

GESTIÓN DE CLAVES DE SEGURIDAD EN OPERACIÓN DE CONECTIVIDAD DUAL

CAMPO TECNOLÓGICO

5 La presente divulgación se refiere a, pero sin limitación, la operación de conectividad dual en el contexto de las redes de acceso de radio, como se define por la norma del proyecto de asociación de 3ª generación (3GPP), tal como la norma 5G que también se denomina Nueva Radio (NR). La divulgación pertenece en particular a la gestión de claves de seguridad en una operación de
10 conectividad dual de este tipo, y más en particular a la gestión de claves de seguridad para nodos secundarios para la operación de conectividad dual.

ANTECEDENTES

La conectividad dual (DC) es un modo de operación en el que un equipo de usuario (UE), que es capaz de transmisión y recepción múltiples, está
15 configurado para utilizar recursos proporcionados por dos nodos de radio diferentes. Un nodo actúa como nodo maestro (MN) y el otro nodo actúa como nodo secundario (SN). El MN y el SN están conectados a través de una interfaz de red y al menos el MN está conectado a la red central. Un grupo de células maestras (MCG) es un grupo de al menos una célula de servicio asociada con el
20 MN, y un grupo de células secundarias (SCG) es un grupo de al menos una célula de servicio asociada con el SN (véanse, por ejemplo, las referencias [1], [2]).

Para protección de integridad y cifrado de señalización de control de recursos de radio (RRC) y datos de usuario, se usa la clave de seguridad K_{gNB} ,
25 que se genera basándose en claves de nivel de estrato sin acceso (NAS). La

K_{gNB} se pueden actualizar para garantizar la movilidad horizontal a través de los nodos sin cambiar la red central (véase, por ejemplo, la referencia [3]).

En el caso de DC, los portadores de radio pueden asignarse al MCG y al SCG, y la movilidad del UE a través del SCG puede ser independiente de la
5 movilidad en el MCG. Por lo tanto, para actualizar las claves de seguridad para portadores de SCG sin impactar en los procedimientos de seguridad en curso para portadores de MCG, se introduce una nueva clave de seguridad K_{SN} para portadores de SCG. La K_{SN} se actualiza por el UE basándose en un valor de contador de SN que se proporciona al UE por el MN (véase, por ejemplo, la
10 referencia [4]).

SUMARIO DE ALGUNAS REALIZACIONES DE EJEMPLO

Sin embargo, existe el problema de que, de acuerdo con la presente norma 5G, después de realizar una adición o cambio condicional (CPAC) de una célula primaria de un grupo de células secundarias (PSCell), o después de
15 realizar un traspaso condicional (CHO), el los datos de configuración de CPAC o CHO se liberan por el UE después de que se haya ejecutado el CPAC o CHO. Además, el mensaje de configuración para CPAC o CHO únicamente puede contener un valor de contador de SN. Por lo tanto, siempre que el UE se ha movido de un SCG de servicio anterior a un SCG de servicio actual, tiene que
20 enviarse un nuevo mensaje de configuración por el MN para preparar el UE para cambios de grupo de células posteriores a posibles SCG objetivo futuros. En este contexto, los posibles SCG objetivo futuros también incluyen el SCG de servicio anterior, ya que el UE de la misma manera tiene que estar preparado para cambiar de vuelta al SCG de servicio anterior. Dado que el mensaje de
25 configuración se transmite mediante señalización de RRC, se genera una

sobrecarga de señalización de RRC significativa, en particular, cuando se realiza un gran número de CPAC o CHO dentro de un tiempo corto. Además, el requisito de enviar el nuevo mensaje de configuración antes de tener capacidad de realizar cambios de grupo de células posteriores limita la movilidad rápida del UE a través de diferentes SCG.

En vista de lo anterior, las realizaciones de ejemplo de la presente divulgación pueden tener, entre otras cosas, el efecto de habilitar que un equipo de usuario realice una actualización de clave de seguridad autónoma sin implicación de red. Por consiguiente, pueden omitirse nuevos mensajes de configuración para CPAC o CHO en ciertas situaciones, de manera que se reduce la sobrecarga de señalización de RRC y se habilita en mayor medida la movilidad rápida del UE a través de diferentes SCG.

De acuerdo con un primer aspecto de ejemplo, se divulga un equipo de usuario. El equipo de usuario se puede configurar para soportar operación de conectividad dual hacia un nodo maestro y un nodo secundario de una red de acceso de radio. El equipo de usuario puede comprender al menos un procesador y al menos una memoria. La al menos una memoria puede almacenar instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el equipo de usuario realice al menos lo siguiente:

- establecer una conexión hacia el nodo maestro;
- recibir información de configuración desde el nodo maestro, en donde la información de configuración puede comprender información de contador de clave que define una secuencia de al menos dos valores de contador de clave diferentes para generar al menos dos claves de seguridad diferentes para al menos dos nodos secundarios objetivo diferentes.

El equipo de usuario puede ser un dispositivo estacionario o un dispositivo móvil. En particular, el equipo de usuario puede ser un dispositivo móvil, tal como un teléfono inteligente, una tableta, un dispositivo ponible, un reloj inteligente, un dispositivo de baja potencia, un dispositivo de IoT, un dispositivo de IIoT, un
5 vehículo, un camión, un dron, un avión, o similares. El equipo de usuario puede, en particular, ser capaz de comunicarse con (transmitir y recibir señales y/o datos a/desde) uno o más otros equipos de usuario. Adicionalmente o como alternativa, el equipo de usuario, en particular, puede ser capaz de comunicarse con (transmitir y recibir señales y/o datos a/desde) al menos un nodo maestro de una
10 red de acceso de radio, el nodo maestro configurado para soportar operación de conectividad dual hacia un nodo secundario de la red de acceso de radio y el equipo de usuario. Adicionalmente o como alternativa, el equipo de usuario, en particular, puede ser capaz de comunicarse con (transmitir y recibir señales y/o datos a/desde) al menos un nodo secundario de una red de acceso de radio, el
15 nodo secundario configurado para soportar operación de conectividad dual hacia un nodo maestro de la red de acceso de radio y el equipo de usuario. En general, el equipo de usuario también puede ser cualquier dispositivo habilitado para comunicación con una red de comunicación y/u otro equipo de usuario.

Un nodo de radio (por ejemplo, un nodo maestro o un nodo secundario)
20 puede entenderse como una estación de comunicación inalámbrica instalada en una ubicación fija o móvil y, en particular, puede ser, o comprender, una entidad de una red de acceso de radio de un sistema de comunicación inalámbrica. Por ejemplo, el nodo de radio puede ser, comprender o ser parte de una estación base de una red de comunicación inalámbrica de cualquier generación (por
25 ejemplo, un gNB, ng-eNB, eNodeB, NodeB, BTS o similares) de una norma de

3GPP. En general, el nodo de radio puede ser o comprender un componente de hardware o software que implementa una cierta funcionalidad. En un ejemplo, el nodo de radio puede ser una función de gestión de ubicación (LMF). En un ejemplo, el nodo de radio puede ser una entidad como se define por la norma 5G de 3GPP o NR (también denominada como gNB). Por consiguiente, aunque puede entenderse que el nodo de radio se implementa en o es un único dispositivo o módulo, el nodo de radio también puede implementarse a través de o comprender múltiples dispositivos o módulos. Como tal, el nodo de radio, en particular, puede implementarse en o ser un dispositivo estacionario. Múltiples nodos de radio pueden establecer, en particular, un sistema o red de comunicación inalámbrica, que puede ser, en particular, un sistema de NR o 5G o cualquier otro sistema de comunicaciones inalámbricas definido por una norma pasada o futura, en particular, sucesoras de las normas 3GPP actuales. En particular, múltiples nodos de radio, por ejemplo, un nodo maestro y uno o más nodos secundarios, se pueden configurar para soportar operación de conectividad dual hacia uno o más equipos de usuario. El nodo de radio puede ser capaz de estar en comunicación directa y/o indirecta con otros nodos de radio o con equipo de usuario.

Como se usa en el presente documento, la información de configuración puede entenderse como cualquier clase de información basándose en la que un equipo de usuario está o puede estar configurado con respecto a la operación de conectividad dual y/o la gestión de claves de seguridad. Por ejemplo, la información de configuración puede ser información de reconfiguración de RRC, en particular, como parte de una solicitud de reconfiguración de RRC hacia un equipo de usuario.

Como se usa en el presente documento, la información de contador de clave puede entenderse como cualquier tipo de información que define al menos un valor de un contador de clave, estando asociado el contador de clave con una clave de seguridad. Por ejemplo, la información de contador de clave puede ser, comprender, ser indicativa de, habilitar determinar o especificar de manera similar explícita o implícitamente al menos un valor anterior, presente o futuro de un contador de clave. Por ejemplo, el valor de contador de clave puede definir un valor de un contador de SN.

Como se usa en el presente documento, una secuencia puede entenderse como una serie ordenada de elementos similares que siguen un cierto patrón. A modo de ejemplo, una secuencia puede tener un elemento inicial y un elemento final, en particular, si la secuencia es una secuencia finita. Como otro ejemplo, una secuencia puede tener un elemento inicial, pero puede no tener un elemento final, en particular, si la secuencia es una secuencia infinita. Por ejemplo, la secuencia puede ser una serie ordenada de números o valores que siguen un cierto patrón. Por ejemplo, una secuencia puede ser una serie ordenada de números enteros, en particular, números enteros no negativos, en donde pueden obtenerse elementos posteriores a partir de elementos precedentes añadiendo iterativamente un valor de paso predefinido. Por ejemplo, el valor de paso predefinido puede ser igual a uno.

Como se usa en el presente documento, un valor de contador de clave puede entenderse como un valor de un contador de clave, estando asociado el contador de clave con una clave de seguridad. Por ejemplo, el valor de contador de clave puede usarse como una entrada de actualización en derivaciones posteriores de la clave de seguridad. Por ejemplo, el valor de contador de clave

puede ser un valor de un contador de SN. Por ejemplo, el valor de contador de clave puede ser un número, en particular, un número entero no negativo.

Como se usa en el presente documento, la información de contador de clave que define una secuencia de al menos dos valores de contador de clave diferentes puede entenderse de tal manera que los al menos dos valores de contador de clave diferentes pueden derivarse de la información de contador de clave de cualquier manera concebible, en un punto de tiempo presente o futuro. Por ejemplo, la información de contador de clave puede definir una secuencia de al menos dos valores de contador de clave diferentes en los que la información de contador de clave es, comprende, es indicativa de, habilita determinar o especifica de manera similar explícita o implícitamente un elemento inicial de la secuencia junto con una regla con respecto a la derivación de elementos adicionales de la secuencia. Por ejemplo, los elementos de la secuencia pueden formar una secuencia monótonamente creciente, en particular una secuencia de números enteros no negativos monótonamente creciente en uno. De esta manera, puede evitarse de una manera particularmente sencilla que los valores de contador de clave se usen más de una vez para la generación de una clave de seguridad.

Como se usa en el presente documento, una clave de seguridad puede entenderse como una pieza de información, en particular, una cadena de caracteres, usada para fines de seguridad en una red de acceso de radio. Por ejemplo, la cadena de caracteres puede comprender números, letras, símbolos, caracteres especiales y similares. Por ejemplo, la clave de seguridad puede ser secreta. Por ejemplo, la clave de seguridad puede ser una clave de seguridad para protección de integridad y/o cifrado de datos, en particular de datos

intercambiados entre un equipo de usuario y un nodo secundario de una red de acceso de radio. Por ejemplo, la clave de seguridad puede ser una clave de seguridad superordenada basándose en la cual se determina una pluralidad de claves de seguridad subordinadas para protección de integridad y/o cifrado, en particular, una primera clave de seguridad subordinada para protección de integridad de señalización RRC, una segunda clave de seguridad subordinada para cifrado de señalización de RRC, una tercera clave de seguridad subordinada para protección de integridad de datos de usuario y una cuarta clave de seguridad subordinada para el cifrado de datos de usuario. Por ejemplo, la clave de seguridad puede ser una clave de seguridad K_{SN} .

Como se usa en el presente documento, el cifrado puede entenderse como un concepto general de conversión de información entre el denominado texto sin formato, que es una forma descifrada de la información en un formato fácilmente legible por un ser humano o un ordenador, y el denominado texto cifrado, que es una forma cifrada de la información en un formato no legible por un ser humano o un ordenador sin un descifrado apropiado. Por consiguiente, el cifrado incluye tanto el cifrado de información de texto sin formato a texto cifrado, como el descifrado de información desde texto cifrado a texto sin formato.

Como se usa en el presente documento, un nodo secundario objetivo puede entenderse como un nodo secundario de una red de acceso de radio, cuyo grupo de células secundarias (SCG) asociado califica o puede calificar, en un punto de tiempo presente o futuro respectivo, para una adición o cambio de PSCell condicional (CPAC) o un traspaso condicional (CHO) hacia el SCG asociado con el nodo secundario objetivo. Por ejemplo, un nodo secundario objetivo es diferente de un nodo secundario de origen, en donde un nodo

secundario de origen como se usa en el presente documento puede entenderse como un nodo secundario asociado con un SCG de servicio actual. Sin embargo, un nodo secundario objetivo también puede ser idéntico a un nodo secundario de origen en el sentido de que el SCG asociado con el nodo secundario de origen califica o puede calificar, en un punto de tiempo futuro, para un CPAC o CHO posterior de vuelta al SCG asociado con el nodo secundario de origen, después de que se haya realizado un CPAC o CHO desde el SCG asociado con el nodo secundario de origen hacia un SCG asociado con un nodo secundario objetivo diferente del nodo secundario de origen.

10 De acuerdo con el primer aspecto de ejemplo, el equipo de usuario puede establecer una conexión hacia el nodo maestro. De esta manera, puede conseguirse que se habilite el intercambio de datos entre el UE y el MN. Por ejemplo, la conexión puede ser una conexión segura, en particular una conexión de señalización de RRC segura.

15 Además, de acuerdo con el primer aspecto de ejemplo, el equipo de usuario puede recibir información de configuración desde el nodo maestro, en donde la información de configuración comprende información de contador de clave que define una secuencia de al menos dos valores de contador de clave diferentes para generar al menos dos claves de seguridad diferentes para al menos dos nodos secundarios objetivo diferentes. En comparación con un
20 escenario, en el que el mensaje de configuración para CPAC o CHO únicamente contiene un valor de contador de clave, y en el que los datos de configuración de CPAC o CHO son liberados por el UE después de que se haya ejecutado el CPAC o CHO, las realizaciones de ejemplo del primer aspecto de ejemplo
25 pueden ser ventajosas en el sentido de que los nuevos mensajes de

configuración para CPAC o CHO pueden omitirse en ciertas situaciones. Por ejemplo, después de que el UE haya realizado un CPAC o CHO desde un SCG asociado con un SN de origen hacia un SCG asociado con un primer SN objetivo y haya usado un primer valor de contador de clave derivado de la información de contador de clave para generar una primera clave de seguridad para el intercambio de datos con el primer SN objetivo, el UE está habilitado para derivar, a partir de la información de contador de clave, un segundo valor de contador de clave y usar el segundo valor de contador de clave para generar una segunda clave de seguridad para el intercambio de datos con un segundo SN objetivo. Por lo tanto, el UE puede realizar de manera autónoma la actualización de clave de seguridad para un CPAC o CHO hacia el SCG asociado con el segundo SN objetivo sin que el MN tenga que transmitir nueva información de configuración para este CPAC o CHO al UE. De esta manera, también se puede lograr que se reduzca la sobrecarga de señalización de RRC y se habilite en mayor medida la movilidad rápida del UE a través de diferentes SCG.

En realizaciones del primer aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el equipo de usuario realice al menos lo siguiente:

- generar una primera clave de seguridad usando un primer valor de contador de clave derivado de la información de contador de clave.

Como se usa en el presente documento, derivar un primer valor de contador de clave a partir de la información de contador de clave puede entenderse de tal manera que el primer valor de contador de clave se obtiene por el equipo de usuario basándose en la información de contador de clave de

cualquier manera concebible. Por ejemplo, el equipo de usuario puede derivar el primer valor de contador de clave en el sentido de que obtiene un primer valor de contador de clave que es idéntico a, comprendido por, indicado por, habilitado para determinar por, o especificado de manera similar explícita o implícitamente en la información de contador de clave. Como se usa en el presente documento, generar una primera clave de seguridad usando un primer valor de contador de clave puede entenderse de tal manera que la primera clave de seguridad se genera por el equipo de usuario basándose en el primer valor de contador de clave de cualquier manera concebible. Por ejemplo, el equipo de usuario puede calcular la primera clave de seguridad usando el primer valor de contador de clave como una entrada de actualización para el cálculo. Al generar una primera clave de seguridad usando un primer valor de contador de clave derivado de la información de contador de clave, se puede lograr que pueda obtenerse por el UE una primera clave de seguridad para protección de integridad y/o cifrado de datos, en particular, de datos a intercambiar entre el UE y un primer SN objetivo.

