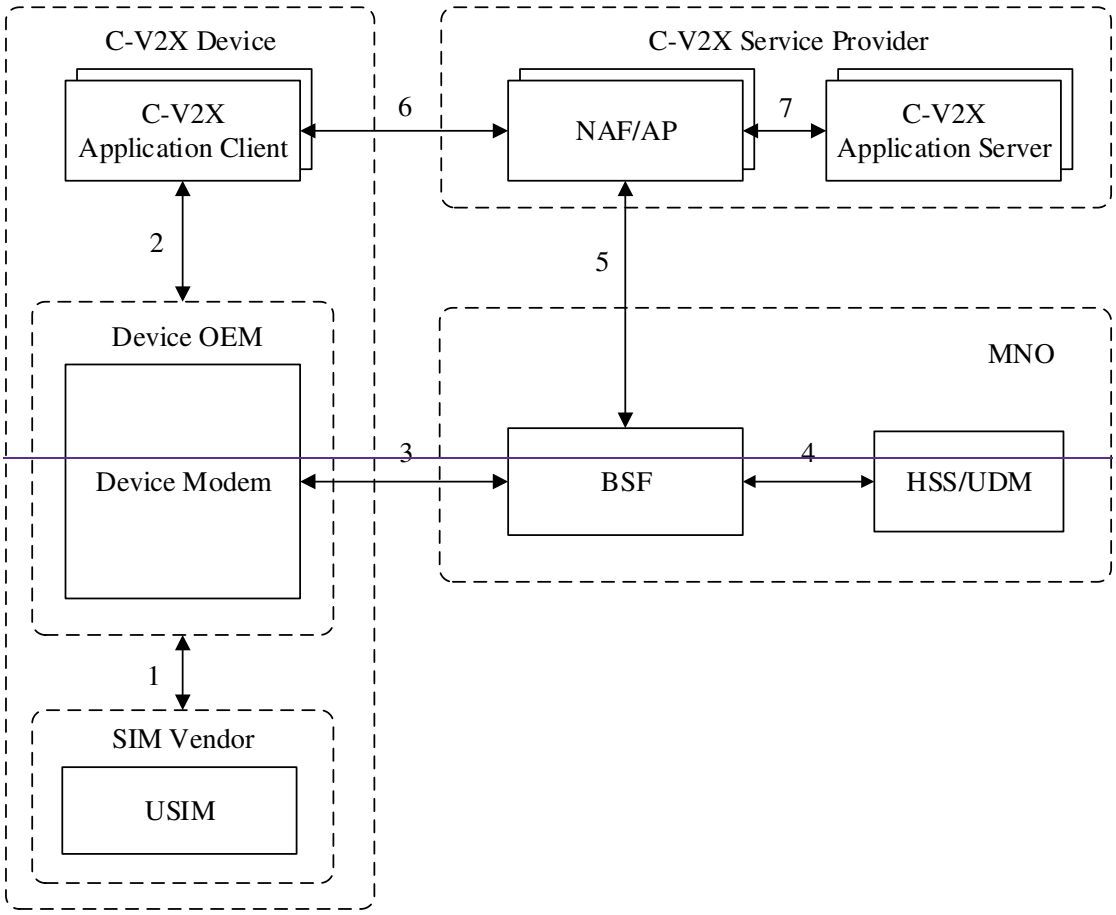

C-V2X Device
C-V2X Application Client
C-V2X Service Provider
NAF/AP
C-V2X Application Server
6
7
2
5
Device OEM
Device Modem
MNO
3
4
BSF
HSS/UDM
1
SIM Vendor
USIM

FIG. 1

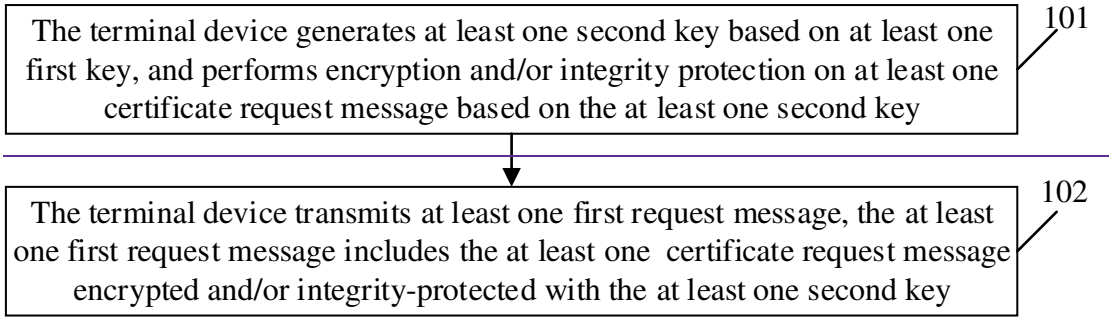

The terminal device generates at least one second key based on at least one first key, and performs encryption and/or integrity protection on at least one certificate request message based on the at least one second key
101
The terminal device transmits at least one first request message, the at least one first request message includes the at least one certificate request message encrypted and/or integrity-protected with the at least one second key
102

FIG. 2

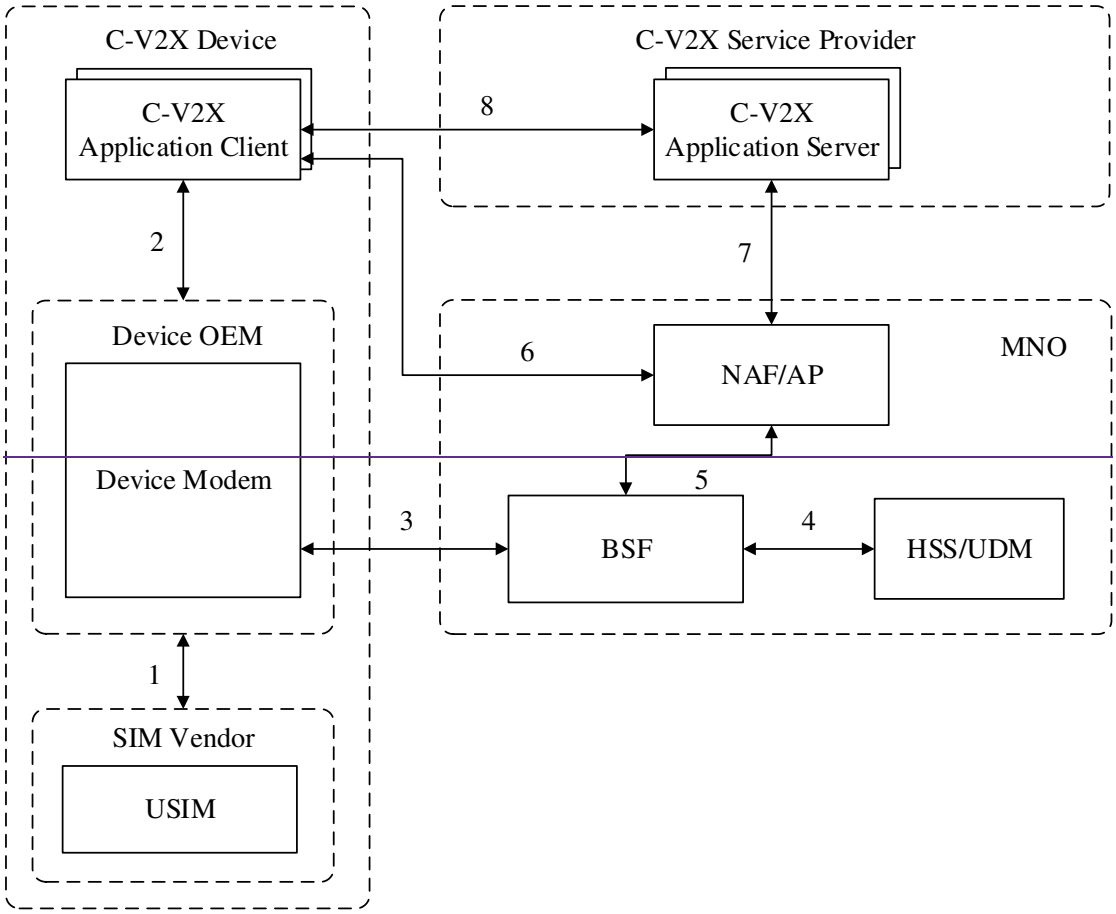

C-V2X Device
C-V2X Application Client
C-V2X Service Provider
C-V2X Application Server
8
2
7
Device OEM
Device Modem
6
NAF/AP
MNO
5
3
BSF
4
HSS/UDM
1
SIM Vendor
USIM

