(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 728 572**

(51) Int. CI.:

H04W 12/12 (2009.01)
H04L 29/06 (2006.01)
H04L 9/08 (2006.01)
H04W 12/10 (2009.01)
H04W 88/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.08.2006 PCT/KR2006/003362**

(87) Fecha y número de publicación internacional: **01.03.2007 WO07024121**

(96) Fecha de presentación y número de la solicitud europea: **25.08.2006 E 06783749 (2)**

(97) Fecha y número de publicación de la concesión europea: **06.03.2019 EP 1932276**

(54) Título: **Procedimiento para la seguridad de telecomunicaciones móviles en una red de comunicaciones móviles y dispositivo para ello**

(30) Prioridad:

26.08.2005 GB 0517484

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.10.2019

(73) Titular/es:

SAMSUNG ELECTRONICS CO., LTD. (100.0%)
129, Samsung-ro, Yeongtong-gu
Suwon-si, Gyeonggi-do, 443-742, KR

(72) Inventor/es:

ROWLEY, MARK y
CHIN, CHEN-HO

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento para la seguridad de telecomunicaciones móviles en una red de comunicaciones móviles y dispositivo para ello

Campo técnico

La presente invención se refiere a las telecomunicaciones móviles y, en particular a una mejora en las cuestiones de seguridad relativas a los mensajes de la interfaz aérea no seguros transmitidos a un dispositivo de comunicación móvil a través de la red de telecomunicaciones móviles.

Técnica antecedente

La presente solicitud no se limita a Sistemas de Telecomunicaciones Móviles Universales (UMTS), y se puede aplicar igualmente a Sistema Global para Comunicaciones Móviles/redes de Servicio de Radio de Paquete General (GSM/GPRS), o de hecho cualquier otra red de telecomunicaciones.

Una arquitectura típica de un sistema de radio celular como el Sistema Universal de Telecomunicaciones Móviles (UMTS) se muestra en la figura 1. El UMTS comprende un equipo de usuario móvil (UE), una red de acceso de radio (RAN) y una o más redes centrales (CN). El UMTS es un sistema de radio de tercera generación que utiliza tecnología de acceso múltiple por división de código de banda ancha (W-CDMA).

La figura 2 muestra una arquitectura más detallada de una red de acceso de radio que comprende estaciones base y controladores de red/estación de radio (RNC/BSC). Las estaciones base manejan la comunicación real a través de la interfaz de radio, cubriendo un área geográfica específica también conocida como una celda. Además de controlar las estaciones base conectadas a él, los RNC incluyen funciones como la asignación de recursos de radio, movilidad local, etc. Un RNC se conecta:

- a una o más redes centrales a través de la interfaz Iu,
- a varias estaciones base (nodos B para el caso de UTRAN) a través de la interfaz Iub y
- posiblemente a uno o más RNCs a través de la interfaz Iur.

La figura 3 proporciona una visión general de los principios de registro y conexión del UE dentro de UMTS con un dominio de servicio de conmutación de circuitos (CS) y un dominio de servicio de conmutación de paquetes (PS). Se pueden encontrar más detalles sobre esto en el sitio web del Proyecto de Asociación de Tercera Generación (3GPP) en http://www.3gpp.org/ en el documento "3GPP TS 33.102 Security Architecture". La identificación de usuario (temporal), la autenticación y el acuerdo de claves se realizan de forma independiente en cada dominio de servicio. El tráfico del plano de usuario se cifra mediante la clave de cifrado acordada para el dominio de servicio correspondiente, mientras que los datos del plano de control se cifran y la integridad se protege mediante las claves de cifrado e integridad de cualquiera de los dominios de servicio.

Los dominios CS y PS de forma individual y de forma asíncrona su establecen un contexto de seguridad con los lados iguales del UE. Este contexto de seguridad se puede considerar, en su forma más simple, establecerse al ejecutar un procedimiento de autenticación que genera las claves de seguridad asociadas y que pertenecen a ese contexto de seguridad. El procedimiento de autenticación es opcional y su ejecución es una decisión de la red. Los procedimientos de autenticación y el contexto de seguridad que se derivan de ellos no garantizan la seguridad de la interfaz de radio. Para garantizar la seguridad de la interfaz de radio, se requiere que se ejecute el procedimiento de configuración de seguridad. El procedimiento de configuración de seguridad garantiza que cualquier mensaje enviado a través de la interfaz aérea sea seguro.

La figura 4 proporciona una breve ilustración simplificada de la secuencia de protocolo de eventos que suceden para una solicitud de servicio de capa 3 normal. El extremo izquierdo de la figura 4 proporciona una vista de la secuencia de procedimientos que conducen a la configuración de Integridad y, por lo tanto, garantizan que los mensajes de señalización "por el aire" (OTA) estén completamente protegidos. Hasta que se complete este procedimiento de configuración de seguridad y se active la protección de la integridad, los mensajes OTA no son seguros.

En la etapa 1, el equipo de usuario y el controlador de red de radio de servicio (SRNC) establecen una conexión RRC. Esto incluye una transferencia de parámetros de seguridad limitados a nivel de RRC y capacidades de seguridad de UE. En la etapa 2, el SRNC almacena parámetros de seguridad limitados y capacidades de seguridad del UE. En la etapa 3, se envía un "mensaje inicial de capa 3 (L3)" con identidad de usuario, secuencia de teclas, etc. al registro de ubicación de visitantes/servidor de soporte GPRS (VLR/SGSN).

En cambio, en la etapa 4, el VLR/SGSN reenvía una generación clave de autenticación para el UE. La etapa 4 es una etapa opcional, que puede o no puede ser ejecutada por la red. En la etapa 5, el VLR/SGSN toma una decisión sobre la integridad y el cifrado requerido. En la etapa 6, el VLR/SGSN solicita la configuración de seguridad enviando un mensaje al SRNC. En la etapa 7, el SRNC inicia los procedimientos de seguridad enviando un mensaje al UE. Los procedimientos de seguridad son completados por el UE enviando un mensaje a SRNC en la etapa 8. En la etapa 9, el SRNC envía un mensaje adicional al VLR/SGSN para completar la configuración de seguridad. En la

etapa 10, los servicios de la capa 3 pueden proceder entre el UE y el SGSN.