En realizaciones del primer aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el equipo de usuario realice al menos lo siguiente:

- usar la primera clave de seguridad para protección de integridad y/o cifrado de datos intercambiados entre el equipo de usuario y un primer nodo secundario objetivo.

De esta manera, puede conseguirse que se realice un intercambio seguro de datos entre el UE y el primer SN objetivo, en particular, un intercambio seguro de datos de acuerdo con la arquitectura de seguridad de la norma 5G.

En realizaciones del primer aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el equipo de usuario realice al menos lo siguiente:

- 5 - procesar la información de contador de clave de tal manera que el equipo de usuario está habilitado para derivar, a partir de la información de contador de clave procesada, al menos un segundo valor de contador de clave, que es diferente del primer valor de contador de clave.

Como se usa en el presente documento, procesar la información de
10 contador de clave puede entenderse de tal manera que la información de contador de clave se modifica por el equipo de usuario de cualquier manera concebible. Por ejemplo, procesar la información de contador de clave puede comprender modificar la secuencia de valores de contador de clave definidos por la información de contador de clave. Por ejemplo, procesar la información de
15 contador de clave puede comprender evitar que el primer valor de contador de clave se reutilice para la generación de claves de seguridad distintas de la primera clave de seguridad. Al procesar la información de contador de clave, se puede lograr que el UE esté habilitado para derivar, a partir de la información de contador de clave procesada, un segundo valor de contador de clave y usar el
20 segundo valor de contador de clave para generar una segunda clave de seguridad para el intercambio de datos con un segundo SN objetivo. Por lo tanto, el UE puede realizar de manera autónoma la actualización de clave de seguridad para un CPAC o CHO futuro hacia el SCG asociado con el segundo SN objetivo sin que el MN tenga que transmitir nueva información de configuración para este
25 CPAC o CHO al UE. De esta manera, también se puede lograr que se reduzca

la sobrecarga de señalización de RRC y se habilite en mayor medida la movilidad rápida del UE a través de diferentes SCG.

En realizaciones del primer aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el equipo de usuario realice al menos lo siguiente:

- generar una segunda clave de seguridad, que es diferente de la primera clave de seguridad, usando el segundo valor de contador de clave derivado de la información de contador de clave procesada.

10 Como se usa en el presente documento, derivar el segundo valor de contador de clave a partir de la información de contador de clave procesada puede entenderse de tal manera que el segundo valor de contador de clave se obtiene por el equipo de usuario basándose en la información de contador de clave procesada de cualquier manera concebible. Por ejemplo, el equipo de usuario puede derivar el segundo valor de contador de clave en el sentido de
15 que obtiene un segundo valor de contador de clave que es idéntico a, comprendido por, indicado por, habilitado para determinar por, o especificado de manera similar explícita o implícitamente en la información de contador de clave procesada. Como se usa en el presente documento, generar una segunda clave de seguridad usando el segundo valor de contador de clave puede entenderse
20 de tal manera que la segunda clave de seguridad se genera por el equipo de usuario basándose en el segundo valor de contador de clave de cualquier manera concebible. Por ejemplo, el equipo de usuario puede calcular la segunda clave de seguridad usando el segundo valor de contador de clave como una
25 entrada de actualización para el cálculo. Al generar una segunda clave de

seguridad usando el segundo valor de contador de clave derivado de la información de contador de clave procesada, se puede lograr que pueda obtenerse por el UE una segunda clave de seguridad para protección de integridad y/o cifrado de datos, en particular, de datos a intercambiar entre el UE

5 y un segundo SN objetivo.

En realizaciones del primer aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el equipo de usuario realice al menos lo siguiente:

- 10 - usar la segunda clave de seguridad para protección de integridad y/o cifrado de datos intercambiados entre el equipo de usuario y un segundo nodo secundario objetivo, que es diferente del primer nodo secundario objetivo.

De esta manera, puede conseguirse que se realice un intercambio seguro de datos entre el UE y el segundo SN objetivo, en particular, un intercambio seguro de datos de acuerdo con la arquitectura de seguridad de la norma 5G.

En realizaciones del primer aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el equipo de usuario realice al menos lo siguiente:

- 20 - procesar adicionalmente la información de contador de clave de tal manera que el equipo de usuario está habilitado para derivar, a partir de la información de contador de clave adicionalmente procesada, al menos un valor de contador de clave adicional, que es diferente del primer valor de contador de clave y diferente del segundo valor de contador de clave.
- 25

Como se usa en el presente documento, procesar adicionalmente la información de contador de clave puede entenderse de tal manera que la información de contador de clave se modifica adicionalmente por el equipo de usuario de cualquier manera concebible. Por ejemplo, procesar adicionalmente

5 la información de contador de clave puede comprender modificar adicionalmente la secuencia de valores de contador de clave definidos por la información de contador de clave. Por ejemplo, procesar adicionalmente la información de contador de clave puede comprender evitar que el segundo valor de contador de clave se reutilice para la generación de claves de seguridad distintas de la

10 segunda clave de seguridad. Al procesar adicionalmente la información de contador de clave, se puede lograr que el UE esté habilitado para derivar, a partir de la información de contador de clave adicionalmente procesada, un valor de contador de clave adicional y usar el valor de contador de clave adicional para generar una segunda clave de seguridad para el intercambio de datos con un

15 SN objetivo adicional. Por lo tanto, el UE puede realizar de manera autónoma la actualización de clave de seguridad para un CPAC o CHO futuro hacia el SCG asociado con el SN objetivo adicional sin que el MN tenga que transmitir nueva información de configuración para este CPAC o CHO al UE. De esta manera, también se puede lograr que se reduzca la sobrecarga de señalización de RRC

20 y se habilite en mayor medida la movilidad rápida del UE a través de diferentes SCG.

En realizaciones de ejemplo del primer aspecto de ejemplo, la información de contador de clave recibida desde el nodo maestro puede definir una lista de al menos dos valores de contador de clave diferentes. Como se usa en el

25 presente documento, una lista puede entenderse como una secuencia que tiene

un elemento final. Por lo tanto, una lista también puede entenderse como una secuencia finita. Como se usa en el presente documento, la información de contador de clave que define una lista de valores de contador de clave puede entenderse de tal manera que la lista de valores de contador de clave puede

5 derivarse de la información de contador de clave de cualquier manera concebible, en un punto de tiempo presente o futuro. Por ejemplo, la información de contador de clave puede ser, comprender, ser indicativa de, habilitar determinar o especificar de manera similar explícita o implícitamente la lista de valores de contador de clave. Por ejemplo, la información de contador de clave

10 puede definir una lista de valores de contador de clave en la que la información de contador de clave especifica explícitamente valores de contador de clave individuales de la lista, en particular todos los valores de contador de clave individuales de la lista. Por ejemplo, la información de contador de clave puede definir una lista de valores de contador de clave en la que la información de

15 contador de clave especifica un primer valor de contador de clave y un número máximo de adiciones, en donde el primer elemento de la lista se obtiene seleccionando el primer valor de contador de clave y los elementos restantes de la lista se obtienen añadiendo iterativamente un valor de paso al primer valor de contador de clave hasta que se haya alcanzado el número máximo de adiciones.

20 Por ejemplo, el valor de paso puede estar predeterminado por el equipo de usuario, o puede especificarse dentro de la información de contador de clave. Por ejemplo, el valor de paso puede ser igual a uno. Por ejemplo, la información de contador de clave puede definir una lista de valores de contador de clave en la que la información de contador de clave especifica un intervalo desde un

25 primer valor de contador de clave de número entero no negativo hasta un valor

de contador de clave de número entero no negativo final, en donde se obtiene la lista seleccionando cada número entero no negativo dentro del intervalo especificado como un elemento de la lista de valores de contador de clave. Mediante la información de contador de clave recibida desde el nodo maestro
5 que define una lista de al menos dos valores de contador de clave diferentes, se puede lograr una definición particularmente sencilla de los al menos dos valores de contador de clave diferentes mediante la información de contador de clave, de modo que, por ejemplo, no se requieren operaciones de cálculo complejas y se ahorran los recursos de procesador respectivos.

10 En realizaciones de ejemplo del primer aspecto de ejemplo, generar la primera clave de seguridad puede comprender usar el primer elemento de lista en la lista de valores de contador de clave como el primer valor de contador de clave. De esta manera, puede conseguirse una derivación particularmente sencilla del primer valor de contador de clave a partir de la información de
15 contador de clave, de manera que, por ejemplo, no se requieren operaciones de cálculo complejas y se ahorran recursos de procesador respectivos.

En realizaciones de ejemplo del primer aspecto de ejemplo, procesar la información de contador de clave puede comprender quitar el primer elemento de lista de la lista de valores de contador de clave. De esta manera, se puede
20 lograr un procesamiento particularmente sencillo de la información de contador de clave, de tal manera que, por ejemplo, no se requieren operaciones de cálculo complejas y se ahorran recursos de procesador respectivos.

En realizaciones de ejemplo del primer aspecto de ejemplo, generar la segunda clave de seguridad puede comprender usar el actualmente primer
25 elemento de lista en la lista de valores de contador de clave como el segundo

valor de contador de clave. De esta manera, puede conseguirse una derivación particularmente sencilla del segundo valor de contador de clave a partir de la información de contador de clave procesada, de manera que, por ejemplo, no se requieren operaciones de cálculo complejas y se ahorran recursos de procesador
5 respectivos.

En realizaciones de ejemplo del primer aspecto de ejemplo, procesar adicionalmente la información de contador de clave puede comprender quitar el actualmente primer elemento de lista de la lista de valores de contador de clave. De esta manera, se puede lograr un procesamiento adicional particularmente
10 sencillo de la información de contador de clave, de tal manera que, por ejemplo, no se requieren operaciones de cálculo complejas y se ahorran recursos de procesador respectivos.

En realizaciones de ejemplo del primer aspecto de ejemplo, la información de configuración puede comprender información de contador de clave que define
15 una lista de al menos dos valores de contador de SN diferentes para generar al menos dos claves de seguridad K_{SN} diferentes para al menos dos nodos secundarios objetivo diferentes. El primer valor de contador de clave puede ser un primer valor de contador de SN. El segundo valor de contador de clave puede ser un segundo valor de contador de SN. La primera clave de seguridad puede
20 ser una primera clave de seguridad K_{SN} . La segunda clave de seguridad puede ser una segunda clave de seguridad K_{SN} .

En realizaciones de ejemplo del primer aspecto de ejemplo, la información de configuración puede comprender una solicitud de reconfiguración de control de recursos de radio.

25 En realizaciones de ejemplo del primer aspecto de ejemplo, la información

de configuración puede comprender información que está relacionada con una adición o cambio condicional de una célula primaria de un grupo de células secundarias asociado con el primer nodo secundario objetivo o relacionada con un traspaso condicional hacia el primer objetivo nodo secundario.

5 En realizaciones de ejemplo del primer aspecto de ejemplo, la información de configuración puede comprender información que está relacionada con una adición o cambio condicional de una célula primaria de un grupo de células secundarias asociado con el segundo nodo secundario objetivo o relacionada con un traspaso condicional hacia el segundo objetivo nodo secundario.

10 En realizaciones de ejemplo del primer aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el equipo de usuario realice al menos uno de los siguientes:

- determinar si se cumple al menos una condición para una adición o
15 cambio condicional de una célula primaria de un grupo de células secundarias asociado con el primer nodo secundario objetivo o al menos una condición para un traspaso condicional hacia el primer nodo secundario objetivo;
- iniciar, a través de un canal de acceso aleatorio, un procedimiento de
20 acceso aleatorio hacia el primer nodo secundario objetivo usando la primera clave de seguridad K_{SN} .

En particular, iniciar, a través de un canal de acceso aleatorio (RACH), un procedimiento de acceso aleatorio hacia el primer nodo secundario objetivo usando la primera clave de seguridad K_{SN} puede realizarse en respuesta a la
25 determinación de que se cumple al menos una condición para una adición o

cambio condicional de una célula primaria de un grupo de células secundarias asociado con el primer nodo secundario objetivo o al menos una condición para un traspaso condicional hacia el primer nodo secundario objetivo.

En realizaciones de ejemplo del primer aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el equipo de usuario realice al menos uno de los siguientes:

- determinar si se cumple al menos una condición para una adición o cambio condicional de una célula primaria de un grupo de células secundarias asociado con el segundo nodo secundario objetivo o al menos una condición para un traspaso condicional hacia el segundo nodo secundario objetivo;
- iniciar, a través de un canal de acceso aleatorio, un procedimiento de acceso aleatorio hacia el segundo nodo secundario objetivo usando la segunda clave de seguridad K_{SN} .

En particular, iniciar, a través de un canal de acceso aleatorio (RACH), un procedimiento de acceso aleatorio hacia el segundo nodo secundario objetivo usando la segunda clave de seguridad K_{SN} puede realizarse en respuesta a la determinación de que se cumple al menos una condición para una adición o cambio condicional de una célula primaria de un grupo de células secundarias asociado con el segundo nodo secundario objetivo o al menos una condición para un traspaso condicional hacia el segundo nodo secundario objetivo.

En realizaciones del primer aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el equipo de usuario realice al menos lo

siguiente:

- transmitir, al nodo maestro, información indicativa de un fallo de conexión.

Por ejemplo, el fallo de conexión puede ser un fallo de una conexión entre el equipo de usuario y un nodo secundario objetivo. Por ejemplo, el fallo de
5 conexión puede ser un fallo de un procedimiento de acceso aleatorio desde el equipo de usuario hacia un nodo secundario objetivo, en particular, un procedimiento de acceso aleatorio a través de RACH. Al transmitir, al nodo maestro, información indicativa de un fallo de conexión, puede conseguirse que el MN sea informado acerca del fallo de conexión, de tal manera que el MN pueda
10 tomar medidas respectivas, si es necesario.

En realizaciones del primer aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el equipo de usuario realice al menos lo siguiente:

- 15 - recibir al menos un elemento de lista adicional para la lista de valores de contador de clave desde el nodo maestro.

En particular, recibir al menos un elemento de lista adicional para la lista de valores de contador de clave desde el nodo maestro puede realizarse después de determinar si el número de elementos de lista de la lista de valores
20 de contador de clave no alcanza un umbral predefinido y en respuesta a la determinación que el número de elementos de lista de la lista de valores de contador de clave no alcanza un umbral predefinido. Por ejemplo, el umbral predefinido puede ser igual a uno. Al recibir al menos un elemento de lista adicional para la lista de valores de contador de clave desde el nodo maestro,
25 puede evitarse que el número de elementos de lista de la lista de valores de

contador de clave alcance un valor excesivamente bajo, en particular cero. En consecuencia, el equipo de usuario, después de que se hayan usado uno o más valores de contador de clave para generar claves de seguridad para uno o más SN objetivo y quitado de la lista, puede proporcionarse con valores de contador de clave adicionales y, por lo tanto, está habilitado para generar claves de seguridad adicionales para SN objetivo adicionales. Por lo tanto, se puede lograr que se mantenga la capacidad del UE para realizar un CPAC o un CHO hacia los SCG asociados con los SN objetivo adicionales. En particular, al recibir continuamente al menos un elemento de lista adicional para la lista de valores de contador de clave desde el nodo maestro, se puede habilitar que se realice por el UE un número teóricamente infinito de CPAC o CHO y, por lo tanto, un número teóricamente infinito de eventos de movilidad autónomos.

En realizaciones de ejemplo del primer aspecto de ejemplo, la información de contador de clave recibida desde el nodo maestro puede comprender un valor de contador de clave y una instrucción para mantener el valor de contador de clave. Como se usa en el presente documento, la información de contador de clave que comprende un valor de contador de clave puede entenderse de tal manera que la información de contador de clave comprende información que especifica explícitamente el valor de contador de clave. Como se usa en el presente documento, una instrucción para mantener el valor de contador de clave puede entenderse como una instrucción hacia un equipo de usuario, no para liberar el valor de contador de clave, sino más bien para procesar continuamente el valor de contador de clave. En particular, puede ordenarse al equipo de usuario que procese el valor de contador de clave después de que se haya generado una clave de seguridad usando el valor de contador de clave y/o

después de que se haya usado la clave de seguridad para un nodo secundario objetivo. Mediante la información de contador de clave recibida desde el nodo maestro que comprende un valor de contador de clave y una instrucción para mantener el valor de contador de clave, se puede lograr una derivación particularmente sencilla del primer valor de contador de clave a partir de la información de contador de clave, de modo que, por ejemplo, no se requieren operaciones de cálculo complejas y se ahorran los recursos de procesador respectivos. Además, los posibles SN objetivo no tienen que aprovisionarse previamente con múltiples claves de seguridad.