FIG. 3

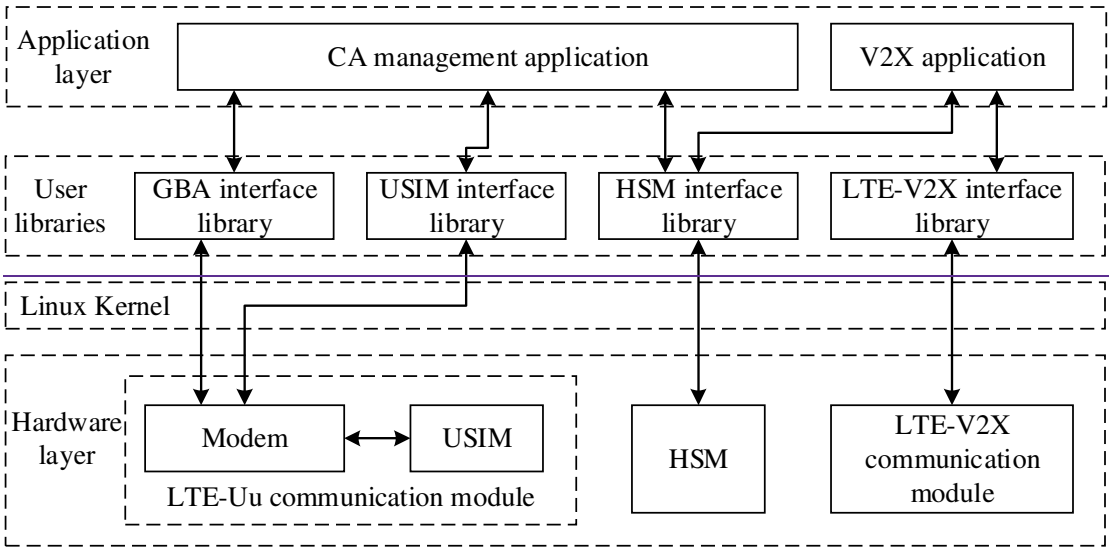

Application layer
CA management application
V2X application
User libraries
GBA interface library
USIM interface library
HSM interface library
LTE-V2X interface library
Linux Kernel
Hardware layer
Modem
USIM
LTE-Uu communication module
HSM
LTE-V2X communication module

FIG. 4

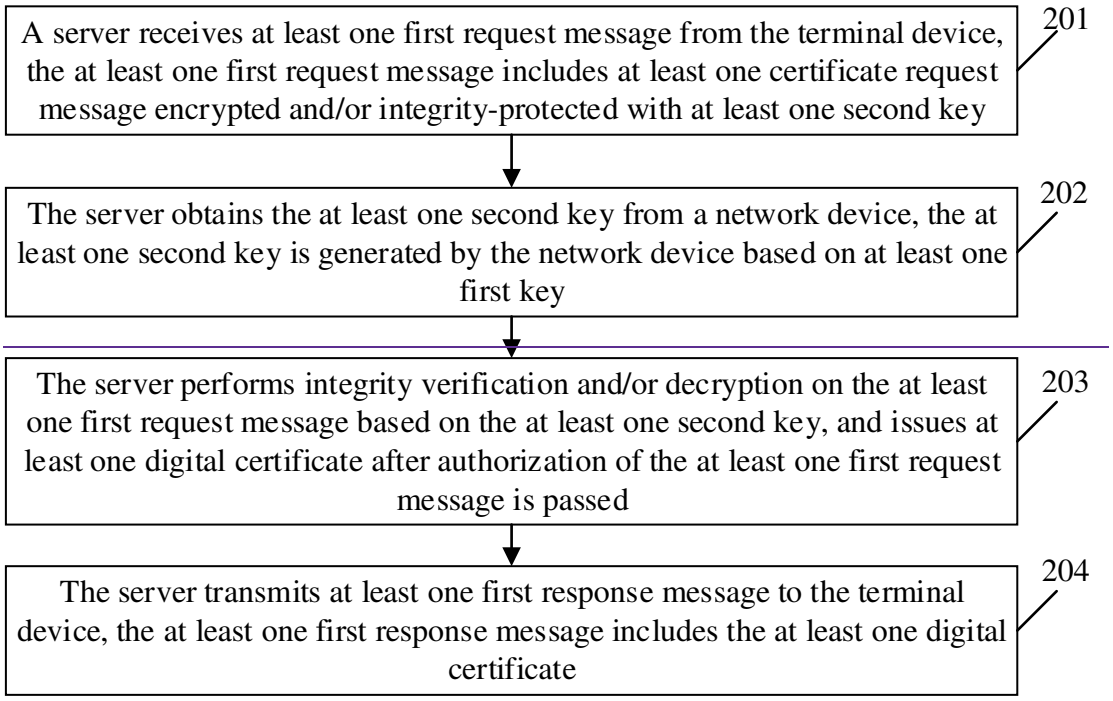

A server receives at least one first request message from the terminal device, the at least one first request message includes at least one certificate request message encrypted and/or integrity-protected with at least one second key
201
The server obtains the at least one second key from a network device, the at least one second key is generated by the network device based on at least one first key
202
The server performs integrity verification and/or decryption on the at least one first request message based on the at least one second key, and issues at least one digital certificate after authorization of the at least one first request message is passed
203
The server transmits at least one first response message to the terminal device, the at least one first response message includes the at least one digital certificate
204

FIG. 5

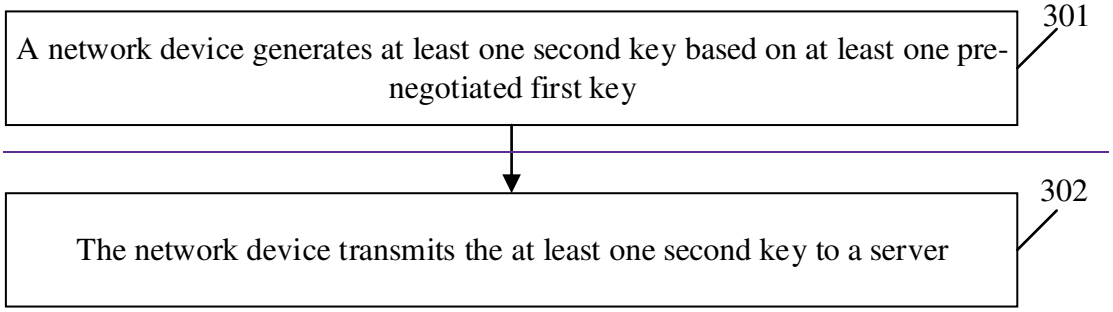

A network device generates at least one second key based on at least one pre-negotiated first key
301
The network device transmits the at least one second key to a server
302

