message is obtained by encrypting and integrity-protecting a message using the first key, and wherein the second key is established using a communication between the wireless device and a second network function.

In another ~~aspect~~example, a wireless communication device is disclosed. The device includes one or more processors configured to generate an encrypted and integrity-protected message, and a transceiver configured to transmit the encrypted and integrity-protected message to a first network function, wherein the encrypted and integrity-protected message is encrypted using a first key that is derived from a second key, wherein the second key is established using a communication with a second network function, and wherein the encrypted and integrity-protected message is obtained by encrypting and integrity-protecting a message.

In another ~~aspect~~ example, a network device is disclosed. The device includes a transceiver configured to receive an encrypted and integrity-protected message from a wireless device, and one or more processors configured to perform a first network function including decrypting the encrypted and integrity-protected message using a first key that is derived from a second key, wherein the encrypted and integrity-protected message is obtained by encrypting and integrity-protecting a message using the first key, and wherein the second key is established using a communication between the wireless device and a second network function.

In another aspect, a wireless communication apparatus comprising a processor configured to implement a method ~~described herein is disclosed~~according to the first or second aspect.

In another ~~aspect~~example, computer readable medium including executable instructions to implement a method described herein is disclosed.

These, and other, aspects are described in the present document.

BRIEF DESCRIPTION OF DRAWINGS

FIG. 1 shows an example of a base station (BS) and user equipment (UE) in wireless communication.

FIG. 2 shows an example architecture for proximity-based services (ProSe).

FIG. 3 shows an example of open discovery security procedure.

FIG. 4 shows an example of K_{AKMA} derivation after primary authentication.

FIG. 5 shows an example of K_{AF} generation from K_{AKMA}.

FIG. 6 shows an example procedure for security protection of the PC3 interface.

CLAIMS

What is claimed is:

1. A method of wireless communication, comprising:

transmitting, by a wireless device to a first network function, an encrypted and integrity-protected message,

wherein the encrypted and integrity-protected message is encrypted using a first key that is derived from a second key,

wherein the wireless device has established the second key using a communication with a second network function, and

wherein the encrypted and integrity-protected message is obtained by encrypting and integrity-protecting a message.

2. The method of claim 1, wherein the first key is used to obtain the encrypted and integrity-protected message by:

generating, by the wireless device, an encryption key and an integrity key based on the first key; and

encrypting the message using the encryption key and integrity-protecting the message using the integrity key.

3. The method of claim 1, wherein the first key includes an authentication and key management for applications (AKMA) application key, and the second key includes an AKMA anchor key.

4. The method of claim 1, wherein the encrypted and integrity-protected message includes a discovery request message that is transmitted through an interface for establishing proximity-based services.

5. The method of claim 1, wherein the encrypted and integrity-protected message includes ~~the~~a discovery request message that includes an AKMA key identifier (A-KID) and a message

authentication code (MAC).

6. The method of claim 5, wherein, in a case that the first network function does not have an active context associated with the A-KID, the first network function transmits, to the second network function, a first request for acquiring the first key to be used by the wireless device.

~~7. The method of claim 6, wherein the first request includes an identity of the first network function that includes a fully qualified domain name (FQDN) and a security protocol identifier for a reference point that carries an application protocol.~~

~~8~~7. The method of any of claims 1-~~7~~6, further comprising:

receiving, by the wireless device, a discovery response message from the first network function; and

checking a message authentication code (MAC) of the discovery response message and decrypting the discovery response message by using the first key or by using the encryption key and ~~the~~ an integrity key generated based on the first key.

~~9~~8. A method of wireless communication, comprising:

receiving, by a first network function, an encrypted and integrity-protected message from a wireless device; and

decrypting the encrypted and integrity-protected message using a first key that is derived from a second key,

wherein the encrypted and integrity-protected message is obtained by encrypting and integrity-protecting a message using the first key, and

wherein the second key is established using a communication between the wireless device and a second network function.

~~10~~9. The method of claim ~~9~~8, wherein the decrypting the encrypted and integrity-protected message using the first key comprises:

generating an encryption key and an integrity key based on the first key;

checking a message authentication code (MAC) of the encrypted and integrity-protected message using the integrity key; and

decrypting the encrypted and integrity-protected message using the encryption key.

~~11~~10. The method of claim ~~9~~8, wherein the second network function determines whether the second network function is configured to provide a service to the first network function based on at least one of a configured local policy, authorization information, or a policy provided by a network repository function using an identity of the first network function.

~~12~~11. The method of claim ~~9~~8, wherein the second network function verifies whether a subscriber is authorized to use AKMA based on presence of the second key identified by an A-KID.

~~13~~12. The method of claim ~~12~~11, wherein, in a case that the second key is present in the second network function, the second network function derives the first key from the second key, or in a case that the second key is not present in the second network function, the second network function transmits, to an application function, a first response for responding to a first request for acquiring the first key, the first key, and an expiration time of the first key.