10 En realizaciones de ejemplo del primer aspecto de ejemplo, generar la primera clave de seguridad puede comprender usar el valor de contador de clave recibido desde el nodo maestro como el primer valor de contador de clave. De esta manera, puede conseguirse una derivación particularmente sencilla del primer valor de contador de clave a partir de la información de contador de clave, de manera que, por ejemplo, no se requieren operaciones de cálculo complejas y se ahorran recursos de procesador respectivos.

20 En realizaciones de ejemplo del primer aspecto de ejemplo, procesar la información de contador de clave puede comprender añadir un valor de paso predefinido al valor de contador de clave recibido desde el nodo maestro. Por ejemplo, el valor de paso predefinido puede ser un número entero positivo, en particular uno. Añadiendo un valor de paso predefinido al valor de contador de clave, se puede lograr un procesamiento particularmente sencillo de la información de contador de clave, de tal manera que, por ejemplo, no se requieren operaciones de cálculo complejas y se ahorran recursos de procesador respectivos.

En realizaciones de ejemplo del primer aspecto de ejemplo, generar la segunda clave de seguridad puede comprender usar el valor de contador de clave actual como el segundo valor de contador de clave. De esta manera, puede conseguirse una derivación particularmente sencilla del segundo valor de contador de clave a partir de la información de contador de clave procesada, de manera que, por ejemplo, no se requieren operaciones de cálculo complejas y se ahorran recursos de procesador respectivos.

En realizaciones de ejemplo del primer aspecto de ejemplo, procesar adicionalmente la información de contador de clave puede comprender añadir el valor de paso predefinido al valor de contador de clave actual. De esta manera, se puede lograr un procesamiento adicional particularmente sencillo de la información de contador de clave, de tal manera que, por ejemplo, no se requieren operaciones de cálculo complejas y se ahorran recursos de procesador respectivos.

En realizaciones de ejemplo del primer aspecto de ejemplo, la información de configuración puede comprender información de contador de clave que define una secuencia de al menos dos valores de contador de SN diferentes para generar al menos dos claves de seguridad K_{SN} diferentes para al menos dos nodos secundarios objetivo diferentes. La información de contador de clave recibida desde el nodo maestro puede comprender un valor de contador de SN y una instrucción para mantener el valor de contador de SN. El primer valor de contador de clave puede ser un primer valor de contador de SN. El segundo valor de contador de clave puede ser un segundo valor de contador de SN. La primera clave de seguridad puede ser una primera clave de seguridad K_{SN} . La segunda clave de seguridad puede ser una segunda clave de seguridad K_{SN} .

En realizaciones de ejemplo del primer aspecto de ejemplo, la información de contador de clave recibida desde el nodo maestro puede definir un número máximo permitido de adiciones del valor de paso predefinido al valor de contador de clave recibido desde el nodo maestro. La al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el equipo de usuario realice al menos lo siguiente

- determinar si se ha alcanzado el número máximo permitido de adiciones;
- en respuesta a la determinación de que se ha alcanzado el número máximo permitido de adiciones, evitar adiciones adicionales del valor de paso predefinido al valor de contador de clave actual.

Por lo tanto, el número de posibles CPAC o CHO realizados por el UE puede especificarse por el MN cuando el MN transmite inicialmente la información de configuración que comprende la información de contador de clave al UE, de modo que el número de eventos de movilidad autónomos del UE puede limitarse.

En realizaciones del primer aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el equipo de usuario realice al menos lo siguiente:

- generar una clave de seguridad adicional, que es diferente de la primera clave de seguridad y diferente de la segunda clave de seguridad, usando el valor de contador de clave adicional derivado de la información de contador de clave adicionalmente procesada.

Como se usa en el presente documento, derivar el valor de contador de clave adicional a partir de la información de contador de clave adicionalmente

procesada puede entenderse de tal manera que el valor de contador de clave adicional se obtiene por el equipo de usuario basándose en la información de contador de clave adicionalmente procesada de cualquier manera concebible. Por ejemplo, el equipo de usuario puede derivar el valor de contador de clave

5 adicional en el sentido de que obtiene un valor de contador de clave adicional que es idéntico a, comprendido por, indicado por, habilitado para determinar por, o especificado de manera similar explícita o implícitamente en la información de contador de clave adicionalmente procesada. Como se usa en el presente documento, generar una clave de seguridad adicional usando el valor de

10 contador de clave adicional puede entenderse de tal manera que la clave de seguridad adicional se genera por el equipo de usuario basándose en el valor de contador de clave adicional de cualquier manera concebible. Por ejemplo, el equipo de usuario puede calcular la clave de seguridad adicional usando el valor de contador de clave adicional como una entrada de actualización para el

15 cálculo. Al generar una clave de seguridad adicional usando el valor de contador de clave adicional derivado de la información de contador de clave adicionalmente procesada, se puede lograr que pueda obtenerse por el UE una clave de seguridad adicional para protección de integridad y/o cifrado de datos, en particular, de datos a intercambiar entre el UE y un SN objetivo adicional.

20 En realizaciones del primer aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el equipo de usuario realice al menos lo siguiente:

- usar la clave de seguridad adicional para protección de integridad y/o

25 cifrado de datos intercambiados entre el equipo de usuario y un nodo

secundario objetivo adicional, que es diferente del segundo nodo secundario objetivo.

De esta manera, puede conseguirse que se realice un intercambio seguro de datos entre el UE y el SN objetivo adicional, en particular, un intercambio
5 seguro de datos de acuerdo con la arquitectura de seguridad de la norma 5G. Con respecto al nodo secundario objetivo adicional, únicamente se requiere que el nodo secundario objetivo adicional sea diferente del segundo nodo secundario objetivo, en particular, en un caso de ejemplo en el que el equipo de usuario realiza un CPAC o CHO desde el SCG asociado con el segundo nodo secundario
10 objetivo hacia el SCG asociado con el nodo secundario objetivo adicional. Sin embargo, el nodo secundario objetivo adicional puede ser idéntico al primer nodo secundario objetivo, por ejemplo, en particular, en un caso en el que el equipo de usuario realiza en primer lugar un CPAC o CHO desde el SCG asociado con el primer nodo secundario objetivo hacia el SCG asociado con el segundo nodo
15 secundario objetivo, y posteriormente realiza un CPAC o CHO desde el SCG asociado con el segundo nodo secundario objetivo de vuelta hacia el SCG asociado con el primer (o adicional) nodo secundario objetivo.

En realizaciones del primer aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al
20 menos un procesador, hacen que el equipo de usuario realice al menos lo siguiente:

- procesar adicionalmente la información de contador de clave de tal manera que el equipo de usuario está habilitado para derivar, a partir de la información de contador de clave adicionalmente procesada, al menos
25 un valor de contador de clave adicional, que es diferente del primer valor

de contador de clave, diferente del segundo valor de contador de clave y diferente de cualquier otro valor de contador de clave derivado previamente de la información de contador de clave no procesada, procesada o adicionalmente procesada.

- 5 Como se usa en el presente documento, procesar adicionalmente la información de contador de clave puede entenderse de tal manera que la información de contador de clave se modifica adicionalmente por el equipo de usuario de cualquier manera concebible. Por ejemplo, procesar adicionalmente la información de contador de clave puede comprender modificar adicionalmente
- 10 la secuencia de valores de contador de clave definidos por la información de contador de clave. Por ejemplo, procesar adicionalmente la información de contador de clave puede comprender evitar que un valor de contador de clave adicional particular se reutilice para la generación de claves de seguridad distintas de la clave de seguridad adicional particular. Al procesar adicionalmente
- 15 la información de contador de clave, se puede lograr que el UE pueda derivar, a partir de la información de contador de clave adicionalmente procesada, al menos un valor de contador de clave adicional y usar el al menos un valor de contador de clave adicional para generar al menos una clave de seguridad adicional para el intercambio de datos con al menos un SN objetivo adicional.
- 20 Por lo tanto, el UE puede realizar de manera autónoma actualización de clave de seguridad para un CPAC o CHO futuro hacia el SCG asociado con el al menos un SN objetivo adicional sin que el MN tenga que transmitir nueva información de configuración para este CPAC o CHO al UE. De esta manera, también se puede lograr que se reduzca la sobrecarga de señalización de RRC y se habilite
- 25 en mayor medida la movilidad rápida del UE a través de diferentes SCG.

Al realizar iterativamente las acciones de generación de una clave de seguridad adicional, usar la clave de seguridad adicional para protección de integridad y/o cifrado, y procesar adicionalmente la información de contador de clave, puede habilitarse que se realice por el UE un número teóricamente infinito de CPAC o CHO y, por lo tanto, un número teóricamente infinito de eventos de movilidad autónomos. Por lo tanto, también se puede lograr que la sobrecarga de señalización de RRC se reduzca significativamente y se habilite en mayor medida significativamente la movilidad rápida del UE a través de diferentes SCG. Sin embargo, en ciertas situaciones, también puede ser deseable limitar el número máximo de posibles CPAC o CHO y, por lo tanto, el número máximo de eventos de movilidad autónoma, que se puede lograr, por ejemplo, definiendo una lista de valores de contador de clave que tienen un número finito de elementos de lista, o definiendo un número máximo permitido de adiciones de un valor de paso predefinido a un valor de contador de clave recibido desde el nodo maestro.

En realizaciones de ejemplo del primer aspecto de ejemplo, la información de configuración puede comprender además información indicativa de al menos una célula secundaria objetivo para la que no se requiere generar una clave de seguridad. Como se usa en el presente documento, una célula puede cubrir, por ejemplo, al menos una parte de un área geográfica atendida por una red de acceso de radio, en particular, de manera que el servicio de radio se proporcione al menos para la parte del área geográfica. Por ejemplo, una célula puede estar asociada con (por ejemplo, atendida por) al menos un nodo de radio. Atender a una célula puede entenderse, por ejemplo, como proporcionar servicio de radio dentro de la célula. Por ejemplo, un nodo de red puede estar asociado con (por

ejemplo, atender) al menos una célula. Por ejemplo, al menos dos células pueden formar un grupo de células, en particular un SCG. Mediante la información de configuración que comprende información indicativa de al menos una célula secundaria objetivo para la que no se requiere generar una clave de seguridad, se puede lograr que se eviten las derivaciones innecesarias de valores de contador de clave a partir de la información de contador de clave, generaciones innecesarias de claves de seguridad y/o procesamientos innecesarios de la información de contador de clave, en particular, si el equipo de usuario se mueve o cambia entre células dentro del mismo SCG. Tales movimientos o cambios entre células dentro del mismo SCG pueden denominarse, por ejemplo, como activación selectiva intra-SN. Pueden realizarse por el UE sin requerir una clave de seguridad actualizada, por ejemplo, ya que la célula secundaria objetivo todavía está asociada al mismo SN.

De acuerdo con el primer aspecto de ejemplo, se divulga también un método respectivo. El método de acuerdo con el primer aspecto de ejemplo puede realizarse por un equipo de usuario. El equipo de usuario se puede configurar para soportar operación de conectividad dual hacia un nodo maestro y un nodo secundario de una red de acceso de radio. El método puede comprender al menos lo siguiente:

- establecer una conexión hacia el nodo maestro;
- recibir información de configuración desde el nodo maestro, en donde la información de configuración comprende información de contador de clave que define una secuencia de al menos dos valores de contador de clave diferentes para generar al menos dos claves de seguridad diferentes para al menos dos nodos secundarios objetivo diferentes.

Dentro del primer aspecto de ejemplo, la divulgación de cualquier instrucción que, cuando se ejecuta por el al menos un procesador del equipo de usuario, hace que el equipo de usuario realice una acción también se considerará como una divulgación de una respectiva acción del método.

5 De acuerdo con el primer aspecto de ejemplo, se divulga también un aparato respectivo. El aparato de acuerdo con el primer aspecto de ejemplo puede comprender medios para realizar un método de acuerdo con el primer aspecto de ejemplo. Dentro del primer aspecto de ejemplo, la divulgación de cualquier acción de método también se considerará como una divulgación de
10 medios para realizar la respectiva acción de método. De la misma manera, la divulgación de cualquier medio para realizar una acción de método se considerará también como una divulgación de la acción del método mismo. El aparato de acuerdo con el primer aspecto de ejemplo puede ser un equipo de usuario. El equipo de usuario se puede configurar para soportar operación de
15 conectividad dual hacia un nodo maestro y un nodo secundario de una red de acceso de radio.

Los medios o funcionalidad del equipo de usuario de acuerdo con el primer aspecto de ejemplo pueden implementarse en hardware y/o software. Pueden comprender uno o múltiples módulos o unidades que proporcionan la
20 funcionalidad respectiva. Pueden comprender, por ejemplo, al menos un procesador para ejecutar código de programa informático para realizar las funciones requeridas, al menos una memoria que almacena el código de programa, o ambos. Como alternativa, estos podrían comprender, por ejemplo, circuitería que se diseña para implementar las funciones requeridas, por ejemplo,
25 implementadas en un conjunto de chips o un chip, como un circuito integrado.

En general, los medios pueden comprender, por ejemplo, uno o más medios de procesamiento o procesadores.

De acuerdo con el primer aspecto de ejemplo, también se divulga un respectivo medio legible por ordenador no transitorio. El medio legible por
5 ordenador no transitorio de acuerdo con el primer aspecto de ejemplo puede comprender instrucciones de programa que, cuando son ejecutadas por un equipo de usuario, hacen que el equipo de usuario realice al menos un método de acuerdo con el primer aspecto de ejemplo. El equipo de usuario se puede configurar para soportar operación de conectividad dual hacia un nodo maestro
10 y un nodo secundario de una red de acceso de radio.

El medio legible por ordenador no transitorio de acuerdo con el primer aspecto de ejemplo podría ser, por ejemplo, un disco o una memoria o similar. Las instrucciones de programa podrían almacenarse en el medio legible por ordenador en forma de instrucciones que codifican el medio legible por
15 ordenador. El medio legible por ordenador puede tener por objeto tomar parte en la operación de un dispositivo, como una memoria interna o externa, por ejemplo, una memoria de solo lectura (ROM) o un disco duro de un ordenador, o puede tener por objeto la distribución del programa, como un disco óptico.

De acuerdo con el primer aspecto de ejemplo, también se divulga un respectivo programa informático. El programa informático de acuerdo con el
20 primer aspecto de ejemplo puede comprender instrucciones que, cuando son ejecutadas por un equipo de usuario, hacen que el equipo de usuario realice al menos un método de acuerdo con el primer aspecto de ejemplo. El equipo de usuario se puede configurar para soportar operación de conectividad dual hacia
25 un nodo maestro y un nodo secundario de una red de acceso de radio.

El programa informático de acuerdo con el primer aspecto de ejemplo puede almacenarse en un medio de almacenamiento legible por ordenador, en particular un medio de almacenamiento legible por ordenador tangible y/o no transitorio. En particular, el programa informático de acuerdo con el primer
5 aspecto de ejemplo puede almacenarse en un medio legible por ordenador no transitorio de acuerdo con el primer aspecto de ejemplo.

De acuerdo con un segundo aspecto de ejemplo, se divulga un nodo maestro de una red de acceso de radio. El nodo maestro se puede configurar para soportar operación de conectividad dual hacia un nodo secundario de la red
10 de acceso de radio y un equipo de usuario. El nodo maestro puede comprender al menos un procesador y al menos una memoria. La al menos una memoria puede almacenar instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el nodo maestro realice al menos lo siguiente:

- establecer una conexión hacia el equipo de usuario;
- 15 - transmitir información de configuración al equipo de usuario, en donde la información de configuración comprende información de contador de clave que define una secuencia de al menos dos valores de contador de clave diferentes para generar al menos dos claves de seguridad diferentes para al menos dos nodos secundarios objetivo diferentes.

20 Estableciendo el nodo maestro una conexión hacia el equipo de usuario, puede lograrse que se habilite el intercambio de datos entre el UE y el MN. Por ejemplo, la conexión puede ser una conexión segura, en particular una conexión de señalización de RRC segura.

Al transmitir información de configuración al equipo de usuario, en donde
25 la información de configuración comprende información de contador de clave que

define una secuencia de al menos dos valores de contador de clave diferentes para generar al menos dos claves de seguridad diferentes para al menos dos nodos secundarios objetivo diferentes, las realizaciones de ejemplo del segundo aspecto de ejemplo pueden ser ventajosas porque el equipo de usuario puede

5 habilitarse para realizar una actualización de clave de seguridad autónoma y, por lo tanto, pueden omitirse los nuevos mensajes de configuración para CPAC o CHO en ciertas situaciones, como ya se ha explicado en el contexto del primer aspecto de ejemplo. De esta manera, también se puede lograr que se reduzca la sobrecarga de señalización de RRC y se habilite en mayor medida la movilidad

10 rápida del UE a través de diferentes SCG.

