

USER AUTHENTICATION METHOD WITH ENHANCED SECURITY

BACKGROUND

5 **[0001]** Embodiments of the inventive concept described herein relate to a user authentication method with enhanced security, and more particularly, relate to a user authentication method, in which it is unnecessary to manage a password of a user in view of a certificate authority, for easily replacing the password in view of the user, determining whether an authentication site is true, and enhancing security
10 through multi-authentication.

[0002] It has become common for financial transactions or a variety of business necessary for user authentication to be conducted through online environments in modern society rather than face-to-face contact. User authentication online needs a more cautious approach rather than face-to-face contact. In most
15 cases, it is requested to install various security programs including an ActiveX program and a keyboard security program or control programs in a user terminal. It is prepared for an outflow of information by enhancing security through security devices such as certificates, security cards, and one time password (OTP) devices.

[0003] An OTP device which is one of representative user authentication
20 methods and has an embedded unique key is provided to a user in advance. If the user accesses an electronic banking network and requests an authentication server (a server of a financial institution) to perform authentication, the OTP device generates an OTP number based on a random number associated with a current time by using the unique as an operation key. The user manually enters the generated OTP number

as a password and sends the OTP number to the authentication server. The authentication server authenticates that the user is a true user using the OTP number.

[0004] However, if the user transacts with a plurality of financial institutions, since he or she has an OTP device provided for each financial institution, he or she should separately purchase an OTP device for each financial institution and should have a plurality of OTP devices. The user should find an authentication device for specific financial institution one by one among the plurality of OTP devices.

[0005] Further, since the user may optionally replace a unique key of an OTP device, if he or she loses the OTP device, he or she should directly visit a financial institution and should be issued a new OTP device. It takes enormous expense and time for financial institutions to issue OTP devices again to all clients if unique keys of OTP devices of the clients flow out.

[0006] Meanwhile, if the user is authenticated or logs in to a related server through a specified password, the related server should register, store, and manage the password of the user and the user should recognize the password. Since the related server requests the user to change the password on a regular basis to prepare for an outflow, it is inconvenient to manage the password.

[0007] In addition, with the development of hacking technologies, an outflow of information, such as screen capturing, a shoulder surfing attack, screen hacking technologies such as screen monitoring, or an outflow of certificates or passwords due to spywares installed in personal computers (PCs), is performed in various manners. Since a professional hacker may decrypt an encrypted password by some degrees of efforts, it is necessary to seek convenience and enhance security in a procedure for user authentication.

[0008] Prior Art Document

SUMMARY

5 **[0009]** Embodiments of the inventive concept provide a user authentication method with enhanced security for overcoming the above-mentioned problems.

[0010] Embodiments of the inventive concept provide a user authentication method for having a simple user authentication procedure and enhancing security.

[0011] Embodiments of the inventive concept provide a user authentication
10 method for a user to determine whether a certificate authority, an authentication server, or the like for authentication is true.

[0012] Embodiments of the inventive concept provide a user authentication method for performing authentication without managing a password of a user in a certificate authority or an authentication server and enhancing security using a multi-
15 element linked to time.

[0013] According to an aspect of an embodiment, a user authentication method using a user terminal and an authentication server may include generating, by the user terminal, a first common authentication key by combining a private password with a mechanical unique key of the user terminal and encrypting the
20 combined information if a user of the user terminal enters the private password for user registration and providing, by the user terminal, the generated first common authentication key to the authentication server, and registering, by the authentication server, the first common authentication key and user information by matching the first common authentication key with the user information, generating, by the
25 authentication server, a server authentication key by combining an embedded unique

key of a certificate authority with the first common authentication key and encrypting the combined information and generating, by the authentication server, first server authentication information by calculating a one time password (OTP) by using the server authentication key as an operation key, and generating, by the user terminal, a second common authentication key by combining the private password with the mechanical unique key of the user terminal and encrypting the combined information if the user enters the private password for authentication, generating, by the user terminal, a user authentication key by combining the unique key of the certificate authority previously provided from the authentication server with the second common authentication key and encrypting the combined information, and generating, by the user terminal, first user authentication information by calculating an OTP by using the user authentication key as an operation key, and performing user authentication based on whether the first server authentication information is identical to the first user authentication information or performing authentication server authentication for determining whether the authentication server is true.

[0014] According to another aspect of an embodiment, a user authentication method may include generating, by a user terminal, a first common authentication key by combining a private password with a mechanical unique key of the user terminal and encrypting the combined information if a user of the user terminal enters the private password for user registration using the user terminal and providing, by the user terminal, the generated first common authentication key to an authentication server, and registering, by the authentication server, the first common authentication key and user information by matching the first common authentication key with the user information, generating, by the authentication server, a server authentication key by combining an embedded unique key of a certificate authority

with the first common authentication key and encrypting the combined information and generating, by the authentication server, server authentication information by calculating an OTP using an operation key generated by combining the server authentication key a gap time value in which a time taken for the user to enter the private password is measured every $1/n$ seconds, wherein n is a positive real number, and a gap time key which is a numeral value extracted by criteria from the gap time value, measuring, by the user terminal, the gap time value if the user enters the private password for authentication and transmitting, by the user terminal, the measured gap time value to the authentication server, generating, by the user terminal, a second common authentication key in real time by combining the private password with the mechanical unique key of the user terminal and encrypting the combined information, generating, by the user terminal, a user authentication key by combining the unique key of the certificate authority previously provided from the authentication server with the second common authentication key and encrypting the combined information, and generating, by the user terminal, user authentication information by calculating an OTP using an operation key generated by combining the user authentication key with the gap time value or the gap time key, and performing user authentication base on whether the server authentication information is identical to the user authentication information.

20

BRIEF DESCRIPTION OF THE FIGURES

[0015] The above and other objects and features will become apparent from the following description with reference to the following figures, wherein like

reference numerals refer to like parts throughout the various figures unless otherwise specified, and wherein:

[0016] FIG. 1 is a drawing schematically illustrating an authentication device used in a user authentication method according to various embodiments;

5 **[0017]** FIG. 2 is a signal sequence diagram illustrating a user authentication method according to an embodiment;

[0018] FIG. 3 is a signal sequence diagram illustrating a user authentication method according to another embodiment; and

[0019] FIG. 4 is a signal sequence diagram illustrating a user authentication
10 method according to another embodiment.

DETAILED DESCRIPTION

[0020] Hereinafter, embodiments of the inventive concept are described with reference to the accompanying drawings so that this disclosure will be thorough and
15 complete and will fully convey the scope of the inventive concept to those skilled in the art.

[0021] FIG. 1 is a drawing schematically illustrating an authentication device
500 used in a user authentication method according to various embodiments.

[0022] As shown in FIG. 1, the authentication device 500 for the user
20 authentication method according to various methods may include a user terminal 100 and an authentication server 200.

[0023] The user terminal 100 may be connected with the authentication
server 200 over a wired and wireless Internet network. A dedicated application
program (hereinafter referred to as “dedicated app”) for user authentication provided
25 from the authentication server 200 may be installed in the user terminal 100. The

user terminal 100 may include a smartphone, a tablet, a personal digital assistant (PDA), and the like, and may also include a mobile terminal which is well known to those skilled in the art. Further, the user terminal 100 may include a desktop personal computer (PC), a laptop, a terminal for thin client, a terminal for zero-client, and the like. Herein, the terminal for thin client may be called a business terminal designed to manage all business at a central server connected thereto over a network in a state where it mounts only essential hardware devices such as a central processing unit (CPU) and a memory. The terminal for zero client may play a role as a terminal, in which it is unnecessary for PC body itself since all of essential components such as a memory are removed, which connects to only a server to process all business at the server.

