them will be apparent from the following exemplary embodiments that will be described in more detail with reference to the accompanying drawings.

15 The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting. As used herein, the singular forms "a," "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprise", "include", "have", etc., when used in this specification, specify the presence of stated features, integers, steps, operations, elements, components, and/or combinations of them but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or combinations thereof.

25 In the following description, it is to be noted that, when the functions of conventional elements and the detailed description of elements related with the present invention may make the gist of the present invention unclear, a detailed

description of those elements will be omitted.

The present invention provides an authentication method configured such that, when a user who wishes to use an online service is authenticated, a signed result of biometric authentication, performed using the mobile terminal of the user, is combined with the identification information of the mobile terminal, the combined information is sent to an authentication service server, and, based on the sent information, the authentication service server verifies not only the signed result of biometric authentication but also whether the user of the mobile terminal is authentic and whether the user is currently in possession of the mobile terminal by interworking with the server of a communications company.

FIG. 2 illustrates a block diagram of an embodiment of an authentication system for providing non-repudiation service according to the present invention.

The authentication system for providing non-repudiation service may include a user's terminal 10, a user's mobile terminal 100, an online service server 300, an authentication service device 200, and a communications company server 400.

The terminal 10 of a user is a communications device for being provided with online services, and may include components for accessing the online service server 300 and providing the user with various kinds of online services provided from the online service server 300. Here, the terminal 10 may use various communications devices such as a common PC, a laptop, a tablet PC, a smart phone, and the like.

The mobile terminal 100 of the user is a communications terminal for performing user authentication when user authentication is required in order for the terminal 10 of the

user to be provided with an online service. A common communications terminal that is capable of performing the non-repudiation service process according to the present invention, such as a smart phone, a tablet PC, or the like, may be used as  
5 the mobile terminal 100, or a special communications terminal optimized to perform the non-repudiation service process according to the present invention may be used.

Desirably, the mobile terminal 100 may include an authentication application for performing the non-repudiation  
10 service process according to the present invention and an authentication apparatus for performing user authentication through biometric authentication. Here, the authentication application and the authentication apparatus may be implemented separately from each other, or may be implemented as a single  
15 configuration in which the authentication application is combined with the authentication apparatus.

The authentication application of the mobile terminal 100 of the user combines the result of biometric authentication of the user, which is performed through the authentication  
20 apparatus in conjunction with the authentication service device 200, with the identification information of the mobile terminal 100, signs the combined information, sends the signed information to the authentication service device 200, and receives the result of verification of the signed information,  
25 information about whether the user of the mobile terminal 100 is authentic, and information about whether the user is in possession of the mobile terminal 100.

Furthermore, the user's mobile terminal 100 may be substituted for the user's terminal 10. For example, the  
30 user's mobile terminal 100 includes a mobile browser installed

therein, and may be provided with online services from the online service server 300 through the mobile browser. Alternatively, an online service application that is capable of executing online services provided from the online service  
5 server 300 is installed in the user's mobile terminal 100, whereby the user's mobile terminal 100 may also function as the user's terminal 10.

The authentication application and the authentication apparatus of the user's mobile terminal 100 will be described  
10 later with reference to the embodiment of the user's mobile terminal 100.

The authentication service device 200 receives and verifies signed information, which is obtained by combining the result of biometric user authentication performed in the mobile  
15 terminal 100 of the user with the identification information of the mobile terminal 100 and signing the combined information. Then, the authentication service device 200 verifies whether the user of the mobile terminal 100 is authentic and whether the user is in possession of the mobile terminal 100 by  
20 interworking with the communications company server 400, thereby providing non-repudiation service.

For example, the authentication service device 200 retains security policies for each authentication service corresponding to a specific online service provided by the online service  
25 server 300, and enables a user to register for and to use the authentication service based on the corresponding security policies. Particularly, the authentication service device 200 receives signed information, which includes the result of biometric user authentication and the identification  
30 information of the user's mobile terminal 100, from the user's

mobile terminal 100, verifies the signed information, and verifies whether the user of the mobile terminal 100 is authentic and whether the user is in possession of the user's mobile terminal 100 through the communications company server  
5 400 based on the user information provided from the online service server 300 and the identification information of the user's mobile terminal 100.

