

REIVINDICACIONES

1. Un dispositivo terminal, 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 al menos:
 - genere una clave de anclaje;
 - reciba un identificador de clave de anclaje para la clave de anclaje;
 - derive 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
 - obtenga, para cada una del conjunto de claves progenitoras de NAS, un 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, se hace que el dispositivo terminal derive, 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 obtener, para cada una del conjunto de claves progenitoras de NAS, un identificador de clave progenitora de NAS, se hace que el dispositivo terminal:
 - reciba los identificadores de clave progenitora de NAS asociados con las claves progenitoras de NAS.

4. El dispositivo terminal de acuerdo con cualquiera de las reivindicaciones 1 a 3, en donde se hace adicionalmente que el dispositivo terminal:

almacene el identificador de clave de anclaje, el conjunto de claves progenitoras de NAS y los identificadores de clave progenitora de NAS respectivos.

5. El dispositivo terminal de acuerdo con cualquiera de las reivindicaciones 1 a 4, 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.

6. El dispositivo terminal de acuerdo con cualquiera de las reivindicaciones 1 a 5, en donde se hace adicionalmente que el dispositivo terminal:

solicite 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

determine 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.

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, se hace que el dispositivo terminal:

envíe, 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 o 7, en donde, para determinar la clave de NAS para la primera conexión de NAS, se hace que el dispositivo terminal:

identifique 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;

determine, 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,

derive una clave vástago de NAS basándose en la clave progenitora de NAS identificada y el valor de TROCEO;

asigne 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

determine que la clave de NAS es la clave vástago de NAS derivada.

9. El dispositivo terminal de acuerdo con cualquiera de las reivindicaciones 6 a 8, en donde la generación de la clave de anclaje se realiza después de la solicitud de establecimiento de la primera conexión de NAS.

10. El dispositivo terminal de acuerdo con cualquiera de las reivindicaciones 6 a 9, en donde se hace adicionalmente que el dispositivo terminal:

derive 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.

11. El dispositivo terminal de acuerdo con cualquiera de las reivindicaciones 6 a 10, en donde se hace adicionalmente que el dispositivo terminal:

solicite 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

determine 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.

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, se hace que el dispositivo terminal:

envíe, 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.

13. El dispositivo terminal de acuerdo con la reivindicación 11 o 12, en donde, para determinar la clave de NAS para la segunda conexión de NAS, se hace que el dispositivo terminal:

identifique 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;

determine, cuando la información relacionada con seguridad asociada con el 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,

derive una clave vástago de NAS basándose en la clave progenitora de NAS identificada y el valor de TROCEO;

asigne 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

determine que la clave de NAS es la clave vástago de NAS derivada.

14. El dispositivo terminal de acuerdo con cualquiera de las reivindicaciones 11 a 13, en donde se hace adicionalmente que el dispositivo terminal:

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

15. El dispositivo terminal de acuerdo con cualquiera de las reivindicaciones 11 a 14, en donde el primer procedimiento de NAS y el segundo procedimiento de NAS son el mismo procedimiento de NAS o diferentes procedimientos de NAS.

16. El dispositivo terminal de acuerdo con cualquiera de las reivindicaciones 6 a 15, en donde se hace adicionalmente que el dispositivo terminal derive claves de estrato de acceso, AS, basándose al menos en parte en la clave de NAS para la conexión de NAS que porta procedimientos de gestión de movilidad de NAS.

17. Un método realizado por un dispositivo terminal, comprendiendo el método:

generar una clave de anclaje;

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 identificador de clave progenitora de NAS.

18. El método de acuerdo con la reivindicación 17, en donde obtener, para cada una del conjunto de claves progenitoras de NAS, un identificador de clave progenitora de NAS comprende 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.

19. El método de acuerdo con la reivindicación 17, en donde obtener, para cada una del conjunto de claves progenitoras de NAS, un identificador de clave progenitora de NAS comprende recibir los identificadores de clave progenitora de NAS asociados con las claves progenitoras de NAS.

