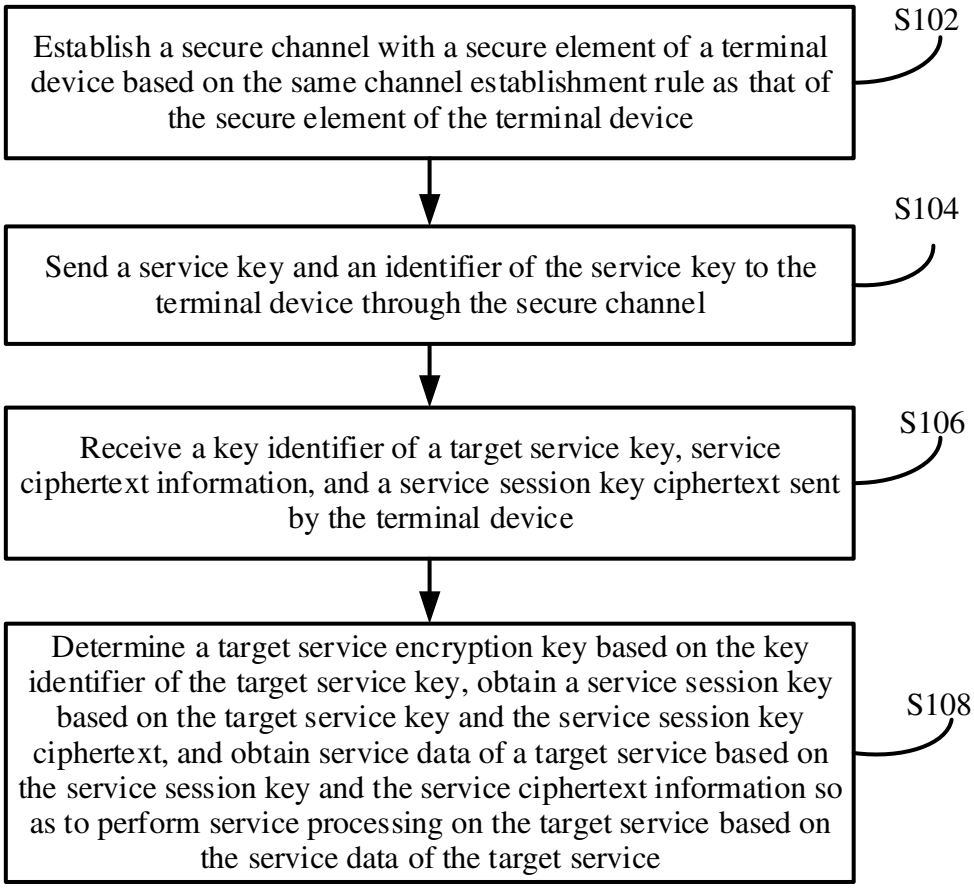

Establish a secure channel with a secure element of a terminal device based on the same channel establishment rule as that of the secure element of the terminal device
S102
Send a service key and an identifier of the service key to the terminal device through the secure channel
S104
Receive a key identifier of a target service key, service ciphertext information, and a service session key ciphertext sent by the terminal device
S106
Determine a target service encryption key based on the key identifier of the target service key, obtain a service session key based on the target service key and the service session key ciphertext, and obtain service data of a target service based on the service session key and the service ciphertext information so as to perform service processing on the target service based on the service data of the target service
S108