In other words, whether the information about the user who wishes to use the online service provided from the online  
10 service server 300 matches the identification information of the user's mobile terminal 100 is checked through the communications company server, whereby whether the user who performs the user authentication process using the user's mobile terminal 100 is authentic and whether the authorized  
15 user is currently in possession of the user's mobile terminal 100 may be confirmed.

Here, the authentication service device 200 may be implemented as a separate device specialized to implement the present invention, or may be implemented as a server in which a  
20 program for providing the non-repudiation service according to the present invention is installed.

The online service server 300 is a device for providing a specific online service to a user. Here, the specific online service may include various services available online, such as  
25 an online service for providing various kinds of information and content, an online service for electronic commerce, and an online service for providing financial services such as Internet banking or the like.

The communications company server 400 is the device owned  
30 by the communications company to which the user's mobile

terminal 100 is subscribed. The communications company server 400 verifies whether the user of the mobile terminal 100 is authentic and whether the mobile terminal 100 is owned by the authorized user by comparing the user information with the identification information of the user's mobile terminal 100 in response to a request to authenticate the user's mobile terminal 100 from the authentication service device 200, and then provides the result of the verification to the authentication service device 200.

As described above, the authentication system for providing non-repudiation service according to the present invention first verifies the result of biometric user authentication, which is performed in the mobile terminal 100 of the user. Also, because the identification information of the user's mobile terminal 100 is included in the signed result of biometric user authentication performed through the mobile terminal 100, the identification information of the user's mobile terminal 100 and the user information delivered from the online service server 300 are combined and used to additionally verify whether the user of the mobile terminal 100 is authentic and whether the user is in possession of the mobile terminal 100 through the server 400 of the corresponding communications company, whereby a more convenient and secure biometric authentication method may be applied and user non-repudiation service may be implemented.

The configuration of the authentication system for providing non-repudiation service according to the present invention will be described in detail with reference to an embodiment.

FIG. 3 illustrates a block diagram of an embodiment of the

authentication service device in the authentication system for providing non-repudiation service according to the present invention.

The authentication service device 200 receives and  
5 verifies the signed information, which includes the result of biometric user authentication performed in the user's mobile terminal 100 and the identification information of the user's mobile terminal 100, verifies whether the user of the mobile terminal 100 is authentic and whether the user is in possession  
10 of the mobile terminal 100 through the communications company server 400 based on the identification information of the user's mobile terminal 100 and the user information delivered from the online service server 300, and provides the result of the verification of whether the user is authentic and whether  
15 the authenticated user is in possession of the mobile terminal 100.

To this end, the authentication service device 200 may include an authentication service registration unit 210, an authentication service processing unit 230, a communications  
20 company server connection unit 250, and the like.

In response to a request to register the use of an authentication service from the authentication application installed in the user's mobile terminal 100, the authentication service registration unit 210 generates information to be  
25 registered, which is required in order to enable the user to use the authentication service, by performing a series of processes for registering the use of the authentication service by working in conjunction with the authentication application, and may register the use of the authentication service for the  
30 user based on the generated information.

Desirably, the authentication service registration unit 210 receives an authentication key, which is created so as to correspond to the user's biometric information when the user's biometric information is registered in the user's mobile terminal 100, and stores the authentication key in connection with the biometrics of the corresponding user.

As an example of registration of the use of an authentication service, the authentication service registration unit 210 generates registration text, which includes the service code for a specific online service and an authentication method based on the security policies of the authentication service corresponding to the online service, provides the generated registration text to the authentication application of the mobile terminal 100, receives both an authentication key, which the authentication application creates by authenticating the user through the biometric authentication method based on the corresponding security policies, and a registration certificate signed with the authentication key, and generates the information about the user who intends to use the authentication service for registration thereof.

Here, the authentication key may use a pair of keys, including a private key and a public key, and the authentication service registration unit 210 may receive the public key from the user's mobile terminal 100 and register the public key in connection with the biometrics of the user.