[0024] In an embodiment, the user terminal 100 may be referred to as all terminals may perform wired and wireless communication which may be used by users. If necessary for explicit classification, a mobile terminal including a smartphone, a tablet, and a PDA may be referred to as a first user terminal and each of a desktop PC, a laptop, a terminal for thin client, and a terminal for zero-client may be referred to as a second user terminal. A reference denotation is used as the same numeral '100'.

[0025] The authentication server 200 may include a server which is used for an authentication procedure such as user authentication at a certificate authority such as a financial institution and may include an authentication server which is well known to those skilled in the art.

[0026] Numbers such as an authentication number and a password for authentication, a unique key, an authentication key, authentication information, and the like used below may be combinations of a character, a special character, a

numeral, and various symbols. It may be apparent that the numbers, the unique key, the authentication key, the authentication information, and the like do not mean simple combinations of only numerals. The numbers, the unique key, the authentication key, the authentication information, and the like may refer to encrypted information or information which is not encrypted.

[0027] Further, hereinafter, various components performed in the user terminal 100 may be components performed by a dedicated app installed in the user terminal 100. Thus, to be performed by the user terminal 100 may mean to be performed by the dedicated app installed in the user terminal 100.

[0028] Further, the term ‘certain criteria’ are used at a plurality locations of the specification. Such certain criteria means there are any criteria or predetermined criteria and do not mean the same terms have the same criteria as each other although the same terms are used at a plurality of locations. Thus, if the term ‘certain criteria’ used herein is used at the plurality of locations, except if specifically noted, it does not mean the same criteria as each other. For example, there are a description of being extracted by certain criteria from a first common authentication key and a description of being extracted by certain criteria from a server authentication key, the certain criteria extracted from the first common authentication key and the certain criteria extracted from the server authentication key do not mean the same criteria as each other. In this case, the certain criteria and the certain criteria are the same as each other, but it is common that they have different criteria.

[0029] Hereinafter, a description will be given of a user authentication method according to embodiments using the user terminal 100 and the authentication server 200 which are basic components.

[0030] FIG. 2 is a signal sequence diagram illustrating a user authentication method according to an embodiment.

[0031] As shown in FIG. 2, a user authentication method according to an embodiment may be started for a user to download and install a dedicated app in a user terminal 100 for user registration. The user registration may be performed in a process of installing the dedicated app and may be performed through a separate process of registering the user after the dedicated app is installed.

[0032] If the user enters user information and a private password for the user registration using the user terminal 100 in step S102, in step S104, the user terminal 100 may generate a first common authentication key by combining the private password entered by the user and a mechanical unique key of the user terminal 100 and encrypting the combined information. Herein, the mechanical unique key of the user terminal 100 may include, for example, a serial number, a universal subscriber identity module (USIM) number, or the like. In addition, the mechanical unique key of the user terminal 100 may include various unique numbers and the like assigned to distinguish the user terminal 100.

[0033] An extraction value extracted from certain criteria from the mechanical unique key of the user terminal 100 or a user phone number may be further added as a component to the first common authentication key. In other words, the first common authentication key may be generated by combining the private password, the mechanical unique key of the user terminal 100, and the extraction value extracted by the certain criteria from the mechanical unique key of the user terminal 100 or the user phone number and encrypting the combined information. The extraction value extracted by the certain criteria from the mechanical unique key of the user terminal 100 or the user phone number may be extracted by certain

criteria (e.g., criteria of extracting even-numbered or odd-numbered digital values from a first digit and sequentially arranging the extracted digital values, criteria of extracting and arranging even numbers, criteria of extracting and arranging odd numbers, or criteria of adding or subtracting a specific numeral to or from each digit value and arranging the added or subtracted digit values) which are predetermined criteria from, for example, the mechanical unique key of the user terminal or the user phone number, which has a structure where a plurality of numerals are arranged.

[0034] The first common authentication key may be generated in the form of a hash encryption value and may be generated by being encrypted using an encryption technology which is well known to those skilled in the art.

[0035] In step S106, the user terminal 100 may transmit the first common authentication key together with the user information to the authentication server 200.

[0036] In step S202, the authentication server 200 may match the first common authentication key transmitted from the user terminal 100 with the user information to register and store the first common authentication key together with the user information. Thus, the process of registering the user may be completed.

[0037] In the related art, if user registration is completed, in general, an authentication server stores a private password. However, according to an embodiment, the authentication server 200 or the user terminal 100 does not store a password, and the authentication server 200 stores only the first common authentication key. Thus, if the user forgets a private password or if the private password flows out, the user terminal 100 may transmit a first common authentication key including a new password to the authentication server 200 through a new registration procedure to register the first common authentication key in the authentication server 200. If the first common authentication key flows out through

hacking and the like, a certificate authority may simply correspond to the outflow by changing extraction criteria of the extraction value extracted by the certain criteria from the mechanical unique key of the user terminal 100 or the user phone number, allowing the user terminal 100 to generate a new first common authentication key,
5 and registering the newly generated first common authentication key.

[0038] In step S204, the authentication server 200 may first generate a server authentication key by combining an embedded unique key of the certificate authority with the first common authentication key and encrypting the combined information and generating first server authentication information synchronized with a time value
10 by calculating a one time password (OTP) by using the server authentication key as an operation key. The first server authentication information may be independently generated irrespective of another procedure after the first common authentication key is registered. In other words, the first server authentication information may be enough to be generated within a time until first user authentication described below
15 is generated after the first common authentication key is registered. The first server authentication information is transmitted to the user terminal 100 at the same time that it is generated, or at a necessary time after it is generated.

[0039] If the user enters the private password for authentication in step S108, in step S110, the user terminal 100 may generate a second common authentication
20 key in real time by combining the private password with the mechanical unique key of the user terminal 100 and encrypting the combined information. The second common authentication key may be generated in the form of a hash encryption value. In addition, the second common authentication key may be generated by being encrypted using an encryption technology which is well known to those skilled in the
25 art.

[0040] If the first common authentication key includes the extraction value extracted by the certain criteria from the mechanical unique key of the user terminal 100 or the user phone number, the extraction value extracted from the mechanical unique key of the user terminal 100 or the user phone number by the same criteria applied when the first common authentication key is generated may be included in the second common authentication key when the second common authentication key is generated. In other words, the method of generating the second common authentication key is the same as the method of generating the first common authentication key.

10 **[0041]** In contrast, the first common authentication key and the second common authentication key may be generated by a method different from the above-mentioned method.

[0042] As an example, to generate the first common authentication key, the user terminal 100 may sequentially extract m (m is a natural number) extraction values by the certain criteria from the mechanical unique key of the user terminal 100 or the user phone number and may combine the private password and the mechanical unique key of the user terminal 100 to each of the extraction values, thus generating corresponding m common authentication keys. Next, the user terminal 100 may transmit the m common authentication keys to the authentication server 200.

