

CLAIMS

1. A simple authentication method using browser web storage, the method comprising the operations in which:

~~on the basis of a received user key, a server generates an authentication token, a public key and a private key, stores the same in a session, and transmits the authentication token, the public key and a session key corresponding to the session to a terminal; a server generates a one-time session and a session key corresponding to the one-time session according to an authentication request, generates an authentication token, a public key and a private key based on a user key received from a terminal and stores the same in the one-time session, and transmits the session key, the authentication token and the public key to the terminal;~~

~~by~~ using the received public key, the terminal encrypts PIN number data entered by a user, and transmits the encrypted data along with the received session key to the server; ~~and~~

~~by using the private key corresponding to the received session key, the server decrypts the PIN number data to perform simple authentication,~~

~~wherein the user key is stored in the web storage of the terminal and is set differently for each device or browser.~~

~~using the private key stored in the one-time session corresponding to the received session key, the server decrypts the received encrypted PIN number data, and identifies whether the decrypted PIN number data matches the PIN number data previously stored in the browser web storage to perform primary authentication;~~

~~when the primary authentication result matches, the terminal encrypts the received authentication token using the received public key and transmits same along with the received session key to the server;~~

~~using the private key stored in the one-time session corresponding to the received session key, the server identifies whether the received encrypted authentication token matches the authentication token stored in the one-time session to perform secondary authentication;~~

and

when the second authentication is completed, the server deletes the one-time session and the session key,

wherein the user key and the PIN number data are stored in the browser web storage and set differently for each device or browser, and

wherein the authentication token, the public key, the private key, the one-time session, and the session key are one-time generated whenever an authentication is requested.

2. The method of claim 1, wherein ~~the public key is stored in a blockchain and used to verify whether the public key has been falsified or forged~~ the user key is encrypted with an encryption algorithm, and the PIN number is hash-encrypted and stored in the browser web storage.

3. The method of claim 1, wherein ~~the performance of the simple authentication comprises:~~

~~restoring, by the server, encrypted PIN number data based on a private key retrieved through the received session key to perform primary authentication;—~~

~~when the primary authentication is passed, encrypting an authentication token by the terminal using the public key, and transmitting the encrypted data along with the received session key to the server; and—~~

~~comparing the authentication token restored based on the private key in the server with the authentication token stored in the session, performing secondary authentication, and then deleting the session~~ the transmission of the public key to the terminal comprises:

determining, by the terminal, whether the user key is stored in the browser web storage; and

when the user key is not stored, registering a PIN number from a user..

4. The method of claim 1, wherein: ~~the user key is encrypted with an encryption algorithm, and a PIN number is hash-encrypted and stored in the web storage.~~

when the primary authentication result does not match, the server updates a number of authentication attempts, and

when the number of authentication attempts is greater than or equal to a predetermined value, the server deletes the PIN number data previously stored in the server.

~~5. The method of claim 1, wherein the transmission of the public key to the terminal comprises:—~~

~~querying an authentication policy of the server; and—~~

~~searching for a user key in the terminal using a simple authentication method or a user public key according to the authentication policy of the server.~~

~~6. The method of claim 1, wherein the transmission of the public key to the terminal further comprises:~~

~~determining, by the terminal, whether the user key is stored in the web storage;~~

~~and—~~

~~when the user key is not stored, registering a PIN number from a user.~~

~~7. The method of claim 1, wherein the performance of the simple authentication is configured to update a number of authentication attempts whenever the PIN number does not match, and delete the PIN number data stored in the server and/or terminal when the number of authentication attempts increases by more than a predetermined number.—~~

~~———8. The method of claim 1, further comprising:—~~

~~extracting a modulus, a private exponent and a public exponent from the generated public key and private key;—~~

~~storing the private exponent in a terminal and storing the modulus and the public exponent in a server; and—~~

