

CLAIMS

Claim 1

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

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;

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;

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.

Claim 2

The method of claim 1, wherein the user key is encrypted with an encryption algorithm, and the PIN number is hash-encrypted and stored in the

browser web storage.

Claim 3

The method of claim 1, wherein 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.

Claim 4

The method of claim 1, wherein:

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.

Claim 5

A simple authentication system using a browser web storage, the system comprising:

a server that:

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.

Claim 6

The system of claim 5, wherein:

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.

Claim 7

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 claim 1, claim 2, claim 3 and claim 4.