20. El método de acuerdo con cualquiera de las reivindicaciones 17 a 19, en donde el método comprende además:

almacenar el identificador de clave de anclaje, el conjunto de claves progenitoras de NAS y los identificadores de clave progenitora de NAS respectivos.

21. El método de acuerdo con cualquiera de las reivindicaciones 17 a 20, 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.

22. El método de acuerdo con cualquiera de las reivindicaciones 17 a 21, en donde

el método comprende además:

- 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

- 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.

23. El método de acuerdo con la reivindicación 22, en donde 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 comprende 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.

24. El método de acuerdo con la reivindicación 22 o 23, en donde determinar una clave de NAS para la primera conexión de NAS comprende:

- 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;

- 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,

- 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.

25. El método de acuerdo con cualquiera de las reivindicaciones 22 a 24, en donde la generación de la clave de anclaje se realiza después de la solicitud de establecimiento de la primera conexión de NAS.

26. El método de acuerdo con cualquiera de las reivindicaciones 22 a 25, en donde el método comprende además:

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.

27. El método de acuerdo con cualquiera de las reivindicaciones 22 a 26, en donde el método comprende además:

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

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.

28. El método de acuerdo con la reivindicación 27, en donde 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 comprende 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.

29. El método de acuerdo con la reivindicación 27 o 28, en donde determinar una clave de NAS para la segunda conexión de NAS comprende:

- 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 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 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.

30. El método de acuerdo con cualquiera de las reivindicaciones 27 a 29, en donde el método comprende además:

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

31. El método de acuerdo con cualquiera de las reivindicaciones 27 a 30, en donde

el primer procedimiento de NAS y el segundo procedimiento de NAS son el mismo procedimiento de NAS o diferentes procedimientos de NAS.

32. El método de acuerdo con cualquiera de las reivindicaciones 22 a 31, en donde el método comprende además:

derivar claves de estrato de acceso, AS, basándose al menos en parte en la clave de NAS para la conexión de NAS que porta procedimientos de gestión de movilidad de NAS.

33. Una entidad de red configurada para implementar la función de gestión de claves de seguridad, que comprende:

al menos un procesador; y

al menos una memoria que almacena instrucciones que, cuando se ejecutan en el al menos un procesador, hacen que la entidad de red:

genere una clave de anclaje con un dispositivo terminal;

derive un identificador de clave de anclaje para la clave de anclaje, y envíe el identificador de clave de anclaje al dispositivo terminal;

derive 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

derive, para cada una del conjunto de claves progenitoras de NAS, un identificador de clave progenitora de NAS basándose en el indicador de NAS respectivo.

34. La entidad de red de acuerdo con la reivindicación 33, en donde se hace adicionalmente que la entidad de red:

almacene el identificador de clave de anclaje, el conjunto de claves

progenitoras de NAS y los identificadores de clave progenitora de NAS respectivos.

35. La entidad de red de acuerdo con la reivindicación 33 o 34, en donde se hace adicionalmente que la entidad de red:

envíe los identificadores de clave progenitora de NAS asociados con las claves progenitoras de NAS al dispositivo terminal.

36. La entidad de red de acuerdo con cualquiera de las reivindicaciones 33 a 35, 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.

37. La entidad de red de acuerdo con cualquiera de las reivindicaciones 33 a 36, en donde se hace adicionalmente que la entidad de red:

reciba, desde una primera entidad de red central, una primera solicitud de una clave de NAS para una primera conexión de NAS que porta un primer procedimiento de NAS;

determine la clave de NAS para la primera conexión de NAS basándose en la primera solicitud; y

envíe la clave de NAS para la primera conexión de NAS a la primera entidad de red central.

