CLAIMS:

1. A method for a user equipment (UE) communicating with a core network, the method comprising:

authenticating, by the core network, a first communication device of the UE, wherein the first communication device of the UE is associated with a first access technology;

generating, by the core network, a security context of the first communication device of the UE when the authentication is successful, wherein the security context of the first communication device comprises a fast re-authentication ID;

receiving, by the core network, a request for authentication from a second communication device of the UE through a second access technology;

determining, by the core network, whether the request for authentication includes a fast re-authentication ID; and

initiating, by the core network, a fast re-authentication procedure in response to determining the request comprises a fast re-authentication ID, wherein initiating the fast re-authentication procedure includes updating, by the core network, the security context of the first communication device of the UE.

2. The method according to the claim 1, wherein updating the security context comprises updating, by the core network, a counter in the security context.

3. The method according to the claim 2, wherein the first access technology is 3 GPP access technology, and the second access technology is non-3GPP access technology.

4. The method according to the claim 2, wherein the first access technology is non-3GPP access technology, and the second access technology is 3GPP access technology.

5. The method according to claim 1, further comprising: transmitting, by the core network, the updated security context to an access network such that the access network uses the updated security context for signaling protection.

6. A method for a user equipment (UE) communicating with a core network, the method comprising:

generating, by the UE, a security context of a first communication device of the UE in response to a successful authentication of the first communication device, wherein the first

communication device is associated with a first access technology, and wherein the security context of the first communication device comprises a fast re-authentication ID;

sending, by the UE, a request to the core network through a second access technology, wherein the request comprises the fast re-authentication ID; and

updating, by the UE, the security context when the first communication device of the UE is authenticated successfully.

7. The method according to the claim 6, wherein updating the security context comprises updating, by the UE, a counter in the security context.

8. The method according to the claim 7, wherein the first access technology is 3GPP access technology, and the second access technology is non-3GPP access technology.

9. The method according to the claim 7, wherein the first access technology is non-3GPP access technology, and the second access technology is 3GPP access technology.

10. An apparatus comprising: at least one memory to store instructions; and at least one processor coupled to the at least one memory, and to execute the stored instructions to:

authenticate a first communication device of a user equipment (UE), wherein the first communication device of the UE is associated with a first access technology;

generate a security context of the first communication device of the UE when the authentication is successful, wherein the security context of the first communication device comprises a fast re-authentication ID;

receive a request for authentication from a second communication device of the user equipment (UE) through a second access technology;

determine whether the request is for fast re-authentication; and

initiate a fast re-authentication procedure in response to determining the request comprises the fast re-authentication ID, wherein the procedure includes updating the security context of the first communication device of the UE.

11. The apparatus according to the claim 10, wherein when updating the security context, the at least one processor further executes the stored instructions to update a counter in the security context.

12. The apparatus according to the claim 11, wherein the first access technology is 3GPP access technology, and the second access technology is non-3GPP access technology.

13. The apparatus according to the claim 11, wherein the first access technology is non-3GPP access technology, and the second access technology is 3GPP access technology.

14. The apparatus according to claim 12, wherein the processor further executes the stored instructions to transmit the updated security context to an access network such that the access network uses the updated security context for signaling protection.

15. A user equipment (UE) for communicating directly with a core network, the UE comprising:

at least one memory to store instructions; and at least one processor coupled to the at least one memory, and to execute the stored instructions to:

generate a security context of first communication device of the UE in response to successfully authenticating the first communication device, wherein the first communication device is associated with a first access technology, and wherein the security context of the first communication device comprises a fast re-authentication ID;

send a request to the core network through a second access technology, wherein the request comprises the fast re-authentication ID; and

update the security context when the first communication device of the UE is authenticated successfully.

16. The UE according to the claim 15, wherein when updating the security context, the at least one processor further executes the stored instructions to update a counter in the security context.

17. The UE according to the claim 16, wherein the first access technology is 3GPP access technology, and the second access technology is non-3GPP access technology.

18. The UE according to the claim 16, wherein the first access technology is non-3GPP access technology, and the second access technology is 3GPP access technology.

19. A non-transitory computer readable medium comprising processor-executable instructions, which when executed by at least one processor, cause the at least one processor to perform the following:

authenticating a first communication device of a user equipment (UE), wherein the first communication device of the UE is associated with a first access technology;

generating a security context of the first communication device in response to successfully authenticating the first communication device wherein the security context of the first communication device comprises a fast re-authentication ID;

receiving a request for authentication from a second communication device of the UE through a second access technology;

determining whether the request is for fast re-authentication; and

initiating a fast re-authentication procedure in response to determining that the request comprises the fast re-authentication ID, wherein the fast re-authentication procedure comprises updating the security context of the first communication device of the UE.

20. A non-transitory computer readable medium comprising processor-executable instructions, which when executed by at least one processor, cause the at least one processor to perform the following:

generating a security context of a first communication device of a user equipment (UE) when the first communication device is successfully authenticated, wherein the first communication device is associated with a first access technology, and wherein the security context of the first communication device comprises a fast re-authentication ID;

sending a request to a core network through a second access technology, wherein the request comprises the fast re-authentication ID; and

updating the security context when the first communication device is successfully authenticated.