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 and a message authentication code (MAC) of the message is calculated using either (1) an authentication and key management for applications (AKMA) application key (K_{AF}) that is derived from an AKMA anchor key (K_{AKMA}), or (2) an encryption key (K_{enc}) and an integrity key (K_{int}) that are derived from the K_{AF}, and wherein K_{enc} is for use by the first network function to decrypt the message in a case that the first network function is able to successfully check the MAC of the message using the K_{int}, otherwise the K_{AF} is for use by the first network function to check the MAC and decrypt the message,

wherein the wireless device has established the K_{AKMA} 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 encrypted and integrity-protected message includes a discovery request message that is transmitted through an interface for establishing proximity-based services.

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

4. The method of claim 3, 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 K_{AF} to be used by the wireless device.

5. The method of any of claims 1 to 4, further comprising:

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

checking the message authentication code (MAC) of the discovery response message and decrypting the discovery response message by using the K_{AF} or by using the K_{int} and K_{enc}.

6. 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 either (1) an authentication and key management for applications (AKMA) application key (K_{AF}) that is derived from an AKMA anchor key (K_{AKMA}), or (2) an encryption key (K_{enc}) and an integrity key (K_{int}) that are derived from the K_{AF}, wherein, in a case that the first network function successfully checks a message authentication code (MAC) of the message by using the K_{int}, the first network function decrypts the message using K_{enc}, otherwise the first network function checks the MAC and decrypts the message using the K_{AF},

wherein the encrypted and integrity-protected message is obtained by encrypting and integrity-protecting a message using the K_{AF}, and

wherein the K_{AKMA} is established using a communication between the wireless device and a second network function.

7. The method of claim 6, 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.

8. The method of claim 6, wherein the second network function verifies whether a subscriber is authorized to use AKMA based on presence of the K_{AKMA} identified by an A-KID.

9. The method of claim 6, 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.

10. The method of any of claims 1 to 9, wherein the first network function includes a direct discovery name management function (DDNMF), and the second network function includes AKMA anchor function.

11. An apparatus for wireless communication, comprising a processor, wherein the processor is configured to implement a method recited in any of claims 1 to 10.