

REIVINDICACIONES

1. Un dispositivo terminal remoto que comprende:

al menos un procesador; y

al menos una memoria que almacena instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el dispositivo terminal remoto al menos:

obtenga una política de selección para seleccionar un código de selección de retransmisor (RSC) de una pluralidad de RSC, estando asociado un RSC de la pluralidad de RSC con un indicador para indicar si el RSC soporta un procedimiento de seguridad de plano de control (CP) o un procedimiento de seguridad de plano de usuario (UP);

basándose en la determinación de que se desencadena la conmutación de trayectoria desde un dispositivo terminal retransmisor de origen con un RSC de origen, seleccione un RSC objetivo basándose en la política de selección, un indicador de origen asociado con el RSC de origen, y una pluralidad de indicadores asociados con la pluralidad de RSC; y

seleccione, para la conmutación de trayectoria, un dispositivo terminal retransmisor objetivo basándose en el RSC objetivo.

2. El dispositivo terminal remoto de la reivindicación 1, en donde se hace que el dispositivo terminal remoto seleccione un dispositivo terminal retransmisor objetivo basándose en el RSC objetivo:

seleccionando el dispositivo terminal retransmisor objetivo con el RSC objetivo que es el mismo que el RSC de origen.

3. El dispositivo terminal remoto de la reivindicación 1 o 2, en donde se hace

además que el dispositivo terminal remoto:

determine la pluralidad de RSC;

obtenga la pluralidad de indicadores; y

determine, basándose en el RSC de origen y la pluralidad de indicadores, si el RSC de origen y la pluralidad de RSC soportan el procedimiento de seguridad de CP o el procedimiento de seguridad de UP.

4. El dispositivo terminal remoto de cualquiera de las reivindicaciones 1-3, en donde se hace que el dispositivo terminal remoto seleccione el RSC objetivo basándose en la política de selección:

seleccionando uno de la pluralidad de RSC para los que el dispositivo terminal remoto tiene una clave raíz válida como el RSC objetivo.

5. El dispositivo terminal remoto de la reivindicación 4, en donde se hace además que el dispositivo terminal remoto seleccione el RSC objetivo basándose en la política de selección:

basándose en la determinación de que el RSC de origen soporta el procedimiento de seguridad de CP, seleccionando, como el RSC objetivo, uno de la pluralidad de RSC para los que el dispositivo terminal remoto tiene la clave raíz válida y que soporta el procedimiento de seguridad de CP.

6. El dispositivo terminal remoto de la reivindicación 4, en donde se hace además que el dispositivo terminal remoto seleccione el RSC objetivo basándose en la política de selección:

basándose en la determinación de que el RSC de origen soporta el procedimiento de seguridad de UP, seleccionando, como el RSC objetivo, uno de la pluralidad de RSC para los que el dispositivo terminal remoto tiene la clave raíz

válida y que soporta el procedimiento de seguridad de UP.

7. El dispositivo terminal remoto de cualquiera de las reivindicaciones 1-6, en donde se hace además que el dispositivo terminal remoto:

genere una solicitud de comunicación directa (DCR) que incluye una identidad (ID) de la clave raíz válida, usándose la clave raíz válida para generar al menos una clave de seguridad para establecer un enlace de seguridad para una comunicación directa entre el dispositivo terminal remoto y el dispositivo terminal retransmisor objetivo.

8. El dispositivo terminal remoto de la reivindicación 3, en donde se hace además que el dispositivo terminal remoto al menos uno de:

basándose en la determinación de que el RSC de origen soporta el procedimiento de seguridad de CP, seleccione, como el RSC objetivo, uno del al menos un RSC candidato que soporta el procedimiento de seguridad de CP;

basándose en la determinación de que el RSC de origen soporta el procedimiento de seguridad de UP, seleccione, como el RSC objetivo, uno de la pluralidad de RSC que soportan el procedimiento de seguridad de UP; o

seleccione aleatoriamente uno de la pluralidad de RSC como el RSC objetivo.