20 **[0043]** The authentication server 200 may select one of the m common authentication keys based on predetermined criteria and may register the selected common authentication key as a first common authentication key. For example, if there are criteria in which the authentication server 200 selects a common authentication key corresponding to a first extraction value among the extraction values and registers the selected common authentication key as the first common

authentication key, unless there are different criteria, the common authentication key corresponding to the first extraction value may be registered as the first common authentication key. However, if there is an authentication key duplicated by the common authentication key among authentication keys registered in the authentication server 200 for another authentication or authentication of another person, to exclude duplication, a common authentication key corresponding to a second extraction value corresponding to a subsequent order or a subsequent degree among the common authentication keys may be selected and registered as the first common authentication key. If there is duplication in the common authentication key corresponding to the second extraction value, a common authentication key corresponding to an extraction value of an order where there is no duplication and may be registered as the first common authentication key.

[0044] If there are other criteria, a common authentication key selected based on the criteria may be registered as the first common authentication key. For example, if there are criteria in which 10 common authentication keys are generated and a common authentication key corresponding to a 5th extraction value is selected, the common authentication key may be selected and registered as the first common authentication key. If there is duplication, a common authentication key corresponding to a subsequent extraction value may be selected and registered as the first common authentication key, or a common authentication key may be selected and registered as the first common authentication key based on other criteria if there are the other criteria.

[0045] The authentication server 200 may provide order value information of the registered first common authentication key or calculation information about the order value to the user terminal 100. If there are previously promised selection

criteria or if the user terminal 100 knows the order value information of the first common authentication key, the process of transmitting the order value information or the calculation information about the order value may be omitted.

[0046] The authentication server 200 may transmit the order value information of the first common authentication key or the calculation information about the order value, included in the first server authentication information or to be independent of each other.

[0047] Herein, if the authentication server 200 transmits the order value information of the first common authentication key or the calculation information about the order value, included in the first authentication information, the first server authentication information should be transmitted to the user terminal 100 before the user terminal 100 generates the second common authentication key.

[0048] The order value information of the first common authentication key may mean information about whether the first common authentication key registered in the authentication server 200 is a common authentication key corresponding to an i th extraction value among m (m is a natural number) common authentication keys or order information of an extraction value included in the first common authentication key among the m extraction values.

[0049] In this case, to generate the second common authentication key, the user terminal 100 may sequentially extract the m extraction values by the certain criteria (e.g., the same criteria as being applied when the first common authentication key is generated) from the mechanical unique key of the user terminal 100 or the user phone number and may select an extraction value corresponding to the order value provided from the authentication server 200 among the extraction values, thus generating the second common authentication key.

[0050] In contrast, the user terminal 100 may extract the extraction corresponding to the order value by certain criteria from the mechanical unique key of the user terminal 100 or the user phone number to generate the second common authentication key. Thus, the second common authentication key may be generated
5 by additionally including the extraction value corresponding to the order value in the private password and the mechanical unique key of the user terminal 100.

[0051] In step S112, the user terminal 100 may generate first user authentication information using the second common authentication key. The description is given above for generating the first server authentication information
10 corresponding to the first user authentication information.

[0052] The user terminal 100 may first generate a user authentication key by combining a unique key of a certificate authority with the second common authentication key and encrypting the combined information and may generate first user authentication information synchronized with a time value by calculating an
15 OTP by using the user authentication key as an operation key. Herein, the unique key of the certificate authority may be provided to the user terminal 100 when the dedicated app is installed in the user terminal 100, or may be provided to the user terminal 100 after it is updated before an authentication procedure is started.

[0053] Herein, an extraction value extracted by certain criteria from the
20 second common authentication key may be further added as a component to the user authentication key. An extraction value extracted by certain criteria from the first common authentication may be further added as a component to the server authentication key. In this case, the extraction value of the second common authentication key added to the user authentication or the extraction value of the first
25 common authentication key added to the server authentication key may be an

extraction extracted from the first common authentication or the second common authentication key based on the same criteria.

[0054] An extraction value extracted by certain criteria from the user authentication key may be further added as a component to the operation key for
5 generating the first user authentication information. An extraction value extracted by certain criteria from the server authentication key may be further added as a component to the operation key for generating the first server authentication information. In this case, the extraction value extracted from the user authentication key and the extraction value extracted from the server authentication key may be
10 extraction values extracted by the same criteria. It is obvious that the methods of generating the first user authentication information and the first server authentication information should be the same as each other and the result values are identical to each other.

[0055] If the user terminal 100 transmits the first user authentication
15 information to the authentication server 200 in step S114, in step S206, the authentication server 200 may perform user authentication based on whether authentication information are identical to each other, that is, whether the first user authentication information and the first server authentication information are identical to each other. The first user authentication information may be entered by
20 the user to be manually transmitted. The first user authentication information may be automatically transmitted. The first user authentication information may be automatically transmitted by a transmission instruction of the user.

[0056] Herein, one or a plurality of user terminals connected with the authentication server 200 may be used as the user terminal 100. For example, the
25 first user terminal 100 may proceed with a procedure of registering a first common

authentication key and the like and the second user terminal 100 may proceed with an authentication procedure, and vice versa. Also, in case of an authentication procedure, first user authentication information may be generated by the first user terminal 100, and input or transmission of the first user authentication information
5 may be performed by the second user terminal 100. In addition, a plurality of user terminals 100 may be used in various procedures.

[0057] The user may verify whether the authentication server 200 is true, whether an access web page connected to the authentication server 200 is true, or whether a service provider or a certificate authority which provides an authentication
10 server is true by comparing the first user authentication information with the first server authentication information through the user terminal 100. In the related art, although there are many examples of configuring a web page similar to an access web page of a certificate authority and confusing users, there are no proper countermeasures to the examples. In an embodiment, the user may verify whether a
15 certificate authority (or a service provider) is true to address the above-mentioned problem.

[0058] For this purpose, if the first server authentication information is generated, in step S205, the authentication server 200 may display the first server authentication information through the access web page or may transmit the first
20 server authentication information to the user terminal 100. If the first server authentication information is displayed or transmitted, the user terminal 100 may determine whether the authentication server 200 is true or whether the access web page is true by comparing the first server authentication information with the first user authentication information. In other words, the user terminal 100 may verify
25 whether the authentication server 200 is true, whether an access web page connected

to the authentication server 200 is true, or whether a service provider or a certificate authority which provides an authentication server is true.

[0059] Herein, if the first server authentication information is transmitted to the user terminal 100 in advance before the second common authentication key is generated, the user terminal 100 may perform authentication server authentication using the first server authentication information transmitted in advance without the necessity of retransmitting or separately transmitting the first server authentication information.

[0060] In an embodiment, the user terminal 100 may perform certificate authority authentication or authentication server authentication of determining whether a certificate authority or the authentication server 200 is true through whether the first server authentication information is identical to the first user authentication information by comparing the first server authentication information with the first user authentication information. The authentication server 200 may perform user authentication through whether the first server authentication is identical to the first user authentication information by comparing the first server authentication information with the first user authentication information.

[0061] Herein, the authentication procedures S205 and S116 of authenticating the authentication server 200 and the user authentication procedures S114 and S206 may be performed at the same time. If authentication is verified after the authentication procedures of authenticating the authentication server 200 is first performed, the user authentication procedures S114 and S206 may be performed.

[0062] FIG. 3 is a signal sequence diagram illustrating a user authentication method according to another embodiment.

