WHAT IS CLAIMED IS:

1. A file sharing method, adapted to be used with a key manager unit and a specified file owned by a first user and to be shared with a second user, the specified file corresponding to a file identifier, the first user having a first user identifier, a first system public key and a first system private key, the second user having a second user identifier, a second system public key and a second system private key, and the method comprising:

the key manager unit realizing a correspondence between the first user identifier and the first system public key in response to a first registration request of the first user and realizing a correspondence between the second user identifier and the second system public key in response to a second registration request of the second user;

the key manager unit acknowledging the specified file and an access-right claim request to the specified file provided by the first user, wherein the access-right claim request comprises the second user identifier and the file identifier;

the key manager unit generating a specified key material for encrypting the specified file into an encrypted file, and generating a specified credential according to the second user identifier and the file identifier in the access-right claim request, the second system public key and the specified key material; and

storing the encrypted file and the specified credential,

whereby, the second user uses the second user identifier, the file identifier and the second system private key to retrieve the specified key material out of the specified credential, and uses the specified key material to decrypt the encrypted file into the specified file.

2. The file sharing method according to claim 1, wherein the first user further has a first authentication public key and a first authentication private key; the second user further has a second authentication public key and a second authentication private key; the key manager unit realizes a correspondence between the first user identifier and the first authentication public key in response to the first registration request of the first user and realizing a correspondence between the second user identifier and the second authentication public key in response to the second registration request of the second user; and the key manager unit executes verification of the second user before the second user is authorized to access the specified file.

3. The file sharing method according to claim 2, wherein the verification of the second user is executed by:

the key manager unit generating a specified byte string randomly to the second user, and requesting a digital signature, which is derived from the second verification private key and the specified byte string, from the second user; and

the key manager unit executing authentication of the digital signature with the second authentication public key to determine whether the second user is eligible for requesting the specified credential from the key manager unit.

4. A file sharing method, adapted to be used with a key manager unit, a first user, a second user and a specified file owned by the second user, the method comprising:

executing a verification of the first user;

generating a second user identifier corresponding to the second user, a file identifier corresponding to the specified file and a verification pass code in response a request from the first user after the first user passes the verification;

transmitting the verification pass code to the second user;

generating a key material corresponding to the file identifier;

issuing an access-right claim request to the key manager unit, wherein the access-right claim request includes the file identifier and a first user identifier corresponding to the first user;

generating a credential according to the file identifier, the first user identifier and a first public key of the first user;

executing a verification of the second user based on the verification pass code;

using the key material to encrypt the specified file into an encrypted file; and

storing the credential and the encrypted file.

5. The file sharing method according to claim 4, wherein the first user passing the verification requests the key manager unit to establish a provisional user and a provisional user agent unit, corresponding to which a provisional public-private key pair and the identity verification pass code, which is transmitted to the provisional user, wherein the provisional user represents the second user, and the key manager unit requests the provisional user agent unit to encrypt the specified file into an encrypted file with the key material, and then stores the credential and the encrypted file.

6. The file sharing method according to claim 4, wherein when the first user accesses the specified, the first key material is retrieved out of the credential with the first user identifier, the file identifier and a private key of the first user, and then the key material is used to decrypt the encrypted file into the specified file.