WHAT IS CLAIMED IS:

1. A user authentication method using a user terminal and an authentication server, the user authentication method comprising:

(1) if a personal password for registration of a user is input by the user, combining the personal password and a mechanical unique key of the user terminal, performing a primary conversion using a unidirectional function, and generating a first common authentication key, and performing a secondary conversion of encrypting the first common authentication key by using an encryption key and providing the encrypted first common authentication key to the authentication server, by the user terminal, and matching the encrypted first common authentication key with user information and registering the encrypted first common authentication key, by the authentication server;

(2) performing a conversion using a unidirectional function while an embedded unique key of an authentication institute and the encrypted first common authentication key are taken as elements and generating a first server authentication key, and performing an OTP operation on the first server authentication key or a second server authentication key that is a converted value of the first server authentication key and generating first server authentication information, by the authentication server;

(3) if the personal password is input by the user for authentication, combining the personal password and the mechanical unique key of the user terminal, performing a primary conversion using a unidirectional function, generating a second common authentication key in real time, performing a secondary conversion of encrypting the second common authentication key by using the

encryption key, and generating an encrypted second common authentication key, performing a conversion using a unidirectional function while the unique key of the authentication institute provided by the authentication server in advance and the encrypted second common authentication key are taken as elements and generating a first user authentication key, and performing an OTP operation on the first user authentication key or a second user authentication key that is a converted value or the first user authentication key and generating first user authentication information, by the user terminal; and

(4) performing a user authentication by the authentication server or an authentication of the authentication server for determining a genuineness of the authentication server by the user terminal, based on 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 a unique key of a dedicated application program installed in the user terminal is added to the first common authentication key or the second common authentication key as an element.

3. The user authentication method of claim 1, wherein (4) comprises:

comparing the first user authentication information and the first server authentication information transmitted from the authentication server and determining a genuineness of the authentication server, by the user terminal, or

comparing the first server authentication information and the first user authentication information transmitted from the user terminal and performing the user authentication, by the authentication server.

4. The user authentication method of claim 1, wherein (2) comprises:

performing a conversion using a unidirectional function while the embedded unique key of the authentication institute and the encrypted first common authentication key are taken as elements, and generating the first server authentication key, by the authentication server;

generating a second server authentication key that is extracted from the first server authentication key through a time extraction value generator by using time information by a specific reference, by the authentication server; and

performing an OTP operation on the second server authentication key and generating the first server authentication information, by the authentication server, and

wherein (3) comprises:

if the encrypted second common authentication key is generated, performing a conversion using a unidirectional function when the unique key of the authentication institute provided by the authentication server in advance and the encrypted second common authentication key are taken as elements, and generating the first user authentication key, by the user terminal;

generating a second user authentication key that is extracted from the first user authentication key through a time extraction value generator by using time information by a specific reference; and

performing an OTP operation on the second user authentication key and generating the first user authentication information, by the user terminal.

5. The user authentication method of claim 1, further comprising: between (3) and (4), or after (4),

performing a conversion using a unidirectional function while a second common authentication key decrypted by using a decryption key or the unencrypted second common authentication key, and the first server authentication information transmitted from the authentication server or the first user authentication information is taken as an element, and generating a third user authentication key, by the user terminal;

performing an OTP operation on the third user authentication key and generate a second user authentication information, by the user terminal;

transmitting the second user authentication information and the decryption key to the authentication server, by the user terminal;

decrypting the encrypted first common authentication key to a first common authentication key by using the decryption key, performing a conversion using a unidirectional function while the first common authentication key and the first user authentication information transmitted from the user terminal or the first server authentication information are taken as elements to generate a third server authentication key, by the authentication server; and

performing an OTP operation on the third server authentication key and generating a second server authentication information, by the authentication server, and

wherein the method further comprises: after (4),

determining whether the second user authentication information and the second server authentication information coincide with each other and performing a user authentication.

