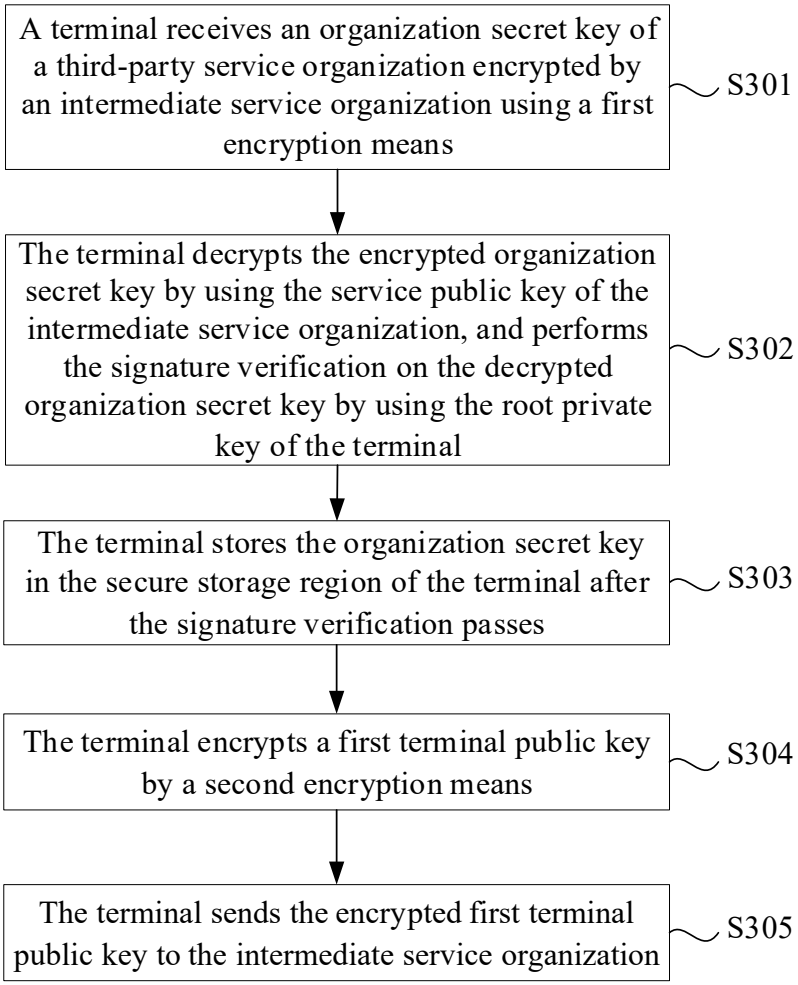
A terminal receives an organization secret key of a third-party service organization encrypted by an intermediate service organization using a first encryption means
S301
The terminal decrypts the encrypted organization secret key by using the service public key of the intermediate service organization, and performs the signature verification on the decrypted organization secret key by using the root private key of the terminal
S302
The terminal stores the organization secret key in the secure storage region of the terminal after the signature verification passes
S303
The terminal encrypts a first terminal public key by a second encryption means
S304
The terminal sends the encrypted first terminal public key to the intermediate service organization
S305

Fig. 3

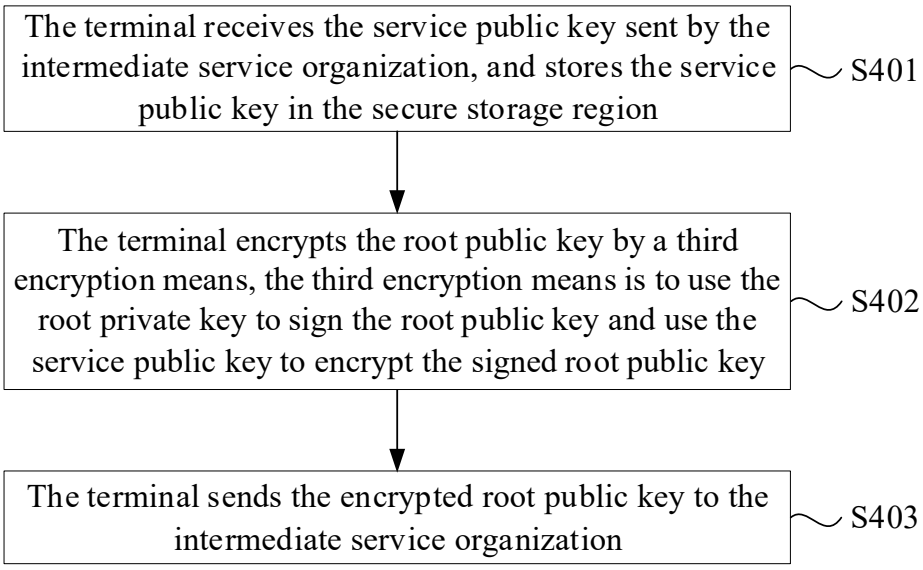
The terminal receives the service public key sent by the intermediate service organization, and stores the service public key in the secure storage region
S401
The terminal encrypts the root public key by a third encryption means, the third encryption means is to use the root private key to sign the root public key and use the service public key to encrypt the signed root public key
S402
The terminal sends the encrypted root public key to the intermediate service organization
S403

Fig. 4