WHAT IS CLAIMED IS:

1. A system for managing data-file transmission and access right to a specified file, comprising:

a first user device having a pair of first public key and first private key and a file encryption key, which is used to encrypt the specified file into an encrypted file;

a second user device having a pair of second public key and second private key; and

a server in communication with the first user device and the second user device, performing identity authentication for the first user device and the second user device,

wherein for transmitting the encrypted file from the first user device to the second user device, the first user device generates a pair of temporary public key and temporary private key, acquires the second public key of the second user device, performs a first key establishment with the second public key, the first private key and the 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, the temporary public key, the encrypted key and the encrypted file to the second user device therevia if both of the first and second user devices pass the identity authentication; and the server or the second user device uses the first public key, the second private key and the temporary public key to perform a second key establishment to retrieve the shared secret, and uses the shared secret, the encrypted key and the encrypted file to retrieve the specified file for the second user device to access, and

wherein the first user device includes a host and a detachable identity

authentication and encryption device in communication with the host via a bus interface, wherein the identity authentication and encryption device stores therein the first private key, which is used to pass the identity authentication, generates the file encryption key and the pair of temporary public key and temporary private key, uses the file encryption key to encrypt the specified file into the encrypted file, acquires the second public key, performs the first key establishment with the second public key, the first private key and the temporary private key to generate the shared secret, uses the shared secret to encrypt the file encryption key into the encrypted key, and transmits the first public key, the temporary public key, the encrypted key and the encrypted file to the second user device, which also passes the identity authentication, via the server.

2. A system for managing data-file transmission and access right to a specified file, comprising:

a first user device having a pair of first public key and first private key and a file encryption key, which is used to encrypt the specified file into an encrypted file;

a second user device having a pair of second public key and second private key; and

a server in communication with the first user device and the second user device, performing identity authentication for the first user device and the second user device,

wherein for transmitting the encrypted file from the first user device to the second user device, the first user device generates a pair of temporary public key and temporary private key, acquires the second public key of the second user device, performs a first key establishment

with the second public key, the first private key and the 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, the temporary public key, the encrypted key and the encrypted file to the second user device therevia if both of the first and second user devices pass the identity authentication; and the server or the second user device uses the first public key, the second private key and the temporary public key to perform a second key establishment to retrieve the shared secret, and uses the shared secret, the encrypted key and the encrypted file to retrieve the specified file for the second user device to access, and

wherein the second user device includes a detachable identity authentication and encryption device; when the identity authentication and encryption device is detachably connected to a bus interface of the second user device, the server executes the identity authentication of the second user device; and the second user device automatically runs a browser program to have a display show a user interface for a user to input data if the second user device passes the identity authentication.

3. The system according to claim 2, wherein the server is a server set including a cipher server, a file server and a Fast Identity Online (FIDO) server, wherein the cipher server performs encryption/decryption for the detachable identity authentication and encryption device, the file server temporarily stores the encrypted file and the browser program, and works as a relying party application server (RP app server) for registration and verification of users, and the FIDO server is disposed at a distant end and allowed to be shared with an external server.