En realizaciones de ejemplo del segundo aspecto de ejemplo, la información de contador de clave transmitida al equipo de usuario puede definir una lista de al menos dos valores de contador de clave diferentes. De esta manera, puede conseguirse una definición particularmente sencilla de los al

15 menos dos valores de contador de clave diferentes mediante la información de contador de clave, de manera que, por ejemplo, no se requieren operaciones de cálculo complejas y se ahorran recursos de procesador respectivos.

En realizaciones de ejemplo del segundo aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son

20 ejecutadas por el al menos un procesador, hacen que el nodo maestro realice al menos lo siguiente:

- generar una lista de al menos dos claves de seguridad diferentes que corresponde a la lista de al menos dos valores de contador de clave diferentes definidos por la información de contador de clave transmitida al
- 25 equipo de usuario.

Como se usa en el presente documento, la lista de claves de seguridad correspondiente a la lista de valores de contador de clave puede entenderse de tal manera que al menos un elemento en la lista de claves de seguridad puede asociarse con un elemento respectivo en la lista de valores de contador de clave, y viceversa. En particular, cada elemento en la lista de claves de seguridad puede asociarse con un elemento respectivo en la lista de valores de contador de clave, y viceversa. Por ejemplo, la correspondencia puede ser tal que para cada número n entre 1 y N , donde N es el número total de elementos de lista, el n -ésimo elemento en la lista de claves de seguridad es una clave de seguridad que se ha generado, en particular por el nodo maestro, usando el n -ésimo elemento en la lista de valores de contador de clave. Viceversa, para cada número n entre 1 y N , donde N es el número total de elementos de lista, el n -ésimo elemento en la lista de valores de contador de clave se usa o se ha usado para generar el n -ésimo elemento en la lista de claves de seguridad. Sin embargo, el orden de los elementos correspondientes en ambas listas no tiene que ser necesariamente idéntico. Por ejemplo, el elemento en la posición n en una lista puede corresponder a un elemento en la posición $n+x$ en la otra lista, donde x es diferente de cero. Generando una lista de al menos dos claves de seguridad diferentes que corresponde a la lista de al menos dos valores de contador de clave diferentes definidos por la información de contador de clave transmitida al equipo de usuario, se puede lograr que se proporcione una correspondiente lista de claves de seguridad.

En realizaciones de ejemplo del segundo aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el nodo maestro realice al

menos lo siguiente:

- transmitir información de solicitud a al menos un nodo secundario objetivo, en donde la información de solicitud comprende la lista generada de claves de seguridad.

5 Como se usa en el presente documento, la información de solicitud puede entenderse como cualquier tipo de información relacionada con la operación de conectividad dual y/o la gestión de claves de seguridad con respecto a al menos un nodo secundario objetivo. Por ejemplo, la información de solicitud puede ser idéntica a o estar comprendida por una solicitud de adición o modificación de SN

10 hacia el al menos un nodo secundario objetivo. Por ejemplo, el al menos un nodo secundario objetivo puede comprender al menos un nodo secundario objetivo asociado con un SCG hacia el que ha de realizarse que se deba habilitar un CPAC o CHO. Por ejemplo, el al menos un nodo secundario objetivo también puede comprender un nodo secundario de origen asociado con un SCG de

15 servicio actual que califica o puede calificar, en un punto de tiempo futuro, para un CPAC o CHO posterior de vuelta al SCG asociado con el nodo secundario de origen. Al transmitir información de solicitud a al menos un nodo secundario objetivo, en donde la información de solicitud comprende la lista generada de claves de seguridad, se puede lograr que el al menos un SN objetivo esté

20 provisto de claves de seguridad que sean consistentes con las claves de seguridad generadas por el UE que usa los elementos en la lista de valores de contador de clave, de modo que el al menos un SN objetivo está habilitado para intercambiar datos de forma segura con el UE, en particular, después de que el UE realiza un CPAC o CHO hacia el SCG asociado con el al menos un SN

25 objetivo. Además, una ventaja particular de transmitir una lista de al menos dos

claves de seguridad diferentes al SN objetivo es que el SN objetivo está habilitado para seleccionar de manera autónoma una clave de seguridad de la lista cuando se realiza un CPAC o CHO hacia el SCG asociado con el SN objetivo, de modo que no se requiere una implicación adicional del MN, en particular, un procedimiento de modificación de SN por el MN. Además, se reduce el requisito de tiempo para preparar los SN objetivo para la ejecución de CPAC o CHO, de manera que se habilita en mayor medida una movilidad rápida del UE a través de diferentes SCG.

En realizaciones de ejemplo del segundo aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el nodo maestro realice al menos lo siguiente:

- recibir, desde un primer nodo secundario objetivo, información indicativa de un cambio de clave de seguridad.

Como se usa en el presente documento, un cambio de clave de seguridad puede entenderse como un evento en el que una clave de seguridad anterior, en particular una clave de seguridad anterior para protección de integridad y/o cifrado de datos intercambiados entre el equipo de usuario y un nodo secundario asociado con un SCG previamente de servicio, se intercambia por una clave de seguridad actual, en particular, una clave de seguridad actual para protección de integridad y/o cifrado de datos intercambiados entre el equipo de usuario y un nodo secundario asociado con un SCG de servicio actual. Como se usa en el presente documento, la información indicativa de un cambio de clave de seguridad puede entenderse como cualquier pieza de información que proporciona una indicación para un cambio de clave de seguridad de cualquier

manera concebible. Por ejemplo, la información indicativa de un cambio de clave de seguridad puede ser información enviada por el primer nodo secundario objetivo que indica que se ha realizado un CPAC o CHO hacia el SCG asociado con el primer nodo secundario objetivo. Al recibir, desde un primer nodo secundario objetivo, información indicativa de un cambio de clave de seguridad, el MN puede realizar un seguimiento de los cambios de clave de seguridad y, por lo tanto, también, por ejemplo, de los CPAC o CHO que se producen, y realizar acciones para lograr que se mantenga la gestión de claves de seguridad para el UE y los SN objetivo.

En realizaciones de ejemplo del segundo aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el nodo maestro realice al menos lo siguiente:

- transmitir, a al menos otro nodo secundario objetivo, una instrucción para quitar el primer elemento de lista de la lista de claves de seguridad, en donde el al menos otro nodo secundario objetivo es diferente del primer nodo secundario objetivo.

Como se usa en el presente documento, quitar el primer elemento de lista de la lista de claves de seguridad puede entenderse como cualquier acción realizada por el al menos otro nodo secundario objetivo que evita que el primer elemento de lista en la lista de claves de seguridad se use como una clave de seguridad para protección de integridad y/o cifrado. Por ejemplo, el primer elemento de lista se puede quitar de la lista de claves de seguridad en el sentido de que el primer elemento de lista se elimina completamente, de manera que el número de elementos de lista se reduce en uno. Por ejemplo, el primer elemento

de lista se puede quitar de la lista de claves de seguridad en el sentido de que el primer elemento de lista se modifica para convertirse en un elemento de lista vacío. Por ejemplo, el primer elemento de lista se puede quitar de la lista de claves de seguridad en el sentido de que el primer elemento de lista se marca
5 como desactivado o no utilizable. En el contexto anterior, el al menos otro nodo secundario objetivo puede comprender, por ejemplo, al menos otro nodo secundario objetivo asociado con un SCG hacia el que puede realizarse un CPAC o CHO en un punto de tiempo futuro. Al transmitir, a al menos otro nodo secundario objetivo, una instrucción para quitar el primer elemento de lista de la
10 lista de claves de seguridad, en donde el al menos otro nodo secundario objetivo es diferente del primer nodo secundario objetivo, se puede lograr que el al menos otro SN objetivo modifique su lista de claves de seguridad de tal manera que la lista de claves de seguridad permanece consistente con la lista de valores de contador de clave procesados por el UE.

15 En realizaciones de ejemplo del segundo aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el nodo maestro realice al menos lo siguiente:

- recibir, desde un segundo nodo secundario objetivo, información
20 indicativa de un cambio de clave de seguridad, en donde el segundo nodo secundario objetivo es diferente del primer nodo secundario objetivo.

Por ejemplo, la información indicativa de un cambio de clave de seguridad puede ser información enviada por el segundo nodo secundario objetivo que indica que se ha realizado un CPAC o CHO hacia el SCG asociado con el
25 segundo nodo secundario objetivo. Al recibir, desde un segundo nodo secundario

objetivo, información indicativa de un cambio de clave de seguridad, en donde el segundo nodo secundario objetivo es diferente del primer nodo secundario objetivo, el MN puede realizar un seguimiento de los cambios de clave de seguridad y, por lo tanto, también, por ejemplo, de los CPAC o CHO que se producen, y realizar acciones para lograr que se mantenga la gestión de claves de seguridad para el UE y los SN objetivo.

En realizaciones de ejemplo del segundo aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el nodo maestro realice al menos lo siguiente:

- transmitir, a al menos un nodo secundario objetivo adicional, una instrucción para quitar el actualmente primer elemento de lista de la lista de claves de seguridad, en donde el al menos un nodo secundario objetivo adicional es diferente del segundo nodo secundario objetivo.

Como se usa en el presente documento, el actualmente primer elemento de lista ha de entenderse como el primer elemento de lista activo o utilizable en la lista de claves de seguridad en el punto de tiempo actual dado. Por ejemplo, el primer elemento de lista activo o utilizable en la lista de claves de seguridad no coincide necesariamente con el primer elemento en la lista, en particular, en un caso en el que el primer elemento en la lista es un elemento de lista vacío o un elemento de lista marcado como desactivado o no utilizable. Como se usa en el presente documento, quitar el actualmente primer elemento de lista de la lista de claves de seguridad puede entenderse como cualquier acción realizada por el al menos otro nodo secundario objetivo que evita que el actualmente primer elemento de lista en la lista de claves de seguridad se use como una clave de

seguridad para protección de integridad y/o cifrado. Por ejemplo, el actualmente primer elemento de lista se puede quitar de la lista de claves de seguridad en el sentido de que el actualmente primer elemento de lista se elimina completamente, de manera que el número de elementos de lista se reduce en uno. Por ejemplo, el actualmente primer elemento de lista se puede quitar de la lista de claves de seguridad en el sentido de que el actualmente primer elemento de lista se modifica para convertirse en un elemento de lista vacío. Por ejemplo, el actualmente primer elemento de lista se puede quitar de la lista de claves de seguridad en el sentido de que el actualmente primer elemento de lista se marca como desactivado o no utilizable. En el contexto anterior, el al menos un nodo secundario objetivo adicional puede comprender, por ejemplo, al menos un nodo secundario objetivo adicional asociado con un SCG hacia el que puede realizarse un CPAC o CHO en un punto de tiempo futuro. Por ejemplo, el al menos un nodo secundario objetivo adicional también puede comprender el primer nodo secundario objetivo, en particular en un caso en el que el SCG asociado con el primer nodo secundario objetivo califica o puede calificar, en un punto de tiempo futuro, para un CPAC o CHO de vuelta al SCG asociado con el primer nodo secundario objetivo. Al transmitir, a al menos un nodo secundario objetivo adicional, una instrucción para quitar el actualmente primer elemento de lista de la lista de claves de seguridad, en donde el al menos un nodo secundario adicional objetivo es diferente del segundo nodo secundario objetivo, se puede lograr que el al menos un SN objetivo adicional modifique su lista de claves de seguridad de tal manera que la lista de claves de seguridad permanece consistente con la lista de valores de contador de clave procesados por el UE.

En realizaciones de ejemplo del segundo aspecto de ejemplo, la al menos

una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el nodo maestro realice al menos lo siguiente:

- recibir, desde el equipo de usuario, información indicativa de un fallo de
5 conexión.

Por ejemplo, el fallo de conexión puede ser un fallo de una conexión entre el equipo de usuario y un nodo secundario objetivo. Por ejemplo, el fallo de conexión puede ser un fallo de un procedimiento de acceso aleatorio desde el equipo de usuario hacia un nodo secundario objetivo, en particular, un
10 procedimiento de acceso aleatorio a través de RACH. Al recibir, desde el equipo de usuario, información indicativa de un fallo de conexión, puede conseguirse que el MN sea informado acerca del fallo de conexión, de tal manera que el MN pueda tomar medidas respectivas, si es necesario.

En realizaciones de ejemplo del segundo aspecto de ejemplo, la al menos
15 una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el nodo maestro realice al menos lo siguiente:

- transmitir, a al menos un nodo secundario objetivo, una instrucción para
20 quitar el actualmente primer elemento de lista de la lista de claves de seguridad.

Por ejemplo, transmitir, a al menos un nodo secundario objetivo, una instrucción para quitar el actualmente primer elemento de lista de la lista de claves de seguridad puede realizarse en respuesta a la recepción, desde el equipo de usuario, de información indicativa de un fallo de conexión. En este
25 contexto, el al menos un nodo secundario objetivo puede comprender, por

ejemplo, un nodo secundario objetivo asociado con un SCG hacia el que no ha sido posible un CPAC o CHO debido a un fallo de conexión, en particular, un fallo de una conexión entre el equipo de usuario y el nodo secundario objetivo. Por ejemplo, el al menos un nodo secundario objetivo también puede comprender al

5 menos un nodo secundario objetivo asociado con un SCG hacia el que puede realizarse un CPAC o CHO en un punto de tiempo futuro. Por ejemplo, el al menos un nodo secundario objetivo también puede comprender un nodo secundario de origen asociado con un SCG de servicio actual que califica o puede calificar, en un punto de tiempo futuro, para un CPAC o CHO posterior de

10 vuelta al SCG asociado con el nodo secundario de origen. Al transmitir, a al menos un nodo secundario objetivo, una instrucción para quitar el actualmente primer elemento de lista de la lista de claves de seguridad, se puede lograr que la lista de claves de seguridad del al menos un SN objetivo permanezca consistente con la lista de valores de contador de clave procesados por el UE,

15 en particular, en un caso en el que se ha producido un fallo de conexión y el UE ya ha procesado la lista de valores de contador de clave de tal manera que un primer valor de contador de clave anteriormente se ha quitado de manera irrecuperable.

En realizaciones de ejemplo del segundo aspecto de ejemplo, la al menos

20 una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el nodo maestro realice al menos lo siguiente:

- transmitir al menos un elemento de lista adicional para la lista de valores de contador de clave al equipo de usuario.
- 25 En particular, transmitir al menos un elemento de lista adicional para la

lista de valores de contador de clave al equipo de usuario puede realizarse después de determinar si el número de elementos de lista de la lista de valores de contador de clave no alcanza un umbral predefinido y en respuesta a la determinación que el número de elementos de lista de la lista de valores de
 5 contador de clave no alcanza un umbral predefinido. Por ejemplo, el umbral predefinido puede ser igual a uno. Al transmitir al menos un elemento de lista adicional para la lista de valores de contador de clave al equipo de usuario, se puede lograr que se mantenga la capacidad del UE para realizar CPAC o CHO, como ya se ha explicado en el contexto del primer aspecto de ejemplo.

10 En realizaciones de ejemplo del segundo aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el nodo maestro realice al menos lo siguiente:

- transmitir al menos un elemento de lista adicional para la lista de claves
 15 de seguridad a al menos un nodo secundario objetivo.

Por ejemplo, el al menos un elemento de lista adicional para la lista de claves de seguridad transmitida al menos a un nodo secundario objetivo puede corresponder con el al menos un elemento de lista adicional para la lista de valores de contador de clave transmitidos al equipo de usuario. Por ejemplo, la
 20 correspondencia puede ser tal que el al menos un elemento de lista adicional para la lista de claves de seguridad es una clave de seguridad que se ha generado, en particular por el nodo maestro, usando el al menos un elemento de lista adicional para la lista de valores de contador de clave. Al transmitir al menos un elemento de lista adicional para la lista de claves de seguridad a al menos un
 25 nodo secundario objetivo, se puede lograr que la lista de claves de seguridad del

al menos un SN objetivo permanezca consistente con la lista de valores de contador de clave procesados por el UE. Además, puede evitarse que el número de elementos de lista de la lista de claves de seguridad alcance un valor excesivamente bajo, en particular cero. Por lo tanto, también se puede lograr que
5 se mantenga la capacidad del UE para realizar un CPAC o un CHO hacia el SCG asociado con el al menos un SN objetivo.

