CLAIMS

1. A key derivation method, comprising:

generating, by an apparatus during authentication, a master session key (MSK) and an extended master session key (EMSK), wherein the apparatus is user equipment (UE) or a chip in the UE;

after receiving an authentication success message from a mobility management function network element, determining, by the apparatus, 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

when determining to derive a Kausf by using the MSK, generating, by the apparatus, a Kausf based on the MSK;

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

the determining whether to derive the Kausf by using the MSK comprises:

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

2. The key derivation method according to claim 1, wherein the generating the Kausf based on the MSK comprises:

generating, by the 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 apparatus currently accesses or an identifier of the apparatus.

3. The key derivation method according to claim 2, wherein the identifier of the apparatus comprises a first identifier of the apparatus, and the first identifier identifies the apparatus in a network other than the 3GPP network.

4. The key derivation method according to claim 1, 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.

5. The key derivation method according to claim 4, 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.

6. The key derivation method according to claim 1, wherein the method comprises performing a following sequence of steps:

first, receiving, on the apparatus, the authentication success message from the mobility management function network element;

second, after receiving the authentication success message, generating the MSK and EMSK; and

third, after generating the MSK, determining, by the apparatus, whether to derive the Kausf using the MSK.

7. A communication apparatus being a user equipment (UE) or a chip in the UE, comprising a processor coupled to a memory storing instructions and configured to execute the instructions to cause the 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

wherein the apparatus stores first configuration information, and the first configuration information comprises second indication information indicating whether to derive the Kausf by using the MSK; and wherein the instructions cause the apparatus to determine whether to derive the Kausf by using the MSK by:

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

8. The communication apparatus according to claim 7, wherein the instructions cause the apparatus to generate the 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.

9. The communication apparatus according to claim 8, wherein the identifier of the apparatus comprises a first identifier of th19sdsdsdsde apparatus, and the first identifier identifies the apparatus in a network other than the 3GPP network.

10. The communication apparatus according to claim 8, wherein the memory of the communication apparatus further stores instructions to, upon determining not to derive the Kausf by using the MSK, derive the Kausf using the EMSK.

11. The communication apparatus according to claim 7, 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.

12. The communication apparatus according to claim 11, 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.

13. The communication apparatus according to claim 7, wherein the instructions cause the apparatus to perform a following sequence of steps:

first, receiving, on the UE, the authentication success message from the mobility management function network element;

second, after receiving the authentication success message, generating the MSK and EMSK; and

third, after generating the MSK, determining, by the apparatus, whether to derive the Kausf using the MSK.

14. A non-transitory computer-readable storage medium comprising instructions, which when executed, cause an apparatus that is one of a user equipment (UE) or a chip in the UE 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

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 the Kausf by using the MSK by:

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

15. The non-transitory computer-readable storage medium according to claim 14, 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.

16. The non-transitory computer-readable storage medium according to claim 15, wherein the identifier of the apparatus comprises a first identifier of the apparatus, and the first identifier identifies the apparatus in a network other than the 3GPP network.

17. The non-transitory computer-readable storage medium according to claim 14, 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.

18. The non-transitory computer-readable storage medium according to claim 14, 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.

19. The non-transitory computer-readable storage medium according to claim 14, wherein the instructions further comprise instructions to, upon determining not to derive the Kausf by using the MSK, derive the Kausf using the EMSK.

20. The communication apparatus according to claim 14, wherein the instructions include

instructions that, when executed, cause the apparatus to perform a following sequence of steps:

first, receiving, on the UE, the authentication success message from the mobility management function network element;

second, after receiving the authentication success message, generating the MSK and EMSK; and

third, after generating the MSK, determining, by the apparatus, whether to derive the Kausf using the MSK.