38. La entidad de red de acuerdo con la reivindicación 37,

en donde, para determinar la clave de NAS para la primera conexión de NAS, se hace que la entidad de red:

identifique la clave progenitora de NAS basándose en el identificador de clave de anclaje y el identificador de clave progenitora de NAS incluidos en la primera

solicitud;

determine, cuando la primera solicitud no comprende un valor de TROCEO, que la clave de NAS es la clave progenitora de NAS identificada;

cuando la primera solicitud comprende un valor de TROCEO,

derive una clave vástago de NAS basándose en la clave progenitora de NAS identificada y el valor de TROCEO;

derive un identificador de clave vástago de NAS para la clave vástago de NAS; y

determine que la clave de NAS es la clave vástago de NAS derivada; y

en donde, para enviar la clave de NAS para la primera conexión de NAS a la primera entidad de red central, se hace que la entidad de red:

envíe la clave progenitora de NAS identificada a la primera entidad de red central, cuando se determina que la clave de NAS es la clave progenitora de NAS identificada; y

envíe la clave vástago de NAS, el identificador de clave vástago de NAS y el identificador de clave progenitora de NAS a la primera entidad de red central, cuando se determina que la clave de NAS es la clave vástago de NAS derivada.

39. La entidad de red de acuerdo con cualquiera de las reivindicaciones 33 a 36, en donde la generación de la clave de anclaje se desencadena tras la recepción de una solicitud de autenticación desde una primera entidad de red central, en donde la solicitud de autenticación se basa en una solicitud desde el dispositivo terminal para el establecimiento de una primera conexión de NAS que porta un primer procedimiento de NAS entre el dispositivo terminal y la primera entidad de red central, y comprende el indicador de NAS que indica el primer procedimiento de NAS.

40. La entidad de red de acuerdo con la reivindicación 39, en donde se hace adicionalmente que la entidad de red:

- derive la clave progenitora de NAS asociada con el primer procedimiento de NAS basándose en la clave de anclaje y el indicador de NAS incluido en la solicitud de autenticación;

- derive el identificador de clave progenitora de NAS para la clave progenitora de NAS derivada basándose en el indicador de NAS;

- cuando la solicitud de autenticación no comprende un valor de TROCEO,

- determine que una clave de NAS para la primera conexión de NAS es la clave progenitora de NAS derivada; y

- envíe la clave progenitora de NAS derivada y el identificador de clave progenitora de NAS a la primera entidad de red central;

- cuando la solicitud de autenticación comprende un valor de TROCEO,

- derive una clave vástago de NAS basándose en la clave progenitora de NAS derivada y el valor de TROCEO;

- derive un identificador de clave vástago de NAS para la clave vástago de NAS;

- determine que la clave de NAS para la primera conexión de NAS es la clave vástago de NAS derivada; y

- envíe la clave vástago de NAS derivada, el identificador de clave vástago de NAS y el identificador de clave progenitora de NAS a la primera entidad de red central.

41. La entidad de red de acuerdo con cualquiera de las reivindicaciones 37, 38 y 40, en donde se hace adicionalmente que la entidad de red:

- derive 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; y
envíe la nueva clave de NAS a la primera entidad de red central.

42. La entidad de red de acuerdo con cualquiera de las reivindicaciones 37 a 41, en donde se hace adicionalmente que la entidad de red:

reciba, desde una segunda entidad de red central, una segunda solicitud de una clave de NAS para una segunda conexión de NAS que porta un segundo procedimiento de NAS;

determine la clave de NAS para la segunda conexión de NAS basándose en la segunda solicitud; y

envíe la clave de NAS para la segunda conexión de NAS a la segunda entidad de red central.

43. La entidad de red de acuerdo con la reivindicación 42,

en donde, para determinar la clave de NAS para la segunda conexión de NAS, se hace adicionalmente que la entidad de red:

identifique la clave progenitora de NAS basándose en el identificador de clave de anclaje y el identificador de clave progenitora de NAS incluidos en la segunda solicitud;

determine, cuando la segunda solicitud no comprende un valor de TROCEO, que la clave de NAS es la clave progenitora de NAS identificada;

cuando la segunda solicitud comprende un valor de TROCEO,

derive una clave vástago de NAS basándose en la clave progenitora de NAS identificada y el valor de TROCEO;