En realizaciones de ejemplo del segundo aspecto de ejemplo, la información de contador de clave transmitida al equipo de usuario puede comprender un valor de contador de clave y una instrucción para mantener el
10 valor de contador de clave. De esta manera, puede conseguirse una derivación particularmente sencilla del primer valor de contador de clave a partir de la información de contador de clave, de manera que, por ejemplo, no se requieren operaciones de cálculo complejas y se ahorran recursos de procesador respectivos.

15 En realizaciones de ejemplo del segundo aspecto de ejemplo, el nodo maestro puede comprender un nodo de gNB-CU-CP. El nodo de gNB-CU-CP puede comprender al menos un procesador y al menos una memoria, en donde las instrucciones pueden almacenarse en la al menos una memoria del nodo de gNB-CU-CP para ser ejecutadas por el al menos un procesador del nodo de gNB-
20 CU-CP. Como se usa en el presente documento, un nodo de gNB-CU-CP puede entenderse como un nodo lógico que aloja el RRC y la parte del plano de control del protocolo de convergencia de datos de paquetes (PDCP) de la unidad central de gNB (gNB-CU) para un en-gNB o un gNB.

En realizaciones de ejemplo del segundo aspecto de ejemplo, la
25 información de configuración puede comprender además información indicativa

de al menos una célula secundaria objetivo para la que no se requiere generar una clave de seguridad. De este modo, se puede lograr que se eviten derivaciones innecesarias de valores de contador de clave a partir de la información de contador de clave, generaciones innecesarias de claves de seguridad y/o procesamientos innecesarios de la información de contador de clave, como ya se ha explicado en el contexto del primer aspecto de ejemplo.

De acuerdo con el segundo aspecto de ejemplo, se divulga también un método respectivo. El método de acuerdo con el segundo aspecto de ejemplo puede realizarse por un nodo maestro de una red de acceso de radio. El nodo maestro se puede configurar para soportar operación de conectividad dual hacia un nodo secundario de la red de acceso de radio y un equipo de usuario. El método puede comprender al menos lo siguiente:

- establecer una conexión hacia el equipo de usuario;
- transmitir información de configuración al equipo de usuario, en donde la información de configuración comprende información de contador de clave que define una secuencia de al menos dos valores de contador de clave diferentes para generar al menos dos claves de seguridad diferentes para al menos dos nodos secundarios objetivo diferentes.

Dentro del segundo aspecto de ejemplo, la divulgación de cualquier instrucción que, cuando se ejecuta por el al menos un procesador del nodo maestro, hace que el nodo maestro realice una acción también se considerará como una divulgación de una acción respectiva del método.

De acuerdo con el segundo aspecto de ejemplo, se divulga también un aparato respectivo. El aparato de acuerdo con el segundo aspecto de ejemplo puede comprender medios para realizar un método de acuerdo con el segundo

aspecto de ejemplo. Dentro del segundo aspecto de ejemplo, la divulgación de cualquier acción de método también se considerará como una divulgación de medios para realizar la respectiva acción de método. De la misma manera, la divulgación de cualquier medio para realizar una acción de método se considerará también como una divulgación de la acción del método mismo. El aparato de acuerdo con el segundo aspecto de ejemplo puede ser un nodo maestro. El nodo maestro se puede configurar para soportar operación de conectividad dual hacia un nodo secundario de la red de acceso de radio y un equipo de usuario.

Los medios o funcionalidad del nodo maestro de acuerdo con el segundo aspecto de ejemplo pueden implementarse en hardware y/o software. Pueden comprender uno o múltiples módulos o unidades que proporcionan la funcionalidad respectiva. Pueden comprender, por ejemplo, al menos un procesador para ejecutar código de programa informático para realizar las funciones requeridas, al menos una memoria que almacena el código de programa, o ambos. Como alternativa, estos podrían comprender, por ejemplo, circuitería que se diseña para implementar las funciones requeridas, por ejemplo, implementadas en un conjunto de chips o un chip, como un circuito integrado. En general, los medios pueden comprender, por ejemplo, uno o más medios de procesamiento o procesadores.

De acuerdo con el segundo aspecto de ejemplo, también se divulga un respectivo medio legible por ordenador no transitorio. El medio legible por ordenador no transitorio de acuerdo con el segundo aspecto de ejemplo puede comprender instrucciones de programa que, cuando son ejecutadas por un nodo maestro, hacen que el nodo maestro realice al menos un método de acuerdo con

el segundo aspecto de ejemplo. El nodo maestro se puede configurar para soportar operación de conectividad dual hacia un nodo secundario de la red de acceso de radio y un equipo de usuario.

El medio legible por ordenador no transitorio de acuerdo con el segundo
5 aspecto de ejemplo podría ser, por ejemplo, un disco o una memoria o similar. Las instrucciones de programa podrían almacenarse en el medio legible por ordenador en forma de instrucciones que codifican el medio legible por ordenador. El medio legible por ordenador puede tener por objeto tomar parte en la operación de un dispositivo, como una memoria interna o externa, por ejemplo,
10 una memoria de solo lectura (ROM) o un disco duro de un ordenador, o puede tener por objeto la distribución del programa, como un disco óptico.

De acuerdo con el segundo aspecto de ejemplo, también se divulga un respectivo programa informático. El programa informático de acuerdo con el segundo aspecto de ejemplo puede comprender instrucciones que, cuando son
15 ejecutadas por un nodo maestro, hacen que el nodo maestro realice al menos un método de acuerdo con el segundo aspecto de ejemplo. El nodo maestro se puede configurar para soportar operación de conectividad dual hacia un nodo secundario de la red de acceso de radio y un equipo de usuario.

El programa informático de acuerdo con el segundo aspecto de ejemplo
20 puede almacenarse en un medio de almacenamiento legible por ordenador, en particular un medio de almacenamiento legible por ordenador tangible y/o no transitorio. En particular, el programa informático de acuerdo con el segundo aspecto de ejemplo puede almacenarse en un medio legible por ordenador no transitorio de acuerdo con el segundo aspecto de ejemplo.

25 De acuerdo con un tercer aspecto de ejemplo, se divulga un nodo

secundario de una red de acceso de radio. El nodo secundario se puede configurar para soportar operación de conectividad dual hacia un nodo maestro de la red de acceso de radio y un equipo de usuario. El nodo secundario puede comprender al menos un procesador y al menos una memoria. La al menos una memoria puede almacenar instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el nodo secundario realice al menos lo siguiente:

- recibir información de solicitud desde el nodo maestro, en donde la información de solicitud comprende una lista de al menos dos claves de seguridad diferentes.

De esta manera, se puede lograr que el nodo secundario esté habilitado para intercambiar datos de forma segura con el equipo de usuario, en particular, después de que el equipo de usuario realice un CPAC o CHO hacia el SCG asociado con el nodo secundario, como ya se ha explicado en el contexto del segundo aspecto de ejemplo. Además, una ventaja particular de que el SN reciba una lista de al menos dos claves de seguridad diferentes es que el SN está habilitado para seleccionar de forma autónoma una clave de seguridad de la lista cuando se realiza un CPAC o CHO hacia el SCG asociado con el SN, de modo que no se requiere una implicación adicional del MN, en particular, un procedimiento de modificación de SN por el MN. Además, se reduce el requisito de tiempo para preparar los SN objetivo para la ejecución de CPAC o CHO, de manera que se habilita en mayor medida una movilidad rápida del UE a través de diferentes SCG.

En realizaciones de ejemplo del tercer aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son

ejecutadas por el al menos un procesador, hacen que el nodo secundario realice al menos lo siguiente:

- determinar si el equipo de usuario establece o intenta establecer una conexión hacia el nodo secundario;
- 5 - en respuesta a la determinación de que el equipo de usuario establece o intenta establecer una conexión hacia el nodo secundario, usar el actualmente primer elemento de lista en la lista de claves de seguridad para protección de integridad y/o cifrado de datos intercambiados entre el nodo secundario y el equipo de usuario.

10 De esta manera, puede conseguirse que se realice un intercambio seguro de datos entre el UE y el SN, en particular, un intercambio seguro de datos de acuerdo con la arquitectura de seguridad de la norma 5G.

En realizaciones de ejemplo del tercer aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son
15 ejecutadas por el al menos un procesador, hacen que el nodo secundario realice al menos lo siguiente:

- transmitir, al nodo maestro, información indicativa de un cambio de clave de seguridad.

De este modo, el MN está habilitado para realizar un seguimiento de los
20 cambios de clave de seguridad y, por lo tanto, también, por ejemplo, de los CPAC o CHO que se producen, y realizar acciones para lograr que se mantenga la gestión de claves de seguridad para el UE y los SN, como ya se ha explicado en el contexto del segundo aspecto de ejemplo.

En realizaciones de ejemplo del tercer aspecto de ejemplo, la al menos
25 una memoria puede almacenar además instrucciones que, cuando son

ejecutadas por el al menos un procesador, hacen que el nodo secundario realice al menos lo siguiente:

- quitar el actualmente primer elemento de lista de la lista de claves de seguridad.

5 Quitar el actualmente primer elemento de lista de la lista de claves de seguridad puede realizarse, por ejemplo, en respuesta al uso del actualmente primer elemento de lista en la lista de claves de seguridad para protección de integridad y/o cifrado de datos intercambiados entre el nodo secundario y el equipo de usuario, o en respuesta a la transmisión, al nodo maestro, de
10 información indicativa de un cambio de clave de seguridad. Retirando el actualmente primer elemento de lista de la lista de claves de seguridad, puede lograrse que la lista de claves de seguridad del SN permanezca consistente con la lista de valores de contador de clave procesados por el UE.

En realizaciones de ejemplo del tercer aspecto de ejemplo, la al menos
15 una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el nodo secundario realice al menos lo siguiente:

- recibir, desde el nodo maestro, una instrucción para quitar el actualmente primer elemento de lista de la lista de claves de seguridad.

20 De esta manera, se puede lograr que el nodo secundario modifique su lista de claves de seguridad de manera que la lista de claves de seguridad del SN permanezca consistente con la lista de valores de contador de clave procesados por el UE, como ya se ha explicado en el contexto del segundo aspecto de ejemplo.

25 En realizaciones de ejemplo del tercer aspecto de ejemplo, la al menos

una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el nodo secundario realice al menos lo siguiente:

- quitar el actualmente primer elemento de lista de la lista de claves de seguridad.

Quitar el actual primer elemento de lista de la lista de claves de seguridad puede realizarse, por ejemplo, en respuesta a la recepción, desde el nodo maestro, de una instrucción para quitar el actualmente primer elemento de lista de la lista de claves de seguridad. Retirando el actualmente primer elemento de lista de la lista de claves de seguridad, puede lograrse que la lista de claves de seguridad del SN permanezca consistente con la lista de valores de contador de clave procesados por el UE.

En realizaciones de ejemplo del tercer aspecto de ejemplo, la al menos una memoria puede almacenar además instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el nodo secundario realice al menos lo siguiente:

- recibir al menos un elemento de lista adicional para la lista de claves de seguridad desde el nodo maestro.

Por ejemplo, el al menos un elemento de lista adicional para la lista de claves de seguridad recibidas por el nodo secundario desde el nodo maestro puede corresponder con el al menos un elemento de lista adicional para la lista de valores de contador de clave transmitidos desde el nodo maestro al equipo de usuario. Por ejemplo, la correspondencia puede ser tal que el al menos un elemento de lista adicional para la lista de claves de seguridad es una clave de seguridad que se ha generado, en particular por el nodo maestro, usando el al

menos un elemento de lista adicional para la lista de valores de contador de clave. Al recibir al menos un elemento de lista adicional para la lista de claves de seguridad desde el nodo maestro, se puede lograr igualmente que la lista de claves de seguridad del SN permanezca consistente con la lista de valores de contador de clave procesados por el UE, en particular, en un caso en el que el MN transmite al UE al menos un elemento de lista adicional para la lista de valores de contador de clave. Además, puede evitarse que el número de elementos de lista de la lista de claves de seguridad alcance un valor excesivamente bajo, en particular cero. Por lo tanto, también se puede lograr que se mantenga la capacidad del UE para realizar un CPAC o un CHO hacia el SCG asociado con el SN.

De acuerdo con el tercer aspecto de ejemplo, se divulga también un método respectivo. El método de acuerdo con el tercer aspecto de ejemplo puede realizarse por un nodo secundario de una red de acceso de radio. El nodo secundario se puede configurar para soportar operación de conectividad dual hacia un nodo maestro de la red de acceso de radio y un equipo de usuario. El método puede comprender al menos lo siguiente:

- recibir información de solicitud desde el nodo maestro, en donde la información de solicitud comprende una lista de al menos dos claves de seguridad diferentes.

Dentro del tercer aspecto de ejemplo, la divulgación de cualquier instrucción que, cuando se ejecuta por el al menos un procesador del nodo secundario, hace que el nodo secundario realice una acción también se considerará como una divulgación de una acción respectiva del método.

De acuerdo con el tercer aspecto de ejemplo, se divulga también un

aparato respectivo. El aparato de acuerdo con el tercer aspecto de ejemplo puede comprender medios para realizar un método de acuerdo con el tercer aspecto de ejemplo. Dentro del tercer aspecto de ejemplo, la divulgación de cualquier acción de método también se considerará como una divulgación de
5 medios para realizar la respectiva acción de método. De la misma manera, la divulgación de cualquier medio para realizar una acción de método se considerará también como una divulgación de la acción del método mismo. El aparato de acuerdo con el tercer aspecto de ejemplo puede ser un nodo secundario. El nodo secundario se puede configurar para soportar operación de
10 conectividad dual hacia un nodo maestro de la red de acceso de radio y un equipo de usuario.

Los medios o funcionalidad del nodo secundario de acuerdo con el tercer aspecto de ejemplo pueden implementarse en hardware y/o software. Pueden comprender uno o múltiples módulos o unidades que proporcionan la
15 funcionalidad respectiva. Pueden comprender, por ejemplo, al menos un procesador para ejecutar código de programa informático para realizar las funciones requeridas, al menos una memoria que almacena el código de programa, o ambos. Como alternativa, estos podrían comprender, por ejemplo, circuitería que se diseña para implementar las funciones requeridas, por ejemplo,
20 implementadas en un conjunto de chips o un chip, como un circuito integrado. En general, los medios pueden comprender, por ejemplo, uno o más medios de procesamiento o procesadores.

De acuerdo con el tercer aspecto de ejemplo, también se divulga un respectivo medio legible por ordenador no transitorio. El medio legible por
25 ordenador no transitorio de acuerdo con el tercer aspecto de ejemplo puede

comprender instrucciones de programa que, cuando son ejecutadas por un nodo secundario, hacen que el nodo secundario realice al menos un método de acuerdo con el tercer aspecto de ejemplo. El nodo secundario se puede configurar para soportar operación de conectividad dual hacia un nodo maestro de la red de acceso de radio y un equipo de usuario.

El medio legible por ordenador no transitorio de acuerdo con el tercer aspecto de ejemplo podría ser, por ejemplo, un disco o una memoria o similar. Las instrucciones de programa podrían almacenarse en el medio legible por ordenador en forma de instrucciones que codifican el medio legible por ordenador. El medio legible por ordenador puede tener por objeto tomar parte en la operación de un dispositivo, como una memoria interna o externa, por ejemplo, una memoria de solo lectura (ROM) o un disco duro de un ordenador, o puede tener por objeto la distribución del programa, como un disco óptico.

De acuerdo con el tercer aspecto de ejemplo, también se divulga un respectivo programa informático. El programa informático de acuerdo con el tercer aspecto de ejemplo puede comprender instrucciones que, cuando son ejecutadas por un nodo secundario, hacen que el nodo secundario realice al menos un método de acuerdo con el tercer aspecto de ejemplo. El nodo secundario se puede configurar para soportar operación de conectividad dual hacia un nodo maestro de la red de acceso de radio y un equipo de usuario.

El programa informático de acuerdo con el tercer aspecto de ejemplo puede almacenarse en un medio de almacenamiento legible por ordenador, en particular un medio de almacenamiento legible por ordenador tangible y/o no transitorio. En particular, el programa informático de acuerdo con el tercer aspecto de ejemplo puede almacenarse en un medio legible por ordenador no

transitorio de acuerdo con el tercer aspecto de ejemplo.

Ha de entenderse que la presentación de las realizaciones divulgadas en el presente documento es simplemente a modo de ejemplos y no limitante.

Otras características de la presente divulgación resultarán evidentes a partir de la siguiente descripción detallada considerada junto con los dibujos adjuntos. Ha de entenderse, sin embargo, que los dibujos se diseñan únicamente para fines de ilustración y no como una definición de los límites de la presente divulgación, para los que debería hacerse referencia a las reivindicaciones adjuntas. Debería entenderse adicionalmente que los dibujos no están dibujados a escala y que estos meramente pretenden ilustrar conceptualmente las estructuras y procedimientos descritos en el presente documento.