Más detalles se pueden encontrar en 3GPP TS 24.008 de radio móvil interfaz de capa 3 especificación; protocolos centrales de red; etapa 3, y especificación del protocolo de control de recursos de radio (RRC) 3GPP TS 25.133, ambas se pueden encontrar en el sitio web del Proyecto de Asociación de Tercera Generación (3GPP) en http://www.3gpp.org/.

En la figura 4 se destaca que la etapa 4, el procedimiento de autenticación es un procedimiento opcional. La red decide si esto debe ejecutarse en función de varios parámetros que van más allá del alcance de esta descripción. Sin embargo, debe tenerse en cuenta que, independientemente de si la autenticación se ejecuta en la red, el procedimiento de configuración de seguridad que activa la protección de la integridad de los mensajes OTA (por el aire) puede tener lugar siempre que exista un contexto de seguridad entre el UE y la red.

La figura 5 muestra la secuencia de protocolo de eventos para una solicitud de capa 3 que no es aceptada (y por lo tanto rechazada) por la red. Esta secuencia de rechazo es la misma independientemente de si el servicio de capa 3 solicitado es para establecer llamadas o sesiones o para registrar el UE en la red.

En la etapa 1, el equipo de usuario y el controlador de red de radio de servicio (SRNC) establecen una conexión RRC. Esto incluye una transferencia de parámetros de seguridad limitados a nivel de RRC y capacidades de seguridad de UE. En la etapa 2, el SRNC almacena parámetros de seguridad limitados y capacidades de seguridad del UE. En la etapa 3, se envía un "mensaje inicial de capa 3 (L3)" con identidad de usuario, secuencia de teclas, etc. al registro de ubicación de visitantes/servidor de soporte GPRS (VLR/SGSN).

En la etapa 4, el VLR/SGSN comprueba la validez de la solicitud de la capa 3. Si la solicitud no es aceptable, el VLR/SGSN rechaza la solicitud en la etapa 5. Este rechazo de solicitud se envía a través de la red al UE sin protección de la integridad.

En base al sistema descrito anteriormente, es posible que un pirata informático o, en palabras de Sistema Universal de Telecomunicaciones Móviles (UMTS) en una "estación de base falsa", instigue ataques de servicio contra los UE proporcionando información falsa dentro de mensajes con la integridad protegida enviados a través de la interfaz aérea al dispositivo de comunicación móvil. Estos ataques pueden causar una "denegación de servicio" (DoS) al usuario móvil.

Incorporado dentro del UMTS, y GSM/GPRS antes de él, hay un temporizador dentro del UE que inhibe los intentos subsiguientes de registro automático en el dominio de PS luego de una falla anormal de un procedimiento de registro. Este temporizador se designa en el sistema como temporizador T3302.

El T3302 tiene un valor predeterminado de 12 minutos, que se utiliza desde el encendido hasta que se asigne un valor diferente para el parámetro. Al UE se le puede asignar un valor diferente para el T3302 en los mensajes de ACEPTAR_ADJUNTO, RECHAZAR_ADJUNTO, ACCEPTAR_ACTUALIZACIÓN_ÁREA_ENRUTADO y RECHAZAR_ACTUALIZACIÓN_ÁREA_ENRUTADO.

El valor asignado al T3302 es entre 2 segundos y 3 horas 6 minutos. Alternativamente, el parámetro T3302 se puede indicar como "desactivado". La consecuencia de configurar T3302 en "desactivado" es que los intentos de registro adicionales en el dominio PS después de la "falla anormal" de un procedimiento de registro están deshabilitados.

Una "falla anormal" se define como sigue. Cuando la red rechaza la solicitud de capa 3 del NAS móvil, la red proporciona una razón en el sistema que se denomina causa de rechazo. Esta causa de rechazo informará al UE qué acción siguiente debe, debería o puede realizar el UE. Si un UE no entiende una causa de rechazo, la causa se denomina caso anormal y las fallas que resultan de estas se llaman fallas anormales. Los casos anormales también cubren a) capa inferior (es decir, fallas de radio) b) tiempo de espera de procedimiento (es decir, no hay respuesta de CN) c) rechazo de CN por una razón que no es de esperar por el UE (por ejemplo, si un UE heredado está activo en una versión posterior de una red, por ejemplo, un CN de la Versión 98 envía una nueva causa de rechazo # 14 a un UE que se construye según las especificaciones de la fase 2 de GSM).

Si no se permiten más intentos de registro, el equipo de usuario se le niega el servicio hasta que se produce una de las siguientes acciones:

a) una solicitud manual es activada por el usuario (por ejemplo, una solicitud manual de servicios PS), o b) el UE pasa por un ciclo de energía (es decir, el usuario apaga la unidad y luego vuelve a encenderla), o c) hay un cambio físico en el área de enrutamiento (por ejemplo, el UE se mueve de una celda a otra).

El UE utiliza el valor predeterminado T3302 desde el encendido y continúa utilizando el valor por defecto hasta que se le asigna un valor diferente.

Un problema adicional puede existir para los UE que ya están registrados en la red. Es decir, un aumento en el número de intentos de registro de red por parte de los UE individuales aún no registrados puede dar como resultado un aumento en el ruido de radio para aquellos UE ya registrados. Además, puede ocurrir una pérdida de servicio

para los UE ya registrados debido a este aumento de ruido y/o una pérdida de ancho de banda debido a la gran cantidad de solicitudes de registro.

Se conocen los peligros de los mensajes no protegidos por el aire (OTA). Por lo tanto, además de la protección de cifrado, el UMTS tiene una protección de la integridad diseñada. Además, el UMTS tiene reglas de autenticación estrictas y algoritmos de la integridad y encriptación elaborados, y también verifica que el móvil pueda verificar que la red es genuina. Se pueden encontrar ejemplos de estos aspectos de seguridad en el sitio web del Proyecto de Asociación de Tercera Generación (3GPP) en http://www.3gpp.org/ en los documentos TS 33.102 y 24.008.