derive un identificador de clave vástago de NAS para la clave vástago de NAS; y

determine que la clave de NAS es la clave vástago de NAS derivada; y

en donde, para enviar la clave de NAS para la segunda conexión de NAS a la segunda entidad de red central, se hace adicionalmente que la entidad de red:

envíe la clave progenitora de NAS identificada a la segunda entidad de red central, basándose en que se determine que la clave de NAS es la clave progenitora de NAS identificada; y

envíe la clave vástago de NAS, el identificador de clave vástago de NAS y el identificador de clave progenitora de NAS a la segunda entidad de red central, basándose en que se determine que la clave de NAS es la clave vástago de NAS derivada.

44. La entidad de red de acuerdo con la reivindicación 42 o 43, en donde se hace adicionalmente que la entidad de red:

derive una nueva clave de NAS para la segunda conexión de NAS basándose en la clave de NAS actual para la segunda conexión de NAS y recuentos de NAS durante un traspaso o durante una actualización de registro de NAS; y

envíe la nueva clave de NAS a la segunda entidad de red central.

45. La entidad de red de acuerdo con cualquiera de las reivindicaciones 37 a 44, en donde la primera entidad de red central está configurada para manejar procedimientos de gestión de movilidad de NAS, y la entidad de red y la primera entidad de red central están coubicadas.

46. Un método realizado por una entidad de red para asegurar una función de gestión de claves, comprendiendo el método:

generar una clave de anclaje con un dispositivo terminal;

derivar un identificador de clave de anclaje para la clave de anclaje, y enviar el 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 identificador de clave progenitora de NAS basándose en el indicador de NAS respectivo.

47. El método de acuerdo con la reivindicación 46, en donde el método comprende además:

almacenar el identificador de clave de anclaje, el conjunto de claves progenitoras de NAS y los identificadores de clave progenitora de NAS respectivos.

48. El método de acuerdo con la reivindicación 46 o 47, en donde el método comprende además:

enviar los identificadores de clave progenitora de NAS asociados con las claves progenitoras de NAS al dispositivo terminal.

49. El método de acuerdo con cualquiera de las reivindicaciones 46 a 48, 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.

50. El método de acuerdo con cualquiera de las reivindicaciones 46 a 49, en donde el método comprende además:

recibir, desde una primera entidad de red central, una primera solicitud de una clave de NAS para una primera conexión de NAS que porta un primer procedimiento de NAS;

determinar la clave de NAS para la primera conexión de NAS basándose en la primera solicitud; y

enviar la clave de NAS para la primera conexión de NAS a la primera entidad de red central.

51. El método de acuerdo con la reivindicación 50, en donde determinar la clave de NAS para la primera conexión de NAS comprende:

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 primera solicitud;

determinar, cuando la primera solicitud no comprende un valor de TROCEO, que la clave de NAS es la clave progenitora de NAS identificada;

cuando la primera solicitud comprende un valor de TROCEO,

derivar una clave vástago de NAS basándose en la clave progenitora de NAS identificada y el valor de TROCEO;

derivar un identificador de clave vástago de NAS para la clave vástago de NAS; y

determinar que la clave de NAS es la clave vástago de NAS derivada; y

en donde enviar la clave de NAS para la primera conexión de NAS a la primera entidad de red central comprende:

enviar la clave progenitora de NAS identificada a la primera entidad de red central, cuando se determina que la clave de NAS es la clave progenitora de NAS identificada; y

enviar la clave vástago de NAS, el identificador de clave vástago de NAS y el identificador de clave progenitora de NAS a la primera entidad de red central, cuando se determina que la clave de NAS es la clave vástago de NAS derivada.

52. El método de acuerdo con cualquiera de las reivindicaciones 46 a 49, en donde la generación de la clave de anclaje se desencadena tras la recepción de una solicitud de autenticación desde una primera entidad de red central, en donde la solicitud de autenticación se basa en una solicitud desde el dispositivo terminal para el establecimiento de una primera conexión de NAS que porta un primer procedimiento de NAS entre el dispositivo terminal y la primera entidad de red central, y comprende el indicador de NAS que indica el primer procedimiento de NAS.