BREVE DESCRIPCIÓN DE LAS FIGURAS

Algunas realizaciones de ejemplo se describirán ahora con referencia a los dibujos adjuntos en los que

- 15 La figura 1 ilustra a modo de ejemplo, en un diagrama esquemático, un entorno de radio en el que pueden realizarse realizaciones de ejemplo de la presente divulgación;
- La figura 2 muestra, en un diagrama de flujo de señalización, realizaciones de ejemplo de métodos de acuerdo con el primer, segundo y tercer aspecto;
- 20 La figura 3 muestra, en un diagrama de flujo de señalización, realizaciones de ejemplo de métodos de acuerdo con el primer y segundo aspecto;
- La figura 4 muestra, en un diagrama de bloques esquemático, en una realización de ejemplo de un equipo de usuario de acuerdo con el primer aspecto;
- 25

La figura 5 muestra, en un diagrama esquemático, una realización de ejemplo de un nodo de radio, tal como un nodo maestro o un nodo secundario, de acuerdo con el segundo o tercer aspecto;

La figura 6 muestra, en una ilustración esquemática, ejemplos de medios de almacenamiento legibles por ordenador tangibles y no transitorios.

DESCRIPCIÓN DETALLADA DE LAS FIGURAS

La siguiente descripción sirve para profundizar en el entendimiento de la presente divulgación y deberá entenderse que complementa, y que ha de leerse, junto con la descripción de realizaciones de ejemplo de la presente divulgación según se proporciona en la sección de SUMARIO anterior de esta memoria descriptiva.

A continuación y con referencia a la figura 1, se describe un entorno de radio de ejemplo, en el que puede aplicarse la presente divulgación. Aunque el sistema de radio específico en los ejemplos a continuación es un sistema 5G, esto solo debe considerarse un ejemplo no limitante.

La figura 1 ilustra a modo de ejemplo, como ejemplo de un UE de acuerdo con el primer aspecto de ejemplo, un equipo de usuario (UE) 101, como ejemplo de un MN de acuerdo con el segundo aspecto de ejemplo, un nodo maestro (MN) 102, y como ejemplos de SN de acuerdo con el tercer aspecto de ejemplo, un nodo secundario de origen (S-SN) 103, un primer nodo secundario objetivo (T-SN1) 104 y un segundo nodo secundario objetivo (T-SN2) 105. Juntos, el MN 102, el S-SN 103, el T-SN1 104 y el T-SN2 105 pueden establecer un sistema o red de comunicación inalámbrica que atiende a un área geográfica dentro de la que está ubicado el UE 101. El UE 101, MN 102 y los SN 103, 104, 105 pueden estar operando en modo de conectividad dual.

El UE 101 puede conectarse con el MN 102 y con uno o más de los SN 103, 104, 105 por medio de enlaces de radio (no mostrados), que pueden corresponder, por ejemplo, a la interfaz Uu de 5G/NR. El MN 102 puede conectarse con uno o más de los SN 103, 104, 105 por medio de enlaces de radio (no mostrados), que pueden corresponder, por ejemplo, a la interfaz Xn de 5G/NR. Los enlaces de radio pueden habilitar la transmisión y/o recepción de información y/o señales entre los dispositivos respectivos.

En algún punto en el tiempo, como se indica por la flecha 110, el UE 101 se mueve desde una primera posición a una segunda posición. Mientras que en la primera posición el UE puede haber sido atendido por una célula de servicio asociada con el S-SN 103, una célula asociada con el T-SN1 104 puede estar atendiendo al UE en la segunda posición. Por lo tanto, durante el movimiento del UE 101 a lo largo de la flecha 110, puede haberse realizado un CPAC o CHO del UE 101 desde el S-SN 103 al T-SN1 104.

Pasando ahora a la figura 2, se muestra un diagrama de flujo de señalización de realizaciones de ejemplo de métodos de acuerdo con el primer, segundo y tercer aspecto. Más específicamente, se muestra la sucesión de acciones y señalización entre un equipo de usuario (UE) 201, un nodo maestro (MN) 202, un nodo secundario de origen (S-SN) 203, un primer nodo secundario objetivo (T-SN1) 104, y un segundo nodo secundario objetivo (T-SN2) 205. El UE 201, MN 202 y los SN 203, 204, 205, generalmente, pueden estar operando en modo de conectividad dual.

En un punto de tiempo especificado, que se indica con 210a, 210b y 210c, el UE 201, después de haber establecido una conexión hacia el MN 202, se conecta con el MN 202. Además, el UE 201 está conectado con el S-SN 203 y

atendido por una célula de servicio asociada con el S-SN 203. El UE 201, el MN 202 y el S-SN 203 están operando en modo de conectividad dual entre sí.

Dentro de la acción 211, el UE 201 transmite una primera información de estado al MN 202. En esta realización de ejemplo, la primera información de estado comprende información de medición relacionada con una medición de intensidades de señal de uno o más SN, en particular, del S-SN 202.

Dentro de la acción 212, el MN 202 decide, basándose en la primera información de estado recibida desde el UE 201, configurar la activación selectiva de T-SN1 204 y T-SN2 205. Además, el MN 202 genera una lista de valores de contador de SN para la clave de seguridad K_{SN} , así como una lista de claves de seguridad K_{SN} correspondientes. En este punto, los valores de contador de SN constituyen un ejemplo no limitante para valores de contador de clave de acuerdo con la presente divulgación, y la clave de seguridad K_{SN} constituye un ejemplo no limitante para una clave de seguridad de acuerdo con la presente divulgación. En esta realización de ejemplo particular, se genera una lista de tres valores de contador de SN diferentes, así como una lista de tres claves de seguridad K_{SN} correspondientes diferentes. Sin embargo, este es únicamente un ejemplo no limitante, y el número de elementos de lista de ambas listas podría ser menor o mayor, en general. En esta realización de ejemplo particular, la 1ª, 2ª y 3ª claves de seguridad K_{SN} en la lista de claves de seguridad K_{SN} se calculan, respectivamente, usando el 1º, 2º y 3º elemento en la lista de valores de contador de SN, de modo que la 1ª (2ª y 3ª) claves de seguridad K_{SN} en la lista de claves de seguridad K_{SN} corresponden al 1º (2º, 3º) valor de contador de SN en la lista de valores de contador de SN. Sin embargo, la correspondencia entre ambas listas también podría ser diferente, en general.

Dentro de la acción 213, el MN 202 transmite información de solicitud al T-SN1 204. En este punto, la información de solicitud comprende una solicitud de adición o cambio de SN. Además, la información de solicitud comprende la lista de claves de seguridad K_{SN} generadas dentro de la acción 212.

5 Dentro de la acción 214, el MN 202 transmite de la misma manera información de solicitud al T-SN2 205. En este punto, la información de solicitud comprende de la misma manera una solicitud de adición o cambio de SN. Además, la información de solicitud comprende de la misma manera la lista de claves de seguridad K_{SN} generadas dentro de la acción 212.

10 Dentro de la acción 215, el MN 202 transmite información de configuración al UE 201. En este punto, la información de configuración comprende una solicitud de reconfiguración de RRC junto con respectiva información de configuración de CPAC o CHO para T-SN1 204 y T-SN2 205. En particular, la información de configuración comprende la lista de valores de contador de SN
15 generados dentro de la acción 212. Dado que la lista de valores de contador de SN define una secuencia de valores de contador de clave, más precisamente tres valores de contador de clave diferentes en esta realización de ejemplo no limitante particular, la lista de valores de contador de SN constituye un ejemplo para información de contador de clave de acuerdo con la presente divulgación.

20 A continuación, se describe un primer CPAC o CHO realizado por el UE 201.

Dentro de la acción 230, el UE 201 determina si se cumplen los requisitos para CPAC o CHO hacia uno o más posibles SN objetivo. En respuesta a la determinación de que se cumplen los requisitos para CPAC o CHO hacia el T-
25 SN1 204, el UE 201 deriva un primer valor de contador de SN seleccionando el

primer elemento en la lista de valores de contador de SN. En este contexto, la lista de valores de contador de clave es ventajosa en el sentido de que permite, de una manera particularmente sencilla, la derivación del primer valor de contador de SN, de manera que, por ejemplo, no se requieren operaciones de cálculo complejas y se ahorran recursos de procesador respectivos. Usando el primer valor de contador de SN como entrada de actualización, el UE 201 calcula a continuación una primera clave de seguridad K_{SN} para T-SN1 204.

Dentro de la acción 231, el UE 201 transmite una segunda información de estado al MN 202. En esta realización de ejemplo, la segunda información de estado es indicativa de una finalización de reconfiguración de RRC. Después de transmitir la segunda información de estado, el UE 201 puede intentar establecer una conexión hacia el T-SN1 204.

Dentro de la acción 232, el MN 202 transmite una tercera información de estado al T-SN1 204. En esta realización de ejemplo, la tercera información de estado es indicativa de una finalización de reconfiguración, en particular, reconfiguración de RRC del UE 201.

Dentro de la acción 233, el T-SN1 204 determina si el UE 201 intenta establecer una conexión hacia el T-SN1 204. En respuesta a la determinación de que el UE 201 intenta establecer una conexión hacia el T-SN1 204, el T-SN1 204, en preparación de un intercambio de datos posterior, selecciona la primera clave de seguridad K_{SN} en su lista de claves de seguridad K_{SN} recibidas desde el MN 202 dentro de la acción 213.

Dentro de la acción 234, el UE 201 y el T-SN1 204 establecen una conexión. En esta realización de ejemplo particular, la conexión se establece en el sentido de que el UE 201 inicia un procedimiento de acceso aleatorio a través

del RACH hacia el T-SN1 204. Después de establecer la conexión, el UE 201 y el T-SN1 204 intercambian datos entre sí usando la primera clave de seguridad K_{SN} para protección de integridad y/o cifrado. Mientras que el UE 201 ha obtenido esta primera clave de seguridad K_{SN} calculándola usando el primer valor de contador de SN como una entrada de actualización, el T-SN1 204 ha obtenido esta primera clave de seguridad K_{SN} seleccionando el primer elemento de lista en la lista de claves de seguridad K_{SN} dentro de la acción 233. En esta realización de ejemplo particular, el UE 201 y el T-SN1 204 calculan un total de cuatro claves de seguridad subordinadas basándose en la primera clave de seguridad K_{SN} . Se usa una primera clave de seguridad subordinada para protección de integridad de señalización de RRC. Se usa una segunda clave de seguridad subordinada para el cifrado de señalización de RRC. Se usa una tercera clave de seguridad subordinada para protección de integridad de datos de usuario. Se usa una cuarta clave de seguridad subordinada para el cifrado de datos de usuario. Al establecer la conexión e intercambiando datos, el UE 201 puede ser atendido ahora por una célula de servicio asociada con el T-SN1 204. El UE 201, el MN 202 y el T-SN1 204 pueden estar operando en modo de conectividad dual entre sí.

Dentro de la acción 235, el UE 201 procesa la lista de valores de contador de SN en el sentido de que elimina el primer elemento en la lista. De esta manera, el segundo elemento anterior en la lista de valores de contador de SN se convierte en el nuevo primer elemento, y el tercer elemento anterior se convierte en el nuevo segundo elemento. Sin embargo, en general, también sería concebible que el primer elemento en la lista no se elimine completamente, sino que únicamente se modifique para convertirse en un elemento de lista vacío, o

se marque como inutilizable, por ejemplo. Al procesar la lista de valores de contador de SN, el UE 201 está habilitado para derivar en un punto de tiempo posterior, a partir de la lista procesada de valores de contador de SN, un segundo valor de contador de SN para generar una segunda clave de seguridad K_{SN} para el intercambio de datos con un segundo SN objetivo. En este contexto, el segundo SN objetivo puede ser el T-SN2 205 o el S-SN 203. Por lo tanto, el UE 201 puede realizar de forma autónoma K_{SN} actualizando un CPAC o CHO hacia el SCG asociado con el segundo SN objetivo sin que el MN 202 tenga que transmitir nueva información de configuración para este CPAC o CHO. De este modo, también se puede lograr que se reduzca la sobrecarga de señalización de RRC y se habilite en mayor medida la movilidad rápida del UE 201 a través de diferentes SCG.

Dentro de la acción 236, el T-SN1 204 transmite, al MN 202, una información indicativa de un cambio de clave. En este ejemplo particular, el cambio de clave es el cambio hacia la primera clave de seguridad K_{SN} usada para protección de integridad y/o cifrado de datos intercambiados entre el UE 201 y el T-SN1 204.

Dentro de la acción 237, el T-SN1 204 elimina la primera clave de seguridad K_{SN} de su lista de claves de seguridad K_{SN} en respuesta al uso de la primera clave de seguridad K_{SN} para protección de integridad y/o cifrado de datos intercambiados entre el UE 201 y el T-SN1 204. De esta manera, el segundo elemento anterior en la lista de K_{SN} claves de seguridad se convierte en el nuevo primer elemento, y el tercer elemento anterior se convierte en el nuevo segundo elemento. Sin embargo, en general, también sería concebible que el primer elemento en la lista no se elimine completamente, sino que únicamente se

modifique para convertirse en un elemento de lista vacío, o se marque como inutilizable, por ejemplo. Al eliminar la primera clave de seguridad K_{SN} , se puede lograr que la lista de claves de seguridad K_{SN} del T-SN1 204 permanezca consistente con la lista de valores de contador de SN procesados por el UE 201.

5 Dentro de la acción 238, el MN 202 transmite, al T-SN2 205, una instrucción para eliminar la primera clave de seguridad K_{SN} en su lista de claves de seguridad K_{SN} recibidas desde el MN 202 dentro de la acción 214.

 Dentro de la acción 239, el T-SN2 205 elimina la primera clave de seguridad K_{SN} en su lista de claves de seguridad K_{SN} en respuesta a la recepción de la instrucción respectiva desde el MN 202. De esta manera, el segundo elemento anterior en la lista de K_{SN} claves de seguridad se convierte en el nuevo primer elemento, y el tercer elemento anterior se convierte en el nuevo segundo elemento. Sin embargo, en general, también sería concebible que el primer elemento en la lista no se elimine completamente, sino que únicamente se modifique para convertirse en un elemento de lista vacío, o se marque como inutilizable, por ejemplo. Al eliminar la primera clave de seguridad K_{SN} , se puede lograr que la lista de claves de seguridad K_{SN} del T-SN2 205 permanezca consistente con la lista de claves de seguridad K_{SN} del T-SN1 204, y con la lista de valores de contador de SN procesados por el UE 201.

20 A continuación, se describe un segundo CPAC o CHO realizado por el UE 201.

 Dentro de la acción 250, el UE 201 determina si se cumplen los requisitos para CPAC o CHO hacia uno o más posibles SN objetivo. En respuesta a la determinación de que se cumplen los requisitos para CPAC o CHO hacia el T-SN2 205, el UE 201 deriva un segundo valor de contador de SN seleccionando

el primer elemento actualmente en la lista de valores de contador de SN. En este contexto, la lista de valores de contador de clave es ventajosa en el sentido de que permite, de una manera particularmente sencilla, la derivación del segundo valor de contador de SN, de manera que, por ejemplo, no se requieren
5 operaciones de cálculo complejas y se ahorran recursos de procesador respectivos. Usando el segundo valor de contador de SN como entrada de actualización, el UE 201 calcula a continuación una segunda clave de seguridad K_{SN} para T-SN2 205.

Dentro de la acción 251, el UE 201 transmite una cuarta información de
10 estado al MN 202. En esta realización de ejemplo, la cuarta información de estado es indicativa de una finalización de reconfiguración de RRC. Después de transmitir la cuarta información de estado, el UE 201 puede intentar establecer una conexión hacia el T-SN2 205.

Dentro de la acción 252, el MN 202 transmite una quinta información de
15 estado al T-SN2 205. En esta realización de ejemplo, la quinta información de estado es indicativa de una finalización de reconfiguración, en particular, reconfiguración de RRC del UE 201.

Dentro de la acción 253, el T-SN2 205 determina si el UE 201 intenta establecer una conexión hacia el T-SN2 205. En respuesta a la determinación de
20 que el UE 201 intenta establecer una conexión hacia el T-SN2 205, el T-SN2 205, en preparación de un intercambio de datos posterior, selecciona la primera clave de seguridad K_{SN} actualmente en su lista de claves de seguridad K_{SN} . Esta primera clave de seguridad K_{SN} actualmente es idéntica a la segunda clave de seguridad K_{SN} en la lista original de claves de seguridad K_{SN} recibidas desde el
25 MN 202 dentro de la acción 214.