When authentication of a user is requested, the authentication service processing unit 230 verifies the signed result of biometric authentication of the corresponding user in conjunction with the authentication application installed in

the mobile terminal 100 of the user, and provides an authentication service in order to verify whether the user is authentic and whether the user is in possession of the mobile terminal 100 through the server 400 of the corresponding communications company based on the identification information of the mobile terminal 100 and the user information delivered from the online service server 300.

For example, the authentication service processing unit 230 may execute the authentication application installed in the user's mobile terminal 100 using a push message or the like. Then, the user authentication service processing unit 230 receives the signed information, which is obtained by combining the result of biometric user authentication with the identification information of the user's mobile terminal 100 and signing the combined information, from the authentication application, and verifies the signed information. Here, the authentication service processing unit 230 may verify the signed information using the authentication key, which is registered in the authentication service registration unit 210.

More desirably, the authentication service processing unit 230 creates a random challenge value in response to a request to authenticate a user, and sends the challenge value to the authentication application of the mobile terminal 100 of the user. Then, the mobile terminal 100 combines the challenge value with the identification number of the USIM of the mobile terminal 100 depending on the result of biometric authentication, applies a hash function to the combined information so as to obtain hashed information, signs the hashed information, and sends both the signed information and the identification number of the USIM of the mobile terminal to

the authentication service unit 230. Accordingly, after receiving the signed information and the identification number of the USIM of the mobile terminal 100, the authentication service unit 230 extracts the hashed information from the received signed information using the authentication key registered in the authentication service registration unit 210, generates verification information by combining the challenge value with the received identification number of the USIM of the mobile terminal 100 and by applying the hash function thereto, and compares the extracted information and the generated verification information, whereby the signed information may be verified.

Also, the authentication service processing unit 230 creates mobile terminal information so as to include the identification information of the user's mobile terminal 100 and the user information delivered from the online service server 300, requests the communications company server 400 to verify whether the user is authentic and whether the user is in possession of the user's mobile terminal 100 based on the mobile terminal information, and determines whether the user is authentic and whether the user is in possession of the user's mobile terminal 100 based on the result delivered from the communications company server 400.

The communications company server connection unit 250 delivers the mobile terminal information, which includes the identification information of the user's mobile terminal 100 and the user information, to the communications company server 400 when the authentication service processing unit 230 requests the communications company server 400 to verify the identification information of the user's mobile terminal 100,

and receives the results of verification of whether the user is authentic and whether the user is in possession of the user's mobile terminal 100 and delivers the received results to the authentication service processing unit 230.

5       Further, the authentication service registration unit 210 and the authentication service processing unit 230 may generate a transaction ID for identifying a process when performing the process, and may perform the process using the transaction ID. Also, a timer may be set when a transaction ID is generated,  
10       and the result of the process may be regarded as being valid only when the process is completed within a preset time period.

      In the above-described authentication service device 200 of the authentication system for providing non-repudiation service according to the present invention, each of the units  
15       may be configured as separate units, or as a server in which a program that is capable of providing an authentication service by performing a series of processes is installed. The authentication service device 200 may first verify the result of biometric user authentication in conjunction with the  
20       authentication application installed in the user's mobile terminal 100, and may additionally provides the result of verification of whether the user is authentic and whether the user is in possession of the user's mobile terminal 100 through the communications company server 400, whereby the user non-  
25       repudiation service may be provided.

      Next, a block diagram of an embodiment of a user's mobile terminal in the authentication system for providing non-repudiation service according to the present invention is described with reference to FIG. 4.

30       The mobile terminal 100 of a user is configured to perform

biometric authentication of the user, to combine the result of biometric authentication with the identification information of the mobile terminal, to sign the combined information, to send the signed information to the authentication service device  
5 200, and then to receive the result of verification of whether the user is authentic and whether the user is in possession of the mobile terminal 100 from the authentication service device 200.

To this end, the user's mobile terminal 100 may include an  
10 authentication application 110, an authentication apparatus 150, and the like, and may further include various components for functioning as a wireless communications terminal.