53. El método de acuerdo con la reivindicación 52, en donde el método comprende además:

- derivar la clave progenitora de NAS asociada con el primer procedimiento de NAS basándose en la clave de anclaje y el indicador de NAS incluido en la solicitud de autenticación;

- derivar el identificador de clave progenitora de NAS para la clave progenitora de NAS derivada basándose en el indicador de NAS;

- cuando la solicitud de autenticación no comprende un valor de TROCEO,

- determinar que una clave de NAS para la primera conexión de NAS es la clave progenitora de NAS derivada; y

- enviar la clave progenitora de NAS derivada y el identificador de clave progenitora de NAS a la primera entidad de red central;

- cuando la solicitud de autenticación comprende un valor de TROCEO,

- derivar una clave vástago de NAS basándose en la clave progenitora de NAS derivada y el valor de TROCEO;

- derivar un identificador de clave vástago de NAS para la clave vástago de NAS;

- determinar que la clave de NAS para la primera conexión de NAS es la

clave vástago de NAS derivada; y

enviar la clave vástago de NAS derivada, el identificador de clave vástago de NAS y el identificador de clave progenitora de NAS a la primera entidad de red central.

54. El método de acuerdo con cualquiera de las reivindicaciones 50, 51 y 53, en donde el método comprende además:

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; y

enviar la nueva clave de NAS a la primera entidad de red central.

55. El método de acuerdo con cualquiera de las reivindicaciones 50 a 54, en donde el método comprende además:

recibir, desde una segunda entidad de red central, una segunda solicitud de una clave de NAS para una segunda conexión de NAS que porta un segundo procedimiento de NAS;

determinar la clave de NAS para la segunda conexión de NAS basándose en la segunda solicitud; y

enviar la clave de NAS para la segunda conexión de NAS a la segunda entidad de red central.

56. El método de acuerdo con la reivindicación 55, en donde determinar la clave de NAS para la segunda conexión de NAS comprende:

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 segunda solicitud;

determinar, cuando la segunda solicitud no comprende un valor de TROCEO, que la clave de NAS es la clave progenitora de NAS identificada;

cuando la segunda solicitud comprende un valor de TROCEO,

derivar una clave vástago de NAS basándose en la clave progenitora de NAS identificada y el valor de TROCEO;

derivar un identificador de clave vástago de NAS para la clave vástago de NAS; y

determinar que la clave de NAS es la clave vástago de NAS derivada; y

en donde enviar la clave de NAS para la segunda conexión de NAS a la segunda entidad de red central comprende:

enviar la clave progenitora de NAS identificada a la segunda entidad de red central, basándose en que se determine que la clave de NAS es la clave progenitora de NAS identificada; y

enviar la clave vástago de NAS, el identificador de clave vástago de NAS y el identificador de clave progenitora de NAS a la segunda entidad de red central, basándose en que se determine que la clave de NAS es la clave vástago de NAS derivada.

57. El método de acuerdo con las reivindicaciones 55 o 56, en donde el método comprende además:

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

enviar la nueva clave de NAS a la segunda entidad de red central.

58. Una entidad de red central configurada para implementar una función de red central, 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 la entidad de red central al menos:

reciba 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

obtenga 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 indicador de NAS que indica el procedimiento de NAS.