FIG. 6

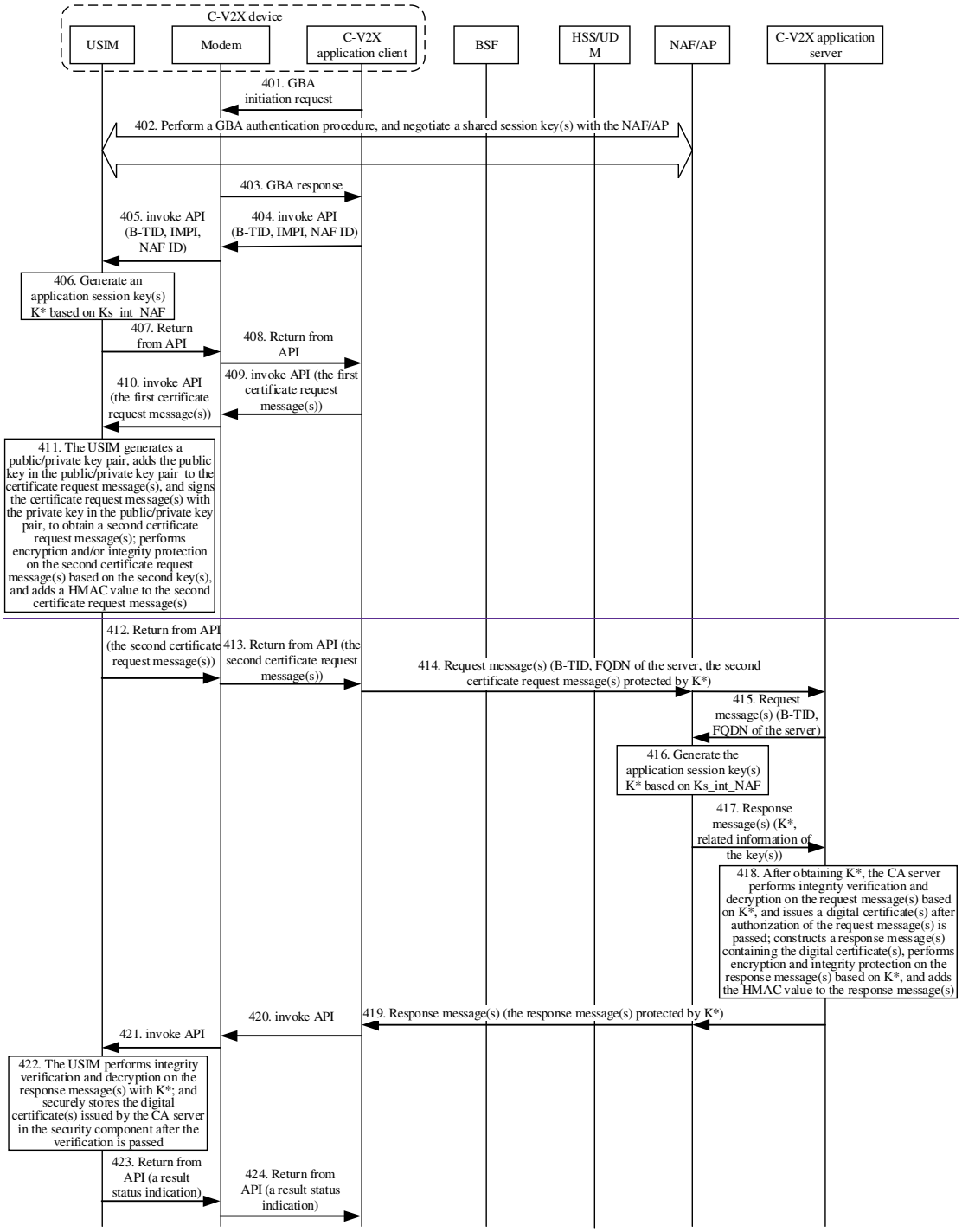

C-V2X device
USIM
Modem
C-V2X application client
BSF
HSS/UDM
NAF/AP
C-V2X application server
401. GBA initiation request
402. Perform a GBA authentication procedure, and negotiate a shared session key(s) with the NAF/AP
403. GBA response
404. invoke API (B-TID, IMPI, NAF ID)
405. invoke API (B-TID, IMPI, NAF ID)
406. Generate an application session key(s) K* based on Ks_int_NAF
407. Return from API
408. Return from API
409. invoke API (the first certificate request message(s))
410. invoke API (the first certificate request message(s))
411. The USIM generates a public/private key pair, adds the public key in the public/private key pair to the certificate request message(s), and signs the certificate request message(s) with the private key in the public/private key pair, to obtain a second certificate request message(s); performs encryption and/or integrity protection on the second certificate request message(s) based on the second key(s), and adds a HMAC value to the second certificate request message(s)
412. Return from API (the second certificate request message(s))
413. Return from API (the second certificate request message(s))
414. Request message(s) (B-TID, FQDN of the server, the second certificate request message(s) protected by K*)
415. Request message(s) (B-TID, FQDN of the server)
416. Generate the application session key(s) K* based on Ks_int_NAF
417. Response message(s) (K*, related information of the key(s))
418. After obtaining K*, the CA server performs integrity verification and decryption on the request message(s) based on K*, and issues a digital certificate(s) after authorization of the request message(s) is passed; constructs a response message(s) containing the digital certificate(s), performs encryption and integrity protection on the response message(s) based on K*, and adds the HMAC value to the response message(s)
419. Response message(s) (the response message(s) protected by K*)
420. invoke API
421. invoke API
422. The USIM performs integrity verification and decryption on the response message(s) with K*; and securely stores the digital certificate(s) issued by the CA server in the security component after the verification is passed
423. Return from API (a result status indication)
424. Return from API (a result status indication)

FIG. 7

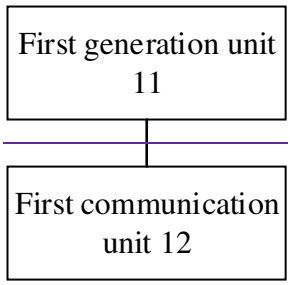


FIG. 8

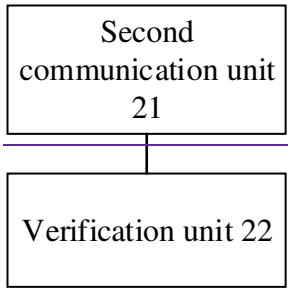


FIG. 9

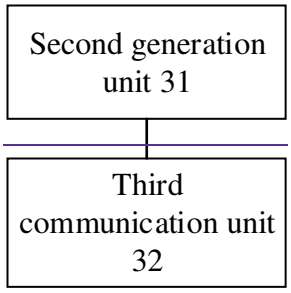


FIG. 10

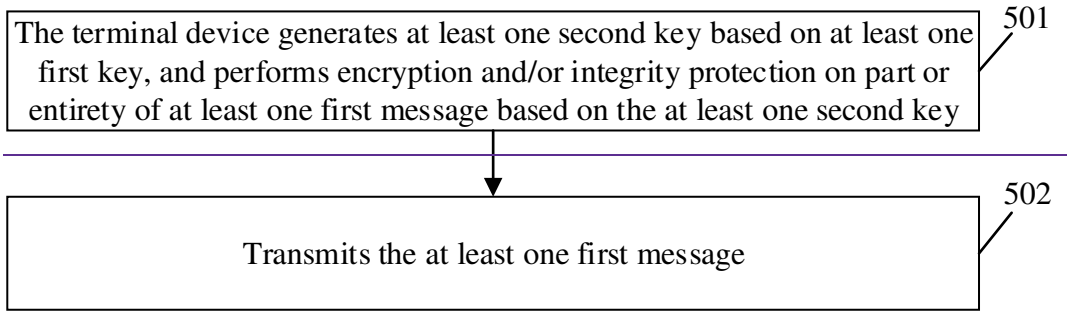

The terminal device generates at least one second key based on at least one first key, and performs encryption and/or integrity protection on part or entirety of at least one first message based on the at least one second key
501
Transmits the at least one first message
502

