CLAIMS

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

generating, by an apparatus 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, 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.

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

receiving, by the 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; and

the determining, by the apparatus, whether to derive a Kausf by using the MSK comprises:

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

3. The method according to claim 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 indicating to derive a Kausf by using the MSK.

4. The method according to claim 1, 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, by the apparatus, whether to derive a Kausf by using the MSK comprises:

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

5. The method according to claim 1, wherein the generating, by the apparatus, a 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.

6. The method according to claim 5, 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.

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:

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. 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.