Dentro de la acción 254, el UE 201 y el T-SN2 205 establecen una conexión. En esta realización de ejemplo particular, la conexión se establece en el sentido de que el UE 201 inicia un procedimiento de acceso aleatorio a través del RACH hacia el T-SN2 205. Después de establecer la conexión, el UE 201 y

5 el T-SN2 205 intercambian datos entre sí usando la segunda clave de seguridad K_{SN} para protección de integridad y/o cifrado. Mientras que el UE 201 ha obtenido esta segunda clave de seguridad K_{SN} calculándola usando el segundo valor de contador de SN como una entrada de actualización, el T-SN1 204 ha obtenido esta segunda clave de seguridad K_{SN} seleccionando el primer elemento

10 actualmente de lista en la lista de claves de seguridad K_{SN} dentro de la acción 253. En esta realización de ejemplo particular, el UE 201 y el T-SN2 205 calculan un total de cuatro claves de seguridad subordinadas basándose en la segunda clave de seguridad K_{SN} . Se usa una primera clave de seguridad subordinada para protección de integridad de señalización de RRC. Se usa una segunda

15 clave de seguridad subordinada para el cifrado de señalización de RRC. Se usa una tercera clave de seguridad subordinada para protección de integridad de datos de usuario. Se usa una cuarta clave de seguridad subordinada para el cifrado de datos de usuario. Al establecer la conexión e intercambiando datos, el UE 201 puede ser atendido ahora por una célula de servicio asociada con el T-

20 SN2 205. El UE 201, el MN 202 y el T-SN2 205 pueden estar operando en modo de conectividad dual entre sí.

Dentro de la acción 255, el UE 201 procesa adicionalmente la lista de valores de contador de SN en el sentido de que elimina el primer elemento actualmente en la lista. De esta manera, el segundo elemento anterior en la lista

25 de valores de contador de SN se convierte en el nuevo primer elemento. Sin

embargo, en general, también sería concebible que el primer elemento utilizable actualmente en la lista no se elimine completamente, sino que únicamente se modifique para convertirse en un elemento de lista vacío, o se marque como inutilizable, por ejemplo. Al procesar adicionalmente la lista de valores de contador de SN, el UE 201 está habilitado para derivar en un punto de tiempo posterior, a partir de la lista adicionalmente procesada de valores de contador de SN, un valor de contador de SN adicional para generar una clave de seguridad K_{SN} adicional para el intercambio de datos con un SN objetivo adicional. En este contexto, el SN objetivo adicional puede ser el T-SN1 204, el S-SN 203 o un T-SN adicional no mostrado en la figura 2. Por lo tanto, el UE 201 puede realizar de forma autónoma K_{SN} actualizando un CPAC o CHO hacia el SCG asociado con el SN objetivo adicional sin que el MN 202 tenga que transmitir nueva información de configuración para este CPAC o CHO. De este modo, también se puede lograr que se reduzca la sobrecarga de señalización de RRC y se habilite en mayor medida la movilidad rápida del UE 201 a través de diferentes SCG.

Dentro de la acción 256, el T-SN2 205 transmite, al MN 202, una información indicativa de un cambio de clave. En este ejemplo particular, el cambio de clave es el cambio hacia la segunda clave de seguridad K_{SN} usada para protección de integridad y/o cifrado de datos intercambiados entre el UE 201 y el T-SN2 205.

Dentro de la acción 257, el T-SN2 205 elimina la primera clave de seguridad K_{SN} actualmente de su lista de claves de seguridad en respuesta al uso de esta clave de seguridad K_{SN} para protección de integridad y/o cifrado de datos intercambiados entre el UE 201 y el T-SN2 205. De esta manera, el segundo elemento anterior en la lista de claves de seguridad K_{SN} se convierte en

el nuevo primer elemento. Sin embargo, en general, también sería concebible que el primer elemento utilizable actualmente en la lista no se elimine completamente, sino que únicamente se modifique para convertirse en un elemento de lista vacío, o se marque como inutilizable, por ejemplo. Al eliminar
5 la primera clave de seguridad K_{SN} actualmente, se puede lograr que la lista de claves de seguridad K_{SN} del T-SN2 205 permanezca consistente con la lista de valores de contador de SN procesados por el UE 201.

Dentro de la acción 258, el MN 202 transmite, al T-SN1 204, una instrucción para eliminar la primera clave de seguridad K_{SN} actualmente en su
10 lista de claves de seguridad K_{SN} recibidas desde el MN 202 dentro de la acción 213.

Dentro de la acción 259, el T-SN1 204 elimina la primera clave de seguridad K_{SN} actualmente en su lista de claves de seguridad en respuesta a la recepción de la instrucción respectiva desde el MN 202. De esta manera, el
15 segundo elemento anterior en la lista de claves de seguridad K_{SN} se convierte en el nuevo primer elemento. Sin embargo, en general, también sería concebible que el primer elemento utilizable actualmente en la lista no se elimine completamente, sino que únicamente se modifique para convertirse en un elemento de lista vacío, o se marque como inutilizable, por ejemplo. Al eliminar
20 la primera clave de seguridad K_{SN} actualmente, se puede lograr que la lista de claves de seguridad K_{SN} del T-SN1 204 permanezca consistente con la lista de claves de seguridad K_{SN} del T-SN2 205, y con la lista de valores de contador de SN procesados adicionalmente por el UE 201.

Aunque no se muestra en la figura 2, el UE 201 puede realizar CPAC o
25 CHO adicionales de manera análoga al primer y segundo CPAC o CHO

explicados anteriormente.

En cualquier punto de tiempo adecuado, en particular, después de que se haya determinado por el UE 201 o por uno o más de T-SN1 204 y T-SN2 205 que la lista de valores de contador de SN, o, respectivamente, la lista de claves de seguridad K_{SN} , no alcanza un umbral predefinido, el UE 201 o uno o más del T-SN1 204 y el T-SN2 205 pueden transmitir información respectiva al MN 202. En respuesta a la recepción de información indicativa de la lista de valores de contador de SN, o, respectivamente, la lista de claves de seguridad K_{SN} , que no alcanza el umbral, el MN 202 puede transmitir al menos un elemento de lista adicional para la lista de valores de contador de SN al UE 201, y transmitir al menos un elemento de lista adicional para la lista de claves de seguridad K_{SN} al SN1 204 y/o T-SN2 205. De esta manera, se puede lograr que se mantenga la capacidad del UE para realizar un CPAC o un CHO hacia los SCG asociados con los SN objetivo.

La figura 3 muestra un diagrama de flujo de señalización de realizaciones de ejemplo de métodos de acuerdo con el primer y segundo aspecto. Más específicamente, se muestra la sucesión de acciones y señalización entre un equipo de usuario (UE) 301, un nodo maestro (MN) 302, un nodo secundario de origen (S-SN) 303, un primer nodo secundario objetivo (T-SN1) 304, y un segundo nodo secundario objetivo (T-SN2) 305. El UE 301, MN 302 y los SN 303, 304, 305, generalmente, pueden estar operando en modo de conectividad dual.

En un punto de tiempo especificado, que se indica con 310a, 310b y 310c, el UE 301, después de haber establecido una conexión hacia el MN 302, se conecta con el MN 302. Además, el UE 301 está conectado con el S-SN 303 y

atendido por una célula de servicio asociada con el S-SN 303. El UE 301, el MN 302 y el S-SN 303 están operando en modo de conectividad dual entre sí.

Dentro de la acción 311, el S-SN 303 transmite una primera información de estado al MN 302. En esta realización de ejemplo, la primera información de estado es indicativa de una necesidad de un CPAC o CHO.

Dentro de la acción 312, el MN 302 transmite información de solicitud al T-SN1 304. En esta realización de ejemplo, la información de solicitud comprende una solicitud de adición o cambio de SN.

Dentro de la acción 313, el T-SN1 304 transmite una segunda información de estado al MN 302. En esta realización de ejemplo, la segunda información de estado es indicativa de un acuse de recibo de una solicitud de adición o cambio de SN.

Dentro de la acción 314, el MN 302 transmite información de solicitud al T-SN2 305. En esta realización de ejemplo, la información de solicitud comprende una solicitud de adición o cambio de SN.

Dentro de la acción 315, el T-SN2 305 transmite una tercera información de estado al MN 302. En esta realización de ejemplo, la tercera información de estado es indicativa de un acuse de recibo de una solicitud de adición o cambio de SN.

Dentro de la acción 316, el MN 302 transmite información de configuración al UE 301. En este punto, la información de configuración comprende una solicitud de reconfiguración de RRC junto con respectiva información de configuración de CPAC o CHO. En particular, la información de configuración comprende un valor de contador de SN para la clave de seguridad K_{SN} y una instrucción para mantener el valor de contador de SN, es decir, para procesar

continuamente el valor de contador de SN en lugar de liberarlo. En este punto, el valor de contador de SN constituye un ejemplo para un valor de contador de clave de acuerdo con la presente divulgación, y la clave de seguridad K_{SN} constituye un ejemplo de una clave de seguridad de acuerdo con la presente divulgación. Además, el valor de contador de SN junto con la instrucción para mantener el valor de contador de SN constituye un ejemplo de información de contador de clave de acuerdo con la presente divulgación, ya que se define una secuencia de al menos dos valores de contador de SN diferentes para generar al menos dos claves de seguridad K_{SN} diferentes para al menos dos SN objetivo diferentes, como se ilustrará con más detalle a continuación. Una ventaja particular de la información de configuración que comprende un valor de contador de SN y una instrucción para mantener el valor de contador de SN es que los posibles SN objetivo no tienen que aprovisionarse previamente con múltiples claves de seguridad K_{SN} , como también se ilustrará con más detalle a continuación.

Dentro de la acción 317, el UE 301 transmite una cuarta información de estado al MN 302. En esta realización de ejemplo, la cuarta información de estado es indicativa de una finalización de reconfiguración de RRC.

A continuación, se describe un primer CPAC o CHO realizado por el UE 301.

Dentro de la acción 330, el UE 301 determina si se cumplen los requisitos para CPAC o CHO hacia uno o más posibles SN objetivo.

Dentro de la acción 331, el UE 301 determina que se cumplen los requisitos para CPAC o CHO hacia el T-SN1 304. En respuesta a la determinación de que se cumplen los requisitos para CPAC o CHO hacia el T-

SN1 304, el UE 301 deriva un primer valor de contador de SN usando el valor de contador de SN recibido desde el MN 302 dentro de la acción 316 como primer valor de contador de SN. En este contexto, mediante la información de contador de SN recibida desde el MN 302 dentro de la acción 316 que comprende un valor
 5 de contador de SN y una instrucción para mantener el valor de contador de SN, se puede lograr una derivación particularmente sencilla del primer valor de contador de SN, de modo que, por ejemplo, no se requieren operaciones de cálculo complejas y se ahorran recursos de procesador respectivos.

Dentro de la acción 332, el UE 301 calcula una primera clave de seguridad
 10 K_{SN} para T-SN1 304 usando el primer valor de contador de SN derivado como entrada de actualización. Además, el UE 301 procesa la información de contador de SN en el sentido de que añade un valor de paso predefinido, en este caso, en particular, un valor de paso de uno, al valor de contador de SN recibido desde el nodo maestro. En otras palabras, el UE 301 aumenta el contador de SN por el
 15 valor de paso, que es igual a uno en este ejemplo no limitante particular. Sin embargo, en general, los valores de paso diferentes de uno son fácilmente concebibles. Al añadir el valor de paso predefinido al valor de contador de SN recibido del nodo maestro, se obtiene un segundo elemento en una secuencia de valores de contador de SN. De esta manera, el UE 301 está habilitado para
 20 derivar en un punto de tiempo posterior, a partir del contador de SN procesado, un segundo valor de contador de SN para generar una segunda clave de seguridad K_{SN} para el intercambio de datos con un segundo SN objetivo. En este contexto, el segundo SN objetivo puede ser el T-SN2 305 o el S-SN 303. Por lo tanto, el UE 301 puede realizar de forma autónoma K_{SN} actualizando un CPAC o
 25 CHO hacia el SCG asociado con el segundo SN objetivo sin que el MN 302 tenga

que transmitir nueva información de configuración para este CPAC o CHO. De este modo, también se puede lograr que se reduzca la sobrecarga de señalización de RRC y se habilite en mayor medida la movilidad rápida del UE 301 a través de diferentes SCG.

- 5 Dentro de la acción 333, el UE 301 transmite una quinta información de estado al MN 302. En esta realización de ejemplo, la quinta información de estado es indicativa de un CPAC o CHO hacia el T-SN1 304.

 Dentro de la acción 334, el MN 302 transmite información de solicitud adicional al T-SN1 304. En esta realización de ejemplo, la información de
10 solicitud adicional comprende una solicitud de modificación de SN y comprende la primera clave de seguridad K_{SN} , que ha sido calculada por el MN 302 independientemente del UE 301.

 Dentro de la acción 335, el T-SN1 304 transmite una sexta información de estado al MN 302. En esta realización de ejemplo, la sexta información de estado
15 es indicativa de un acuse de recibo de una solicitud de modificación de SN.

 Dentro de la acción 336, el MN 302 transmite una séptima información de estado al S-SN 303. En esta realización de ejemplo, la séptima información de estado es indicativa de un CPAC o CHO, en particular, un CPAC o CHO hacia el T-SN1 304.

20 Dentro de la acción 337, el MN 302 transmite una octava información de estado al T-SN1 304. En esta realización de ejemplo, la octava información de estado es indicativa de una finalización de una modificación de SN.

 Dentro de la acción 338, el UE 301 y el T-SN1 304 establecen una conexión. El UE 301 y el T-SN1 304 intercambian datos entre sí usando la
25 primera clave de seguridad K_{SN} para protección de integridad y/o cifrado. En esta

realización de ejemplo particular, el UE 301 y el T-SN1 304 calculan un total de cuatro claves de seguridad subordinadas basándose en la primera clave de seguridad K_{SN} . Se usa una primera clave de seguridad subordinada para protección de integridad de señalización de RRC. Se usa una segunda clave de seguridad subordinada para el cifrado de señalización de RRC. Se usa una tercera clave de seguridad subordinada para protección de integridad de datos de usuario. Se usa una cuarta clave de seguridad subordinada para el cifrado de datos de usuario. Estableciendo la conexión e intercambiando datos, el UE 301 puede ser atendido ahora por una célula de servicio asociada con el T-SN1 304, de manera que se complete CPAC o CHO. El UE 301, el MN 302 y el T-SN1 304 pueden estar operando en modo de conectividad dual entre sí.

A continuación, se describe un segundo CPAC o CHO realizado por el UE 301.

Dentro de la acción 350, el UE 301 determina si se cumplen los requisitos para CPAC o CHO hacia uno o más posibles SN objetivo.

Dentro de la acción 351, el UE 301 determina que se cumplen los requisitos para CPAC o CHO de vuelta hacia el S-SN 303. En respuesta a la determinación de que se cumplen los requisitos para CPAC o CHO de vuelta hacia el S-SN 303, el UE 301 deriva un segundo valor de contador de SN usando el valor de contador de SN actual, es decir, el valor de contador de SN recibido desde el MN 302 aumentado en uno, como segundo valor de contador de SN. En este contexto, mediante la información de contador de SN recibida desde el MN 302 dentro de la acción 316 que comprende un valor de contador de SN y una instrucción para mantener el valor de contador de SN, se puede lograr una derivación particularmente sencilla del segundo valor de contador de SN, de

modo que, por ejemplo, no se requieren operaciones de cálculo complejas y se ahorran recursos de procesador respectivos.

Dentro de la acción 352, el UE 301 calcula una segunda clave de seguridad K_{SN} para S-SN 303 usando el segundo valor de contador de SN derivado como entrada de actualización. Además, el UE 301 procesa adicionalmente la información de contador de SN en el sentido de que añade, una vez más, el valor de paso predefinido al valor de contador de SN actual. En otras palabras, el UE 301 aumenta una vez más el contador de SN por el valor de paso, que es igual a uno en este ejemplo no limitante particular. Al añadir el valor de paso predefinido al valor de contador de SN actual, se obtiene un tercer elemento en una secuencia de valores de contador de SN. De esta manera, el UE 301 está habilitado para derivar en un punto de tiempo posterior, a partir del contador de SN procesado adicional, un valor de contador de SN adicional para generar una clave de seguridad K_{SN} adicional para el intercambio de datos con un SN objetivo adicional. En este contexto, el SN objetivo adicional puede ser el T-SN1 304, el T-SN2 305 o un T-SN adicional no mostrado en la figura 3. Por lo tanto, el UE 301 puede realizar de forma autónoma K_{SN} actualizando un CPAC o CHO hacia el SCG asociado con el SN objetivo adicional sin que el MN 302 tenga que transmitir nueva información de configuración para este CPAC o CHO. De este modo, también se puede lograr que se reduzca la sobrecarga de señalización de RRC y se habilite en mayor medida la movilidad rápida del UE 301 a través de diferentes SCG.