FIG. 11

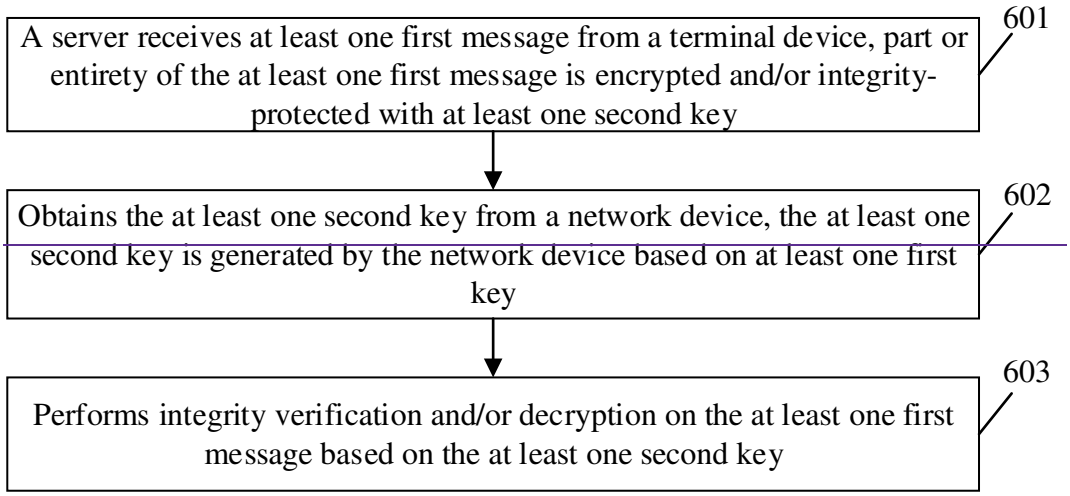

A server receives at least one first message from a terminal device, part or entirety of the at least one first message is encrypted and/or integrity-protected with at least one second key
601
Obtains the at least one second key from a network device, the at least one second key is generated by the network device based on at least one first key
602
Performs integrity verification and/or decryption on the at least one first message based on the at least one second key
603

FIG. 12

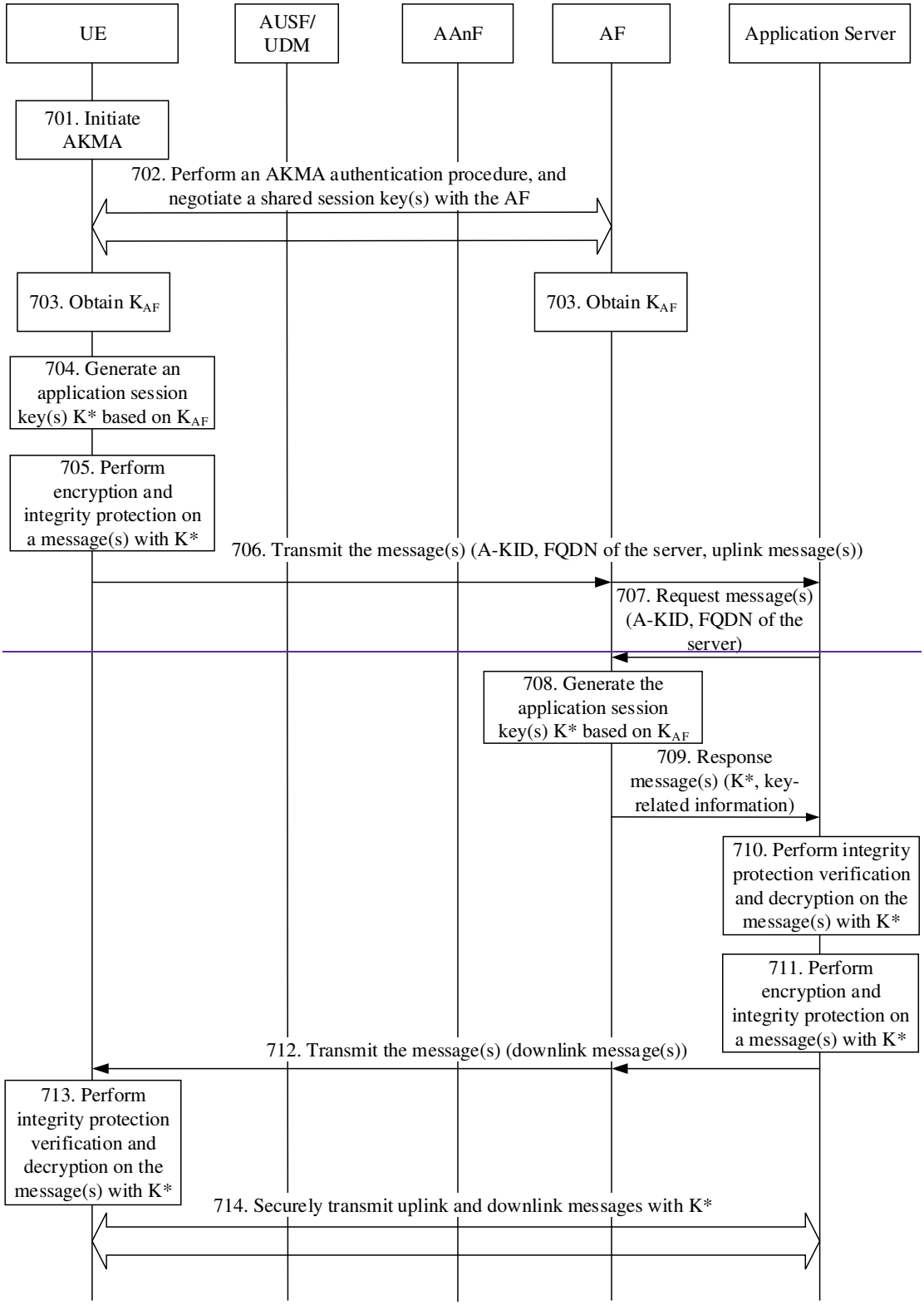

UE
AUSF/ UDM
AAnF
AF
Application Server
701. Initiate AKMA
702. Perform an AKMA authentication procedure, and negotiate a shared session key(s) with the AF
703. Obtain K_{AF}
703. Obtain K_{AF}
704. Generate an application session key(s) K* based on K_{AF}
705. Perform encryption and integrity protection on a message(s) with K*
706. Transmit the message(s) (A-KID, FQDN of the server, uplink message(s))
707. Request message(s) (A-KID, FQDN of the server)
708. Generate the application session key(s) K* based on K_{AF}
709. Response message(s) (K*, key-related information)
710. Perform integrity protection verification and decryption on the message(s) with K*
711. Perform encryption and integrity protection on a message(s) with K*
712. Transmit the message(s) (downlink message(s))
713. Perform integrity protection verification and decryption on the message(s) with K*
714. Securely transmit uplink and downlink messages with K*