FIG. 1A

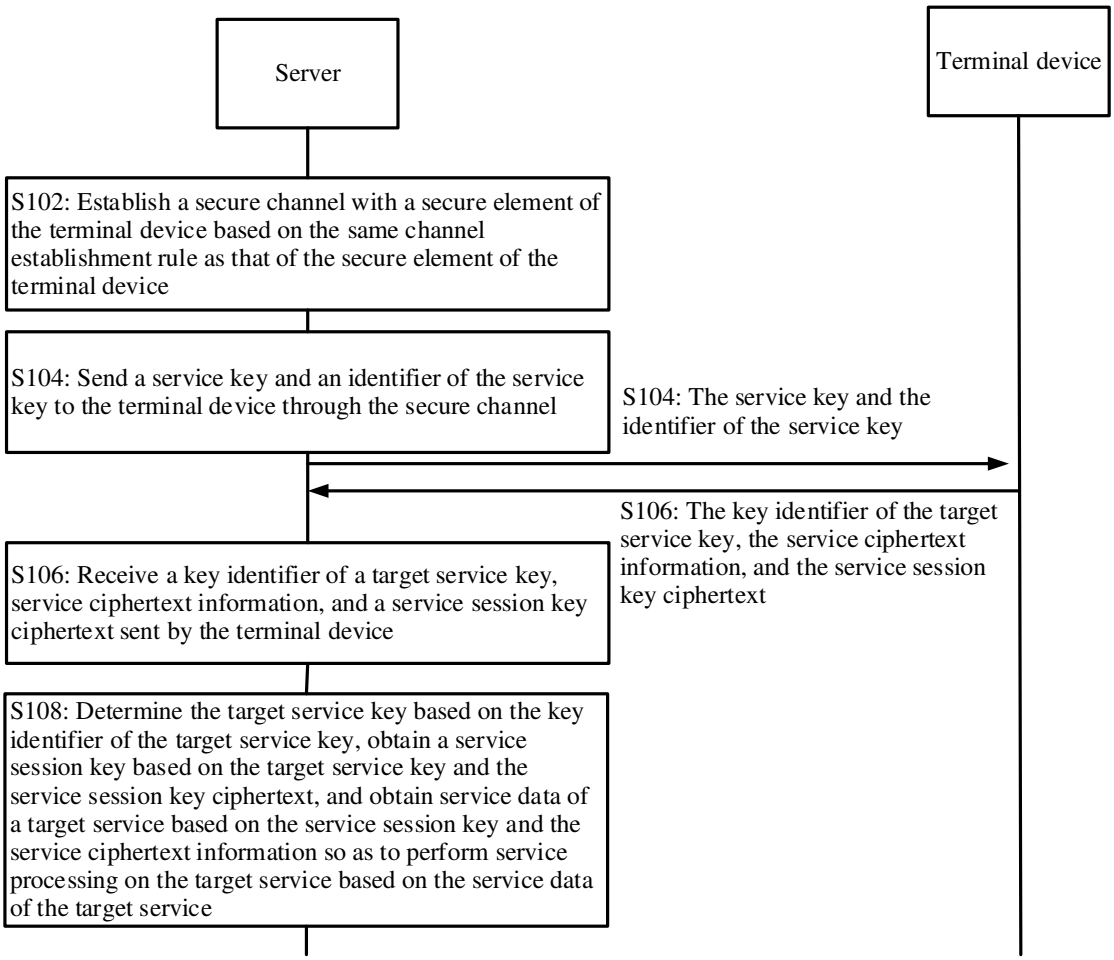

Server
Terminal device
S102: Establish a secure channel with a secure element of the terminal device based on the same channel establishment rule as that of the secure element of the terminal device
S104: Send a service key and an identifier of the service key to the terminal device through the secure channel
S104: The service key and the identifier of the service key
S106: The key identifier of the target service key, the service ciphertext information, and the service session key ciphertext
S106: Receive a key identifier of a target service key, service ciphertext information, and a service session key ciphertext sent by the terminal device
S108: Determine the target service key based on the key identifier of the target service key, obtain a service session key based on the target service key and the service session key ciphertext, and obtain service data of a target service based on the service session key and the service ciphertext information so as to perform service processing on the target service based on the service data of the target service