[0063] As shown in FIG. 3, a user authentication method according to another embodiment may be started for a user to download and install a dedicated app in a user terminal 100 for user registration. The user registration may be performed in a process of installing the dedicated app and may be performed through
5 a separate process of registering the user after the dedicated app is installed.

[0064] If the user enters user information and a private password for the user registration using the user terminal 100 in step S122, in step S124, the user terminal 100 may generate a first common authentication key by combining the private password entered by the user and a mechanical unique key of the user terminal 100
10 and encrypting the combined information. Herein, the mechanical unique key of the user terminal 100 may include, for example, a serial number, a USIM number, or the like. In addition, the mechanical unique key of the user terminal 100 may include various unique numbers and the like assigned to distinguish the user terminal 100.

[0065] An extraction value extracted from certain criteria from the
15 mechanical unique key of the user terminal 100 or a user phone number may be further added as a component to the first common authentication key. In other words, the first common authentication key may be generated by combining the private password, the mechanical unique key of the user terminal 100, and the extraction value extracted by the certain criteria from the mechanical unique key of the user
20 terminal 100 or the user phone number and encrypting the combined information. The extraction value extracted by the certain criteria from the mechanical unique key of the user terminal 100 or the user phone number may be extracted by certain criteria (e.g., criteria of extracting even-numbered or odd-numbered digital values from a first digit and sequentially arranging the extracted digital values, criteria of
25 extracting and arranging even numbers, criteria of extracting and arranging odd

numbers, or criteria of adding or subtracting a specific numeral to or from each digit value and arranging the added or subtracted digit values) which are predetermined criteria from, for example, the mechanical unique key of the user terminal 100 or the user phone number, which has a structure where a plurality of numerals are arranged.

5 **[0066]** The first common authentication key may be generated in the form of a hash encryption value and may be generated by being encrypted using an encryption technology which is well known to those skilled in the art.

[0067] In step S126, the user terminal 100 may transmit the first common authentication key together with the user information to the authentication server 200.

10 **[0068]** In step S222, the authentication server 200 may match the first common authentication key transmitted from the user terminal 100 with the user information to register and store the first common authentication key together with the user information. Thus, the process of registering the user may be completed.

[0069] In the related art, if user registration is completed, in general, an authentication server stores a private password. However, according to another embodiment, the authentication server 200 or the user terminal 100 does not store a password, and the authentication server 200 stores only the first common authentication key. Thus, if the user forgets a private password or if the private password flows out, the user terminal 100 may transmit a first common authentication key including a new password to the authentication server 200 through a new registration procedure to register the first common authentication key in the authentication server 200. If the first common authentication key flows out through hacking and the like, a certificate authority may simply correspond to the outflow by changing extraction criteria of the extraction value extracted by the certain criteria from the mechanical unique key of the user terminal 100 or the user phone number,

allowing the user terminal 100 to generate a new first common authentication key, and registering the newly generated first common authentication key.

[0070] In step S223, the authentication server 200 may first generate a server authentication key by combining an embedded unique key of the certificate authority with the first common authentication key and encrypting the combined information and may generate first server authentication information synchronized with a time value by calculating an OTP by using the server authentication key as an operation key. The first server authentication information may be independently generated irrespective of another procedure after the first common authentication key is registered. In other words, the first server authentication information may be enough to be generated within a time until first user authentication described below is generated after the first common authentication key is registered.

[0071] Further, if it is necessary to transmit the first server authentication information to the user terminal 100, a time when the first server authentication information is transmitted may vary if necessary. The first server authentication information is transmitted to the user terminal 100 at the same time that it is generated, or at a necessary time after it is generated. In FIG. 3, an embodiment is exemplified as the first server authentication information is transmitted to the user terminal 100 at the same time that it is generated. In step S225, the first server authentication information may be transmitted to the user terminal 100 at the same time that it is generated. In addition, the first server authentication information may be transmitted at a different time. For example, the first server authentication information may be transmitted at a time close to a time when the first user authentication information is generated or may be transmitted after the first user authentication information is generated.

[0072] If the user enters the private password using the user terminal 100 for authentication in step S128, in step 128, the user terminal 100 may measure a gap time value. In step S130, the measured gap time value may be transmitted to the authentication server 200.

5 **[0073]** The gap time value may refer to a time value in which a time taken for the user to enter the private password for authentication is measured every $1/n$ (n is a positive real number) seconds. Herein, the $1/n$ seconds may refer to a time unit of a range which may be divided in hard or software of the user terminal 100. For example, it may be expressed that it takes 10 seconds on a second basis to enter a
10 private password from a first digit value to the last digit value. However, if the time taken to enter the private password is measured every $1/1000$ seconds, the measured value '10436' may be obtained. Alternatively, if the time taken to enter the private password is measured every $1/1000000$ seconds or every $1/10000000000$ seconds, the measured value including many numerals may be obtained.

15 **[0074]** Herein, if a time interval from a time when an input window for inputting the private password is displayed on a screen to a time when a first digit value of the private password is entered is defined as a first time interval and if a time interval from a time when the last digit value of the private password is entered to a time when a signal of an input key (or an enter key) for providing notification
20 that the input of the private password is completed is input is defined as a second time interval, the gap time value may be a time measurement value from one time in the first time interval to one time in the second time interval.

[0075] If receiving the gap time value from the user terminal 100, in step S227, the authentication server 200 may match the gap time value with the user
25 information, the first common authentication key, and the like to store and register

the gap time value together with the user information, the first common authentication key, and the like.

[0076] As the private password is entered, in step S132, the user terminal 100 may generate a second common authentication key in real time by combining the private password with the mechanical unique key of the user terminal 100 and encrypting the combined information. The second common authentication key may be generated in the form of a hash encryption value. In addition, the second common authentication key may be generated by being encrypted using an encryption technology which is well known to those skilled in the art.

[0077] In this case, if the first common authentication key includes the extraction value extracted by the certain criteria from the mechanical unique key of the user terminal 100 or the user phone number, the extraction value extracted from the mechanical unique key of the user terminal 100 or the user phone number by the same criteria applied when the first common authentication key is generated may be included in the second common authentication key when the second common authentication is generated. In other words, the method of generating the second common authentication key is the same as the method of generating the first common authentication key.

[0078] In contrast, the first common authentication key and the second common authentication key may be generated by a method different from the above-mentioned method.

[0079] As an example, to generate the first common authentication key, the user terminal 100 may sequentially extract m (m is a natural number) extraction values by the certain criteria from the mechanical unique key of the user terminal 100 or the user phone number and may combine the private password and the

mechanical unique key of the user terminal 100 to each of the extraction values, thus generating corresponding m common authentication keys. Next, the user terminal 100 may transmit the m common authentication keys to the authentication server 200.

[0080] The authentication server 200 may select one of the m common

5 authentication keys based on predetermined criteria and may register the selected common authentication key as a first common authentication key. For example, if there are criteria in which the authentication server 200 selects a common authentication key corresponding to a first extraction value among the extraction values and registers the selected common authentication key as the first common
10 authentication key, unless there are different criteria, the common authentication key corresponding to the first extraction value may be registered as the first common authentication key. However, if there is an authentication key duplicated by the common authentication key among authentication keys registered in the authentication server 200 for another authentication or authentication of another
15 person, to exclude duplication, a common authentication key corresponding to a second extraction value corresponding to a subsequent order or a subsequent degree among the common authentication keys may be selected and registered as the first common authentication key. If there is duplication in the common authentication key corresponding to the second extraction value, a common authentication key
20 corresponding to an extraction value of an order where there is no duplication and may be registered as the first common authentication key.