FIG. 13

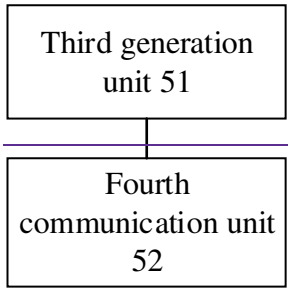


FIG. 14

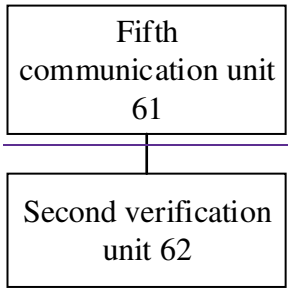


FIG. 15

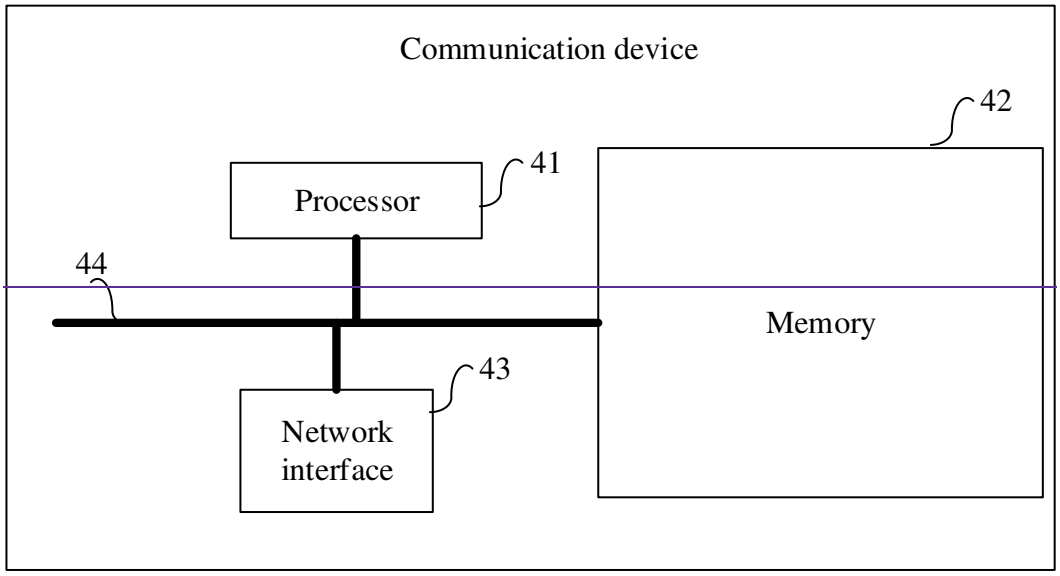


FIG. 16

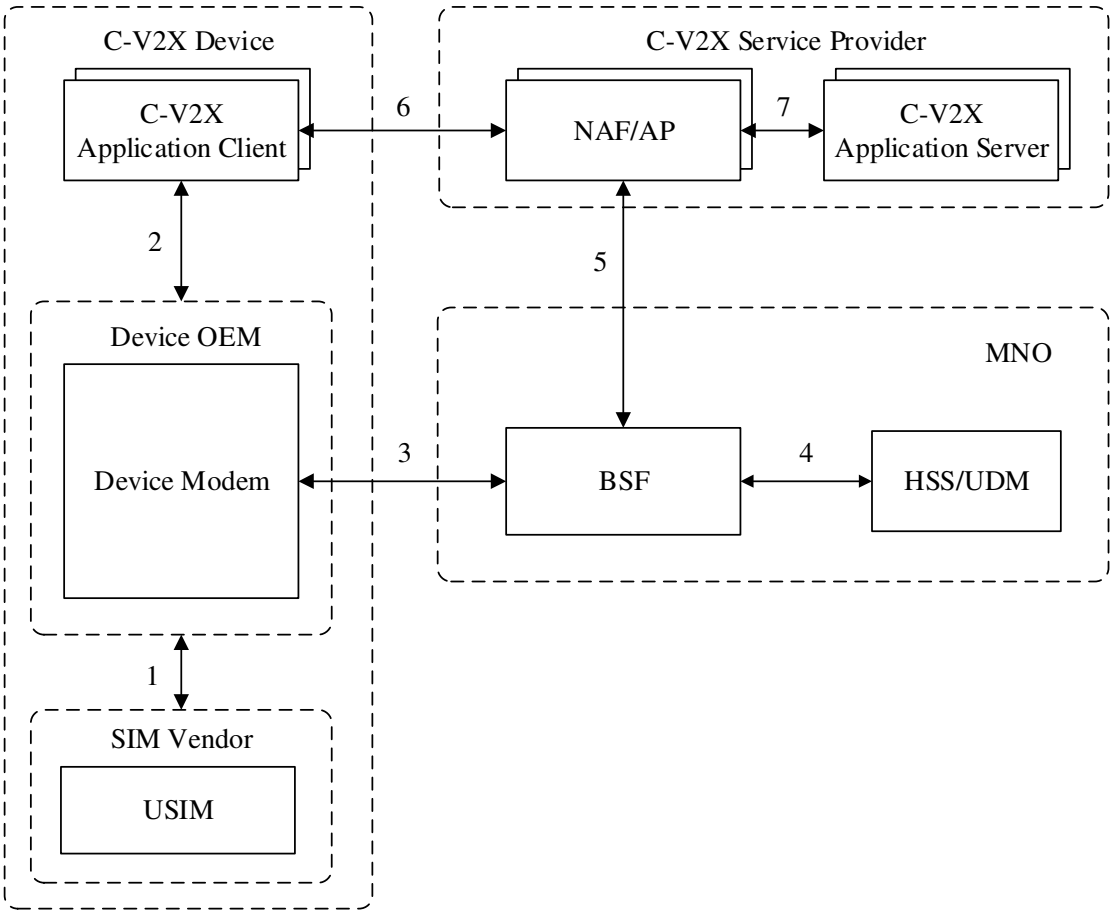

C-V2X Device
C-V2X Application Client
C-V2X Service Provider
NAF/AP
C-V2X Application Server
6
7
2
5
Device OEM
Device Modem
MNO
3
BSF
4
HSS/UDM
1
SIM Vendor
USIM

FIG. 1

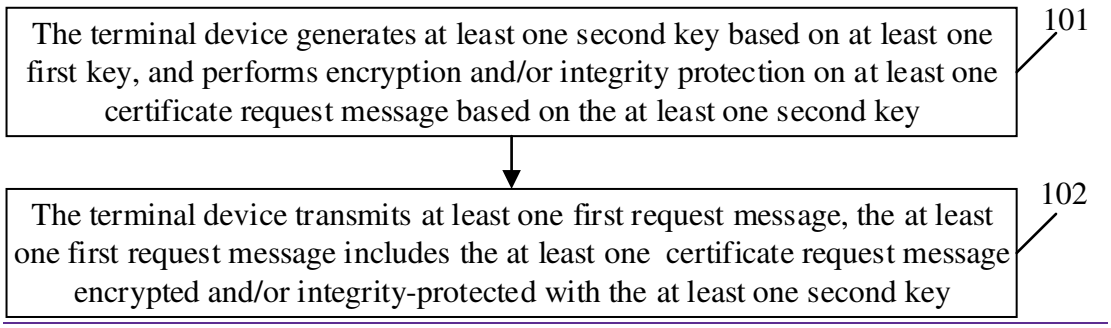

The terminal device generates at least one second key based on at least one first key, and performs encryption and/or integrity protection on at least one certificate request message based on the at least one second key
101
The terminal device transmits at least one first request message, the at least one first request message includes the at least one certificate request message encrypted and/or integrity-protected with the at least one second key
102