Con el fin de asegurar mensajes OTA en UMTS debe ser ejecutada la protección de la integridad. La protección de la integridad comienza después de que se ejecuta opcionalmente el procedimiento de autenticación y acuerdo de clave (AKA). Aunque no es necesario ejecutar el AKA cada vez que el UE accede a la red, la protección de la integridad debe iniciarse lo antes posible cada vez que el UE accede a la red. Por lo tanto, los aspectos de seguridad en UMTS solo pueden aplicarse una vez que la red y el UE ejecutan la protección de la integridad y, por lo tanto, hacen que los mensajes OTA sean seguros.

En UMTS la protección de la integridad se desencadena por la red central (CN) una vez que la CN ha recibido y procesado el primer mensaje de capa 3 del NAS (estrato de no acceso) y encuentra la solicitud de capa 3 del NAS aceptable, la CN procede además con esa solicitud de capa 3 del NAS. Si el CN encuentra inaceptable el primer mensaje de solicitud de capa 3 del NAS del UE, el CN rechaza al UE enviando un mensaje de rechazo en forma de un mensaje RECHAZAR_ADJUNTO o RECHAZAR_ACTUALIZACIÓN_ÁREA_ENRUTADO. El procedimiento de seguridad que activa la protección de la integridad de los mensajes OTA no se inicia, ya que se piensa que, si el CN rechaza una solicitud de servicio, no es necesario habilitar la seguridad ya que se espera que la transacción de la red del UE se termine. Esto significa que los mensajes de rechazo OTA al móvil que no tienen integridad protegida no son seguros.

Además, es posible para el parámetro de temporizador T3302 en los mensajes de rechazo RECHAZAR_ADJUNTO y RECHAZAR_ACTUALIZACIÓN_ÁREA_ENRUTADO para ser manipulados con el fin de instigar un ataque de denegación de servicio contra el UE. Esto podría ser posible interceptando los mensajes de rechazo de la red y posteriormente corrompiendo los parámetros del temporizador T3302. Sin embargo, es más probable que un pirata informático potencial construya un mensaje de rechazo completamente falso (RECHAZAR_ADJUNTO o un RECHAZAR_ACTUALIZACIÓN_ÁREA_ENRUTADO) y lo envíe al UE.

Por lo tanto, un pirata informático puede instigar un ataque de denegación de servicio contra cualquier UMTS móvil mediante la manipulación de los parámetros en los mensajes RECHAZAR_ADJUNTO o RECHAZAR_ACTUALIZACIÓN_ÁREA_ENRUTADO que no tienen la integridad protegida.

En el peor de los casos, como se ha explicado anteriormente, este ataque de denegación de servicio puede bloquear los móviles fuera de servicio PS hasta que la UE se mueve físicamente, el usuario activa una solicitud específica para los servicios de PS o el usuario lleva a cabo un reinicio de energía.

En GSM/GPRS y UMTS para la versión 5, el sistema ha sido diseñado con un bucle de proceso mediante el cual se repetirá un procedimiento intento de registro que falla anormalmente. Las repeticiones de registro están controladas por temporizadores (distintos de T3302) y el movimiento del UE dentro de la red. Un UE intentará el procedimiento de registro 5 veces antes de que se inicie T3302.

Por lo tanto, hasta la versión 5 de UMTS existe estadísticamente más que una buena posibilidad de que cualquier rechazo de registro y su información, si están corrompidos por un pirata informático, se actualicen por el siguiente rechazo de registro genuino o se vuelvan irrelevantes por un registro exitoso o una actualización de registro. Sin embargo, la red no necesariamente actualiza ningún parámetro dañado en T3302, ya que es opcional para que la red proporcione un parámetro para T3302. Además, una red no puede determinar si un pirata informático ha proporcionado previamente un valor corrupto para T3302. Por lo tanto, se aplicará un T3302 dañado que no se actualice cuando finalice la repetición del procedimiento de registro. Además, el T3302 dañado se utilizará la próxima vez que el móvil llegue a una situación en la que el T3302 deba iniciarse nuevamente.

Un problema con esta solución existente es que, dado que cada aparición de una condición anormal cuenta como una falta de un intento procedimiento de registro, un pirata informático puede, mediante el "forzado" de 5 ocurrencias sucesivas de fallos anormales, poner fin a la todo el proceso del proceso de registro realiza un bucle, por lo que se inicia T3302.

El problema descrito anteriormente se ve agravada por un cambio a la versión 6 de la especificación NAS por la introducción de un medio para pasar por alto la solución existente. En la versión 6 de UMTS, existe la misma solución implícita de repetir el procedimiento de registro 5 veces antes de iniciar el temporizador T3302. Por lo tanto, existe una posibilidad igualmente buena de que una red genuina actualice un parámetro T3302 dañado. Sin embargo, al igual que en la versión previa 6, no hay garantía de que la red actualizará T3302 y la red no sabe que un pirata informático ha corrompido a T3302.

Además, los cambios a la versión 6 de la especificación NAS permiten la repetición de bucle de procedimiento de

registro para terminar inmediatamente si se reciben ciertas causas de rechazo por el UE. Los cambios a la versión 6 se pueden encontrar en Tdoc NI-041602 en el sitio web de 3GPP indicado anteriormente.

Por lo tanto, un pirata informático no sólo puede corromper el valor del sistema de T3302, sino que también proporcionan una causa de rechazo que fuerza al móvil a detener los intentos de registro automáticos adicionales hasta que se cambie el T3302 dañado.

El documento WO 2004/073347 se refiere a un procedimiento para procesar un mensaje de seguridad en una capa de control de recursos de radio (RRC) de un sistema de comunicaciones móviles. El procedimiento para procesar un mensaje de seguridad incluye las etapas para recibir el mensaje de seguridad (S31), almacenar las variables anteriores relacionadas con la seguridad, realizar una verificación de la integridad (S34) en el mensaje de seguridad recibido, descartar (S37) o procesar (S36) el mensaje de seguridad según el resultado de la verificación de la integridad (S34) y actualización de las variables relacionadas con la seguridad (S33). Por consiguiente, se proporciona un procedimiento de procesamiento de mensajes de control de configuración de seguridad que incluye una verificación de la integridad del mensaje de seguridad recibido.