The authentication application 110 performs the process of authenticating a user in conjunction with the authentication  
15 service device 200 when the user intends to use an online service. Specifically, the authentication application 110 registers the use of the authentication service for the user in the authentication service device 200 in advance, and when authentication of the user is required in order to use the  
20 online service provided from the online service server 300, it extracts the identification information from the mobile terminal 100 of the user depending on the result of biometric authentication of the user, which is performed through the authentication apparatus 150, combines the identification  
25 information with the result of biometric authentication, signs the combined information, and sends the signed information to the authentication service device 200. Here, the identification information of the mobile terminal 100 may be the identification number of the USIM embedded in the mobile  
30 terminal, and, depending on the circumstances, it may be

various kinds of information with which the mobile terminal can be identified, such as the phone number of the mobile terminal, the serial number of the mobile terminal, or the like.

For example, the authentication application 110 requests  
5 the authentication service device 200 to start performing an authentication process and receives a random challenge number from the authentication service device 200. Then, the authentication application 110 applies a hash function to information, in which the challenge number and the  
10 identification number of the USIM of the mobile terminal 100 are combined depending on the result of biometric user authentication, signs the information to which the hash function is applied, and sends the signed information to the authentication service device 200.

15 Subsequently, the authentication application 110 receives the result of verification of whether the user is authentic and whether the user is in possession of the mobile terminal 100 from the authentication service device 200.

Here, the authentication application 110 may be installed  
20 in a separate device embedded in or connected to the user's mobile terminal 110. Alternatively, it may be a computer program for executing a series of processes for providing the non-repudiation service according to the present invention by operating basic components of the user's mobile terminal 100.

25 The authentication apparatus 150 serves to authenticate a user, and desirably includes the means for recognizing the biometric information of the user and registers the biometric information of the user using the means for recognizing the biometric information. Accordingly, when authentication of the  
30 user is required, the authentication apparatus 150 may perform

biometric user authentication. Here, the biometric information may selectively include biometric information obtainable through various biometric methods such as fingerprint recognition, iris recognition, face recognition, voice  
5 recognition, and the like, and the user's mobile terminal 100 may selectively include the means for recognizing the selected biometric information in order to perform biometric authentication in conjunction with the authentication apparatus  
150.

10 Also, the authentication apparatus 150 may include a means for managing an authentication key in order to create and store the authentication key of a user and to manage the certificate corresponding to the authentication key. Here the means for managing the authentication key creates an authentication key  
15 so as to correspond to the biometric information of a user when the biometric information of the user is registered, stores the created authentication key, and provides information signed with the stored authentication key to the authentication application 110 upon receiving a request to sign the  
20 information from the authentication application 110. Here, the authentication key may use a pair of keys, including a private key and a public key, in which case the public key, created when the biometric information of the user is registered, is registered in the authentication service device 200 by being  
25 provided through the authentication application 110.

In the embodiment of FIG. 4, the authentication application 110 and the authentication apparatus 150 are depicted as being separate, but according to need, they may be combined and included in the user's mobile terminal 110.

30 Further, when the online service, provided from the online

service server 300, is used in the user's mobile terminal 100, an online service application 170, which works in conjunction with the online service server 300 in order to enable the use of the corresponding online service therein, may be  
5 additionally installed in the user's mobile terminal 100.

Here, when user authentication is required in order to use the online service provided from the online service server 300, the online service application 170 may request the authentication application 110 of the user's mobile terminal  
10 100 to perform a user authentication process, and the authentication application 110 may perform the authentication process in response to the request from the online service application 170.

Here, the online service application 170 may be a computer  
15 program for executing a series of processes for providing online service between the user's mobile terminal 100 and the online service server 300.

As described above, the mobile terminal 100 of a user performs biometric user authentication using the biometric  
20 information of the user when user authentication is required to use an online service, combines the result of biometric user authentication with the identification information of the mobile terminal 100, signs the combined information, sends the signed information to the authentication service server 200,  
25 and thereby helps the authentication service server 200 verify whether the user is authentic and whether the user is in possession of the mobile terminal 100 based on the received information, whereby more convenient authentication using biometrics may be performed and non-repudiation service may be  
30 provided.

Both easier biometric authentication and non-repudiation service may be performed at the same time by applying the above-described authentication system for providing non-repudiation service according to the present invention. In 5 this regard, the present invention proposes a method for providing non-repudiation service.