[0081] If there are other criteria, a common authentication key selected based on the criteria may be registered as the first common authentication key. For example, if there are criteria in which 10 common authentication keys are generated

25 and a common authentication key corresponding to a 5th extraction value is selected,

the common authentication key may be selected and registered as the first common authentication key. If there is duplication, a common authentication key corresponding to a subsequent extraction value may be selected and registered as the first common authentication key, or a common authentication key may be selected and registered as the first common authentication key based on other criteria if there are the other criteria.

[0082] The authentication server 200 may provide order value information of the registered first common authentication key or calculation information about the order value to the user terminal 100. If there are previously promised selection criteria or if the user terminal 100 knows the order value information of the first common authentication key, the process of transmitting the order value information or the calculation information about the order value may be omitted.

[0083] The authentication server 200 may transmit the order value information of the first common authentication key or the calculation information about the order value, included in the first server authentication information or to be independent of each other.

[0084] Herein, if the authentication server 200 transmits the order value information of the first common authentication key or the calculation information about the order value, included in the first authentication information, in step S225, the first server authentication information should be transmitted to the user terminal 100 before the user terminal 100 generates the second common authentication key.

[0085] The order value information of the first common authentication key may mean information about whether the first common authentication key registered in the authentication server 200 is a common authentication key corresponding to an i th extraction value among m (m is a natural number) common authentication keys or

order information of an extraction value included in the first common authentication key among the m extraction values.

[0086] In this case, to generate the second common authentication key, the user terminal 100 may sequentially extract the m extraction values by the certain criteria (e.g., the same criteria as being applied when the first common authentication key is generated) from the mechanical unique key of the user terminal 100 or the user phone number and may select an extraction value corresponding to the order value provided from the authentication server 200 among the extraction values, thus generating the second common authentication key.

[0087] In contrast, the user terminal 100 may extract the extraction value corresponding to the order value by certain criteria from the mechanical unique key of the user terminal 100 or the user phone number to generate the second common authentication key. Thus, the second common authentication key may be generated by additionally including the extraction value corresponding to the order value in the private password and the mechanical unique key of the user terminal 100.

[0088] In step S134, the user terminal 100 may generate first user authentication information using the second common authentication key. The description is given above for generating the first server authentication information corresponding to the first user authentication information.

[0089] The user terminal 100 may first generate a user authentication key by combining the unique key of the certificate authority with the second common authentication key and encrypting the combined information and may generate first user authentication information synchronized with a time value by calculating an OTP by using the user authentication key as an operation key. Herein, the unique key of the certificate authority may be provided to the user terminal 100 when the

dedicated app is installed in the user terminal 100, or may be provided to the user terminal 100 after it is updated before an authentication procedure is started.

[0090] Herein, an extraction value extracted by certain criteria from the second common authentication key may be further added as a component to the user authentication key. An extraction value extracted by certain criteria from the first common authentication may be further added as a component to the server authentication key. In this case, the extraction value of the second common authentication key added to the user authentication or the extraction value of the first common authentication key added to the server authentication key may be an extraction extracted from the first common authentication or the second common authentication key based on the same criteria.

[0091] An extraction value extracted by criteria from the user authentication key may be further added as a component to the operation key for generating the first user authentication information. An extraction value extracted by certain criteria from the server authentication key may be further added as a component to the operation key for generating the first server authentication information. In this case, the extraction value extracted from the user authentication key and the extraction value extracted from the server authentication key may be extraction values extracted by the same criteria. It is obvious that the methods of generating the first user authentication information and the first server authentication information should be the same as each other and the result values are identical to each other.

[0092] In such state, the user terminal 100 may transmit the first user authentication information to the authentication server 200. The authentication server 200 may perform primary user authentication by comparing the first user authentication information with the first server authentication information to

determine whether the first user authentication information is identical to the first server authentication information.

[0093] In other words, if the user terminal 100 transmits the first user authentication information to the authentication server 200, the authentication server
5 200 may perform primary user authentication based on whether authentication information are identical to each other, that is, whether the first user authentication information and the first server authentication information are identical to each other. The first user authentication information may be entered by the user to be manually transmitted. The first user authentication information may be automatically
10 transmitted without a specific instruction or mention. The first user authentication information may be automatically transmitted by a transmission instruction of the user.

[0094] Herein, one or a plurality of user terminals connected with the authentication server 200 may be used as the user terminal 100. For example, the
15 first user terminal 100 may proceed with a procedure of registering a first common authentication key and the like and the second user terminal 100 may proceed with an authentication procedure, and vice versa. Also, in case of an authentication procedure, first user authentication information may be generated by the first user terminal 100, and input or transmission of the first user authentication information
20 may be performed by the second user terminal 100. In addition, the plurality of user terminals 100 may be used in various procedures.

[0095] The process of performing the primary user authentication by comparing the first user authentication information with the first server authentication information to determine whether the first user authentication

information is identical to the first server authentication information may be elected and omitted if necessary.

[0096] The user may verify whether the authentication server 200 is true, whether an access web page connected to the authentication server 200 is true, or
5 whether a service provider or a certificate authority which provides an authentication server is true by comparing the first user authentication information with the first server authentication information through the user terminal 100.

[0097] For this purpose, if the first server authentication information is generated, in step S225, the authentication server 200 may display the first server
10 authentication information through the access web page or may transmit the first server authentication information to the user terminal 100. If the first server authentication information is displayed or transmitted, in step S135, the user terminal 100 may determine whether the authentication server 200 is true or whether the access web page is true by comparing the first server authentication information with
15 the first user authentication information. In other words, the user terminal 100 may perform authentication server authentication for verifying whether the authentication server 200 is true, whether an access web page connected to the authentication server 200 is true, or whether a service provider or a certificate authority which provides an authentication server is true.

[0098] Herein, if the first server authentication information is transmitted to
20 the user terminal 100 in advance before the second common authentication key is generated in step S225, the user terminal 100 may perform authentication server authentication using the first server authentication information transmitted in advance without the necessity of retransmitting or separately transmitting the first
25 server authentication information.

[0099] As a result, the user terminal 100 may perform certificate authority authentication or authentication server authentication of determining whether a certificate authority or the authentication server 200 is true through whether the first server authentication information is identical to the first user authentication
5 information by comparing the first server authentication information with the first user authentication information. The authentication server 200 may perform user authentication through whether the first server authentication is identical to the first user authentication information by comparing the first server authentication information with the first user authentication information.

10 **[00100]** Herein, the authentication procedures S225 and S135 of authenticating the authentication server 200 and the user authentication procedures may be performed at the same time. If authentication is verified after the authentication procedures of authenticating the authentication server 200 is first performed, the user authentication procedures may be performed. As one of the user
15 authentication and the authentication server authentication is selected, an authentication process may be performed. In FIG. 3, an embodiment is exemplified as only authentication of the authentication server 200 is performed.

[00101] The user terminal 100 may generate an operation key by including a variety of authentication information, an authentication key, and at least one of
20 extraction values in the gap time value or a gap time key which is a numeral value extracted by certain criteria from the gap time value. Also, in step S136, the user terminal 100 may generate second user authentication information synchronized with a time value using the operation key.