FIG. 1B

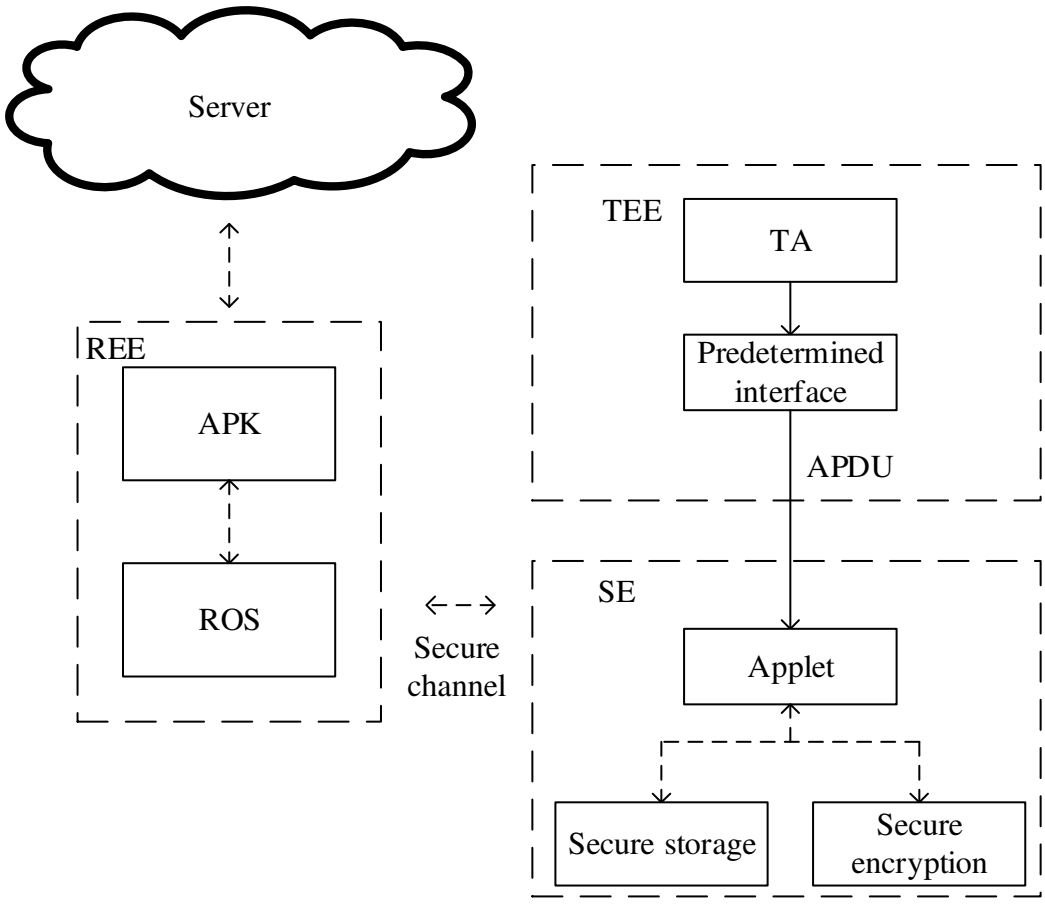

Server
REE
APK
ROS
Secure channel
TEE
TA
Predetermined interface
APDU
SE
Applet
Secure storage
Secure encryption