6. The user authentication method of claim 4, further comprising: between (3) and (4), or after (4),

performing a conversion using a unidirectional function while a second common authentication key decrypted by using a decryption key or the unencrypted second common authentication key, and the first server authentication information transmitted from the authentication server or the first user authentication information is taken as element, and generating a third user authentication key, by the user terminal;

generating a fourth user authentication key that is extracted from the third user authentication key through a time extraction value generator by using time information by a specific reference, by the user terminal; and

performing an OTP operation on the fourth user authentication key and generating a second user authentication information,

wherein the method further comprises:

transmitting the second user authentication information and the decryption key to the authentication server, by the user terminal;

decrypting the encrypted first common authentication key to a first common authentication key by using the decryption key, performing a conversion using a unidirectional function while the first user authentication information transmitted from the user terminal or the first server authentication information and the first common authentication key are taken as elements to generate a third server authentication key, by the authentication server; and

generating a fourth server authentication key that is extracted from the third server authentication key through a time extraction value generator by a specific reference by using time information, by the authentication server; and

performing an OTP operation on the fourth server authentication key and generating a second server authentication information,

wherein the method further comprises: after (4),

determining whether the second user authentication information and the second server authentication information coincide with each other and performing a user authentication.

7. The user authentication method of claim 5, wherein (3) further comprises:

measuring a gap time value that is a time value that is obtained by measuring a time consumed to input a personal password for authentication by the user in unit of 1/n (n is a positive real number) seconds and transmitting the gap time value to the authentication server, by the user terminal;

wherein when the third user authentication key is generated by the user terminal, the gap time value or a gap time key that is a number value extracted from the gap time value by a specific reference is added as an element, and

wherein when the authentication server generates the third server authentication key, the time gap value or the gap time key is added as an element.

8. The user authentication method of claim 6, wherein (3) further comprises:

measuring a gap time value that is a time value that is obtained by measuring a time consumed to input a personal password for authentication by the user in unit of 1/n (n is a positive real number) seconds and transmitting the gap time value to the authentication server, by the user terminal;

wherein when the third user authentication key is generated by the user terminal, the gap time value or a gap time key that is a number value extracted from the gap time value by a specific reference is added as an element, and

wherein when the authentication server generates the third server authentication key, the gap time value or the gap time key is added as an element.

9. The user authentication method of claim 5 or 6, wherein the unidirectional function comprises a hash function as a function for mapping data having an arbitrary length to data of a fixed length, and

wherein a symmetrical key encryption scheme in which an encryption key and a decryption key are the same is used in the encryption for the secondary conversion.

10. The user authentication method of claim 5 or 6, wherein a verification key for verifying integrity of data is added to transmission target data comprising authentication information or an authentication key transmitted from the user terminal or the authentication server and is transmitted,

wherein a first OTP operation value, which was obtained by performing OTP operations on the transmission target data, is added to the verification key, and

wherein, when the user terminal or the authentication server receives the data, the integrity of the authentication is verified by comparing a second OTP operation value, which was obtained by performing OTP operations on the received data, and the verification key.

11. The user authentication method of claim 6, wherein the authentication server requests an additional manual input of the second user authentication information from the user terminal when a plurality of first server authentication information is transmitted in a specific time, and compares the manually input second user authentication information and the second server authentication information and performs a user authentication if the second user authentication information is transmitted through a manual input.

12. The user authentication method of claim 6 or 11, further comprising:

requesting a third user authentication information from the user terminal, by the authentication server; and

if the third user authentication information is transmitted through the user terminal, determining whether the third user authentication information and a third server authentication information coincide with each other and performing a user authentication, by the authentication server,

wherein the third user authentication information is generated by performing a conversion using a unidirectional function while the unique key of the authentication institute and the fourth user authentication key are taken as elements to generate a fifth user authentication key, and performing an OTP operation on the fifth user authentication key, by the user terminal, and

wherein the third server authentication information is generated by performing a conversion using a unidirectional function while the unique key of the authentication institute and the fourth server authentication key are taken as elements to generate a fifth server authentication key, and performing an OTP operation on the fifth server authentication key, by the authentication server.

13. The user authentication method of claim 5 or 6, further comprising:

the user terminal detects a symptom of an attack comprising hacking while the authentication procedure of (1) to (4) is performed, and compulsorily stops the authentication procedure by generating a compulsory stop signal for compulsorily stopping the authentication procedure and transmitting the compulsory stop signal to the authentication server when the symptom of an attack is detected.