[00102] For example, the user terminal 100 may generate an operation key by
25 additionally combining at least one selected among the first user authentication

information, an extraction value extracted by certain criteria from the first user authentication information, the user authentication key, an extraction value extracted by certain criteria from the user authentication key, the second common authentication key, and an extraction value extracted by certain criteria from the second common authentication key with the gap time value or the gap time key and may generate second user authentication information synchronized with a time value by calculating an OTP using the operation key.

[00103] The authentication server 200 may generate an operation key by including a variety of authentication information, an authentication key, and at least one of extraction values in the gap time value or a gap time key which is a numeral value extracted by certain criteria from the gap time value. Also, in step S228, the authentication server 200 may generate second server authentication information using the operation key.

[00104] Herein, the gap time value used in the authentication server 200 may refer to a gap time value which is transmitted from the user terminal 100 and is previously stored in the authentication server 200. Also, the gap time key used in the user terminal 100 or the gap time key used in the authentication server 200 may be an extraction value separately extracted by the same extraction criteria.

[00105] For example, in step S228, the authentication server 200 may generate an operation key by additionally combining at least one selected among the first server authentication information, an extraction value extracted by certain criteria from the first server authentication information, the server authentication key, an extraction value extracted by certain criteria from the server authentication key, the first common authentication key, and an extraction value extracted by certain criteria from the first common authentication key with the gap time value or the gap time key

and may generate second server authentication information synchronized with a time value to correspond to second user authentication information by calculating an OTP using the operation key.

[00106] In detail, the second user authentication information may be generated
5 by calculating an OTP using the operation key generated by combining the extraction value extracted by the certain criteria from the first user authentication information and the user authentication key with the gap time value or the gap time key. The second server authentication information may be generated by calculating an OTP using the operation key generated by combining the extraction value extracted by the
10 certain criteria from the first sever authentication information and the server authentication key with the gap time value or the gap time key.

[00107] As another example, the second user authentication information may be generated by calculating an OTP using the operation key generated by combining the user authentication key and the extraction value extracted by the certain criteria
15 from the user authentication key with the gap time value or the gap time key. The second server authentication information may be generated by calculating an OTP using the operation key generated by combining the sever authentication key and the extraction value extracted by the certain criteria from the server authentication key with the gap time value or the gap time key.

20 **[00108]** In addition, the second user authentication information and the second server authentication information may be generated by various combinations.

[00109] if the user terminal 100 transmits the second user authentication information to the authentication server 200 in step S138, in step S230, the authentication server 200 may perform user authentication based on whether
25 authentication information are identical to each other, that is, whether the second

user authentication information and the second server authentication information are identical to each other. The second user authentication information may be entered by the user to be manually transmitted. The second user authentication information may be automatically transmitted. The second user authentication information may be automatically transmitted by a transmission instruction of the user.

[00110] Herein, the second user authentication information may be generated by the first user terminal 100, and input or transmission of the second user authentication information may be performed through the second user terminal 100. In addition, the plurality of user terminals 100 may be used in various procedures.

[00111] According to another embodiment, the primary user authentication may be performed using the first server authentication information and the first user authentication information, and the secondary user authentication information may be performed using the second server authentication information and the second user authentication information. Also, the first server authentication information and the first user authentication information may be used for authentication of the authentication server 200 (e.g., authentication for verifying where a web page, a certificate authority, or an authentication service provider is true), and the second server authentication information and the second user authentication may be used for user authentication.

[00112] The primary user authentication and the secondary user authentication may be performed in such a manner as to perform the primary user authentication and perform the secondary user authentication if the second user authentication information and the second server authentication information are generated. In another manner, after the second user authentication information and the second server authentication information are generated, the primary user authentication and

the second user authentication may be performed in such a manner as to be sequentially performed.

[00113] Further, if the first server authentication information and the first user authentication information is used for authentication of the authentication server 200 (e.g., authentication for verifying where a web page, a certificate authority, or an authentication service provider is true) and if the second server authentication information and the second user authentication is used for user authentication, the second user authentication information and the second server authentication may be generated after authentication of the authentication server 200 is performed. Thus, the user authentication may be performed using the second user authentication information and the second server authentication. In contrast, after the second server authentication information and the second user authentication information are generated, authentication of the authentication server 200 using the first server authentication information and the first user authentication information may be performed and user authentication using the second server authentication information and the second user authentication information may be sequentially performed.

[00114] FIG. 4 is a signal sequence diagram illustrating a user authentication method according to another embodiment.

[00115] As shown in FIG. 4, a user authentication method according to another embodiment may be started for a user to download and install a dedicated app in a user terminal 100 for user registration. The user registration may be performed in a process of installing the dedicated app and may be performed through a separate process of registering the user after the dedicated app is installed.

[00116] If the user enters user information and a private password for the user registration through the user terminal 100 in step S152, in step S154, the user

terminal 100 may generate a first common authentication key by combining the private password entered by the user and a mechanical unique key of the user terminal 100 and encrypting the combined information. Herein, the mechanical unique key of the user terminal 100 may include, for example, a serial number, a
5 USIM number, or the like. In addition, the mechanical unique key of the user terminal 100 may include various unique numbers and the like assigned to distinguish the user terminal 100.

[00117] An extraction value extracted from certain criteria from the mechanical unique key of the user terminal 100 or a user phone number may be
10 further added as a component to the first common authentication key. In other words, the first common authentication key may be generated by combining the private password, the mechanical unique key of the user terminal 100, and the extraction value extracted by the certain criteria from the mechanical unique key of the user terminal 100 or the user phone number and encrypting the combined information.

[00118] The extraction value extracted by the certain criteria from the mechanical unique key of the user terminal 100 or the user phone number may be
15 extracted by certain criteria (e.g., criteria of extracting even-numbered or odd-numbered digital values from a first digit and sequentially arranging the extracted digital values, criteria of extracting and arranging even numbers, criteria of
20 extracting and arranging odd numbers, or criteria of adding or subtracting a specific numeral to or from each digit value and arranging the added or subtracted digit values) which are predetermined criteria from, for example, the mechanical unique key of the user terminal or the user phone number, which has a structure where a plurality of numerals are arranged.

[00119] The first common authentication key may be generated in the form of a hash encryption value and may be generated by being encrypted using an encryption technology which is well known to those skilled in the art.

[00120] In step S156, the user terminal 100 may transmit the first common authentication key together with the user information to the authentication server 200.

[00121] In step S252, the authentication server 200 may match the first common authentication key transmitted from the user terminal 100 with the user information to register and store the first common authentication key together with the user information. Thus, the process of registering the user may be completed.

[00122] In the related art, if user registration is completed, in general, an authentication server stores a private password. However, according to another embodiment, the authentication server 200 or the user terminal 100 does not store a password, and the authentication server 200 stores only the first common authentication key. Thus, if the user forgets a private password or if the private password flows out, the user terminal 100 may transmit a first common authentication key including a new password to the authentication server 200 through a new registration procedure to register the first common authentication key in the authentication server. If the first common authentication key flows out through hacking and the like, a certificate authority may simply correspond to the outflow by changing extraction criteria of the extraction value extracted by the certain criteria from the mechanical unique key of the user terminal 100 or the user phone number, allowing the user terminal 100 to generate a new first common authentication key, and registering the newly generated first common authentication key.

[00123] If the user enters the private password using the user terminal 100 for authentication in step S158, in step 158, the user terminal 100 may measure a gap

time value. In step S160, the measured gap time value may be transmitted to the authentication server 200.