FIG. 2

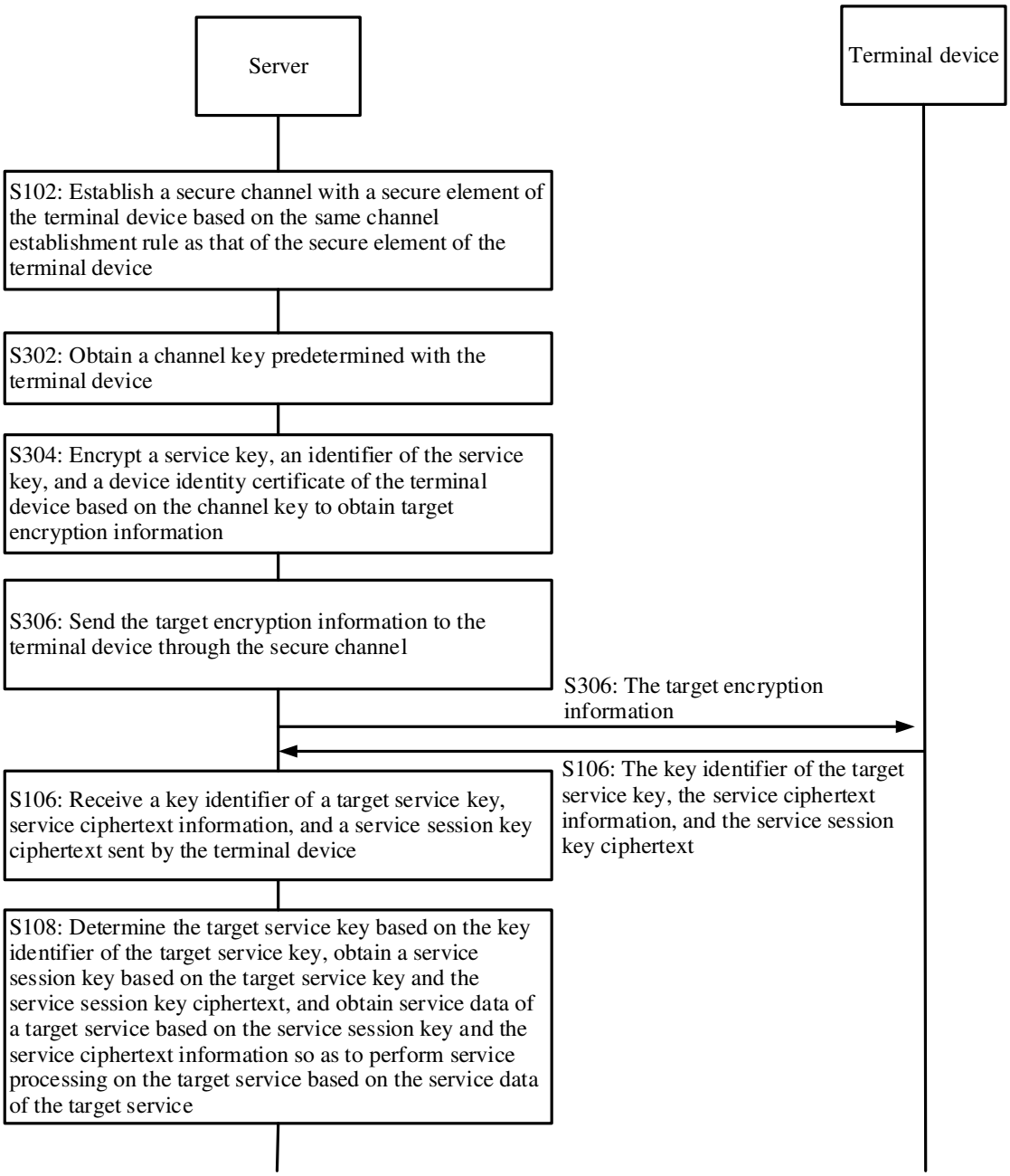

Server
Terminal device
S102: Establish a secure channel with a secure element of the terminal device based on the same channel establishment rule as that of the secure element of the terminal device
S302: Obtain a channel key predetermined with the terminal device
S304: Encrypt a service key, an identifier of the service key, and a device identity certificate of the terminal device based on the channel key to obtain target encryption information
S306: Send the target encryption information to the terminal device through the secure channel
S306: The target encryption information
S106: The key identifier of the target service key, the service ciphertext information, and the service session key ciphertext
S106: Receive a key identifier of a target service key, service ciphertext information, and a service session key ciphertext sent by the terminal device
S108: Determine the target service key based on the key identifier of the target service key, obtain a service session key based on the target service key and the service session key ciphertext, and obtain service data of a target service based on the service session key and the service ciphertext information so as to perform service processing on the target service based on the service data of the target service

FIG. 3

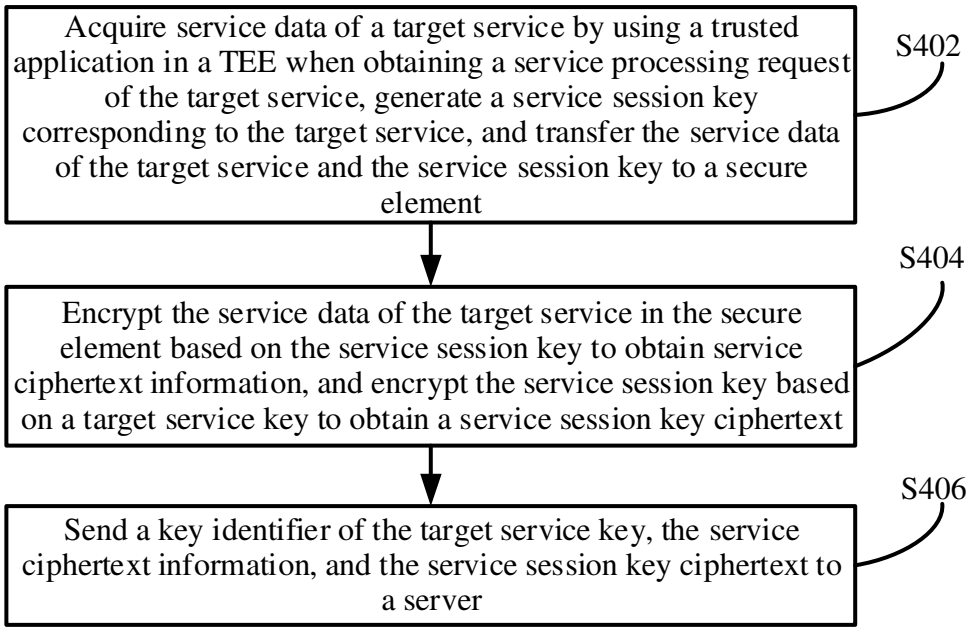

Acquire service data of a target service by using a trusted application in a TEE when obtaining a service processing request of the target service, generate a service session key corresponding to the target service, and transfer the service data of the target service and the service session key to a secure element
S402
Encrypt the service data of the target service in the secure element based on the service session key to obtain service ciphertext information, and encrypt the service session key based on a target service key to obtain a service session key ciphertext
S404
Send a key identifier of the target service key, the service ciphertext information, and the service session key ciphertext to a server
S406