The method for providing non-repudiation service according to the present invention may be largely divided into the verification of biometric user authentication performed in the 10 mobile terminal of a user and the process in which whether the user is authentic and whether the user is actually in possession of the mobile terminal are verified in the authentication service device through a communications company server. The processes will be described with reference to the 15 following embodiment.

As described above, the authentication service device according to the present invention may be implemented as a server. In the following embodiment, an example in which the authentication service device is implemented as a server is 20 described, and thus the authentication service device is referred to as an authentication service server. Also, although the process performed by the authentication service server differs from the process performed by a user's mobile terminal, the process performed by the authentication server 25 and the process performed by the user's mobile terminal are integrated, and the integrated process will be described for the convenience of description.

FIG. 5 illustrates a flowchart of an embodiment of a process for providing non-repudiation service according to the 30 present invention.

The embodiment of FIG. 5 shows the case in which the user's mobile terminal 100 is not distinguished from the user's terminal, and thus an online service is used in the user's mobile terminal 100. Accordingly, the embodiment of FIG. 5 is  
5 the embodiment of a method for providing non-repudiation service when the user's mobile terminal 100 is provided with an online service from the online service server 300.

When the user's mobile terminal 100 accesses the online service server 300 and requests the use of an online service at  
10 step S110, the online service server 300 requests the authentication service server 200 to authenticate the user at step S120. Here, the online service server 300 may send the information about the user, registered in the online service server 300, to the authentication service server 200, and may  
15 additionally send information about the corresponding online service along with the information about the user.

When user authentication is required in order to use the online service, the authentication application installed in the user's mobile terminal 100 is executed at step S130. Here, the  
20 authentication application performs a series of authentication processes according to the preset security policies. Because the present invention is based on biometric authentication, the user's mobile terminal 100 recognizes the biometric information of the user and performs user authentication at step S140 based  
25 on previously registered biometric information of the user.

If biometric user authentication is performed through the authentication apparatus installed in the user's mobile terminal 100, the authentication application requests the authentication apparatus installed in the user's mobile  
30 terminal 100 to perform biometric authentication of the user,

whereby biometric authentication of the user may be performed through the authentication apparatus.

Before, after, or at the same time as the performance of biometric authentication of the user, the authentication application extracts identification information of the user's mobile terminal 100 at step S150. Here, the identification information may be various kinds of information with which the mobile terminal registered in the communications company server can be identified, such as the identification number of a USIM embedded in the mobile terminal, the phone number of the mobile terminal, the serial number of the mobile terminal, or the like. The embodiment of FIG. 5 shows the case in which the identification number of the USIM of the user's mobile terminal 100 is used as the identification information.

Also, depending on the result of biometric authentication of the user, the authentication application combines the identification number of the USIM of the user's mobile terminal with the result of biometric authentication, signs the combined information with a previously retained private key at step S160, and sends the signed information to the authentication service server 200 at step S170. For example, when a challenge value for authentication is delivered from the authentication service server 200 according to the user authentication method, the authentication application combines the challenge value, which is the result of biometric authentication, with the identification number of the USIM, signs the combined information, and sends the signed information to the authentication service server 200.

In this case, if the authentication apparatus for creating and managing an authentication key is provided, the

authentication application sends the combined information to the authentication apparatus, and the combined information may be signed with the previously retained private key in the authentication apparatus. Also, when sending the signed  
5 information, the authentication application may send the identification number of the USIM, extracted from the user's mobile terminal 100, along with the signed information.

The authentication service server 200 verifies the signed information sent from the authentication application of the  
10 user's mobile terminal 100. Here, the authentication service server 200 may retain an authentication key corresponding to the biometrics of the user, which was received from the user's mobile terminal 100 when the use of authentication service was registered therein, and the authentication service server 200  
15 verifies the signed information at step S210 using the retained authentication key corresponding to the user. For example, if the authentication service server 200 has created a challenge value and sent it to the authentication application according to the user authentication method, the authentication service  
20 server 200 may extract the challenge value from the signed information sent from the authentication application using the authentication key, whereby the signed information may be verified based on the challenge value.