[00124] The gap time value may refer to a time value in which a time taken for the user to enter a private password for authentication is measured every $1/n$ (n is a positive real number) seconds. Herein, the $1/n$ seconds may refer to a time unit of a range which may be divided in hard or software of the user terminal 100. For example, it may be expressed that it takes 10 seconds on a second basis to enter a private password from a first digit value to the last digit value. However, if the time taken to enter the private password is measured every $1/1000$ seconds, the measured value '10436' may be obtained. Alternatively, if the time taken to enter the private password is measured every $1/1000000$ seconds or every $1/10000000000$ seconds, the measured value including many numerals may be obtained.

[00125] Herein, if a time interval from a time when an input window for entering the private password is displayed on a screen to a time when a first digit value of the private password is entered is defined as a first time interval and if a time interval from a time when the last digit value of the private password is entered to a time when a signal of an input key (or an enter key) for providing notification that the input of the private password is completed is input is defined as a second time interval, the gap time value may be a time measurement value from one time in the first time interval to one time in the second time interval.

[00126] If receiving the gap time value from the user terminal 100, in step S254, the authentication server 200 may match the gap time value with the user information, the first common authentication key, and the like to store and register the gap time value together with the user information, the first common authentication key, and the like.

[00127] As the private password is entered, in step S162, the user terminal 100 may generate a second common authentication key in real time by combining the private password with the mechanical unique key of the user terminal 100 and encrypting the combined information. The second common authentication key may
5 be generated in the form of a hash encryption value. In addition, the second common authentication key may be generated by being encrypted using an encryption technology which is well known to those skilled in the art.

[00128] In this case, if the first common authentication key includes the extraction value extracted by the certain criteria from the mechanical unique key of
10 the user terminal 100 or the user phone number, the extraction value extracted from the mechanical unique key of the user terminal 100 or the user phone number by the same criteria applied when the first common authentication key is generated may be included in the second common authentication key when the second common authentication is generated. In other words, the method of generating the second
15 common authentication key is the same as the method of generating the first common authentication key.

[00129] In contrast, the first common authentication key and the second common authentication key may be generated by a method different from the above-mentioned method.

20 **[00130]** As an example, to generate the first common authentication key, the user terminal 100 may sequentially extract m (m is a natural number) extraction values by the certain criteria from the mechanical unique key of the user terminal 100 or the user phone number and may combine the private password and the mechanical unique key of the user terminal 100 to each of the extraction values, thus

generating corresponding m common authentication keys. Next, the user terminal 100 may transmit the m common authentication keys to the authentication server 200.

[00131] The authentication server 200 may select one of the m common authentication keys based on predetermined criteria and may register the selected common authentication key as a first common authentication key. For example, if there are criteria in which the authentication server 200 selects a common authentication key corresponding to a first extraction value among the extraction values and registers the selected common authentication key as the first common authentication key, unless there are different criteria, the common authentication key corresponding to the first extraction value may be registered as the first common authentication key. However, if there is an authentication key duplicated by the common authentication key among authentication keys registered in the authentication server 200 for another authentication or authentication of another person, to exclude duplication, a common authentication key corresponding to a second extraction value corresponding to a subsequent order or a subsequent degree among the common authentication keys may be selected and registered as the first common authentication key. If there is duplication in the common authentication key corresponding to the second extraction value, a common authentication key corresponding to an extraction value of an order where there is no duplication and may be registered as the first common authentication key.

[00132] If there are other criteria, a common authentication key selected based on the criteria may be registered as the first common authentication key. For example, if there are criteria in which 10 common authentication keys are generated and a common authentication key corresponding to a 5th extraction value is selected, the common authentication key may be selected and registered as the first common

authentication key. If there is duplication, a common authentication key corresponding to a subsequent extraction value may be selected and registered as the first common authentication key, or a common authentication key may be selected and registered as the first common authentication key based on other criteria if there are the other criteria.

[00133] The authentication server 200 may provide order value information of the registered first common authentication key or calculation information about the order value to the user terminal 100. If there are previously promised selection criteria or if the user terminal 100 knows the order value information of the first common authentication key, the process of transmitting the order value information or the calculation information about the order value may be omitted.

[00134] The authentication server 200 may transmit the order value information of the first common authentication key or the calculation information about the order value, included in the server authentication information or to be independent of each other.

[00135] Herein, if the authentication server 200 transmits the order value information of the first common authentication key or the calculation information about the order value, included in the authentication information, the server authentication information should be transmitted to the user terminal before the user terminal 100 generates the second common authentication key.

[00136] In this case, if the user terminal 100 transmits the gap time value to the authentication server 200, the authentication server 200 may immediately generate server authentication information. Herein, if transmitting the order value information of the first common authentication key or the calculation information about the order information, included in the server authentication information, the

user terminal 100 may progress in such a manner as to generate a second common authentication key using the order value information of the first common authentication key or the calculation information about the order value.

[00137] The order value information of the first common authentication key may mean information about whether the first common authentication key registered in the authentication server 200 is a common authentication key corresponding to an i th extraction value among m (m is a natural number) common authentication keys or order information of an extraction value included in the first common authentication key among the m extraction values.

[00138] In this case, to generate the second common authentication key, the user terminal 100 may sequentially extract the m extraction values by the certain criteria (e.g., the same criteria as being applied when the first common authentication key is generated) from the mechanical unique key of the user terminal 100 or the user phone number and may select an extraction value corresponding to the order value provided from the authentication server 200 among the extraction values, thus generating the second common authentication key.

[00139] In contrast, the user terminal 100 may extract the extraction value corresponding to the order value by certain criteria from the mechanical unique key of the user terminal 100 or the user phone number to generate the second common authentication key. Thus, the second common authentication key may be generated by including the extraction value corresponding to the order value in the private password and the mechanical unique key of the user terminal 100.

[00140] In step S164, the user terminal 100 may generate user authentication information using the second common authentication key and the gap time value. IN step S256, the authentication server 164 may generate server authentication

information using the first common authentication key and the gap time value. The description is given above for generating the first server authentication information corresponding to the first user authentication information.

[00141] In step S164, the user terminal 100 may first generate a user authentication key by combining a unique key of a certificate authority with the second common authentication key and encrypting the combined information and may generate user authentication information synchronized with a time value by calculating an OTP using an operation key generated by combining the user authentication key with the gap time value or a gap time key which is a numeral value extracted by certain criteria from the gap time value.

[00142] Herein, the unique key of the certificate authority may be provided to the user terminal 100 when the dedicated app is installed in the user terminal 100, or may be provided to the user terminal 100 after it is updated before an authentication procedure is started.

[00143] In step S256, the authentication server 200 may first generate a server authentication key by combining an embedded unique key of the certificate authority with the first common authentication key and encrypting the combined information and may generate server authentication information synchronized with a time value by calculating an OTP by using an operation key generated by combining the server authentication key with the gap time value or a gap time key which is a numeral value extracted by certain criteria from the gap time value.

[00144] Herein, the gap time value used in the authentication server 200 may refer to a gap time value which is transmitted from the user terminal 100 and is previously stored in the authentication server 200. Also, the gap time key used in the

user terminal 100 or the gap time key used in the authentication server 200 may be an extraction value separately extracted by the same extraction criteria.