FIG. 4A

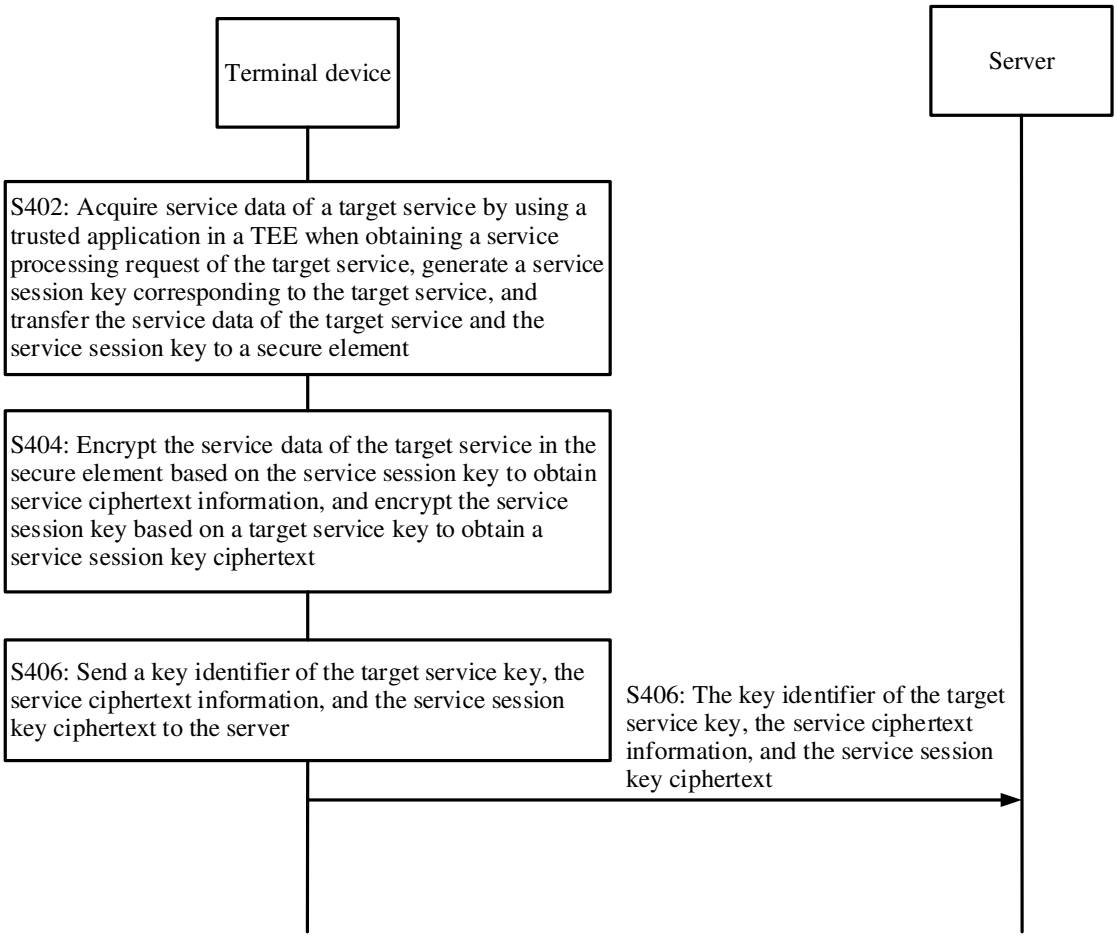

Terminal device
Server
S402: Acquire service data of a target service by using a trusted application in a TEE when obtaining a service processing request of the target service, generate a service session key corresponding to the target service, and transfer the service data of the target service and the service session key to a secure element
S404: Encrypt the service data of the target service in the secure element based on the service session key to obtain service ciphertext information, and encrypt the service session key based on a target service key to obtain a service session key ciphertext
S406: Send a key identifier of the target service key, the service ciphertext information, and the service session key ciphertext to the server
S406: The key identifier of the target service key, the service ciphertext information, and the service session key ciphertext