9. El dispositivo terminal remoto de la reivindicación 8, en donde se hace además que el dispositivo terminal remoto:

genere una DCR que incluye un identificador oculto de suscripción (SUCI) usado para desencadenar un procedimiento de autenticación de servicios basados en proximidad (ProSe) del dispositivo terminal remoto.

10. El dispositivo terminal remoto de cualquiera de las reivindicaciones 1-9, en

donde la política de selección comprende al menos uno de:

un orden de selección basado en el procedimiento de seguridad de CP o el procedimiento de seguridad de UP que soportan el RSC de origen y el RSC objetivo;

o

una política de autenticación a usar por el dispositivo terminal remoto para determinar si desencadenar un procedimiento de autenticación de ProSe.

11. El dispositivo terminal remoto de cualquiera de las reivindicaciones 1-10, en donde la política de selección está preconfigurada por una red móvil pública terrestre doméstica (HPLMN) del dispositivo terminal remoto o basándose en una implementación del dispositivo terminal remoto.

12. Un dispositivo terminal remoto que comprende:

al menos un procesador; y

al menos una memoria que almacena instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el dispositivo terminal remoto al menos:

obtenga una política de autenticación a usar por el dispositivo terminal remoto para determinar si desencadenar un procedimiento de autenticación de servicios basados en proximidad (ProSe); y

determine desencadenar el procedimiento de autenticación de ProSe al menos basándose en la política de autenticación.

13. El dispositivo terminal remoto de la reivindicación 12, en donde la política de autenticación se basa en movilidad del dispositivo terminal remoto.

14. El dispositivo terminal remoto de la reivindicación 12 o 13, en donde se hace

que el dispositivo terminal remoto determine desencadenar el procedimiento de autenticación de ProSe:

determinando desencadenar el procedimiento de autenticación de ProSe basándose en que el dispositivo terminal remoto se mueva a una nueva red móvil pública terrestre (PLMN) de servicio.

15. El dispositivo terminal remoto de cualquiera de las reivindicaciones 12-14, en donde se hace que el dispositivo terminal remoto determine desencadenar el procedimiento de autenticación de ProSe:

determinando desencadenar el procedimiento de autenticación de ProSe basándose en que el dispositivo terminal remoto selecciona un dispositivo terminal retransmisor en la nueva PLMN de servicio.

16. El dispositivo terminal remoto de cualquiera de las reivindicaciones 12-15, en donde se hace además que el dispositivo terminal remoto determine desencadenar el procedimiento de autenticación de ProSe:

determinando desencadenar el procedimiento de autenticación de ProSe basándose en que una clave raíz es no válida, en donde la clave raíz se usa para generar al menos una clave de seguridad para establecer un enlace de seguridad para la comunicación directa entre el dispositivo terminal remoto y el dispositivo terminal retransmisor.

17. El dispositivo terminal remoto de cualquiera de las reivindicaciones 12-16, en donde el procedimiento de autenticación de ProSe comprende un procedimiento de seguridad de plano de control (CP), y se hace que el dispositivo terminal remoto determine desencadenar el procedimiento de autenticación de ProSe al menos basándose en la política de autenticación:

determinando desencadenar el procedimiento de autenticación de ProSe basándose en la política de autenticación independientemente del cambio de un RSC, siendo la generación de la clave raíz independiente del RSC.

18. Un dispositivo de función de servidor de autenticación (AUSF) que comprende:

al menos un procesador; y

al menos una memoria que almacena instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el dispositivo de AUSF al menos:

genere una clave raíz independiente de un código de selección de retransmisor (RSC), usándose la clave raíz para generar al menos una clave de servicios basados en proximidad (ProSe) para establecer un enlace de seguridad para una comunicación directa entre un dispositivo terminal remoto y un dispositivo terminal retransmisor; y

transmita, a un dispositivo de función de anclaje de ProSe (PAnF), una solicitud de registro de clave de ProSe sin el RSC.

19. El dispositivo de AUSF de la reivindicación 18, en donde se hace además que el dispositivo de AUSF:

transmita, al dispositivo de PAnF, una solicitud de obtención de clave de ProSe para desencadenar un procedimiento de autorización de servicio de retransmisión del dispositivo terminal remoto basándose en el RSC.