El documento WO 2005/079035 se refiere a un procedimiento para establecer una asociación de seguridad para asegurar el tráfico enviado a través de una red de señalización SS7 entre nodos de señalización, de modo que los parámetros de la asociación de seguridad sean conocidos por cada nodo de señalización involucrado. El procedimiento comprende el uso del protocolo de intercambio de claves de Internet para negociar dichos parámetros entre los nodos de señalización, enviándose mensajes de intercambio de claves de Internet a través de la red SS7. ERICSSON ET AL: Comprobación de la integridad de los mensajes MM/GMM y protección de la integridad durante llamadas de emergencia ", PROYECTO 3GPP; N-000744, PROYECTO DE ASOCIACIÓN DE 3ª GENERACIÓN (3GPP), CENTRO DE COMPETENCIA MÓVIL; 650, ROUTE DES LUCIOLES; F-06921 SOPHIA-ANTIPOLIS CEDEX; FRANCE vol. TSG CN, n.º Düsseldorf, Alemania; 20000719, 19 de julio de 2000 (2000-07-19), XP050047960, se refiere a la verificación de la integridad de los mensajes MM/GMM y la protección de la integridad durante las llamadas de emergencia.

Divulgación de la invención

Problema técnico

La presente invención pretende superar o al menos aliviar algunos o todos los problemas mencionados anteriormente.

Solución técnica

Se proporciona un procedimiento y un dispositivo de comunicación móvil de la invención como se define en las reivindicaciones 1 y 6, respectivamente.

En un aspecto, la presente invención proporciona un procedimiento de funcionamiento de un dispositivo de comunicación móvil en una red de telecomunicaciones móviles, comprendiendo el procedimiento las etapas del dispositivo de comunicación móvil: recibir un mensaje de integridad no protegida con un valor de parámetro incluido en el mismo para implementarse en el dispositivo de comunicación móvil; utilizando un valor predeterminado almacenado en el dispositivo de comunicación móvil en lugar del valor del parámetro recibido.

En un aspecto adicional, la presente invención proporciona un procedimiento de comunicación a través de una red de comunicación móvil utilizando una interfaz aérea para comunicarse con un dispositivo de comunicación móvil, en el que mensajes de integridad protegida y de integridad no protegida se transmiten a la comunicación móvil dispositivo, dichos mensajes incluyen valores de parámetros que deben implementarse en el dispositivo de comunicación móvil, el procedimiento comprende la etapa de: asegurar que el dispositivo de comunicación móvil utiliza un valor válido para el parámetro, el valor válido permitiendo la comunicación a través de la red para continuar.

Efectos ventajosos

La presente invención proporciona un procedimiento fácil de implementar y todavía eficaz de prevenir un ataque de denegación de servicio en los UE.

Breve descripción de los dibujos

Las realizaciones específicas de la presente invención se describirán ahora sólo a modo de ejemplo, con referencia a algunos de los dibujos adjuntos, en los que:

La figura 1 muestra una arquitectura típica de una red celular conocida;
La figura 2 muestra una arquitectura de red UTRAN conocida más detallada;
La figura 3 muestra una descripción general de los principios conocidos de registro y conexión de UE dentro de UMTS;
La figura 4 muestra una secuencia de eventos de procedimiento conocidos que conducen a una interfaz de radio

protegida por integridad;
La figura 5 muestra la secuencia conocida de eventos que conducen a una red que rechaza una solicitud de acceso al servicio de capa 3 de los UE;
La figura 6 muestra un diagrama de flujo que representa las etapas tomados para implementar la realización de una de las presentes invenciones.

Mejor modo de llevar a cabo la invención

Primera realización

A continuación, se describirá una primera realización de la presente invención. Cuando un UE recibe un valor para el parámetro T3302 en un mensaje OTA de integridad no protegida, por ejemplo, en los mensajes RECHAZAR_ADJUNTO o RECHAZAR_ACTUALIZACIÓN_ÁREA_ENRUTADO, el UE no implementa ese valor de parámetro. En cambio, el UE utiliza un valor predeterminado que se sabe que es seguro.

Es decir, el UE utilizará

A) el valor utilizado actualmente de T3302, como un valor implementado previamente al recibir un mensaje OTA de identidad protegida o el valor predeterminado si un valor OTA no ha implementado previamente un valor actualizado, o
B) el valor por defecto de T3302.

La elección de si la opción A o B se pone en práctica es una opción predeterminada, y está integrado en el software del UE.

Este procedimiento se muestra en la figura 6, en el que el UE inicia el procedimiento de registro en la etapa S601. Luego, un pirata informático envía un mensaje de correo electrónico de integridad no protegida, que incluye un valor para el parámetro T3302, al UE, como se muestra en la etapa S603.

En la etapa S605, el UE utiliza un valor predeterminado para el T3302 parámetro que se almacena dentro del UE.

El UE entonces o bien se mueve a la etapa S607 o la etapa S609, dependiendo de qué solución se implementa en el software del UE.

Para la opción A, en la etapa S607, el UE ignora cualquier valor de parámetros para T3302 en el mensaje de integridad no protegida y utiliza su valor se utiliza actualmente para ese parámetro en su lugar. El valor utilizado actualmente puede ser su valor predeterminado o un valor establecido cuando se recibe un mensaje OTA de integridad protegida anterior.

Para la opción B, en la etapa S609, el equipo UE siempre utiliza su valor de parámetro predeterminado para T3302.

El procedimiento termina entonces en la etapa S611.

Como esta primera realización de la invención se implementa utilizando una solución basada UE, el software de UE necesita mejoras. Los nuevos UE pueden actualizarse antes de enviar los UE al cliente. Para los UE existentes que ya están en funcionamiento en el campo, la introducción de esta solución requerirá una recuperación de esos UE o una actualización del software "por el aire".

Segunda realización

Esta segunda realización de la presente invención se utiliza en relación con la primera realización.

Además de las características de la primera realización, la red no está habilitada para proporcionar un valor para T3302 en cualquier mensaje OTA de integridad no protegida. Si dicha actualización se proporciona en cualquiera de estos mensajes OTA de integridad no protegida, por ejemplo, por un pirata informático, el UE no la implementará. Es decir, el UE llevará a cabo el procedimiento descrito anteriormente de acuerdo con la primera realización.