Dentro de la acción 353, el UE 301 transmite una novena información de estado al MN 302. En esta realización de ejemplo, la novena información de estado es indicativa de un CPAC o CHO hacia el S-SN 303.

Dentro de la acción 354, el MN 302 transmite información de solicitud adicional al S-SN 303. En esta realización de ejemplo, la información de solicitud adicional comprende una solicitud de modificación de SN y comprende la segunda clave de seguridad K_{SN} , que ha sido calculada por el MN 302
5 independientemente del UE 301.

Dentro de la acción 355, el S-SN 303 transmite una décima información de estado al MN 302. En esta realización de ejemplo, la décima información de estado es indicativa de un acuse de recibo de una solicitud de modificación de SN.

10 Dentro de la acción 356, el MN 302 transmite una undécima información de estado al T-SN1 304. En esta realización de ejemplo, la undécima información de estado es indicativa de un CPAC o CHO, en particular, un CPAC o CHO hacia el S-SN 303.

Dentro de la acción 357, el MN 302 transmite una duodécima información
15 de estado al S-SN 303. En esta realización de ejemplo, la duodécima información de estado es indicativa de una finalización de una modificación de SN.

Dentro de la acción 358, el UE 301 y el S-SN 303 establecen una conexión. El UE 301 y el S-SN 303 intercambian datos entre sí usando la segunda clave de seguridad K_{SN} para protección de integridad y/o cifrado. En
20 esta realización de ejemplo particular, el UE 301 y el S-SN 303 calculan un total de cuatro claves de seguridad subordinadas basándose en la segunda clave de seguridad K_{SN} . Se usa una primera clave de seguridad subordinada para protección de integridad de señalización de RRC. Se usa una segunda clave de seguridad subordinada para el cifrado de señalización de RRC. Se usa una
25 tercera clave de seguridad subordinada para protección de integridad de datos

de usuario. Se usa una cuarta clave de seguridad subordinada para el cifrado de datos de usuario. Estableciendo la conexión e intercambiando datos, el UE 301 puede ser atendido ahora por una célula de servicio asociada con el S-SN 303, de manera que se complete CPAC o CHO. El UE 301, el MN 302 y el S-SN 303
5 pueden estar operando en modo de conectividad dual entre sí.

Aunque no se muestra en la figura 3, el UE 301 puede realizar CPAC o CHO adicionales de manera análoga al primer y segundo CPAC o CHO explicados anteriormente.

En realizaciones de ejemplo, la información de contador de clave
10 comprendida por la información de reconfiguración transmitida desde el MN 302 al UE 301 dentro de la acción 316 puede definir un número máximo permitido de adiciones del valor de paso predefinido al valor de contador de SN recibido desde el nodo maestro. Por ejemplo, la información de contador de clave puede comprender un valor de parada para el contador de SN que no puede superarse.
15 El UE 301 puede determinar, a continuación, en particular, cuándo se procesa o se procesa adicionalmente el contador de SN, si se ha alcanzado el número máximo permitido de adiciones. Por ejemplo, el UE 301 puede determinar si se ha alcanzado el valor de parada. Si se determina que se ha alcanzado el número máximo permitido de adiciones, el UE 301 puede evitar adiciones adicionales del
20 valor de paso predefinido al valor de contador de SN actual. Además, el UE 301 puede transmitir respectiva información al MN 302. Mediante el procedimiento anterior, el número de posibles CPAC o CHO realizados por el UE 301 puede especificarse por el MN 302 cuando el MN 302 transmite inicialmente la información de configuración al UE 301, de manera que puede limitarse el
25 número de eventos de movilidad autónoma del UE 301.

En las realizaciones de ejemplo descritas junto con las figuras 2 y 3, la información de configuración también puede indicar al UE 201, 301 al menos una célula secundaria objetivo para la que no se requiere generar una clave de seguridad K_{SN} . De este modo, se puede evitar derivaciones innecesarias de valores de contador de SN, generaciones innecesarias de claves de seguridad K_{SN} y/o procesamientos innecesarios de la información de contador de clave, en particular, si el UE 201, 301 se mueve o cambia entre células dentro del mismo SCG.

En las realizaciones de ejemplo descritas junto con las figuras 2 y 3, el MN 202, 302 puede comprender un nodo de gNB-CU-CP que realiza las acciones descritas del MN 202, 302.

Volviendo ahora a la figura 4, se muestra un diagrama de bloques de una realización de ejemplo de un UE 400 de acuerdo con el primer aspecto. Por ejemplo, el UE 400 puede ser uno de un teléfono inteligente, un ordenador de tableta, un ordenador portátil, un reloj inteligente, una banda inteligente, un dispositivo de IoT o un vehículo o una parte del mismo.

El UE 400 comprende un procesador 401. El procesador 401 puede representar un único procesador o dos o más procesadores, que están, por ejemplo, al menos parcialmente acoplados, por ejemplo, a través de un bus. El procesador 401 ejecuta el código de programa almacenado en la memoria de programa 402 (por ejemplo, el código de programa que hace que el UE 400 en conexión con el nodo de radio 500 realice una o más de las realizaciones de un método de acuerdo con la presente divulgación o partes de la misma, cuando es ejecutado en el procesador 401) e interactúa con una memoria principal 403. La memoria de programa 402 también puede contener un sistema operativo para el

procesador 401. Algunas o todas las memorias 402 y 403 también pueden incluirse en el procesador 401.

Una o ambas de una memoria principal y una memoria de programa de un procesador (por ejemplo, la memoria de programa 402 y la memoria principal 5 403) podrían estar conectadas de manera fija al procesador (por ejemplo, el procesador 401) o al menos parcialmente extraíbles del procesador, por ejemplo, en la forma de una tarjeta o dispositivo de memoria.

Una memoria de programa (por ejemplo, la memoria de programa 402) puede ser, por ejemplo, memoria no volátil. Puede ser, por ejemplo, una memoria 10 FLASH (o una parte de la misma), cualquiera de una memoria ROM, PROM, EPROM, MRAM o FeRAM (o una parte de la misma) o un disco duro (o una parte del mismo), por nombrar solo unos pocos ejemplos no limitantes. Por ejemplo, una memoria de programa puede comprender, por ejemplo, una primera sección de memoria que está instalada de manera fija, y una segunda sección de 15 memoria que es extraíble, por ejemplo, en forma de una tarjeta de memoria SD extraíble.

Una memoria principal (por ejemplo, la memoria principal 403) puede ser, por ejemplo, una memoria volátil. Puede ser, por ejemplo, una memoria DRAM, para dar un ejemplo no limitante. Puede usarse, por ejemplo, como memoria de 20 trabajo para el procesador 401 cuando se ejecuta un sistema operativo, una aplicación, un programa y/o similares.

El procesador 401 puede controlar además una interfaz de comunicación 404 (por ejemplo, interfaz de radio) configurada para recibir y/o transmitir datos y/o información. Por ejemplo, la interfaz de comunicación 404 se puede 25 configurar para transmitir y/o recibir señales de radio desde un nodo de radio, tal

como un nodo maestro o un nodo secundario, en particular, como se describe en el presente documento. Debe entenderse que cualquier procesamiento basado en código de programa informático requerido para recibir y/o evaluar señales de radio puede almacenarse en una memoria propia de la interfaz de comunicación 404 y ejecutarse por un procesador propio de la interfaz de comunicación 404 y/o puede almacenarse, por ejemplo, en la memoria 403 y ejecutarse, por ejemplo, por el procesador 401.

La interfaz de comunicación 404 puede configurarse, en particular, para comunicarse de acuerdo con un sistema de comunicación celular como un sistema de comunicación celular de 2G/3G/4G/5G o de generación futura. El UE 400 puede usar la interfaz de radio 404 para comunicarse con un nodo de radio, tal como un nodo maestro o un nodo secundario, en particular, como se describe en el presente documento.

Por ejemplo, la interfaz de comunicación 404 puede comprender además una interfaz de radio de BLE y/o Bluetooth que incluye un transmisor, receptor o transceptor de BLE. Por ejemplo, la interfaz de radio 404 puede comprender adicionalmente o como alternativa una interfaz de radio de WLAN que incluye al menos un transmisor, receptor o transceptor de WLAN.

Los componentes 402, 403 y 404 del UE 400 pueden conectarse, por ejemplo, con el procesador 401 por medio de uno o más buses en serie y/o paralelos.

Debe entenderse que el UE 400 puede comprender diversos otros componentes. Por ejemplo, el UE 400 puede comprender opcionalmente una interfaz de usuario (por ejemplo, una pantalla táctil, un teclado, un panel táctil, una pantalla, etc.).

La figura 5 es un diagrama de bloques de una realización de ejemplo de un nodo de radio 500, tal como un nodo maestro 500 o un nodo secundario 500. Por ejemplo, el nodo de radio 500 se puede configurar para planificar y/o transmitir señales al UE 400, y/o a uno o más nodos de radio 500 adicionales, como se ha descrito anteriormente.

El nodo de radio 500 comprende un procesador 501. El procesador 501 puede representar un único procesador o dos o más procesadores, que están, por ejemplo, al menos parcialmente acoplados, por ejemplo, a través de un bus. El procesador 501 ejecuta un código de programa almacenado en la memoria de programa 502 (por ejemplo, el código de programa que hace que el nodo de radio 500 realice en solitario, junto con el UE 400, y/o junto con uno o más nodos de radio 500 adicionales, una o más de las realizaciones de un método de acuerdo con la presente divulgación o partes del mismo, cuando se ejecuta en el procesador 501), e interactúa con una memoria principal 503.

La memoria de programa 502 también puede comprender un sistema operativo para el procesador 501. Algunas o todas las memorias 502 y 503 también pueden incluirse en el procesador 501.

Además, el procesador 501 puede controlar una interfaz de comunicación 504 que está configurada, por ejemplo, para comunicarse de acuerdo con un sistema de comunicación celular como un sistema de comunicación celular 2G/3G/4G/5G. La interfaz de comunicación 504 del nodo de radio 500 puede realizarse por unidades de entrada de radio, por ejemplo, y puede proporcionarse para la comunicación entre el dispositivo de red y el dispositivo terminal.

Los componentes 502, 503 y 504 del nodo de radio 500 pueden conectarse, por ejemplo, con el procesador 501 por medio de uno o más buses

en serie y/o paralelos.

Debe entenderse que el nodo de radio 500 puede comprender diversos otros componentes.

La figura 6 es una ilustración esquemática de ejemplos de medios de almacenamiento legibles por ordenador tangibles y no transitorios de acuerdo con la presente divulgación que pueden usarse, por ejemplo, para implementar la memoria 402 de la figura 4 o la memoria 502 de la figura 5. Para este fin, la figura 6 muestra una memoria flash 600, que puede soldarse o unirse, por ejemplo, a una placa de circuito impreso, una unidad de estado sólido 601 que comprende una pluralidad de chips de memoria (por ejemplo, chips de memoria flash), una unidad de disco duro magnético 602, una tarjeta digital segura (SD) 603, un lápiz de memoria de bus serie universal (USB) 604, un medio de almacenamiento óptico 605 (tal como, por ejemplo, un CD-ROM o DVD) y un medio de almacenamiento magnético 606.

Cualquier conexión presentada en las realizaciones descritas ha de entenderse en el sentido de que los componentes implicados se acoplan operativamente. Por lo tanto, las conexiones pueden ser directas o indirectas con cualquier número o combinación de elementos intermedios, y puede haber meramente una relación funcional entre los componentes.

Además, como se usa en este texto, el término 'circuitería' se refiere a cualquiera de lo siguiente:

- (a) implementaciones de circuito solo de hardware (tales como implementaciones en circuitería solo analógica y/o digital);
- (b) combinaciones de circuitos y software (y/o firmware), tales como:
 - (i) una combinación de procesador(es), o

- (ii) secciones de procesador(es)/software (incluyendo procesador(es) de señales digitales), software y memoria(s) que trabajan conjuntamente para hacer que un aparato, tal como un teléfono móvil, realice diversas funciones); y
- 5 (c) circuitos, tales como un(os) microprocesador(es) o una sección de un(os) microprocesador(es), que requieren software o firmware para su funcionamiento, incluso si el software o firmware no está físicamente presente.

Esta definición de 'circuitaría' es aplicable a todos los usos de este término en este texto, incluyendo en cualquier reivindicación. Como un ejemplo adicional, como se usa en este texto, el término 'circuitaría' cubre también una implementación de solamente un procesador (o múltiples procesadores) o sección de un procesador y su software y/o firmware adjunto. El término 'circuitaría' también cubre, por ejemplo, un circuito integrado de banda base o un

10

15 circuito integrado de procesador de aplicaciones para un teléfono móvil.

Cualquiera de los procesadores mencionados en este texto, en particular, pero sin limitación, los procesadores 401 y 501 de las figuras 4 y 5, podría ser un procesador de cualquier tipo adecuado. Cualquier procesador puede comprender, pero sin limitación, uno o más microprocesadores, uno o más

20

procesadores con procesadores de señales digitales adjuntos, uno o más procesadores sin un(os) procesador(es) de señales digitales adjuntos, uno o más chips de ordenador de propósito especial, una o más matrices de puertas programables en campo (FPGA), uno o más controladores, uno o más circuitos integrados específicos de la aplicación (ASIC), o uno o más ordenadores. La

25

estructura/hardware relevante se ha programado de una forma tal como para

llevar a cabo la función descrita.

Además, cualquiera de las acciones o etapas descritas o ilustradas en el presente documento puede implementarse usando instrucciones ejecutables en un procesador de propósito general o de propósito especial y almacenarse en un medio de almacenamiento legible por ordenador (por ejemplo, disco, memoria o similar) para ser ejecutadas por un procesador de este tipo. Debería entenderse que las referencias a 'medio de almacenamiento legible por ordenador' abarcan circuitos especializados tales como FPGA, ASIC, dispositivos de procesamiento de señales y otros dispositivos.

Como se usa en el presente documento, "al menos uno de los siguientes: <una lista de dos o más elementos>" y "al menos uno de <una lista de dos o más elementos>" y enunciados similares, donde la lista de dos o más elementos se une mediante "y" u "o", significan al menos uno cualquiera de los elementos, o al menos dos cualesquiera o más de los elementos, o al menos todos los elementos.

Puede entenderse que la expresión "A, o B, o C, o una combinación de los mismos" o "al menos uno de A, B y C" no es exhaustiva e incluye al menos lo siguiente: (i) A, o (ii) B, o (iii) C, o (iv) A y B, o (v) A y C, o (vi) B y C, o (vii) A y B y C.

Se entenderá que las realizaciones divulgadas en el presente documento son únicamente a modo de ejemplo, y que cualquier característica presentada para una realización de ejemplo particular puede usarse con cualquier aspecto de la presente divulgación por sí sola o en combinación con cualquier característica presentada para la misma u otra realización de ejemplo particular y/o en combinación con cualquier otra característica no mencionada. Se

entenderá además que cualquier característica presentada para una realización de ejemplo en una categoría particular también puede usarse de una forma correspondiente en una realización de ejemplo de cualquier otra categoría.

ABREVIATURAS

5	3GPP	Proyecto de asociación de 3ª generación
	CHO	Traspaso condicional
	CPAC	Adición o cambio de PSCell condicional
	DC	Conectividad dual
	LMF	Función de gestión de ubicación
10	MCG	Grupo de células maestras
	MN	Nodo maestro
	NAS	Estrato sin acceso
	NR	Nueva radio
	PSCell	Célula primaria de SCG (célula de SCG primaria)
15	RACH	Canal de acceso aleatorio
	SCG	Grupo de células secundarias
	SN	Nodo secundario
	S-SN	Nodo secundario de origen
	RRC	Control de recursos de radio
20	T-SN	Nodo secundario objetivo
	UE	Equipo de usuario

REFERENCIAS

- [1] 3GPP TS 36.300 V 17.1.0 "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 17)", junio de 2022.

- [2] 3GPP TS 37.340 V17.1.0 "Evolved Universal Terrestrial Radio Access (E-UTRA) and NR; Multi-connectivity; Stage 2 (Release 17)", junio de 2022.
- [3] 3GPP TS 38.331 V17.1.0 "NR; Radio Resource Control (RRC) protocol specification (Release 17)", junio de 2022.
- 5 [4] 3GPP TS 33.501 V17.6.0 "Security architecture and procedures for 5G system (Release 17)", junio de 2022.