FIG. 2

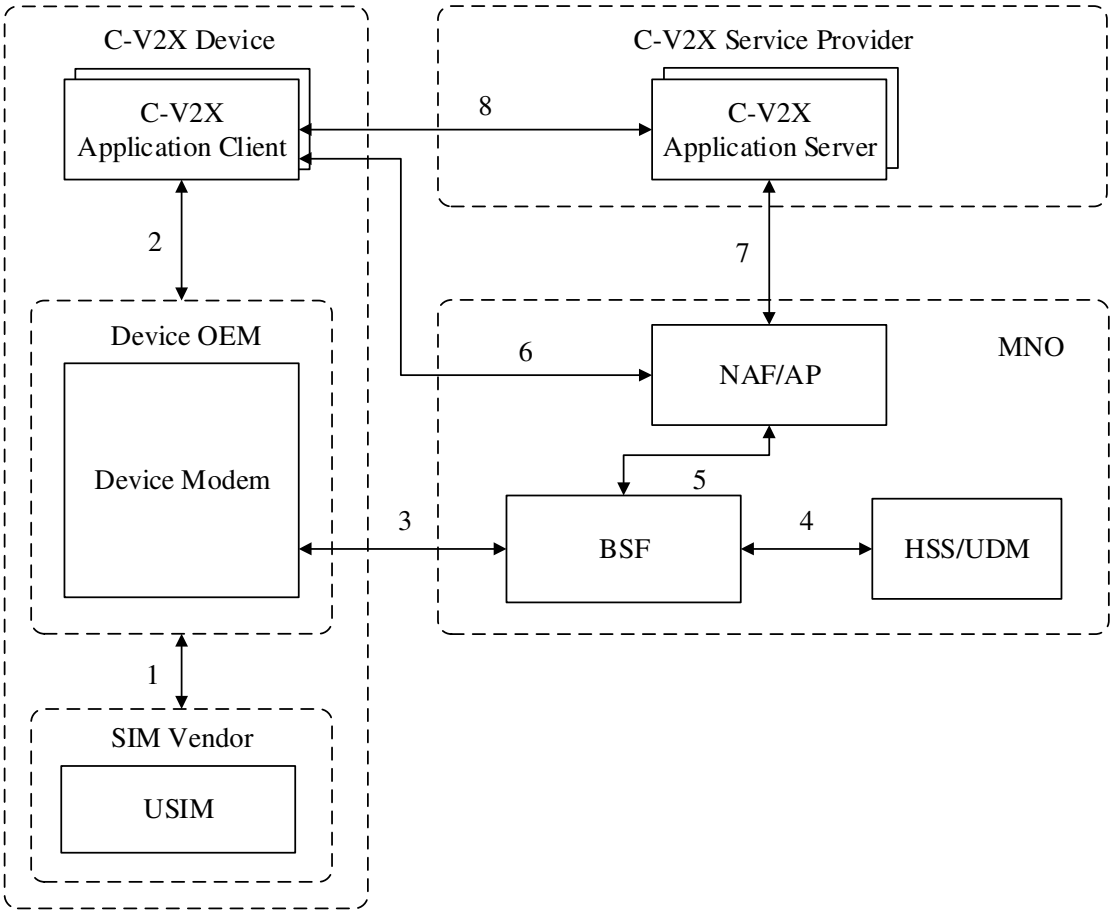

C-V2X Device
C-V2X Application Client
C-V2X Service Provider
C-V2X Application Server
8
2
7
Device OEM
Device Modem
6
NAF/AP
MNO
5
3
BSF
4
HSS/UDM
1
SIM Vendor
USIM

FIG. 3

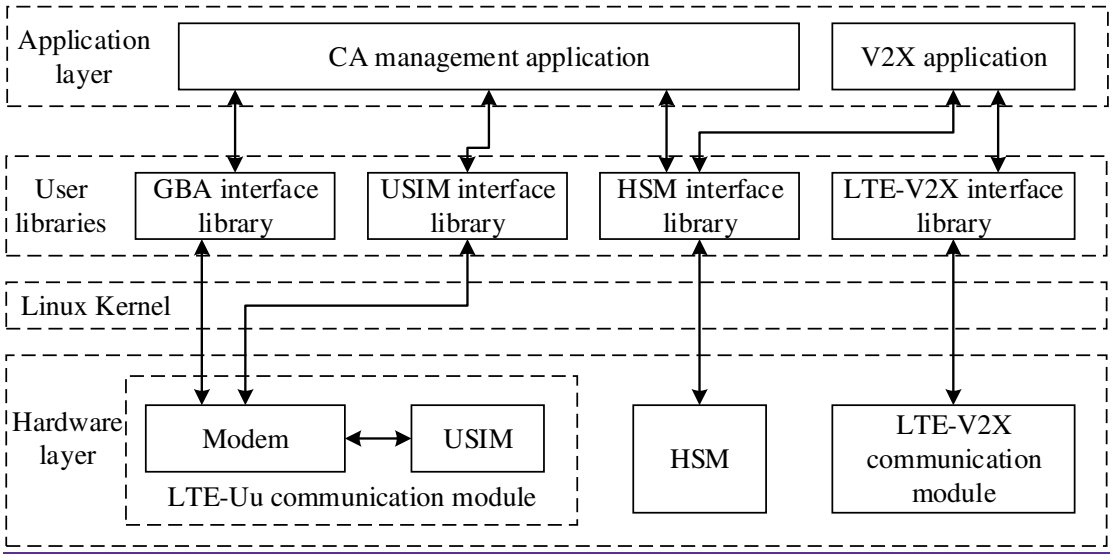

Application layer
CA management application
V2X application
User libraries
GBA interface library
USIM interface library
HSM interface library
LTE-V2X interface library
Linux Kernel
Hardware layer
Modem
USIM
LTE-Uu communication module
HSM
LTE-V2X communication module

FIG. 4

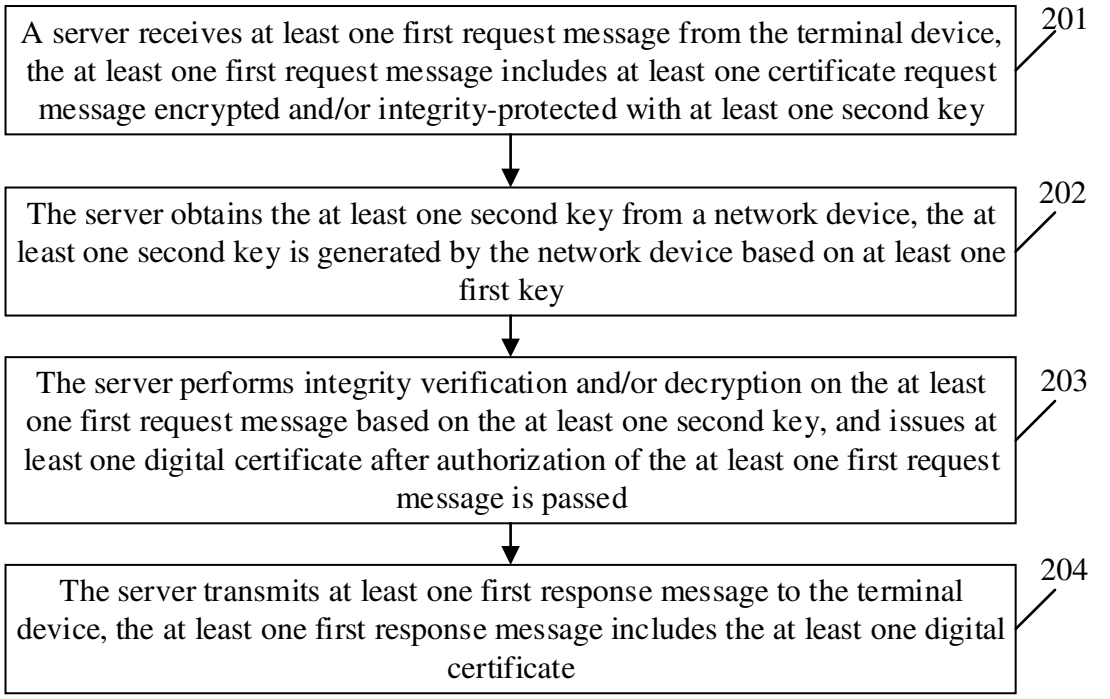

A server receives at least one first request message from the terminal device, the at least one first request message includes at least one certificate request message encrypted and/or integrity-protected with at least one second key
201
The server obtains the at least one second key from a network device, the at least one second key is generated by the network device based on at least one first key
202
The server performs integrity verification and/or decryption on the at least one first request message based on the at least one second key, and issues at least one digital certificate after authorization of the at least one first request message is passed
203
The server transmits at least one first response message to the terminal device, the at least one first response message includes the at least one digital certificate
204