Se entenderá que, con el fin de poner en práctica esta realización, las nuevas versiones de la red pueden adoptar fácilmente esta solución. Sin embargo, para las versiones anteriores de la red, será necesario implementar una solución de software para los nodos de la red operativa.

Al igual que en la primera realización, se requerirá una actualización de cualquier software de UE más antiguo.

Tercera realización

Esta tercera realización se utiliza en combinación con la primera realización descrita anteriormente. En esta realización, la red tiene la obligación de proporcionar siempre un valor válido para T3302 al finalizar el registro o la actualización del registro.

Una red no sería consciente de los ataques exitosos anteriores sobre el valor de parámetro para T3302, y así,

cuando un UE se conecta a la red el valor dañado por T3302 todavía se puede establecer en el equipo de usuario.

Por lo tanto, en esta realización, la red proporciona un valor de parámetro válido para T3302 en el ACEPTAR_ADJUNTO y los mensajes ACEPTAR_ACTUALIZACIÓN_ÁREA_ENRUTADO siendo enviados al UE después de completado el registro. Por lo tanto, incluso si un pirata informático ha corrompido la versión de UE de T3302 y así ha cambiado el parámetro del temporizador antes de un registro exitoso, la red genuina, al aceptar el intento de registro y/o la actualización de registro, actualizará el valor del parámetro en T3302 a un valor válido.

Como los mandatos realización anteriormente descrita de la red para actualizar la información potencialmente corrompida en el UE, los cambios necesarios son completamente en el lado de la red. Por lo tanto, esta realización es efectiva incluso para los UE operativos ya existentes. No se requieren actualizaciones para estos UE operativos. Sin embargo, tanto las redes existentes como las nuevas requerirán una actualización para implementar el cambio.

Se entenderá que las realizaciones de la presente invención se describen en el presente documento a modo de ejemplo solamente, y que varios cambios y modificaciones pueden hacerse sin apartarse del alcance de la invención.

Se entenderá que la presente invención puede extenderse para cubrir cualquier información crucial, temporizadores o parámetros que se envían a un UE en un mensaje OTA de integridad no protegida, que, si dicha información, temporizadores o parámetros están corrompidos por un pirata informático, resultará en un ataque de denegación de servicio.

Se entenderá además que la invención puede aplicarse a cualquier mensaje recibido por el dispositivo de comunicación móvil que no sea seguro.

REIVINDICACIONES

1. Un procedimiento de operación de un dispositivo de comunicación móvil en una red de telecomunicaciones móviles, en el que el dispositivo de comunicación móvil comprende un temporizador T3302 que inhibe los intentos subsiguientes automáticos de registro en un dominio de paquetes conmutados, PS, luego de una falla anormal de un procedimiento de registro, comprendiendo el procedimiento las etapas del dispositivo de comunicación móvil:

recibir (603) un mensaje sin la integridad protegida que incluye un valor de un parámetro;
utilizando (S605) un valor predeterminado almacenado en el dispositivo de comunicación móvil en lugar del valor recibido del parámetro;
en el que el valor del parámetro es un valor asociado con el temporizador T3302 y el valor predeterminado es el valor predeterminado del parámetro del dispositivo de comunicación móvil.

2. El procedimiento según la reivindicación 1, en el que el valor predeterminado es un valor del parámetro que está siendo utilizado actualmente por el dispositivo de comunicación móvil.

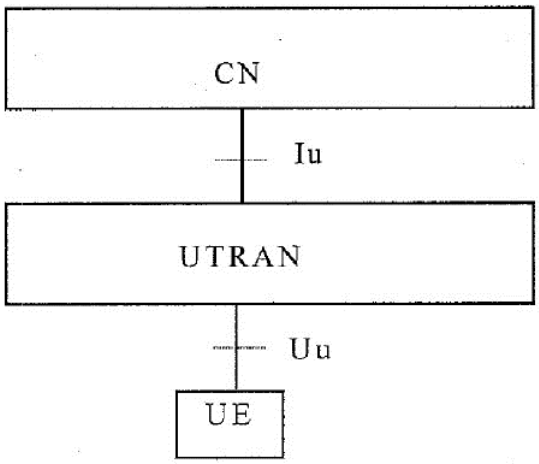
3. El procedimiento según la reivindicación 1, en el que los mensajes sin la integridad protegida sin el valor del parámetro son proporcionados por una entidad de red.

4. El procedimiento según la reivindicación 1, en el que
el dispositivo de comunicación móvil recibe el valor del parámetro desde una entidad de red en un mensaje de integridad protegida si el dispositivo de comunicación móvil completa un registro e implementa el valor del parámetro recibido en el mensaje de integridad protegida.

5. El procedimiento según la reivindicación 1, en el que el mensaje de integridad no protegida comprende un
valor de un parámetro asociado con un temporizador, y el temporizador determina cuánto tiempo debe esperar el dispositivo de comunicación móvil antes de un intento adicional de registrarse en una entidad de red.

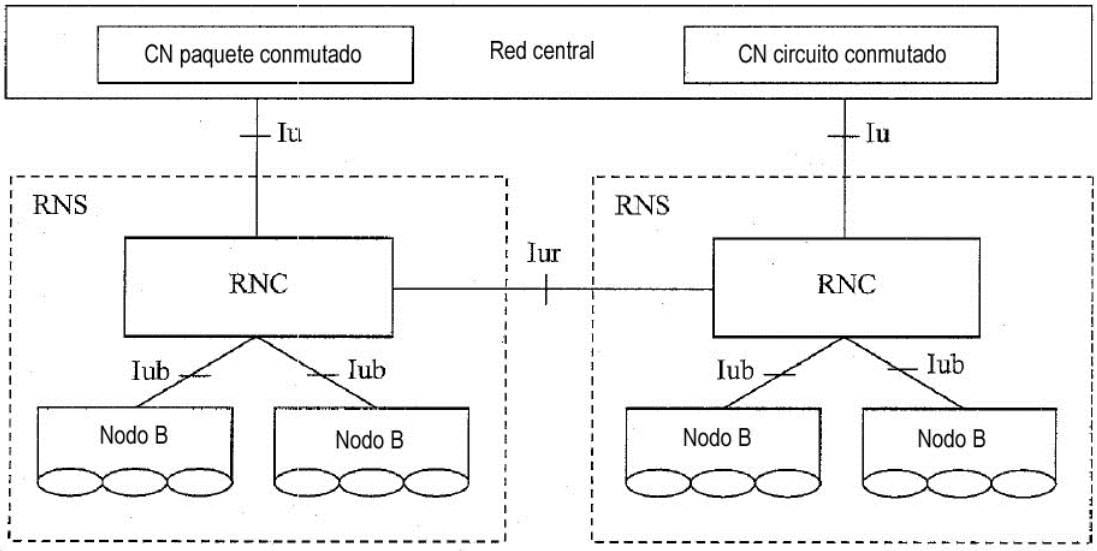
6. Un dispositivo de comunicación móvil adaptado para llevar a cabo el procedimiento de cualquiera de las reivindicaciones 1 a 5.