FIG. 4B

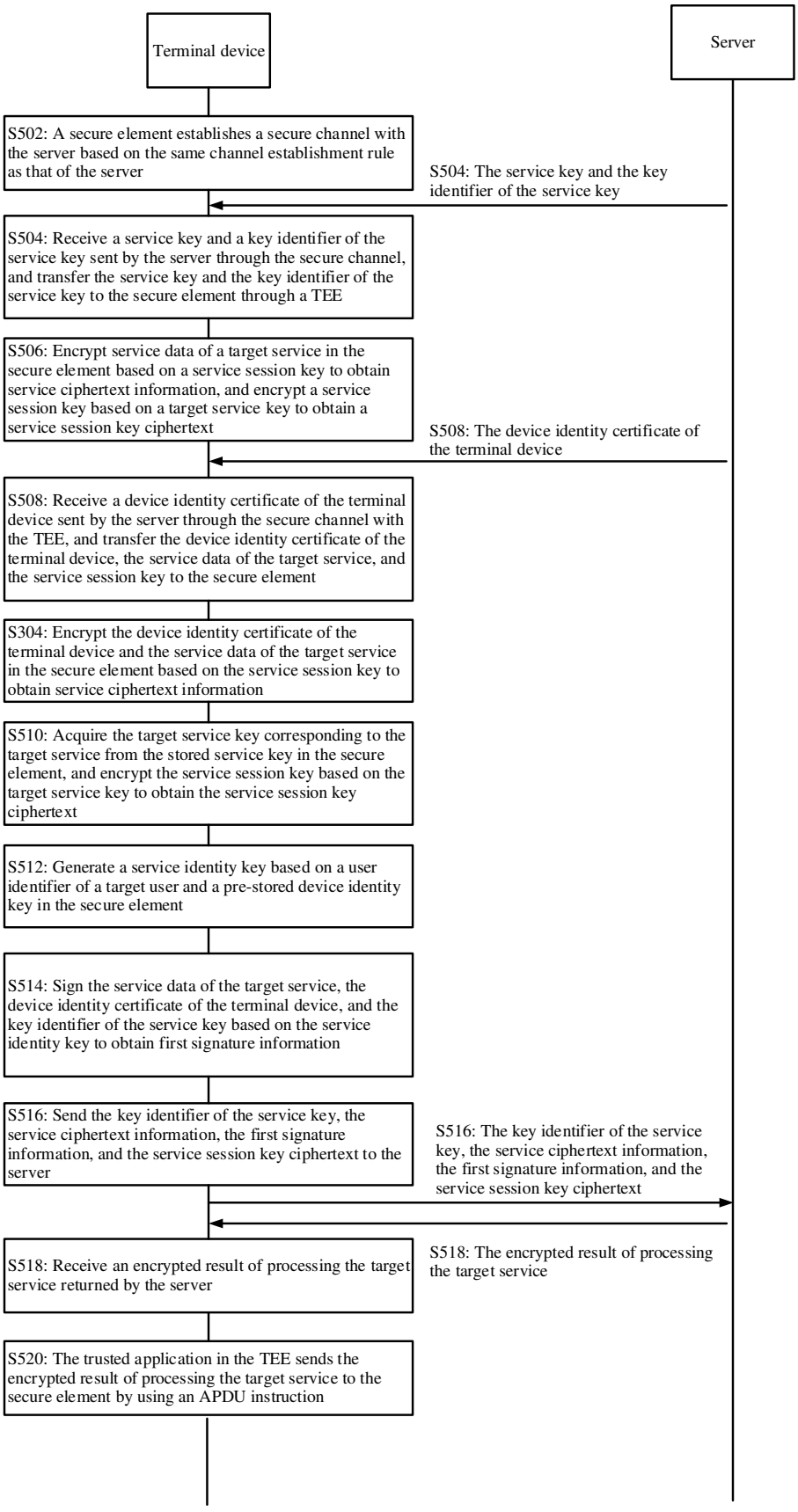

Terminal device
Server
S502: A secure element establishes a secure channel with the server based on the same channel establishment rule as that of the server
S504: The service key and the key identifier of the service key
S504: Receive a service key and a key identifier of the service key sent by the server through the secure channel, and transfer the service key and the key identifier of the service key to the secure element through a TEE
S506: Encrypt service data of a target service in the secure element based on a service session key to obtain service ciphertext information, and encrypt a service session key based on a target service key to obtain a service session key ciphertext
S508: The device identity certificate of the terminal device
S508: Receive a device identity certificate of the terminal device sent by the server through the secure channel with the TEE, and transfer the device identity certificate of the terminal device, the service data of the target service, and the service session key to the secure element
S304: Encrypt the device identity certificate of the terminal device and the service data of the target service in the secure element based on the service session key to obtain service ciphertext information
S510: Acquire the target service key corresponding to the target service from the stored service key in the secure element, and encrypt the service session key based on the target service key to obtain the service session key ciphertext
S512: Generate a service identity key based on a user identifier of a target user and a pre-stored device identity key in the secure element
S514: Sign the service data of the target service, the device identity certificate of the terminal device, and the key identifier of the service key based on the service identity key to obtain first signature information
S516: Send the key identifier of the service key, the service ciphertext information, the first signature information, and the service session key ciphertext to the server
S516: The key identifier of the service key, the service ciphertext information, the first signature information, and the service session key ciphertext
S518: Receive an encrypted result of processing the target service returned by the server
S518: The encrypted result of processing the target service
S520: The trusted application in the TEE sends the encrypted result of processing the target service to the secure element by using an APDU instruction