FIG. 5

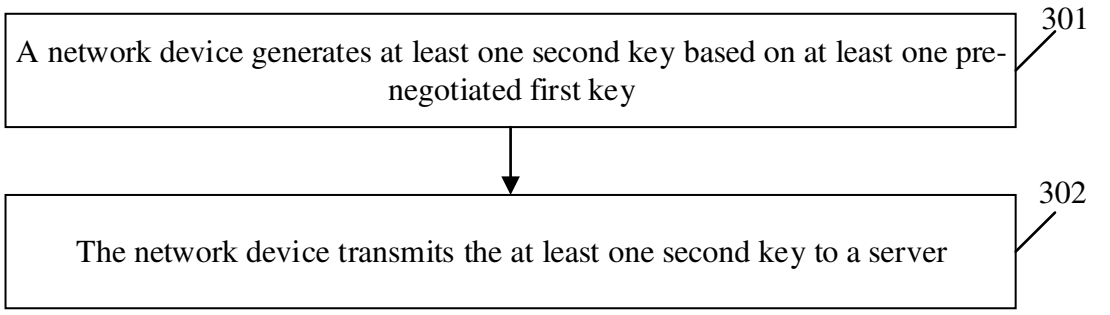

A network device generates at least one second key based on at least one pre-negotiated first key
301
The network device transmits the at least one second key to a server
302

FIG. 6

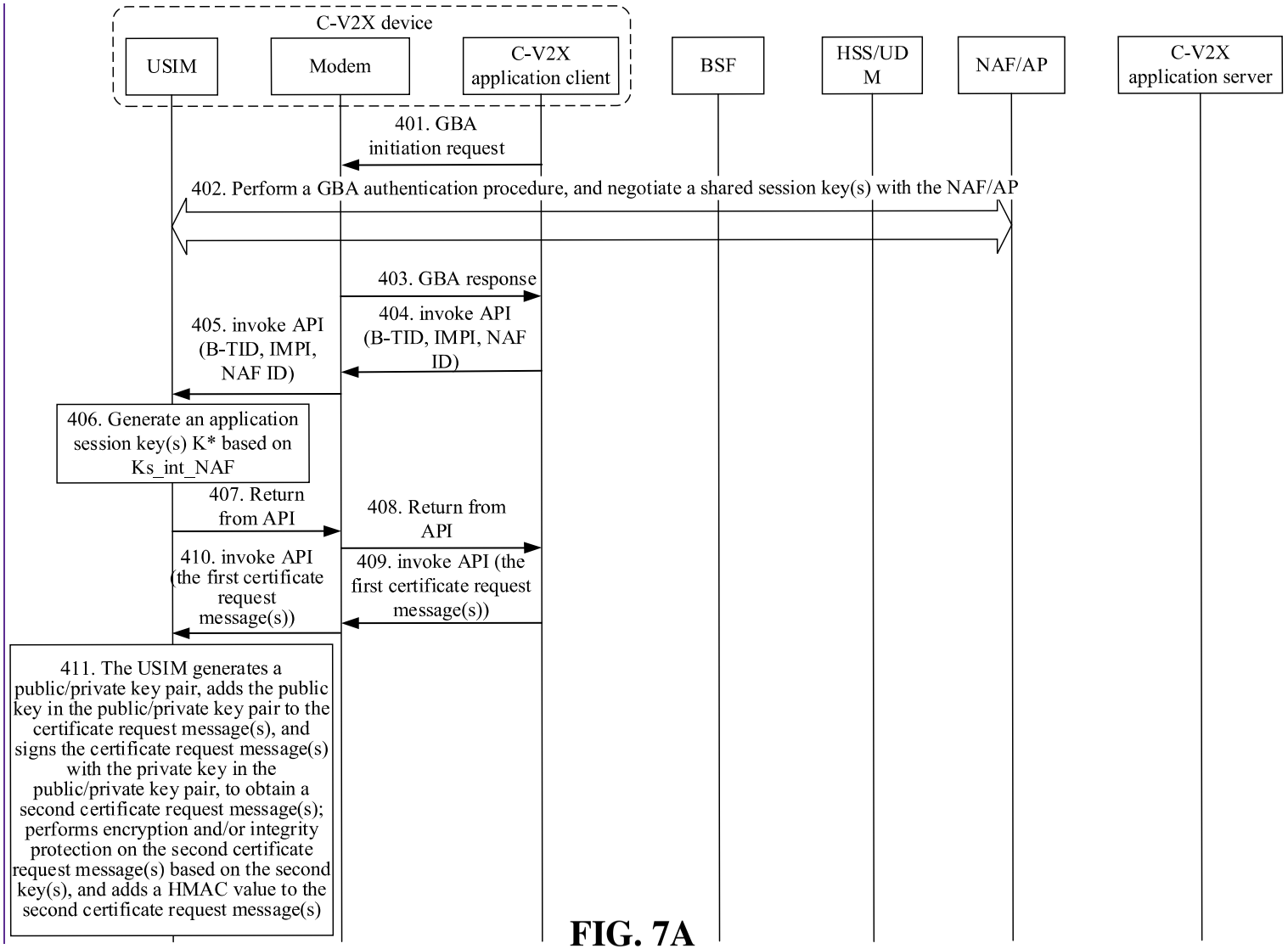

C-V2X device
USIM
Modem
C-V2X application client
BSF
HSS/UDM
NAF/AP
C-V2X application server
401. GBA initiation request
402. Perform a GBA authentication procedure, and negotiate a shared session key(s) with the NAF/AP
403. GBA response
404. invoke API (B-TID, IMPI, NAF ID)
405. invoke API (B-TID, IMPI, NAF ID)
406. Generate an application session key(s) K* based on Ks_int_NAF
407. Return from API
408. Return from API
409. invoke API (the first certificate request message(s))
410. invoke API (the first certificate request message(s))
411. The USIM generates a public/private key pair, adds the public key in the public/private key pair to the certificate request message(s), and signs the certificate request message(s) with the private key in the public/private key pair, to obtain a second certificate request message(s); performs encryption and/or integrity protection on the second certificate request message(s) based on the second key(s), and adds a HMAC value to the second certificate request message(s)

