CLAIMS

1. A slice isolation method, comprising:

obtaining, by a first network device, information about a first slice of user equipment; and

obtaining, by the first network device, a second key if the information about the first slice does not match information about a second slice that the user equipment requests to access, wherein the second key is for performing security protection on the information about the second slice and/or information in a process in which the user equipment accesses the second slice.

2. The method according to claim 1, wherein the information about the first slice comprises an attribute of the first slice, and the information about the second slice comprises an attribute of the second slice; and

the obtaining, by the first network device, a second key if the information about the first slice does not match information about a second slice that the user equipment requests to access comprises:

obtaining, by the first network device, the second key if the attribute of the first slice does not match the attribute of the second slice.

3. The method according to claim 1 or 2, wherein the obtaining, by the first network device, a second key comprises:

generating, by the first network device, the second key based on a first key, wherein the first key is for performing security protection on the information about the first slice and/or information that is in a process in which the user equipment accesses the first slice.

4. The method according to claim 3, wherein the generating, by the first network device, the second key based on a first key comprises:

generating, by the first network device, the second key based on the first key if an isolation requirement of the first slice is higher than an isolation requirement of the second slice.

5. The method according to claim 1 or 2, wherein the obtaining, by the first network device, a second key comprises:

performing, by the first network device, re-authentication on the user equipment; and

generating, by the first network device, the second key if the re-authentication performed by the first network device on the user equipment succeeds.

6. The method according to claim 5, wherein the performing, by the first network device, re-

authentication on the user equipment comprises:

performing, by the first network device, network re-authentication on the user equipment if an isolation requirement of the first slice is lower than an isolation requirement of the second slice.

7. The method according to any one of claims 2 to 6, wherein that the attribute of the first slice does not match the attribute of the second slice comprises:

the attribute of the first slice or the attribute of the second slice does not allow simultaneous use with a slice of any other attribute;

the attribute of the first slice allows simultaneous use with only a slice that has a same slice/service type SST, wherein an SST of the attribute of the second slice is different from an SST of the attribute of the first slice;

the attribute of the second slice allows simultaneous use with only a slice that has a same slice/service type SST, wherein an SST of the attribute of the first slice is different from an SST of the attribute of the second slice;

the attribute of the first slice allows simultaneous use with only a slice that has a same slice differentiator SD, wherein an SD of the attribute of the second slice is different from an SD of the attribute of the first slice; or

the attribute of the second slice allows simultaneous use with only a slice that has a same slice differentiator SD, wherein an SD of the attribute of the first slice is different from an SD of the attribute of the second slice.

8. The method according to any one of claims 2 to 7, further comprising:

sending, by the first network device, a registration accept message to the user equipment if the attribute of the first slice matches the attribute of the second slice.

9. The method according to claim 8, wherein that the attribute of the first slice matches the attribute of the second slice comprises:

the attribute of the first slice or the attribute of the second slice allows simultaneous use with a slice of any other attribute;

the attribute of the first slice allows simultaneous use with only a slice that has a same SST, wherein an SST of the attribute of the second slice is the same as an SST of the attribute of the first slice;

the attribute of the second slice allows simultaneous use with only a slice that has a same SST, wherein an SST of the attribute of the first slice is the same as an SST of the attribute of the second

slice;

the attribute of the first slice allows simultaneous use with only a slice that has a same SD, wherein an SD of the attribute of the second slice is the same as an SD of the attribute of the first slice;

the attribute of the second slice allows simultaneous use with only a slice that has a same SD, wherein an SD of the attribute of the first slice is the same as an SD of the attribute of the second slice; or

the second slice and the first slice are mapped to same single network slice selection assistance information S-NSSAI.

10. A slice isolation method, comprising:

sending, by user equipment, a first request message to a first network device, wherein the first request message is for requesting to access a second slice;

receiving, by the user equipment, a first indication message from the first network device, wherein the first indication message indicates the user equipment to obtain a second key; and

obtaining, by the user equipment, the second key, wherein the second key is for performing security protection on information about the second slice and/or information that is in a process in which the user equipment accesses the second slice.

11. The method according to claim 10, wherein the obtaining, by the user equipment, the second key comprises:

obtaining, by the user equipment, a first key, wherein the first key is for performing security protection on information about a first slice and/or information that is in a process in which the user equipment accesses the first slice; and

generating, by the user equipment, the second key based on the first key.

12. The method according to claim 10, wherein the obtaining, by the user equipment, the second key comprises:

performing, by the user equipment, re-authentication with the first network device; and

generating, by the user equipment, the second key if the re-authentication performed by the user equipment with the first network device succeeds.

13. The method according to any one of claims 10 to 12, further comprising:

receiving, by the user equipment, a registration accept message from the first network device.

14. A communication apparatus, comprising means for performing the method according to

any one of claims 1 to 9, or the method according to any one of claims 10 to 13.

15. A communication apparatus, comprising a processor configured to execute computer-executable instructions stored in a memory to perform the method according to any one of claims 1 to 9, or the method according to any one of claims 10 to 13.