FIG. 5

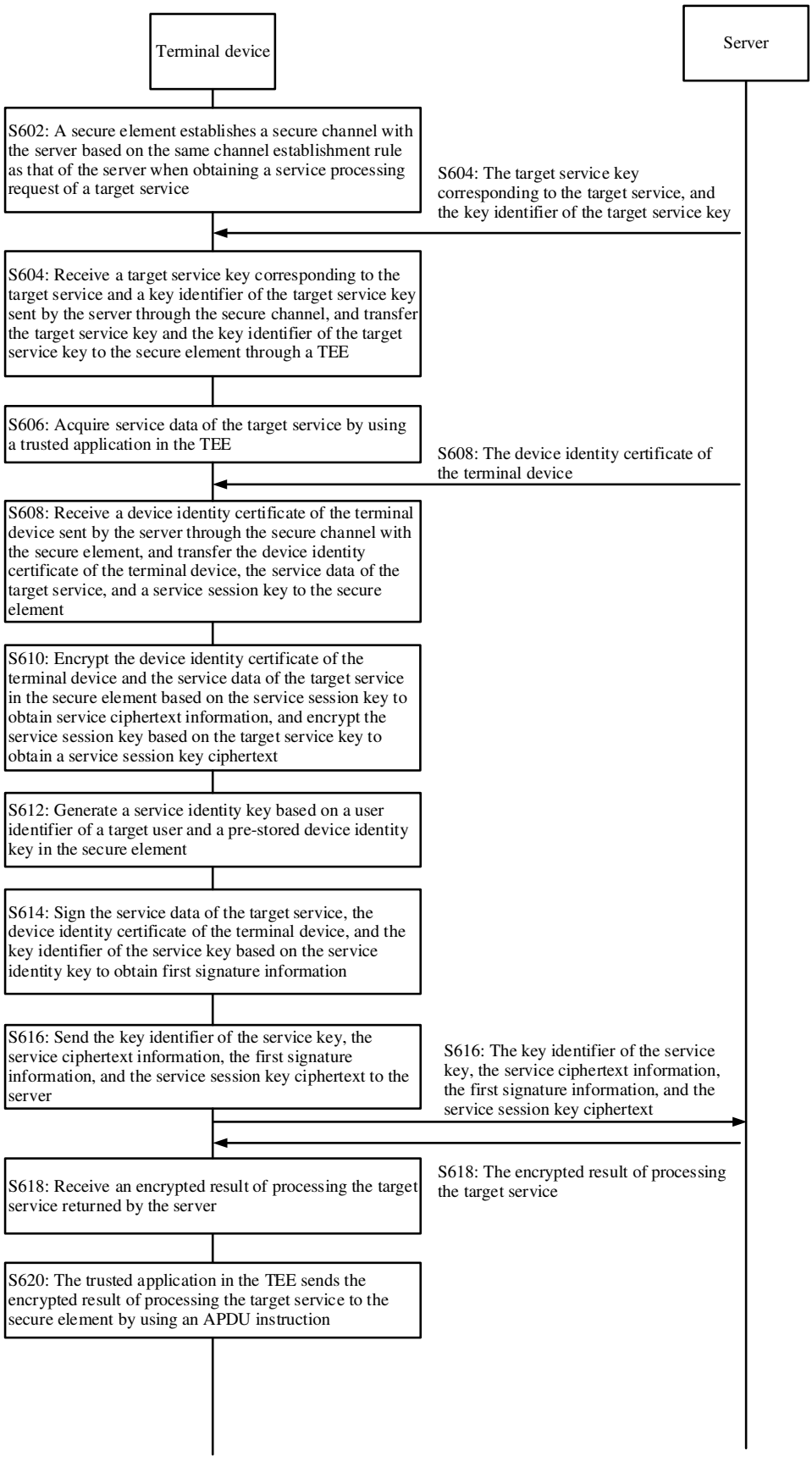

Terminal device
Server
S602: A secure element establishes a secure channel with the server based on the same channel establishment rule as that of the server when obtaining a service processing request of a target service
S604: The target service key corresponding to the target service, and the key identifier of the target service key
S604: Receive a target service key corresponding to the target service and a key identifier of the target service key sent by the server through the secure channel, and transfer the target service key and the key identifier of the target service key to the secure element through a TEE
S606: Acquire service data of the target service by using a trusted application in the TEE
S608: The device identity certificate of the terminal device
S608: Receive a device identity certificate of the terminal device sent by the server through the secure channel with the secure element, and transfer the device identity certificate of the terminal device, the service data of the target service, and a service session key to the secure element
S610: Encrypt the device identity certificate of the terminal device and the service data of the target service in the secure element based on the service session key to obtain service ciphertext information, and encrypt the service session key based on the target service key to obtain a service session key ciphertext
S612: Generate a service identity key based on a user identifier of a target user and a pre-stored device identity key in the secure element
S614: Sign the service data of the target service, the device identity certificate of the terminal device, and the key identifier of the service key based on the service identity key to obtain first signature information
S616: Send the key identifier of the service key, the service ciphertext information, the first signature information, and the service session key ciphertext to the server
S616: The key identifier of the service key, the service ciphertext information, the first signature information, and the service session key ciphertext
S618: Receive an encrypted result of processing the target service returned by the server
S618: The encrypted result of processing the target service
S620: The trusted application in the TEE sends the encrypted result of processing the target service to the secure element by using an APDU instruction

