ABSTRACT

A data communication method capable of performing a synchronization processing at two or more computer terminals while ensuring security. A server certificate and a public key are transmitted through a host-side terminal to a guest-side terminal, whereby the guest-side terminal authenticates the server, and a guest-side hash key used in a hash function, as well as the hash function, are encrypted with the public key. A web server decrypts the hash key and the hash function, creates a digest of the contents with the guest-side hash key, and transmits the digest through the host-side terminal to the guest-side terminal. The guest-side terminal receives the contents and digest received from the host-side terminal, and compares this digest and a digest created from the received contents, whereby security can be ensured when the synchronization processing is performed.



162162



G00002