20. El dispositivo de AUSF de la reivindicación 18 o 19, en donde se hace además que el dispositivo de AUSF:

genere la al menos clave de seguridad de ProSe basándose al menos en el

RSC, siendo la al menos clave de seguridad de ProSe específica de RSC.

21. El dispositivo de AUSF de cualquiera de las reivindicaciones 18-20, en donde la clave raíz comprende una clave de usuario remoto de ProSe de plano de control (CP-PRUK).

22. Un método que comprende:

obtener, en un dispositivo terminal remoto, una política de selección para seleccionar un código de selección de retransmisor (RSC) de una pluralidad de RSC, estando asociado un RSC de la pluralidad de RSC con un indicador para indicar si el RSC soporta un procedimiento de seguridad de plano de control (CP) o un procedimiento de seguridad de plano de usuario (UP);

basándose en la determinación de que se desencadena la conmutación de trayectoria desde un dispositivo terminal retransmisor de origen con un RSC de origen, seleccionar un RSC objetivo basándose en la política de selección, un indicador de origen asociado con el RSC de origen, y una pluralidad de indicadores asociados con la pluralidad de RSC; y

seleccionar, para la conmutación de trayectoria, un dispositivo terminal retransmisor objetivo basándose en el RSC objetivo.

23. Un método que comprende:

obtener, en un dispositivo terminal remoto, una política de autenticación a usar por el dispositivo terminal remoto para determinar si desencadenar un procedimiento de autenticación de servicios basados en proximidad (ProSe); y

determinar desencadenar el procedimiento de autenticación de ProSe al menos basándose en la política de autenticación.

24. Un método que comprende:

generar, en un dispositivo de función de servidor de autenticación (AUSF), una clave raíz independiente de un código de selección de retransmisor (RSC), usándose la clave raíz para generar al menos una clave de servicios basados en proximidad (ProSe) para establecer un enlace de seguridad para una comunicación directa entre un dispositivo terminal remoto y un dispositivo terminal retransmisor; y

transmitir, a un dispositivo de función de anclaje de ProSe (PAnF), una solicitud de registro de clave de ProSe sin el RSC.

25. Un aparato que comprende medios para:

obtener una política de selección para seleccionar un código de selección de retransmisor (RSC) de una pluralidad de RSC, estando asociado un RSC de la pluralidad de RSC con un indicador para indicar si el RSC soporta un procedimiento de seguridad de plano de control (CP) o un procedimiento de seguridad de plano de usuario (UP);

basándose en la determinación de que se desencadena la conmutación de trayectoria desde un dispositivo terminal retransmisor de origen con un RSC de origen, seleccionar un RSC objetivo basándose en la política de selección, un indicador de origen asociado con el RSC de origen, y una pluralidad de indicadores asociados con la pluralidad de RSC; y

seleccionar, para la conmutación de trayectoria, un dispositivo terminal retransmisor objetivo basándose en el RSC objetivo.

26. Un aparato que comprende medios para:

obtener una política de autenticación a usar por el dispositivo terminal remoto para determinar si desencadenar un procedimiento de autenticación de servicios basados en proximidad (ProSe); y

determinar desencadenar el procedimiento de autenticación de ProSe al menos basándose en la política de autenticación.

27. Un aparato que comprende medios para:

generar una clave raíz independiente de un código de selección de retransmisor (RSC), usándose la clave raíz para generar al menos una clave de servicios basados en proximidad (ProSe) para establecer un enlace de seguridad para una comunicación directa entre un dispositivo terminal remoto y un dispositivo terminal retransmisor; y

transmitir, a un dispositivo de función de anclaje de ProSe (PAnF), una solicitud de registro de clave de ProSe sin el RSC.

28. Un medio legible por ordenador que comprende instrucciones de programa que, cuando son ejecutadas por un aparato, hacen que el aparato realice al menos uno de los métodos de las reivindicaciones 22-24.