CLAIMS

~~What is claimed is:~~

1. A key derivation method, wherein the method comprises:

~~receiving, by user equipment UE, an authentication success message from a mobility management function network element, wherein the authentication success message indicates that the UE is successfully authenticated by an authentication device;~~

generating, ~~by the UE~~by an apparatus during authentication, a master session key (MSK) and an extended master session key (EMSK) ~~based on the authentication success message~~;

after receiving an authentication success message from a mobility management function network element, determining, by the ~~UE~~apparatus, whether to derive an authentication service key (Kausf) by using the MSK~~the authentication device is located outside a 3rd generation partnership project 3GPP network~~; wherein the authentication success message indicates that the apparatus is successfully authenticated by an authentication device; and

when determining to derive a Kausf by using the MSK~~the authentication device is located outside the 3GPP network~~, generating, by the ~~UE~~apparatus, a~~n authentication service key~~ Kausf based on the MSK.

~~2. The method according to claim 1, wherein the method further comprises:~~

~~when the authentication device is located inside the 3GPP network, generating, by the UE, Kausf based on the EMSK.~~

~~3~~2. The method according to claim 1 ~~or 2~~, wherein the method further comprises:

receiving, by the ~~UE~~apparatus, first indication information from the mobility management function network element, wherein the first indication information indicates to derive a Kausf by using the MSK~~that the authentication device is located outside the 3GPP network or inside the 3GPP network~~; and

the determining, by the ~~UE~~apparatus, whether to derive a Kausf by using the MSK ~~the authentication device is located outside a 3GPP network~~ comprises:

determining, by the ~~UE~~apparatus based on the first indication information, whether to derive a Kausf by using the MSK ~~the authentication device is located outside the 3GPP network~~.

~~4~~3. The method according to claim ~~3~~2, wherein the first indication information comprises anti-bidding down between architectures (ABBA), and when a value of the ABBA is a non-zero

value~~, the ABBA~~ indicating~~s~~ to derive a Kausf by using the MSK ~~that the authentication device is located outside the 3GPP network~~.

~~5~~4. The method according to claim 1 ~~or 2~~, wherein the ~~UE~~apparatus stores first configuration information, and the first configuration information comprises second indication information indicating whether to derive a Kausf by using the MSK ~~the authentication device is located outside the 3GPP network~~; and

the determining, by the ~~UE~~apparatus, whether to derive a Kausf by using the MSK~~the authentication device is located outside a 3GPP network~~ comprises:

determining, by the ~~UE~~apparatus based on the second indication information, whether to derive a Kausf by using the MSK~~the authentication device is located outside the 3GPP network~~.

~~6. The method according to claim 1 or 2, wherein the determining, by the UE, whether the authentication device is located outside a 3GPP network comprises:~~

~~when the UE obtains an identifier of the authentication device, determining, by the UE, that the authentication device is located outside the 3GPP network; and~~

~~when the UE does not obtain the identifier of the authentication device, determining, by the UE, that the authentication device is located inside the 3GPP network.~~

~~7~~5. The method according to ~~any one of~~ claim~~s~~ 1 ~~to 6~~, wherein the generating, by the ~~UE~~apparatus, a ~~an authentication service key~~ Kausf based on the MSK comprises:

generating, by the ~~UE~~apparatus, the Kausf based on the MSK and a generation parameter, wherein

the generation parameter comprises one or more of the following: an identifier of a serving network that the ~~UE~~apparatus currently accesses or an identifier of the ~~UE~~apparatus.

~~8~~6. The method according to claim ~~7~~5, wherein the identifier of the ~~UE~~apparatus comprises a first identifier of the ~~UE~~apparatus, and the first identifier identifies the ~~UE~~apparatus in a network other than the 3GPP network.

7. The method according to claim 4, wherein a first authentication credential corresponding to the first configuration information is preconfigured in the apparatus, wherein the generating the MSK and the EMSK comprises:

generating, by the apparatus, the MSK and the EMSK based on the first authentication credential.

8. The method according to claim 7, further comprising:

selecting, by the apparatus, a first network based on an identifier broadcast by a network, and

determining, by the apparatus, the first authentication credential corresponding to the first network.

9. A communication apparatus, comprising a processor coupled to a memory storing instructions and configured to execute the instructions to cause the apparatus to:~~9. A key derivation method, wherein the method comprises:~~

generate, during authentication, a master session key (MSK) and an extended master session key (EMSK);

after receiving an authentication success message from a mobility management function network element, determine whether to derive an authentication service key (Kausf) by using the MSK; wherein the authentication success message indicates that the apparatus is successfully authenticated by an authentication device; and

generate a Kausf based on the MSK when determining to derive a Kausf by using the MSK.

10. The apparatus according to claim 9, wherein the apparatus stores first configuration information, and the first configuration information comprises second indication information indicating whether to derive a Kausf by using the MSK; and wherein the instructions cause the apparatus to determine whether to derive an authentication service key (Kausf) by using the MSK by:

determining, based on the second indication information, whether to derive a Kausf by using the MSK.