59. La entidad de red central de acuerdo con la reivindicación 58, en donde, para obtener una clave de NAS para la conexión de NAS, se hace que la entidad de red central:

determine si se requiere una autenticación para el dispositivo terminal basándose en la solicitud de establecimiento de la conexión de NAS; y

basándose en la determinación de que se requiere la autenticación,

desencadene el envío de una solicitud de autenticación, en donde la solicitud de autenticación comprende el indicador de NAS que indica el procedimiento de NAS;

reciba un identificador de clave de anclaje y un identificador de clave progenitora de NAS asociado con el indicador de NAS;

envíe una solicitud para la clave de NAS, en donde la solicitud comprende el identificador de clave de anclaje y el identificador de clave progenitora de NAS;

reciba, cuando la solicitud no comprende un valor de TROCEO, la clave progenitora de NAS identificada por el identificador de clave de anclaje y el identificador de clave progenitora de NAS como la clave de NAS; y

reciba, cuando la solicitud comprende además un valor de TROCEO, la clave vástago de NAS basándose en el identificador de clave de anclaje, el identificador de clave progenitora de NAS y el valor de TROCEO como la clave de NAS, un identificador de clave vástago de NAS para la clave vástago de NAS, y el identificador de clave progenitora de NAS.

60. La entidad de red central de acuerdo con la reivindicación 59, en donde, para obtener una clave de NAS para la conexión de NAS, se hace adicionalmente que la entidad de red central:

basándose en la determinación de que se requiere la autenticación,

desencadene el envío de una solicitud de autenticación, en donde la solicitud de autenticación comprende el indicador de NAS que indica el procedimiento de NAS;

reciba, cuando la solicitud de autenticación no comprende un valor de TROCEO, la clave progenitora de NAS asociada con el indicador de NAS como la clave de NAS; y

reciba, cuando la solicitud de autenticación comprende además un valor de TROCEO, la clave vástago de NAS asociada con el indicador de NAS como la clave de NAS, un identificador de clave vástago de NAS para la clave vástago de NAS, y el identificador de clave progenitora de NAS asociado con la clave progenitora de NAS basándose en la cual se deriva la clave vástago de NAS.

61. La entidad de red central de acuerdo con la reivindicación 59 o 60, en donde, para obtener una clave de NAS para la conexión de NAS, se hace adicionalmente que la entidad de red central:

basándose en la determinación de que no se requiere la autenticación,

verifique si el dispositivo terminal se ha registrado con éxito;

envíe, cuando el dispositivo terminal se verifica como registrado con éxito, una solicitud para la clave de NAS, en donde la solicitud comprende un identificador de clave de anclaje y un identificador de clave progenitora de NAS;

reciba, cuando la solicitud no comprende un valor de TROCEO, la clave progenitora de NAS identificada por el identificador de clave de anclaje y el identificador de clave progenitora de NAS como la clave de NAS; y

reciba, cuando la solicitud comprende además un valor de TROCEO, la clave vástago de NAS basándose en el identificador de clave de anclaje, el identificador de clave progenitora de NAS y el valor de TROCEO como la clave de NAS, un identificador de clave vástago de NAS para la clave vástago de NAS, y el identificador de clave progenitora de NAS.

62. La entidad de red central de acuerdo con cualquiera de las reivindicaciones 58 a 61, en donde se hace adicionalmente que la entidad de red central:

genere un valor de TROCEO basándose en al menos uno de los siguientes: un identificador, ID, de sesión de unidad de datos de protocolo, PDU; información de asistencia de selección de segmento de red único, S-NSSAI; o un identificador de conjunto de funciones de red.

63. La entidad de red central de acuerdo con cualquiera de las reivindicaciones 58 a 62, en donde se hace adicionalmente que la entidad de red central derive claves de estrato de acceso, AS, basándose al menos en parte en la clave de NAS para la conexión de NAS que porta procedimientos de gestión de movilidad de NAS.

64. La entidad de red central de acuerdo con cualquiera de las reivindicaciones 58 a 63, en donde la entidad de red central es una entidad de red de origen en un traspaso o una actualización de registro de NAS, y en donde se hace adicionalmente

que la entidad de red central:

- derive una nueva clave de NAS para la conexión de NAS basándose en la clave de NAS actual para la conexión de NAS y recuentos de NAS; y

- proporcione la nueva clave de NAS a una entidad de red objetivo en el traspaso o la actualización de registro de NAS.

65. Un método realizado por una entidad de red central configurada para implementar una función de red central, que comprende:

- 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 indicador de NAS que indica el procedimiento de NAS.

