

D E S C R I P T I O N

Title of Invention:

~~FILE SERVER APPARATUS AND FILE SERVER SYSTEM~~

5

Technical Field

An embodiment according to the present invention relates to a file server apparatus and a file server system.

10

Background Art

In general, for example, as a system used for sharing data on a network, a file server system is known. As an example of this file server system, there is a so-called electronic post-office box system. The electronic post-office box system corresponds to a post-office box configured to send/receive electronic data over, for example, a network.

According to this electronic post-office box system, a service of receiving sensitive electronic data (hereinafter referred to as confidential data) on behalf of users is provided to the users.

The electronic post-office box system comprises an electronic post-office box server that provides the electronic post-office box service, a sending apparatus used by a sender who sends confidential data to the electronic post-office box server, and a receiving apparatus used by a recipient who receives the confidential data from the electronic post-office box

C L A I M S

1. A file server apparatus which is connected to a sending apparatus used by a sender who sends data and a receiving apparatus used by a recipient who receives the data, characterized by comprising:

reception means for receiving post office box's encrypted data obtained by encrypting the data using a post office box's public key from the sending apparatus;

re-encryption key storage means for storing a re-encryption key that is used for re-encrypting post office box's encrypted data, which is obtained by encrypting the data using the post office box's public key, into recipient's encrypted data, which is obtained by encrypting the data using a recipient's public key that is different from the post office box's public key and forms a pair with a recipient's secret key managed in the receiving apparatus;

re-encryption means for re-encrypting the received post office box's encrypted data into the recipient's encrypted data using the re-encryption key stored in the re-encryption key storage means; and

transmission means for transmitting the re-encrypted recipient's encrypted data to the receiving apparatus.

~~2. The apparatus according to claim 1, characterized by further comprising encrypted data storage means for storing the re encrypted recipient's encrypted data,~~

~~wherein the transmission means transmits the recipient's encrypted data stored in the encrypted data storage means to the receiving apparatus in response to a request from the recipient.~~

~~3. The apparatus according to claim 1, characterized by further comprising encrypted data storage means for storing the received post office box's encrypted data,~~

~~wherein the re encryption means re encrypts the post office box's encrypted data stored in the encrypted data storage means into the recipient's encrypted data using the re encryption key stored in the re encryption key storage means in response to a request from the recipient.~~

14. A file server system characterized by comprising:
a sending apparatus used by a sender who sends data; a receiving apparatus used by a recipient who receives the data; and a file server apparatus connected to the sending and receiving apparatuses,

wherein the sending apparatus comprises:

input means for inputting the data in accordance with an operation of the sender; and

encryption means for encrypting the input data using a post-office box's public key to acquire post-office box's encrypted data,

the file server apparatus comprises:

5 re-encryption key storage means for storing a re-encryption key used for re-encrypting the post-office box's encrypted data, which is obtained by encrypting the data using the post-office box's public key, into recipient's encrypted data, which is obtained by encrypting the data
10 using a recipient's public key different from the post-office box's public key; and

re-encryption means for re-encrypting the post-office box's encrypted data acquired by the encryption means into the recipient's encrypted data using the re-encryption key
15 stored in the re-encryption key storage means, and

the receiving apparatus comprises:

secret key storage means for storing a recipient's secret key which forms a pair with the recipient's public key;

20 decryption means for decrypting the re-encrypted recipient's encrypted data using the recipient's secret key stored in the secret key storage means;—and

output means for outputting data obtained by decrypting the recipient's encrypted data;—

~~5. The system according to claim 4, characterized in that the receiving apparatus further comprises:~~

recipient's key generation means for generating the recipient's public key and the recipient's secret key which
5 forms a pair with the recipient's public key;

recipient's secret key storage processing means for storing the generated recipient's secret key in the secret key storage means;

post-office box's key generation means for generating
10 the post-office box's public key and a post-office box's secret key which forms a pair with the post-office box's public key; and

re-encryption key generation means for generating the re-encryption key using the recipient's public key and the
15 recipient's secret key generated by the recipient's key generation means and the post-office box's public key and the post-office box's secret key generated by the post-office box's key generation means,

the file server apparatus further comprises:

20 post-office box's public key storage means for storing the post-office box's public key generated by the post-office box's key generation means; and

re-encryption key storage processing means for storing the re-encryption key generated by the re-encryption key

generation means in the re-encryption key storage means,
and

the encryption means included in the sending apparatus
encrypts the input data by using the post-office box's
5 public key stored in the post-office box's public key
storage means included in the file server apparatus.