

REIVINDICACIONES

1. Un dispositivo terminal, que comprende medios para:
generar una clave de anclaje;
5 recibir un identificador de clave de anclaje para la clave de anclaje;
derivar un conjunto de claves progenitoras de estrato sin acceso, NAS,
basándose en la clave de anclaje, un identificador de abono e indicadores de
NAS que indican diferentes procedimientos de NAS; y
obtener, para cada una del conjunto de claves progenitoras de NAS, un
10 identificador de clave progenitora de NAS.
2. El dispositivo terminal de acuerdo con la reivindicación 1, en donde, para
obtener, para cada una del conjunto de claves progenitoras de NAS, un
identificador de clave progenitora de NAS, el dispositivo terminal comprende
15 medios para derivar, para cada una del conjunto de claves progenitoras de NAS,
el identificador de clave progenitora de NAS basándose en el indicador de NAS
respectivo.
3. El dispositivo terminal de acuerdo con la reivindicación 1, en donde, para
20 obtener, para cada una del conjunto de claves progenitoras de NAS, un
identificador de clave progenitora de NAS, el dispositivo terminal comprende
medios para:
recibir los identificadores de clave progenitora de NAS asociados con las claves
progenitoras de NAS.

4. El dispositivo terminal de acuerdo con cualquiera de la reivindicación 1, en donde el dispositivo terminal comprende medios para:
almacenar el identificador de clave de anclaje, el conjunto de claves progenitoras de NAS y los identificadores de clave progenitora de NAS respectivos.

5

5. El dispositivo terminal de acuerdo con la reivindicación 1, en donde el identificador de clave progenitora de NAS asociado con una clave progenitora de NAS tiene el mismo valor que el indicador de NAS basándose en el cual se deriva la clave progenitora de NAS.

10

6. El dispositivo terminal de acuerdo con la reivindicación 1, en donde el dispositivo terminal comprende medios para:
solicitar el establecimiento de una primera conexión de NAS que porta un primer procedimiento de NAS entre el dispositivo terminal y una primera entidad de red central; y

15

determinar una clave de NAS para la primera conexión de NAS basándose en información relacionada con seguridad asociada con el primer procedimiento de NAS desde la primera entidad de red central.

20

7. El dispositivo terminal de acuerdo con la reivindicación 6, en donde, para solicitar el establecimiento de la primera conexión de NAS que porta el primer procedimiento de NAS entre el dispositivo terminal y la primera entidad de red central, el dispositivo terminal comprende medios para:

25

enviar, a la primera entidad de red central, una primera solicitud de conexión de NAS que comprende el identificador de clave de anclaje y el indicador de NAS

que indica el primer procedimiento de NAS.

8. El dispositivo terminal de acuerdo con la reivindicación 6, en donde, para determinar la clave de NAS para la primera conexión de NAS, el dispositivo terminal comprende medios para:
- 5 identificar la clave progenitora de NAS basándose en el identificador de clave de anclaje y el identificador de clave progenitora de NAS incluidos en la información relacionada con seguridad asociada con el primer procedimiento de NAS;
- 10 determinar, cuando la información relacionada con seguridad no comprende un valor de TROCEO, que la clave de NAS es la clave progenitora de NAS identificada;
- cuando la información relacionada con seguridad comprende un valor de TROCEO,
- 15 derivar una clave vástago de NAS basándose en la clave progenitora de NAS identificada y el valor de TROCEO;
- asignar un identificador de clave vástago de NAS incluido en la información relacionada con seguridad asociada con el primer procedimiento de NAS a la clave vástago de NAS derivada; y
- determinar que la clave de NAS es la clave vástago de NAS derivada.

20

9. El dispositivo terminal de acuerdo con la reivindicación 6, en donde la generación de la clave de anclaje se realiza después de la solicitud de establecimiento de la primera conexión de NAS.

- 25 10. El dispositivo terminal de acuerdo con la reivindicación 6, en donde el

dispositivo terminal comprende además medios para:

derivar una nueva clave de NAS para la primera conexión de NAS basándose en la clave de NAS actual para la primera conexión de NAS y recuentos de NAS durante un traspaso o durante una actualización de registro de NAS.

5

11. El dispositivo terminal de acuerdo con la reivindicación 6, en donde el dispositivo terminal comprende además medios para:

solicitar el establecimiento de una segunda conexión de NAS que porta un segundo procedimiento de NAS entre el dispositivo terminal y una segunda entidad de red central; y

10

determinar una clave de NAS para la segunda conexión de NAS basándose en información relacionada con seguridad asociada con el segundo procedimiento de NAS desde la segunda entidad de red central.

15

12. El dispositivo terminal de acuerdo con la reivindicación 11, en donde, para solicitar el establecimiento de la segunda conexión de NAS que porta el segundo procedimiento de NAS entre el dispositivo terminal y la segunda entidad de red central, el dispositivo terminal comprende medios para:

enviar, a la segunda entidad de red central, una segunda solicitud de conexión de NAS que comprende el identificador de clave de anclaje y el indicador de NAS que indica el segundo procedimiento de NAS.

20

13. El dispositivo terminal de acuerdo con la reivindicación 11, en donde, para determinar la clave de NAS para la segunda conexión de NAS, el dispositivo terminal comprende medios para:

25

identificar la clave progenitora de NAS basándose en el identificador de clave de anclaje y el identificador de clave progenitora de NAS incluidos en la información relacionada con seguridad asociada con el segundo procedimiento de NAS;
determinar, cuando la información relacionada con seguridad asociada con el
5 segundo procedimiento de NAS no comprende un valor de TROCEO, que la clave de NAS es la clave progenitora de NAS identificada;
cuando la información relacionada con seguridad asociada con el segundo procedimiento de NAS comprende un valor de TROCEO,
derivar una clave vástago de NAS basándose en la clave progenitora de NAS
10 identificada y el valor de TROCEO;
asignar un identificador de clave vástago de NAS incluido en la información relacionada con seguridad asociada con el segundo procedimiento de NAS a la clave vástago de NAS derivada; y
determinar que la clave de NAS es la clave vástago de NAS derivada.

15

14. Una entidad de red configurada para implementar la función de gestión de claves de seguridad, que comprende medios para:
generar una clave de anclaje con un dispositivo terminal;
derivar un identificador de clave de anclaje para la clave de anclaje, y enviar el
20 identificador de clave de anclaje al dispositivo terminal;
derivar un conjunto de claves progenitoras de estrato sin acceso, NAS, basándose en la clave de anclaje, un identificador de abono e indicadores de NAS que indican diferentes procedimientos de NAS; y
derivar, para cada una del conjunto de claves progenitoras de NAS, un
25 identificador de clave progenitora de NAS basándose en el indicador de NAS

respectivo.

15. Una entidad de red central configurada para implementar una función de red central, que comprende medios para:

5 recibir desde un dispositivo terminal una solicitud de establecimiento de una conexión de NAS que porta un procedimiento de NAS entre el dispositivo terminal y la entidad de red central; y

obtener una clave de NAS para la conexión de NAS, en donde la clave de NAS es una clave progenitora de NAS o una clave vástago de NAS asociada con un

10 indicador de NAS que indica el procedimiento de NAS.