[00145] An extraction value extracted by certain criteria from the second common authentication key may be further added as a component to the user authentication key. An extraction value extracted by certain criteria from the first common authentication may be further added as a component to the server authentication key. In this case, the extraction value of the second common authentication key added to the user authentication or the extraction value of the first common authentication key added to the server authentication key may be an extraction extracted from the first common authentication or the second common authentication key based on the same criteria.

[00146] An extraction value extracted by criteria from the user authentication key may be further added as a component to the operation key for generating the user authentication information. An extraction value extracted by certain criteria from the server authentication key may be further added as a component to the operation key for generating the server authentication information. In this case, the extraction value extracted from the user authentication key and the extraction value extracted from the server authentication key may be extraction values extracted by the same criteria.

[00147] In such state, in step S166, the user terminal 100 may transmit the user authentication information to the authentication server 200. In step S258, the authentication server 200 may perform user authentication by comparing the user authentication information with the server authentication information to determine whether the user authentication information is identical to the server authentication information.

[00148] In other words, if the user terminal 100 transmits the user authentication information to the authentication server 200, in step S258, the authentication server 200 may perform user authentication based on whether authentication information are identical to each other, that is, whether the user authentication information and the server authentication information are identical to each other. The user authentication information may be entered by the user to be manually transmitted. The user authentication information may be automatically transmitted. The user authentication information may be automatically transmitted by a transmission instruction of the user.

10 **[00149]** Herein, one or a plurality of user terminals connected with the authentication server 200 may be used as the user terminal 100. For example, the first user terminal 100 may proceed with a procedure of registering a first common authentication key and the like and the second user terminal 100 may proceed with an authentication procedure, and vice versa. Also, in case of an authentication procedure, user authentication information may be generated by the first user terminal 100, and input or transmission of the user authentication information may be performed by the second user terminal 100. In addition, the plurality of user terminals 100 may be used in various procedures.

[00150] According to embodiments, the user authentication may be performed using the gap time value or the gap time key which does not attempt or are not defined in the related art. Other than the above-mentioned embodiments, components for generating authentication information for user authentication using the gap time value or gap time key and the private password may be changed in various manners by adding various components to the components. Also, the gap time key or the gap time value may be added to the method of generating

authentication information, well known to those skilled in the art. Such components may be included in embodiments.

5 **[00151]** As described above, according to various embodiments, the authentication method may enhance security by simply corresponding to an outflow of a password or other personal information when the password or personal information flows out and may easily perform user authentication. Further, the authentication method may perform user authentication by checking whether an authentication server, a certificate authority, a web site, or the like for authentication is true and ensuring integrity and exclusiveness.

10 **[00152]** While the inventive concept has been described with reference to exemplary embodiments, it will be apparent to those skilled in the art that various changes and modifications may be made without departing from the spirit and scope of the inventive concept. Therefore, it should be understood that the above embodiments are not limiting, but illustrative.

WHAT IS CLAIMED IS:

1. A user authentication method comprising:

a user registering step of generating, by a user terminal, a first common authentication key obtained by combining a personal password input by a user and a mechanical unique key of the user terminal and providing the first common authentication key to an authentication server, and matching, by the authentication server, the first common authentication key with user information and registering the first common authentication key;

a step of generating, by the authentication server, first server authentication information, based on a server authentication key generated by combining a unique key of an authentication institute and the first common authentication key;

a step of, if the personal password for authentication is input by the user, generating, by the user terminal, a second common authentication key obtained by combining the personal password and a mechanical unique key of the user terminal;

a step of generating, by the user terminal, first user authentication information, based on a user authentication key generated by combining the unique key of the authentication institute and the second common authentication key; and

a comparison/determination step of determining whether the first server authentication information and the first user authentication information coincide with each other.

2. The user authentication method of claim 1, wherein the user registering step and the second common key generating step are performed by a dedicated application installed in the user terminal.

5 3. The user authentication method of claim 1, wherein an extraction value extracted from the mechanical unique key of the user terminal or a phone number of the user by a specific reference is added to the first common authentication key and the second common authentication key.

10 4. The user authentication method of claim 3, further comprising:
a step of, if the first common authentication is leaked when the first common authentication key and the second common authentication key further includes the extraction value, changing, by the authentication server, an extraction reference of the extraction value.

15 5. The user authentication method of claim 1, wherein the comparison/determination step comprises:

a step of receiving, by the user terminal, the first server authentication information from a specific server;

20 a step of determining, by the user terminal, comparing the first server authentication information and the first user authentication information to determine whether the first server authentication information and the first user authentication information coincide with each other; and

a step of, if the first server authentication information and the first user authentication information do not coincide with each other, determining the

25

specific server as a server that misrepresents itself as the authentication institute.

6. The user authentication method of claim 1, wherein in the first
5 server authentication information generating step, the first server authentication information is generated based on a first gap time value registered in the authentication server in advance or a value obtaining by combining a gap time key that is a number value extracted from the first gap time value by a specific reference, in the server authentication key,
10 wherein in the second common authentication information generating step, a second gap time value when the personal password is input is measured, and
wherein in the first user authentication information generating step, the first user authentication information is generated based on the second gap time
15 vale or a value obtained by combining a gap time key that is a number value extracted from the second gap time value by a specific reference, in the user authentication key, and
wherein the first gap time value and the second gap time value are time values obtained by measuring a period of time consumed to input the personal
20 password in unit of $1/n$ (n is an arbitrary positive real number) seconds.

7. The user authentication method of claim 1, wherein in the user registering step, the user terminal sequentially extracts m (m is an arbitrary natural number) extraction values from the mechanical unique key of the user
25 terminal by a specific reference, generates m common authentication keys

corresponding to the extraction values, and transmits the m common authentication keys to the authentication server, and the authentication server registers a common authentication key selected from the m common authentication keys as the first common authentication key,

5 wherein in the second common authentication information generating step, generating the second common authentication key by selecting an extraction value having a sequence value corresponding to the first common authentication key, from the m extraction values sequentially extracted from the mechanical key of the user terminal by a specific reference, and

10 wherein the sequence value is a value used as a reference for selecting the first common authentication key from the m extraction values, and is a value that is stored in the user terminal or received from the authentication server when the second common authentication key is generated.

15 8. The user authentication method of claim 1, further comprising:
 a step of generating, by the user terminal, second user authentication information, based on a value obtained by adding at least one of the first user authentication information, an extraction value extracted from the first user authentication information by a specific reference, the user authentication key,
20 an extraction value extracted from the user authentication key by a specific reference, the second common authentication key, and an extraction value extracted from the second common authentication key, to a gap time value or a gap time key that is a number value extracted from the gap time value by a specific reference;

a step of generating, by the authentication server, second server authentication information, based on a value obtained by adding at least one of the first server authentication information, an extraction value extracted from the first server authentication information by a specific reference, the server authentication key, an extraction value extracted from the server authentication key by a specific reference, the first common authentication key, and an extraction value extracted from the first common authentication key by a specific reference, to the gap time value or a gap time key that is a number value extracted from the gap time value by a specific reference; and

a step of determining whether the second user authentication information and the second server authentication information coincide with each other,

wherein the second common authentication information generating step further comprises:

a step of, by the user terminal, measuring a gap time value and transmitting the gap time value to the authentication server, and

wherein the gap time value is a time value obtained by measuring a period of time consumed to input the personal password for authentication in unit of $1/n$ (n is an arbitrary positive real number) seconds.