FIG. 6

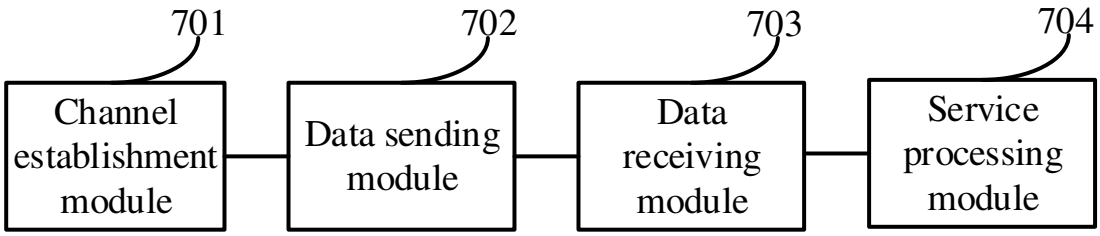


FIG. 7

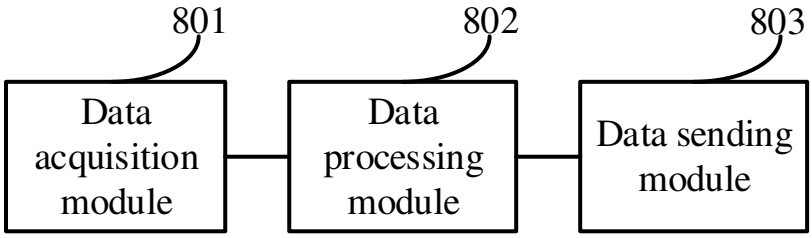


FIG. 8

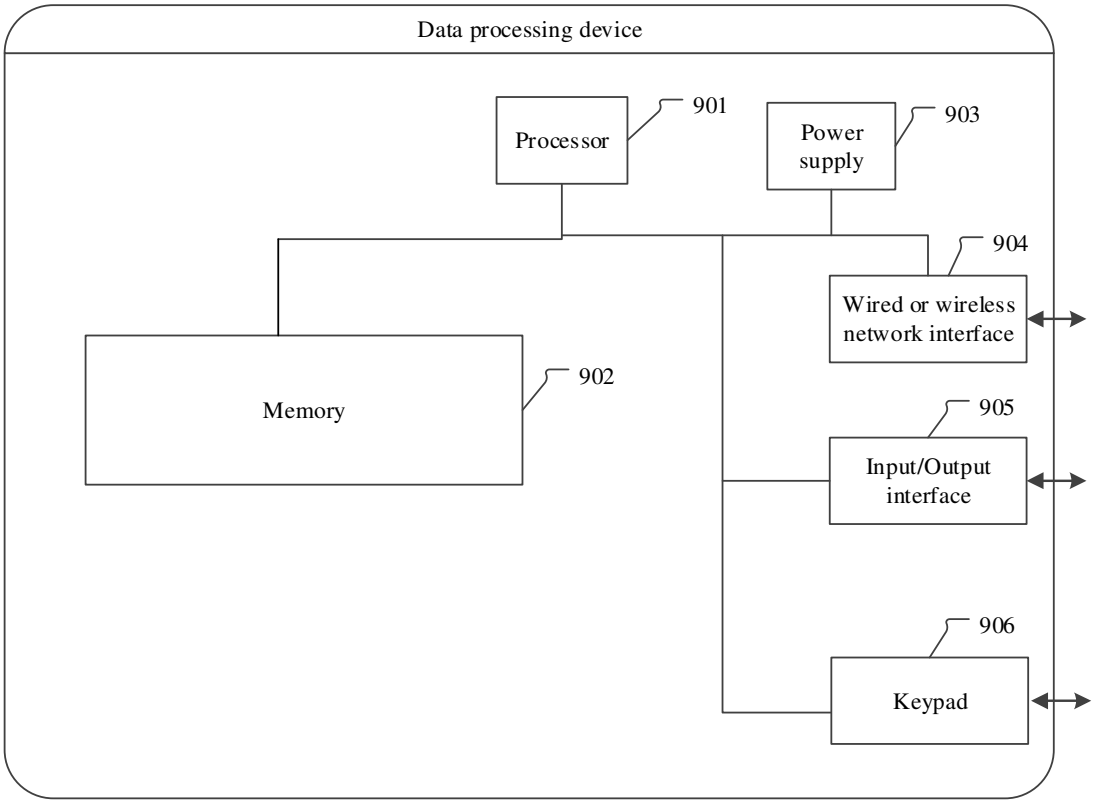


FIG. 9