14. A user authentication method using a user terminal and an authentication server, the user authentication method comprising:

(1) if a procedure for registration of a user is started by a user, performing a primary conversion using a unidirectional function while a mechanical unique key of the user terminal is taken as an element and generating a first common authentication key, and performing a secondary conversion of encrypting the first common authentication key and providing the encrypted first common authentication key to the authentication server, by the user terminal, and matching the encrypted first common authentication key with user information to register the encrypted first common authentication key, by the authentication server;

(2) performing a conversion using a unidirectional function while an embedded unique key of an authentication institute and the encrypted first common authentication key are taken as elements and generating a first server authentication key, and performing an OTP operation on the first server authentication key or a second server authentication key that is a converted value of the first server authentication key and generating first server authentication information, by the authentication server;

(3) if an authentication procedure is started by the user for authentication, performing a primary conversion using a unidirectional function while a mechanical unique key of the user terminal is taken as an element, generating a second common authentication key in real time, performing a secondary conversion of encrypting the second common authentication key and generate an encrypted second common authentication key, performing a conversion using a unidirectional function while the unique key of the authentication institute provided by the authentication server in advance and the encrypted second common authentication key are taken as elements to generate a first user authentication key, performing an OTP operation on the first user authentication key or a second user authentication key that is a converted value of the first user authentication key and generating first user authentication information; and

(4) performing a user authentication by the authentication server or an authentication of the authentication server for determining a genuineness of the authentication server by the user terminal, based on whether the first server authentication information and the first user authentication information coincide with each other.

15. The user authentication method of claim 14, wherein a first encryption key for encrypting the first common authentication key and a second encryption key for encrypting the second common authentication key are generated by performing a conversion using a unidirectional function while a personal password input by the user as an element or are generated at random.

16. The user authentication method of claim 15, wherein the first encryption key and the second encryption key are generated by combining the

personal password and a mechanical unique key of the user terminal and performing a conversion using a unidirectional function, the mechanical unique key of the user terminal being added as an element.

17. The user authentication method of claim 16, wherein when the first common authentication key, the second common authentication key, the first encryption key, and the second encryption key are generated, a unique key of a dedicated application installed in the user terminal is added as an element.

18. The user authentication method of claim 15, wherein (2) comprises:

performing a conversion using a unidirectional function while the embedded unique key of the authentication institute and the encrypted first common authentication key are taken as elements, and generating the first server authentication key, by the authentication server;

generating a second server authentication key that is extracted from the first server authentication key through a time extraction value generator by using time information by a specific reference, by the authentication server; and

performing an OTP operation on the second server authentication key and generating the first server authentication information, by the authentication server, and

wherein (3) comprises:

if the encrypted second common authentication key is generated, performing a conversion using a unidirectional function when the unique key of the authentication institute provided by the authentication server in advance and the

encrypted second common authentication key are taken as elements, and generating the first user authentication key, by the user terminal;

generating a second user authentication key that is extracted from the first user authentication key through a time extraction value generator by using time information by a specific reference; and

performing an OTP operation on the second user authentication key and generating the first user authentication information, by the user terminal.

19. The user authentication method of claim 15, further comprising: between (3) and (4), or after (4),

performing a conversion using a unidirectional function while a second common authentication key decrypted by using a decryption key or the unencrypted second common authentication key, and the first server authentication information transmitted from the authentication server or the first user authentication information are taken as elements, and generating a third user authentication key, by the user terminal;

performing an OTP operation on the third user authentication key and generate a second user authentication information, by the user terminal;

wherein the method further comprises:

transmitting the second user authentication information and the decryption key to the authentication server, by the user terminal;

decrypting the encrypted first common authentication key to a first common authentication key by using the decryption key, performing a conversion using a unidirectional function while the first common authentication key and the first user authentication information transmitted from the user terminal or the first server

authentication information are taken as elements, to generate a third server authentication key, by the authentication server; and

performing an OTP operation on the third server authentication key and generating a second server authentication information, by the authentication server, and

wherein the method further comprises: after (4),

determining whether the second user authentication information and the second server authentication information coincide with each other and performing a user authentication.