FIG. 7A

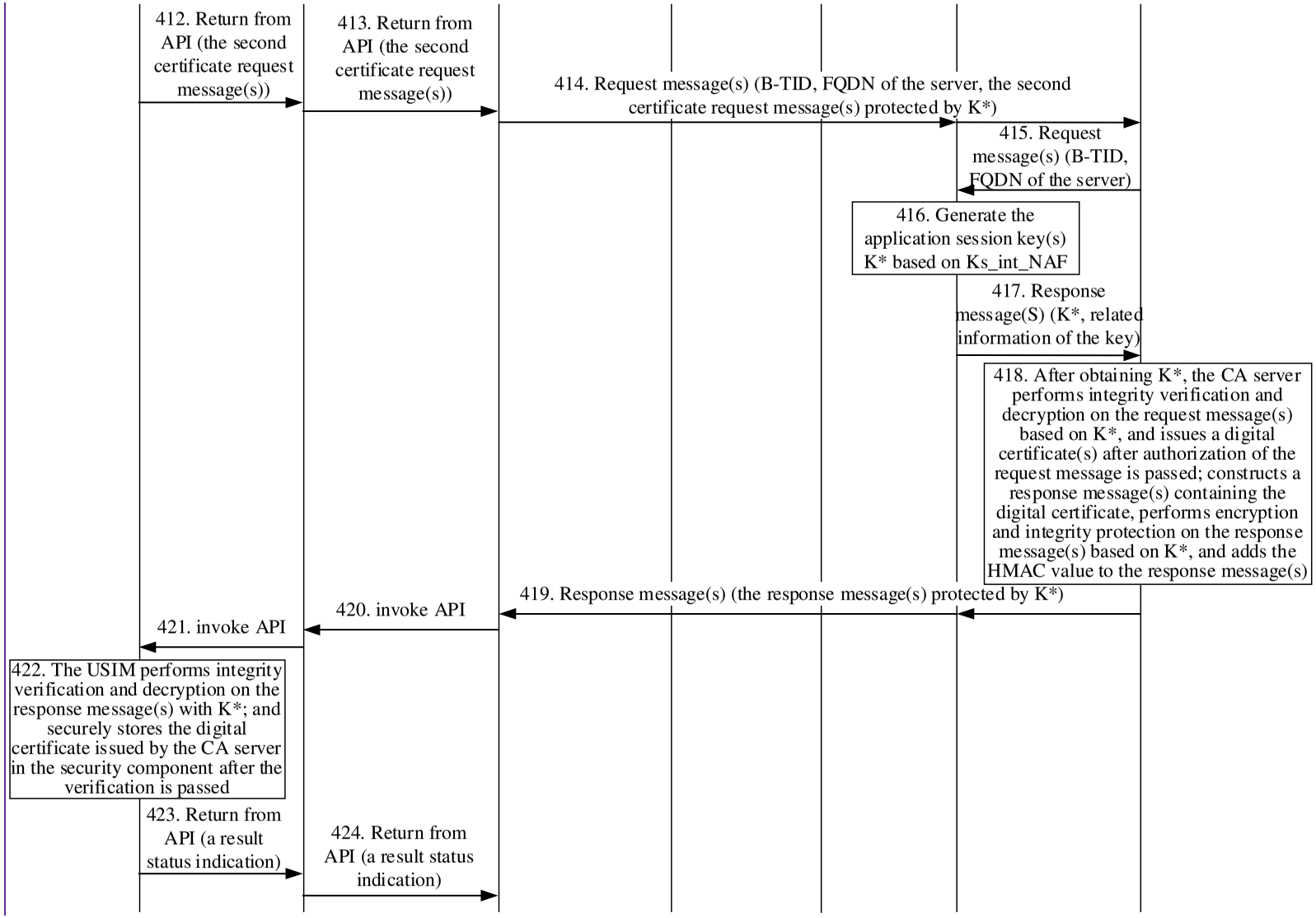

412. Return from API (the second certificate request message(s))
413. Return from API (the second certificate request message(s))
414. Request message(s) (B-TID, FQDN of the server, the second certificate request message(s) protected by K*)
415. Request message(s) (B-TID, FQDN of the server)
416. Generate the application session key(s) K* based on Ks_int_NAF
417. Response message(S) (K*, related information of the key)
418. After obtaining K*, the CA server performs integrity verification and decryption on the request message(s) based on K*, and issues a digital certificate(s) after authorization of the request message is passed; constructs a response message(s) containing the digital certificate, performs encryption and integrity protection on the response message(s) based on K*, and adds the HMAC value to the response message(s)
419. Response message(s) (the response message(s) protected by K*)
420. invoke API
421. invoke API
422. The USIM performs integrity verification and decryption on the response message(s) with K*; and securely stores the digital certificate issued by the CA server in the security component after the verification is passed
423. Return from API (a result status indication)
424. Return from API (a result status indication)

FIG. 7B

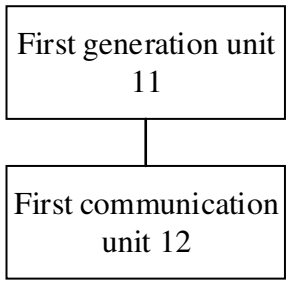


FIG. 8

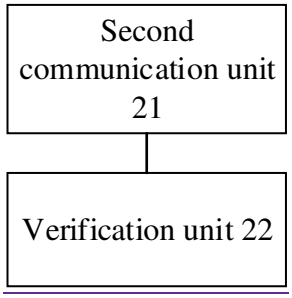


FIG. 9

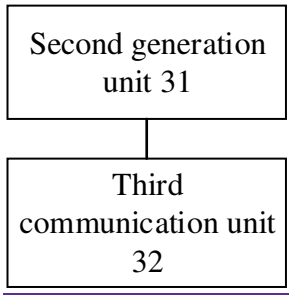


FIG. 10

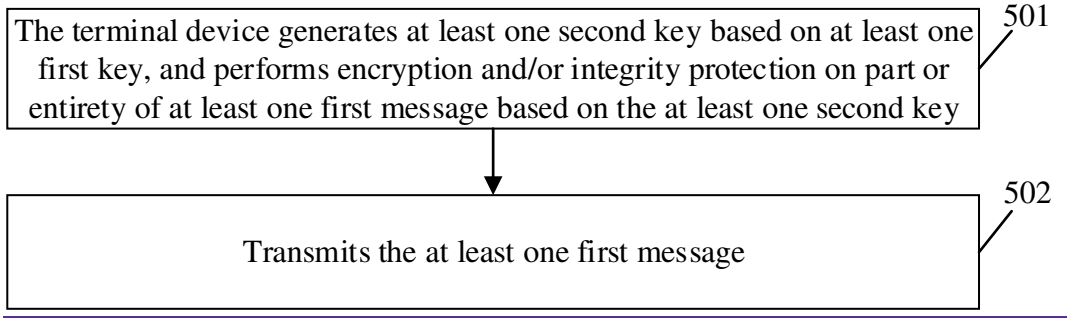


FIG. 11

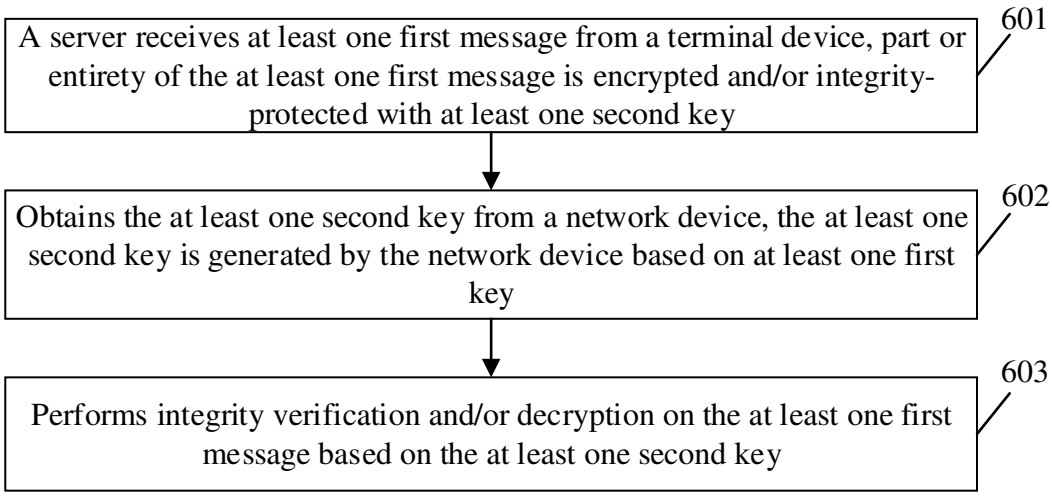

A server receives at least one first message from a terminal device, part or entirety of the at least one first message is encrypted and/or integrity-protected with at least one second key
601
Obtains the at least one second key from a network device, the at least one second key is generated by the network device based on at least one first key
602
Performs integrity verification and/or decryption on the at least one first message based on the at least one second key
603

FIG. 12