

ABSTRACT OF DISCLOSURE

SYSTEM AND METHOD FOR MANAGING DATA-FILE TRANSMISSION AND ACCESS RIGHT TO DATA FILES

A first user device has first public and private keys and a file encryption key for encrypting the specified file into an encrypted file. A second user device has second public and private keys. A server is in communication with the first and second user devices. The first user device generates temporary public and private keys, performs a first key establishment with the second public key, first private key and temporary private key to generate a shared secret, and uses the shared secret to encrypt the file encryption key into an encrypted key. The server allows the first user device to transmit the first public key, temporary public key, encrypted key and encrypted file to the second user device therevia if both of the first and second user devices pass the identity authentication performed thereby; and the server or the second user device uses the first public key, second private key and temporary public key to perform a second key establishment to retrieve the shared secret, and uses the shared secret, encrypted key and encrypted file to retrieve the specified file for the second user device to access.

[Figure 1]