[Fig. 1]

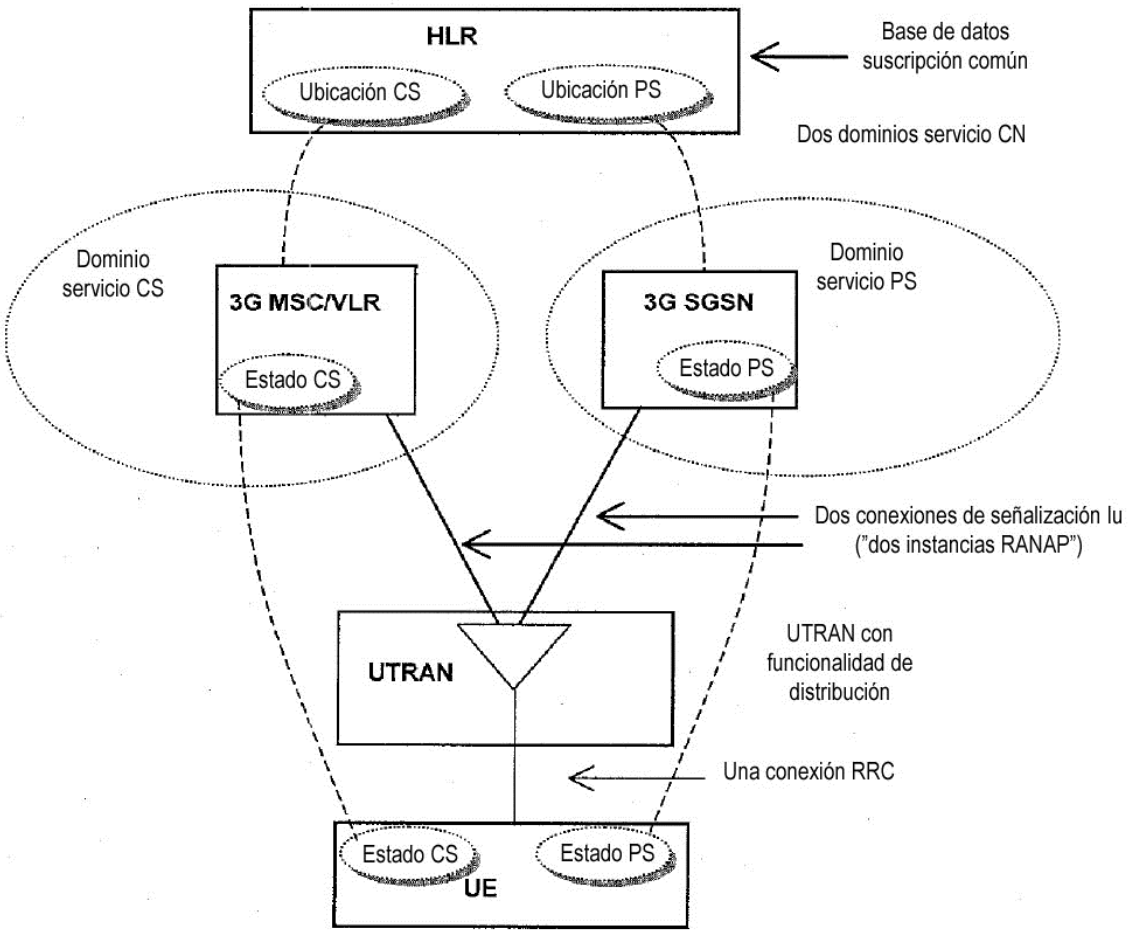


UTRAN	Red de acceso de radio terrestre UMTS
CN	Red central
UE	Equipo de usuario

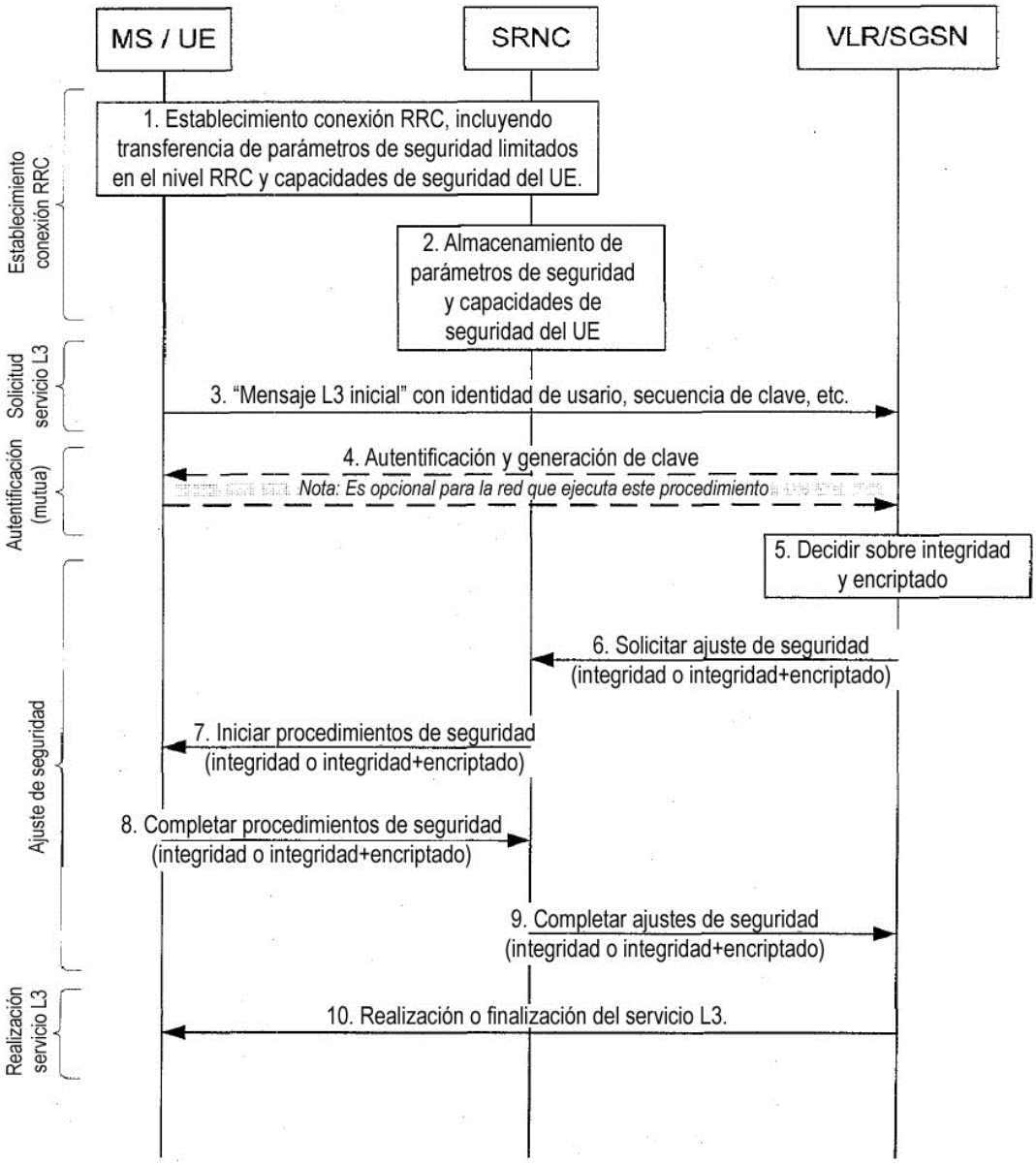
[Fig. 2]



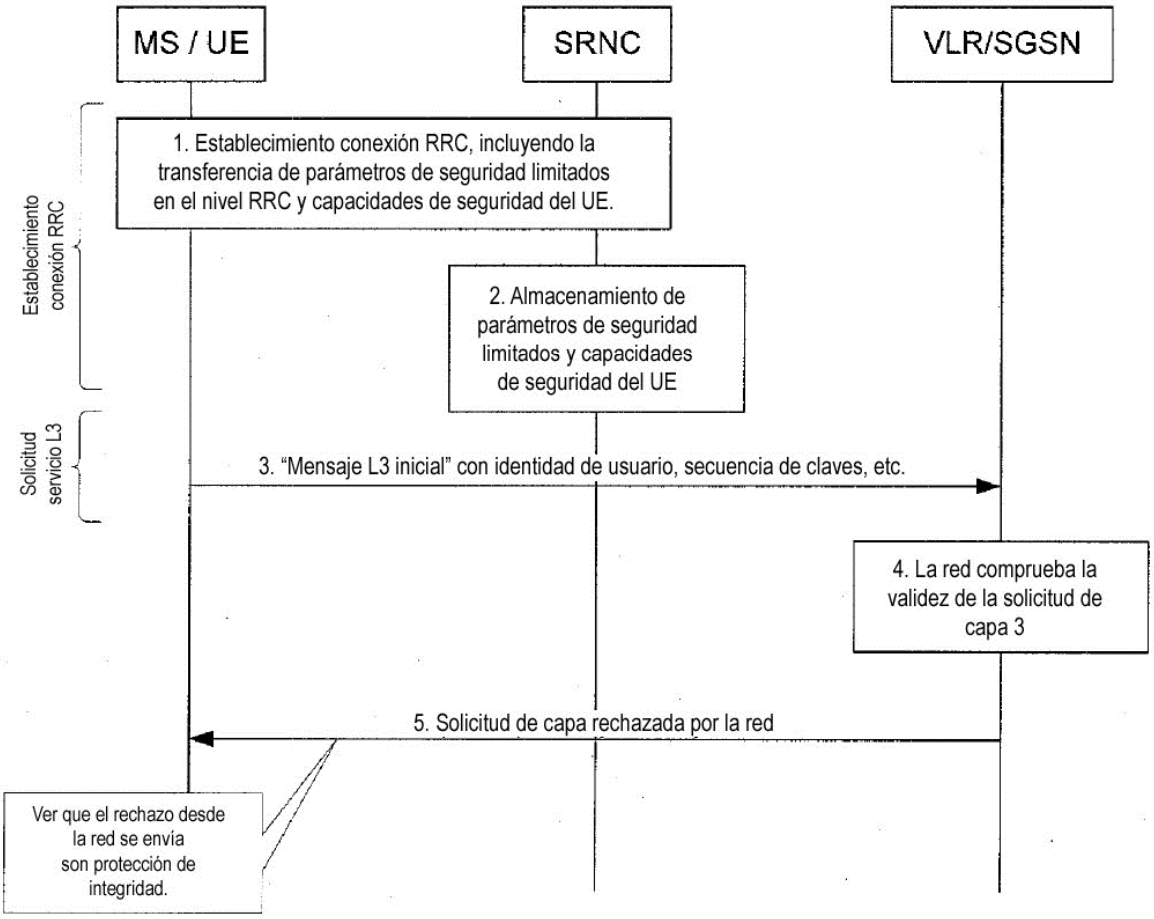
[Fig. 3]


HLR
Ubicación CS
Ubicación PS
Base de datos suscripción común
Dos dominios servicio CN
Dominio servicio CS
3G MSC/VLR
Estado CS
Dominio servicio PS
3G SGSN
Estado PS
Dos conexiones de señalización Iu ("dos instancias RANAP")
UTRAN
UTRAN con funcionalidad de distribución
Una conexión RRC
Estado CS
Estado PS
UE