~~performing simple authentication using the private key generated using the private exponent stored in the terminal and the modulus stored in the server and the public key generated using the modulus and the public exponent stored in the server.—~~

~~9. The method of claim 8, wherein the performance of the simple authentication comprises:~~

~~transmitting, by the server, the modulus to the terminal upon a simple authentication request;—~~

~~generating a private key using the modulus received by the terminal and the stored private exponent;—~~

~~encrypting data and performing digital signature using the generated private key;—~~

~~transmitting the encrypted data and digital signature to a server; and—~~

~~discarding the private key.~~

~~10. The method of claim 9, wherein the performance of the simple authentication further comprises:—~~

~~generating, by the server, a public key using the modulus and the public exponent;—~~

~~decrypting the encrypted data received from the terminal using the generated public key, and performing verification using the digital signature; and—~~

~~discarding the public key.~~

~~115. A simple authentication system using browser web storage, the system comprising:~~

~~a server that:— generates an authentication token, a public key and a private key and stores the same in a session on the basis of a received user key, transmits the authentication token, the public key and a session key corresponding to the session to a terminal, and performs simple authentication by decrypting the PIN number data using the private key corresponding to the received session key upon receipt of the encrypted data and the session key from the terminal;—~~

~~and a terminal that requests to issue a public key on the basis of a user key, encrypts PIN number data entered by a user by using the public key received from the server, and transmits the encrypted data along with the received session key to the server;—~~

~~wherein the user key is stored in the terminal web storage and set differently for~~

~~each device or browser.~~

generates a one-time session and a session key corresponding to the one-time session according to an authentication request,

generates an authentication token, a public key and a private key based on a user key received from a terminal and stores same in the one-time session,

transmits the session key, the authentication token and the public key to the terminal,

decrypts the encrypted PIN number data using the private key stored in the one-time session corresponding to the received session key upon receipt of the encrypted PIN number data and the session key from the terminal,

identifies whether the decrypted PIN number data matches the PIN number data previously stored in the browser web storage to perform primary authentication,

identifies whether the received encrypted authentication token matches the authentication token stored in the one-time session to perform secondary authentication using the private key stored in the one-time session corresponding to the received session key upon receipt of the encrypted authentication token and the session key from the terminal, and

deletes the one-time session and the session key when the secondary authentication is completed; and

a terminal that:

requests the server to issue a public key on the basis of the user key,

encrypts PIN number data entered by the user using the public key received from the server, and transmits the encrypted data along with the received session key to the server, and

when the primary authentication result matches, encrypts the received authentication token using the received public key and transmits same along with the received session key to the server,

wherein the user key and the PIN number data are stored in the browser web storage and set differently for each device or browser, and

wherein the authentication token, the public key, the private key, the one-time session, and the session key are one-time generated whenever an authentication is requested.

~~126. The system of claim 115, wherein: the public key is stored in a blockchain and used to verify whether the public key has been falsified or forged.~~

when the primary authentication result does not match, the server updates a number of authentication attempts, and

when the number of authentication attempts is greater than or equal to a predetermined value, the server deletes the PIN number data previously stored in the server.

~~13. The system of claim 11, wherein:—~~

~~the server restores encrypted PIN number data based on a private key retrieved through the received session key to perform primary authentication;—~~

~~when the primary authentication is passed, the terminal encrypts an authentication token using the public key, and transmits the encrypted data along with the received session key to the server; and—~~

~~the server compares the authentication token restored based on the private key with the authentication token stored in the session, and performs secondary authentication, and then delete the session.—~~

~~14. The system of claim 11, wherein the server is configured to update a number of authentication attempts whenever the restored PIN number does not match, and delete the PIN number data stored in the server and/or terminal when the number of authentication attempts increases by more than a predetermined number.—~~

~~157. A simple authentication program combined with a computer that is hardware, and stored in a medium to execute the method of any one of among claims 1, to 10 claim 2, claim 3 and claim 4.~~