20. The user authentication method of claim 18, further comprising: between (3) and (4), or after (4),

performing a conversion using a unidirectional function while a second common authentication key decrypted by using a decryption key or the unencrypted second common authentication key, and the first server authentication information transmitted from the authentication server or the first user authentication information is taken as an element, and generating a third user authentication key, by the user terminal;

generating a fourth user authentication key that is extracted from the third user authentication key through a time extraction value generator by using time information by a specific reference, by the user terminal; and

performing an OTP operation on the fourth user authentication key and generating a second user authentication information,

wherein the method further comprises:

transmitting the second user authentication information and the decryption key to the authentication server, by the user terminal;

decrypting the encrypted first common authentication key to a first common authentication key by using the decryption key, performing a conversion using a unidirectional function while the first user authentication information transmitted from the user terminal or the first server authentication information and the first common authentication key are taken as elements, to generate a third server authentication key, by the authentication server; and

generating a fourth server authentication key that is extracted from the third server authentication key through a time extraction value generator by a specific reference by using time information, by the authentication server; and

performing an OTP operation on the fourth server authentication key and generating a second server authentication information, and

wherein the method further comprises: after (4),

determining whether the second user authentication information and the second server authentication information coincide with each other and performing a user authentication.

21. The user authentication method of claim 19, wherein (3) further comprises:

measuring a gap time value that is a time value that is obtained by measuring a time consumed to input a personal password for authentication by the user in unit of 1/n (n is a positive real number) seconds and transmitting the gap time value to the authentication server, by the user terminal;

wherein when the third user authentication key is generated by the user terminal, the gap time value or a gap time key that is a number value extracted from the gap time value by a specific reference is added as an element, and

wherein when the authentication server generates the third server authentication key, the time gap value or the gap time key is added as an element.

22. The user authentication method of claim 20, wherein (3) further comprises:

measuring a gap time value that is a time value that is obtained by measuring a time consumed to input a personal password for authentication by the user in unit of 1/n (n is a positive real number) seconds and transmitting the gap time value to the authentication server, by the user terminal;

wherein when the third user authentication key is generated by the user terminal, the gap time value or a gap time key that is a number value extracted from the gap time value by a specific reference is added as an element, and

wherein when the authentication server generates the third server authentication key, the time gap value or the gap time key is added as an element.

23. The user authentication method of claim 14 or 15, wherein a verification key for verifying integrity of data is added to transmission target data comprising authentication information or an authentication key transmitted from the user terminal or the authentication server and is transmitted,

wherein a first OTP operation value, which was obtained by performing OTP operations on the transmission target data, is added to the verification key, and

wherein, when the user terminal or the authentication server receives the data, the integrity of the authentication is verified by comparing a second OTP operation value, which was obtained by performing OTP operations on the received data, and the verification key.

24. The user authentication method of claim 20, wherein the authentication server requests an additional manual input of the second user authentication information from the user terminal when a plurality of first server authentication information is transmitted in a specific time, and compares the manually input second user authentication information and the second server authentication information and performs a user authentication if the second user authentication information is transmitted through a manual input.

25. The user authentication method of claim 20 or 24, further comprising:

requesting a third user authentication information from the user terminal, by the authentication server; and

if the third user authentication information is transmitted through the user terminal, determining whether the third user authentication information and a third server authentication information coincide with each other and performing a user authentication, by the authentication server,

wherein the third user authentication information is generated by performing a conversion using a unidirectional function while the unique key of the authentication institute and the fourth user authentication key are taken as elements to generate a fifth user authentication key, and performing an OTP operation on the fifth user authentication, by the user terminal, and

wherein the third server authentication information is generated by performing a conversion using a unidirectional function while the unique key of the authentication institute and the fourth server authentication key are taken as elements to generate a fifth server authentication key, and performing an OTP operation on the fifth server authentication, by the authentication server.

26. The user authentication method of claim 14 or 15, wherein the user terminal detects a symptom of an attack comprising hacking while the authentication procedure of (1) to (4) is performed, and compulsorily stops the authentication procedure by generating a compulsory stop signal for compulsorily stopping the authentication procedure and transmitting the compulsory stop signal to the authentication server when the symptom of an attack is detected.