~~14~~13. The method of claim ~~9~~8, wherein the encrypted and integrity-protected message received from the wireless device includes a discovery request message that is transmitted through an interface for establishing proximity-based services.

~~15. The method of claim 14, further comprising:~~

~~encrypting and integrity-protecting, by the first network function, a discovery response message based on the first key; and~~

~~transmitting the encrypted and integrity-protected discovery response message to the wireless device.~~

~~16. The method of claim 15, wherein the first key is used to encrypt and integrity-protect the discovery response message by:~~

~~generating an encryption key and an integrity key based on the first key; and~~

~~encrypting the discovery response message using the encryption key and integrity-protecting the discovery response message using the integrity key.~~

~~17~~14. The method of any of claims 1-~~16~~13, wherein the first network function includes a direct discovery name management function (DDNMF), and the second network function includes AKMA anchor function.

~~18. The method of any of claims 1-16, wherein the second network function includes AKMA anchor function.~~

~~19. A wireless communication device, comprising:~~

~~one or more processors configured to generate an encrypted and integrity-protected message; and~~

~~a transceiver configured to transmit the encrypted and integrity-protected message to a first network function,~~

~~wherein the encrypted and integrity-protected message is encrypted using a first key that is derived from a second key,~~

~~wherein the second key is established using a communication with a second network function, and~~

~~wherein the encrypted and integrity-protected message is obtained by encrypting and integrity-protecting a message.~~

~~20. The device of claim 19, wherein the first key is used to obtain the encrypted and integrity-protected message by:~~

~~generating, by the wireless device, an encryption key and an integrity key based on the first key; and~~

~~encrypting the message using the encryption key and integrity-protecting the message using the integrity key.~~

~~21. The device of claim 19, wherein the first key includes an authentication and key~~

management for applications (AKMA) application key, and the second key includes an AKMA anchor key.

22. The device of claim 19, wherein the encrypted and integrity-protected message includes a discovery request message that is transmitted through an interface for establishing proximity-based services.

23. The device of claim 19, wherein the discovery request message includes an AKMA key identifier (A-KID) and a message authentication code (MAC).

24. The device of claim 23, wherein, in a case that the first network function does not have an active context associated with the A-KID, the first network function transmits, to the second network function, a first request for acquiring the first key to be used by the wireless device.

25. The device of claim 24, wherein the first request includes an identity of the first network function that includes a fully qualified domain name (FQDN) and a security protocol identifier for a reference point that carries an application protocol.

26. The device of any of claims 19-25, wherein:

the transceiver is further configured to receive a discovery response message from the first network function; and

the one or more processors are further configured to check a message authentication code (MAC) of the discovery response message and perform a decryption on the discovery response message based on the first key or the encryption key and the integrity key generated based on the first key.

27. A network device, comprising:

a transceiver configured to receive an encrypted and integrity-protected message from a wireless device; and

one or more processors configured to perform a first network function including decrypting the encrypted and integrity-protected message using a first key that is derived from a

second key,

wherein the encrypted and integrity-protected message is obtained by encrypting and integrity-protecting a message using the first key, and

wherein the second key is established using a communication between the wireless device and a second network function.

28. The device of claim 27, wherein the decrypting the encrypted and integrity-protected message using the first key comprises:

generating an encryption key and an integrity key based on the first key;

checking a message authentication code (MAC) of the encrypted and integrity-protected message using the integrity key; and

decrypting the encrypted and integrity-protected message using the encryption key.

29. The device of claim 27, wherein the second network function determines whether the second network function is configured to provide a service to the first network function based on at least one of a configured local policy, authorization information, or a policy provided by a network repository function using an identity of the first network function.

30. The device of claim 27, wherein the second network function verifies whether a subscriber is authorized to use AKMA based on presence of the second key identified by an A-KID.

31. The device of claim 30, wherein, in a case that the second key is present in the second network function, the second network function derives the first key from the second key, or in a case that the second key is not present in the second network function, the second network function transmits, to an application function, a first response for responding to a first request for acquiring the first key, the first key, and an expiration time of the first key.

32. The device of claim 27, wherein the message received from the wireless device includes a discovery request message that is transmitted through an interface for establishing proximity-based services.

~~33. The device of claim 32, wherein:~~

~~the one or more processors are further configured to encrypt and integrity-protect a discovery response message based on the first key; and~~

~~the transceiver is further configured to transmit the encrypted and integrity-protected discovery response message to the wireless device.~~

~~34. The device of claim 33, wherein the first key is used to encrypt and integrity-protect the discovery response message by:~~

~~generating an encryption key and an integrity key based on the first key; and~~

~~encrypting the discovery response message using the encryption key and integrity-protecting the discovery response message using the encryption key.~~

~~35~~15. An apparatus for wireless communication, comprising a processor, wherein the processor is configured to implement a method recited in any of claims 1 to ~~18~~14.

~~36. A computer readable program storage medium having code stored thereon, the code, when executed by a processor, causing the processor to implement a method recited in any of claims 1 to 18.~~