11. The apparatus according to claim 9, wherein the instructions cause the apparatus to generate a Kausf based on the MSK by:

generating the Kausf based on the MSK and a generation parameter, wherein

the generation parameter comprises one or more of the following: an identifier of a serving network that the apparatus currently accesses or an identifier of the apparatus.

12. The apparatus according to claim 10, wherein a first authentication credential corresponding to the first configuration information is preconfigured in the apparatus, wherein the instructions cause the apparatus to generate the MSK and the EMSK by:

generating the MSK and the EMSK based on the first authentication credential.

13. The apparatus according to claim 12, wherein the instructions further cause the apparatus

to:

select a first network based on an identifier broadcast by a network, and

determine the first authentication credential corresponding to the first network.

14. The apparatus according to claim 9, wherein the instructions further cause the apparatus to:

receive first indication information from the mobility management function network element, wherein the first indication information indicates to derive a Kausf by using the MSK; and

the the instructions cause the apparatus to determine whether to derive a Kausf by using the MSK by:

determining, based on the first indication information, whether to derive a Kausf by using the MSK; wherein the first indication information comprises anti-bidding down between architectures, ABBA, and when a value of the ABBA is a non-zero value indicating to derive a Kausf by using the MSK.

15. The apparatus according to claim 9, wherein the apparatus is user equipment (UE) or a chip in the UE.

16. ~~sending, by an authentication service function AUSF network element, a first trigger indication to an authentication device, wherein the first trigger indication is used to trigger to authenticate user equipment UE;~~

~~receiving, by the AUSF network element, an authentication success message and a first key from the authentication device, wherein the authentication success message indicates that the UE is successfully authenticated by the authentication device;~~

~~generating, by the AUSF network element, an authentication service key Kausf based on the first key; and~~

~~sending, by the AUSF network element, the authentication success message and third indication information to a mobility management function network element, wherein the third indication information indicates that the authentication device is located outside a 3rd generation partnership project 3GPP network or inside the 3GPP network.~~

~~10. The method according to claim 9, wherein the generating, by the AUSF network element, an authentication service key Kausf based on the first key comprises:~~

~~generating, by the AUSF network element, Kausf based on the first key and a generation parameter, wherein~~

the generation parameter comprises one or more of the following: an identifier of a serving network that the UE currently accesses or an identifier of the UE.

11. The method according to claim 10, wherein the identifier of the UE comprises a first identifier of the UE, and the first identifier identifies the UE in a network other than the 3GPP network.

12. The method according to any one of claims 9 to 11, wherein before the sending, by an AUSF network element, a first trigger indication to an authentication device, the method further comprises:

determining, by the AUSF network element, that the UE needs to perform authentication with the authentication device.

13. The method according to claim 12, wherein the determining, by the AUSF network element, that the UE needs to perform authentication with the authentication device comprises:

receiving, by the AUSF network element, a second identifier of the UE from the mobility management function network element, wherein the second identifier is a subscription concealed identifier SUCI or a subscription permanent identifier SUPI; and

determining, by the AUSF network element based on the second identifier, that the UE needs to perform authentication with the authentication device.

14. The method according to claim 12, wherein the determining, by the AUSF network element, that the UE needs to perform authentication with the authentication device comprises:

receiving, by the AUSF network element, a second identifier of the UE from the mobility management function network element, wherein the second identifier is a subscription concealed identifier SUCI or a subscription permanent identifier SUPI; and

sending, by the AUSF network element, a first request message to a unified data management UDM network element, wherein the first request message comprises the SUCI or the SUPI;

receiving, by the AUSF network element, a first response message from the UDM network element, wherein the first response message comprises an identifier of the authentication device; and

determining, by the AUSF network element based on the identifier of the authentication device, that the UE needs to perform authentication with the authentication device.

15. The method according to any one of claims 9 to 14, wherein the method further comprises:

determining, by the AUSF network element, the first identifier of the UE based on the second

identifier of the UE, wherein the first identifier identifies the UE in a network other than the 3GPP network, the second identifier is the SUCI or the SUPI, and the second identifier is received by the AUSF network element from the mobility management function network element; and

sending, by the AUSF network element, the first identifier to the authentication device, wherein the first trigger indication is specifically used to trigger to authenticate the UE based on an authentication credential corresponding to the first identifier.

16. A key derivation method, wherein the method comprises:

receiving, by a mobility management function network element, an authentication success message and third indication information from an authentication service function AUSF network element, wherein the authentication success message indicates that user equipment UE is successfully authenticated by an authentication device, and the third indication information indicates that the authentication device is located outside a 3rd generation partnership project 3GPP network or inside the 3GPP network; and

sending, by the mobility management function network element, the authentication success message and first indication information to the UE, wherein the first indication information indicates that the authentication device is located outside the 3GPP network or inside the 3GPP network, and the first indication information is determined based on the third indication information.

17. The method according to claim 16, wherein the first indication information comprises anti-bidding down between architectures ABBA, and the method further comprises:

determining, by the mobility management function network element, that a value of the ABBA is a non-zero value, wherein when the value of the ABBA is the non-zero value, the ABBA indicates that the authentication device is located outside the 3GPP network.