Desirably, the authentication key may use a pair of keys,  
25 including a public key and a private key, and the authentication service server 200 may receive and store the public key corresponding to the biometrics of the user in advance.

When verification of the signed information is completed,  
30 the authentication service server 200 generates mobile terminal

information by combining the identification number of the USIM of the user's mobile terminal 100 with the user information delivered from the online service server 300, sends the mobile terminal information to the corresponding communications  
5 company server 400, and thereby requests verification of whether the user is authentic and whether the user is in possession of the user's mobile terminal 100 at step S230 based on the mobile terminal information.

The communications company server 400 checks whether the  
10 user is authentic and whether the user is the owner of the mobile terminal based on the user information, which is registered in connection with the identification number of the USIM, and then provides the result of checking to the authentication service server 200 at step S250.

15 Based on the result provided from the communications company server 400, the authentication service server 200 generates an authentication result about whether the user is authentic and whether the user is in possession of the mobile terminal 100 at step S260 and provides the authentication  
20 result to the user's mobile terminal 100 and the online service server 300 at steps S270 and S280.

Depending on the authentication result sent from the authentication service server 200, the online service server 300 may provide the corresponding online service to the user's  
25 mobile terminal 100 at step S300.

FIG. 6 illustrates a flowchart of another embodiment of a method for providing non-repudiation service according to the present invention.

The embodiment of FIG. 6 shows the case in which the  
30 user's terminal 10 and the user's mobile terminal 100 are

configured as separate devices. Accordingly, when the user's terminal 10 is provided with an online service from the online service server 300, user authentication is performed through the user's mobile terminal 100.

5        When the user's terminal 10 accesses the online service server 300 and requests the use of an online service at step S410, the online service server 300 requests the authentication service server 200 to authenticate the user at step S420. Here, as in the embodiment of FIG. 5, the online service server  
10    300 may send the user information registered therein to the authentication service server 200, and may additionally send information about the corresponding online service along with the user information.

      In response to the request for user authentication from  
15    the online service server 300, the authentication service server 200 triggers the user's mobile terminal 100 corresponding to the user information to execute an authentication application at step S430, and thus the authentication application installed in the user's mobile  
20    terminal 100 is executed at step S440.

      When the authentication application installed in the user's mobile terminal 100 is executed, the authentication application performs a series of authentication processes based on the preset security policies. As in the embodiment of FIG.  
25    5, the user's mobile terminal 100 performs biometric authentication of the user at step S450, extracts the identification number of the USIM at step S460 depending on the result of biometric authentication, signs the information, in which the result of biometric authentication is combined with  
30    the identification number of the USIM, with a private key at

step S470, and sends the signed information to the authentication service server 200 at step S480.

Then, the authentication service server 200 verifies the signed information sent from the user mobile terminal 100 using  
5 a public key at step S510, generates mobile terminal information at step S520 by combining the identification number of the USIM of the user's mobile terminal 100 with the user information delivered from the online service server 300, sends the mobile terminal information to the corresponding  
10 communications company server 400, and thereby requests it to authenticate the user and verify whether the user is in possession of the user's mobile terminal 100 at step S530 depending on the mobile terminal information.

Based on the mobile terminal information delivered from  
15 the authentication service server 200, the communications company server 400 checks whether the user is authentic and whether the user is in possession of the mobile terminal and provides the result of checking to the authentication service server 200 at step S550. Then, the authentication service  
20 server 200 generates an authentication result indicating whether the user is authentic and whether the user is in possession of the user's mobile terminal 100 at step S560 based on the result provided from the communications company server 400 and provides the generated authentication result to the  
25 user's mobile terminal 100 and the online service server 300 at steps S570 and S580.

Depending on the authentication result received from the authentication service server 200, the online service server 300 may provide the corresponding online service to the user's  
30 terminal 10 at step S600.

The present invention is characterized in that the user's mobile terminal 100 signs information, which includes both the result of biometric authentication and the identification information of the user's mobile terminal 100, with an authentication key, and provides the signed information to the authentication service server 200, whereby the authentication service server 200 verifies whether the user is authentic and whether the user is in possession of the user's mobile terminal 100 based on the signed information through the corresponding communications company server 400. In this regard, the process between the user's mobile terminal 100 and the authentication service server 200, in which the result of biometric authentication is combined with the identification information of the user's mobile terminal and the combined information is signed, will be described in detail with reference to the flowchart of the embodiment illustrated in FIG. 7.