66. El método de acuerdo con la reivindicación 65, en donde obtener una clave de NAS para la conexión de NAS comprende:

- determinar si se requiere una autenticación para el dispositivo terminal basándose en la solicitud de establecimiento de la conexión de NAS; y

- basándose en la determinación de que se requiere la autenticación,

- desencadenar el envío de una solicitud de autenticación, en donde la solicitud de autenticación comprende el indicador de NAS que indica el procedimiento de NAS;

- recibir un identificador de clave de anclaje y un identificador de clave progenitora de NAS asociado con el indicador de NAS;

- enviar una solicitud para la clave de NAS, en donde la solicitud comprende el identificador de clave de anclaje y el identificador de clave progenitora de NAS;

recibir, cuando la solicitud no comprende un valor de TROCEO, la clave progenitora de NAS identificada por el identificador de clave de anclaje y el identificador de clave progenitora de NAS como la clave de NAS; y

recibir, cuando la solicitud comprende además un valor de TROCEO, la clave vástago de NAS basándose en el identificador de clave de anclaje, el identificador de clave progenitora de NAS y el valor de TROCEO como la clave de NAS, un identificador de clave vástago de NAS para la clave vástago de NAS, y el identificador de clave progenitora de NAS.

67. El método de acuerdo con la reivindicación 66, en donde obtener una clave de NAS para la conexión de NAS comprende además:

basándose en la determinación de que se requiere la autenticación,

desencadenar el envío de una solicitud de autenticación, en donde la solicitud de autenticación comprende el indicador de NAS que indica el procedimiento de NAS;

recibir, cuando la solicitud de autenticación no comprende un valor de TROCEO, la clave progenitora de NAS asociada con el indicador de NAS como la clave de NAS; y

recibir, cuando la solicitud de autenticación comprende además un valor de TROCEO, la clave vástago de NAS asociada con el indicador de NAS como la clave de NAS, un identificador de clave vástago de NAS para la clave vástago de NAS, y el identificador de clave progenitora de NAS asociado con la clave progenitora de NAS basándose en la cual se deriva la clave vástago de NAS.

68. El método de acuerdo con la reivindicación 66 o 67, en donde obtener una clave de NAS para la conexión de NAS comprende además:

basándose en la determinación de que no se requiere la autenticación,

verificar si el dispositivo terminal se ha registrado con éxito;

enviar, cuando el dispositivo terminal se verifica como registrado con éxito, una solicitud para la clave de NAS, en donde la solicitud comprende un identificador de clave de anclaje y un identificador de clave progenitora de NAS;

recibir, cuando la solicitud no comprende un valor de TROCEO, la clave progenitora de NAS identificada por el identificador de clave de anclaje y el identificador de clave progenitora de NAS como la clave de NAS; y

recibir, cuando la solicitud comprende además un valor de TROCEO, la clave vástago de NAS basándose en el identificador de clave de anclaje, el identificador de clave progenitora de NAS y el valor de TROCEO como la clave de NAS, un identificador de clave vástago de NAS para la clave vástago de NAS, y el identificador de clave progenitora de NAS.

69. El método de acuerdo con cualquiera de las reivindicaciones 65 a 68, en donde el método comprende además:

generar un valor de TROCEO basándose en al menos uno de los siguientes: un identificador, ID, de sesión de unidad de datos de protocolo, PDU; información de asistencia de selección de segmento de red único, S-NSSAI; o un identificador de conjunto de funciones de red.

70. El método de acuerdo con cualquiera de las reivindicaciones 65 a 69, en donde la entidad de red central es una entidad de red de origen en un traspaso o una actualización de registro de NAS, y en donde el método comprende además:

derivar una nueva clave de NAS para la conexión de NAS basándose en la clave de NAS actual para la conexión de NAS y recuentos de NAS; y

proporcionar la nueva clave de NAS a una entidad de red objetivo en el traspaso o la actualización de registro de NAS.