18. A key derivation system, wherein the system comprises an authentication service function AUSF network element and a mobility management function network element;

the AUSF network element is configured to send a first trigger indication to an authentication device, wherein the first trigger indication is used to trigger to authenticate UE; receive an authentication success message and a first key from the authentication device, wherein the authentication success message indicates that the UE is successfully authenticated by the authentication device; generate an authentication service key Kausf based on a first key; and send the authentication success message and third indication information to the mobility management

function network element, wherein the third indication information indicates that the authentication device is located outside a 3rd generation partnership project 3GPP network or inside the 3GPP network; and

the mobility management function network element is configured to receive the authentication success message and the third indication information from the AUSF network element; and send the authentication success message and first indication information to the UE, wherein the first indication information indicates that the authentication device is located outside the 3GPP network or inside the 3GPP network, and the first indication information is determined based on the third indication information.

19. The system according to claim 18, wherein the first indication information comprises anti-bidding down between architectures ABBA, and when a value of the ABBA is a non-zero value, the ABBA indicates that the authentication device is located outside the 3GPP network.

20. The system according to claim 18 or 19, wherein

the AUSF network element is specifically configured to generate Kausf based on the first key and a generation parameter, wherein

the generation parameter comprises one or more of the following: an identifier of a serving network that the UE currently accesses or an identifier of the UE.

21. The system according to claim 20, wherein the identifier of the UE comprises a first identifier of the UE, and the first identifier identifies the UE in a network other than the 3GPP network.

22. The system according to any one of claims 18 to 21, wherein

the AUSF network element is further configured to determine that the UE needs to perform authentication with the authentication device.

23. The system according to claim 22, wherein

the AUSF network element is specifically configured to receive a second identifier of the UE from the mobility management function network element, wherein the second identifier is a subscription concealed identifier SUCI or a subscription permanent identifier SUPI; and determine, based on the second identifier, that the UE needs to perform authentication with the authentication device.

24. The system according to claim 22, wherein

the AUSF network element is specifically configured to receive a second identifier of the UE

~~from the mobility management function network element, wherein the second identifier is a subscription concealed identifier SUCI or a subscription permanent identifier SUPI; send a first request message to a unified data management UDM network element, wherein the first request message comprises the SUCI or the SUPI; receive a first response message from the UDM network element, wherein the first response message comprises an identifier of the authentication device; and determine, based on the identifier of the authentication device, that the UE needs to perform authentication with the authentication device.~~

~~25. The system according to any one of claims 18 to 24, wherein~~

~~the AUSF network element is further configured to determine the first identifier of the UE based on the second identifier of the UE; and send the first identifier to the authentication device, wherein the first identifier identifies the UE in a network other than the 3GPP network, the second identifier is the SUCI or the SUPI, the second identifier is received by the AUSF network element from the mobility management function network element, and the first trigger indication is specifically used to trigger to authenticate the UE based on an authentication credential corresponding to the first identifier.~~

~~26. A communication apparatus, wherein the apparatus comprises a processing module and a transceiver module, and the processing module and the transceiver module are used by the apparatus to implement the method according to any one of claims 1 to 17.~~

~~27. A communication apparatus, wherein the apparatus comprises a processor coupled to a memory, the memory is configured to store a program, and when the program is executed by the processor, the apparatus is enabled to perform the method according to any one of claims 1 to 17.~~

A computer-readable storage medium comprising instructions, which when executed, cause an apparatus to:

generate, during authentication, a master session key (MSK) and an extended master session key (EMSK);

after receiving an authentication success message from a mobility management function network element, determine whether to derive an authentication service key (Kausf) by using the MSK; wherein the authentication success message indicates that the apparatus is successfully authenticated by an authentication device; and

generate a Kausf based on the MSK when determining to derive a Kausf by using the MSK.

17. The computer-readable storage medium according to claim 16, wherein the apparatus

stores first configuration information, and the first configuration information comprises second indication information indicating whether to derive a Kausf by using the MSK; and wherein the instructions cause the apparatus to determine whether to derive an authentication service key (Kausf) by using the MSK by:

determining, based on the second indication information, whether to derive a Kausf by using the MSK.

18. The computer-readable storage medium according to claim 16, wherein the instructions cause the apparatus to generate a Kausf based on the MSK by:

generating the Kausf based on the MSK and a generation parameter, wherein

the generation parameter comprises one or more of the following: an identifier of a serving network that the apparatus currently accesses or an identifier of the apparatus.

19. The computer-readable storage medium according to claim 17, wherein a first authentication credential corresponding to the first configuration information is preconfigured in the apparatus, wherein the instructions cause the apparatus to generate the MSK and the EMSK by:

generating the MSK and the EMSK based on the first authentication credential.

20. The computer-readable storage medium according to claim 16, wherein the instructions further cause the apparatus to:

select a first network based on an identifier broadcast by a network, and

determine the first authentication credential corresponding to the first network.

~~28. A computer-readable storage medium, storing a computer program, wherein when the computer program is executed, a computer is enabled to perform the method according to any one of claims 1 to 17.~~