In the process of authenticating a user who intends to use an online service, when the authentication application 110 of the user's mobile terminal 100 is executed at step S710, the authentication application 110 accesses the authentication service server 200 and request the start of user authentication at step S720.

In response to the request to start user authentication from the authentication application 110, the authentication service server 200 creates a random challenge value for authenticating the corresponding user at step S730 and sends the challenge value to the authentication application 110 at step S740.

The authentication application 110 receives the challenge value, which is obtained as the start of user authentication,

extracts the identification number of the USIM from the user's mobile terminal 100 at step S750, and combines the extracted identification number of the USIM with the received challenge value at step S760.

5       Also, with the start of user authentication, the authentication apparatus 150 of the user's mobile terminal 100 performs biometric authentication at step S810 by recognizing the biometric information of the user. Here, the biometric authentication performed by the authentication apparatus 150  
10 may be performed in response to the request to start user authentication from the authentication application 110.

When biometric authentication of the user succeeds, the authentication apparatus 150 sends the result of biometric authentication to the authentication application 110 at step  
15 S820. Because biometric authentication has succeeded, the authentication application 110 sends the combined information, which includes the identification number of the USIM and the challenge value, to the authentication apparatus 150 at step S830 and requests that the combined information be signed.

20       In response to the request from the authentication application 110 to sign the combined information, the authentication apparatus 150 signs the combined information with a previously retained private key at step S840. Here, after a hash function is applied to the combined information so  
25 as to obtain hashed information, the hashed information is signed with the private key, and the signed information is provided to the authentication application 110 at step S850. Then, the authentication application 110, having received the signed information, sends the identification number of the USIM  
30 of the user's mobile terminal 100 along with the signed

information to the authentication service server 200 at step S860.

The authentication service server 200 generates verification information at step S910 by combining the  
5 identification number of the USIM, sent from the authentication application 100, with the challenge value, which was created when user authentication was started.

Then, the authentication service server 200 verifies the signed information using a public key, which is retained to  
10 correspond to the biometrics of the user. Specifically, the hashed information is extracted from the signed information using the public key at step S920, the hash function is applied to the verification information, and the extracted information is compared with the verification information to which the hash  
15 function was applied at step S930, whereby whether the signed information is valid may be verified at step S940.

Through the above-described processes, biometric authentication of the user, which is performed in the user's mobile terminal 100, is verified by the authentication services  
20 server 200.

When the result of verification is valid, the authentication service server 200 generates mobile terminal information by combining the user information delivered from the online service server 300 with the identification  
25 information of the user's mobile terminal 100 and requests the communications company server 400 to verify the mobile terminal information, whereby whether the user is authentic and whether the user is in possession of the user's mobile terminal 100 may be verified through the communications company server 400,  
30 which was described above with reference to FIGS. 5 and 6.

As described above, according to the present invention, the mobile terminal of a user signs information in which the identification information of the mobile terminal is combined with the result of biometric authentication of the user and  
5 sends the signed information to an authentication service server, whereby the authentication service server verifies not only the signed information about the biometric authentication but also whether the user is authentic and whether the user is in possession of the mobile terminal by interworking with a  
10 communications company server. Therefore, authentication that realizes both the convenience of biometric authentication and the provision of non-repudiation service may be performed.

The above description is merely an illustration of the technical spirit of the present invention, and those having  
15 ordinary knowledge in the technical field to which the present invention pertains can make modifications and variations within the range that does not depart from the essential characteristics of the present invention. Accordingly, the disclosed embodiments of the present invention are not intended  
20 to limit the technical spirit of the present invention but to illustrate the technical spirit of the present invention, and the scope of the technical spirit of the present invention is not limited to these embodiments. The range of protection of the present invention should be interpreted based on the  
25 following claims, and all technical spirit within the range equivalent to the claims should be construed as falling within the range of the rights of the present invention.

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 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 device.

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.