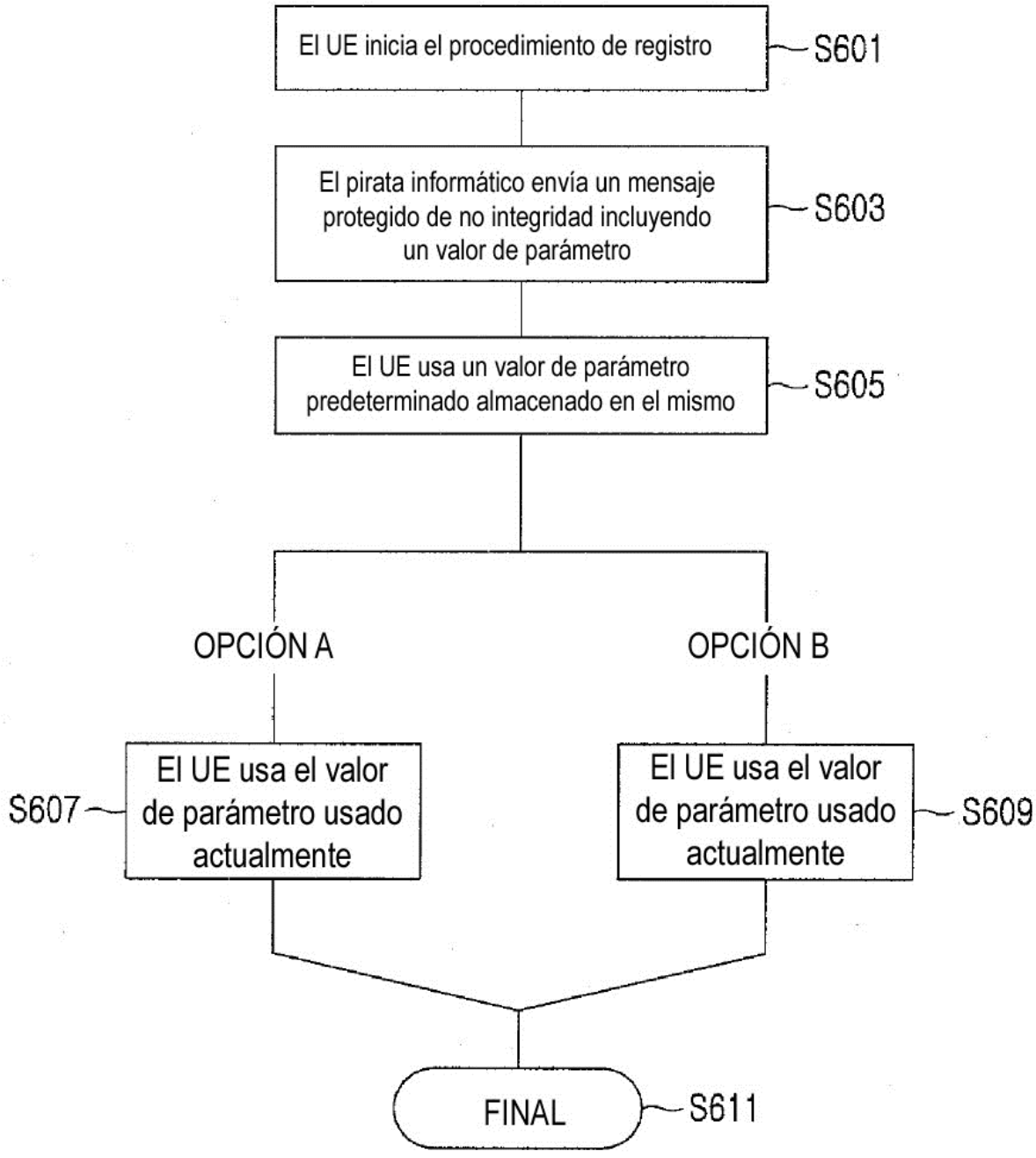
[Fig. 4]


MS / UE
SRNC
VLR/SGSN
Establecimiento conexión RRC
1. Establecimiento conexión RRC, incluyendo transferencia de parámetros de seguridad limitados en el nivel RRC y capacidades de seguridad del UE.
2. Almacenamiento de parámetros de seguridad y capacidades de seguridad del UE
Solicitud servicio L3
3. "Mensaje L3 inicial" con identidad de usario, secuencia de clave, etc.
Autentificación (mutua)
4. Autentificación y generación de clave
Nota: Es opcional para la red que ejecuta este procedimiento
5. Decidir sobre integridad y encriptado
6. Solicitar ajuste de seguridad (integridad o integridad+encriptado)
Ajuste de seguridad
7. Iniciar procedimientos de seguridad (integridad o integridad+encriptado)
8. Completar procedimientos de seguridad (integridad o integridad+encriptado)
9. Completar ajustes de seguridad (integridad o integridad+encriptado)
Realización servicio L3
10. Realización o finalización del servicio L3.

[Fig. 5]


MS / UE
SRNC
VLR/SGSN
1. Establecimiento conexión RRC, incluyendo la transferencia de parámetros de seguridad limitados en el nivel RRC y capacidades de seguridad del UE.
Establecimiento conexión RRC
2. Almacenamiento de parámetros de seguridad limitados y capacidades de seguridad del UE
Solicitud servicio L3
3. "Mensaje L3 inicial" con identidad de usuario, secuencia de claves, etc.
4. La red comprueba la validez de la solicitud de capa 3
5. Solicitud de capa rechazada por la red
Ver que el rechazo desde la red se envía son protección de integridad.

[Fig. 6]


El UE inicia el procedimiento de registro
S601
El pirata informático envía un mensaje protegido de no integridad incluyendo un valor de parámetro
S603
El UE usa un valor de parámetro predeterminado almacenado en el mismo
S605
OPCIÓN A
OPCIÓN B
S607
El UE usa el valor de parámetro usado actualmente
El UE usa el valor de parámetro usado actualmente
S609
FINAL
S611